Lucent Technologies
Bell Labs Innovations

MultiMedia Communications eXchange

System Administrator's Guide

and Technical Reference Manual

Release 2.0M
555-027-813
Issue 1
July 1997

Copyright, Trademark, and Legal Notices

DEFINITY, AUDIX, and CONVERSANT are registered trademarks and 4ESS and 5ESS are trademarks of Lucent Technologies. Windows is a trademark of Microsoft Corporation. Lynx and LynxOS are trademarks of Lynx Real-Time Systems, Inc. Pentium is a registered trademark of Intel Corporation. UNIX is a trademark of Novell Corporation. Hewlett-Packard and HP are registered trademarks of the Hewlett-Packard corporation. Sun, Sun Microsystems, Sun Workstation, and Solaris (computer and peripherals) are registered trademarks and Solaris (operating system utilities) is a trademark of Sun Microsystems, Inc.

Warranty

Lucent Technologies provides a limited warranty on this product. Refer to the “Limited Use Software License Agreement” card provided with your package.

Every effort has been made to ensure that the information in this book is complete and accurate at the time of printing. However, information is subject to change.

Federal Communications Commission statement

Part 15: Class A statement. This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Canadian Department of Communications (DOC) interference information.

This digital apparatus does not exceed the Class A limits for radio noise emissions set out in the radio interference regulations of the Canadian Department of Communications.

Le Présent Appareil Nomérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la class A préscrites dans le reglement sur le brouillage radioélectrique édicté par le ministére des Communications du Canada.

European Union declaration of conformity

Lucent Technologies Business Communications Systems declares that the Multimedia Communications eXchange equipment specified in this document conforms to the referenced European Union (EU) Directives and Harmonized Standards listed below:

EMC Directive 89/336/EEC
Low-Voltage Directive73/23/EEC

The "CE" mark affixed to the equipment means that it conforms to the above directives.

Toll Fraud

Toll fraud is the unauthorized use of your telecommunications system by an unauthorized party, for example, persons other than your company's employees, agents, subcontractors, or persons working on your company's behalf. Note that there may be a risk of toll fraud associated with your telecommunications system and, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

You and your system manager are responsible for the security of your system, such as programming and configuring your equipment to prevent unauthorized use. The system manager is also responsible for reading all installation, instruction, and system administration documents provided with this product in order to fully understand the features that can introduce risk of toll fraud and the steps that can be taken to reduce that risk. Lucent Technologies does not warrant that this product is immune from or will prevent unauthorized use of common-carrier

telecommunication services or facilities accessed through or connected to it. Lucent Technologies will not be responsible for any charges that result from such unauthorized use.

If you suspect that you are being victimized by toll fraud and you need technical support or assistance, call Technical Service Center Toll Fraud Intervention Hotline at 1 800 643-2353.

Ordering information

To order this document, ask for

Document No. 555-027-813
Comcode 108042144
Issue 1.0, July 28, 1997

You can order Lucent documentation by mail, telephone, or fax.

Mailing address

Lucent Technologies Publications Center
P.O. Box 4100
Crawfordsville, IN 47933
USA

Telephone numbers

1 800 457-1235 (US)
317 361-5353 (international)

Fax numbers

1 800 457-1764 (US)
317 361-5355 (international)

Standing orders

You can place standing orders for Lucent documents. Standing orders make sure that your documentation is always up-to-date. Updates are sent automatically as they appear and billed to the account you designate. For more information on standing orders for this and other Lucent documents, contact the Lucent Technologies Publications Center.

Comments

To comment on this document, return the comment card at the front of the document.

Acknowledgments

This document was prepared by Product Documentation Development, Business Communications Systems, Lucent Technologies, Denver, CO, Columbus, OH, Middletown, NJ, and Mount Airy, NJ, USA.

Contents

Preface

The *MMCX Technical Reference* guides you through the design, implementation, and support of an MMCX multimedia communications network. It covers installation, routine maintenance, troubleshooting and repair of the MMCX server hardware and its LynxOS-based software. The MMCX team has accordingly designed the book for *system administrators*. If you are an end user of the MMCX desktop application, you should consult the *MMCX User's Guide* for installation and troubleshooting advice.

The duties of an MMCX administrator

As an MMCX system administrator, you will be responsible for integrating the MMCX server and clients into an existing voice and data telecommunications network. You should thus have a thorough understanding of your network layout, equipment, and capabilities, as well as a basic grounding in the fundamentals of telephony and networking in general. If network administrative responsibility is divided among several people or groups in your organization, you should know who handles problems with your LAN, WAN, desktop PCs, PBX, and public carrier access. You will often have to coordinate with them when resolving MMCX problems.

Since the MMCX server operates under the LynxOS operating system, you should also be familiar with UNIX-type operating systems and commands.

Technical support

Since every site and network is different, you may encounter problems not covered in this volume. For these situations, Lucent Technologies maintains a Multimedia Application Customer Support

(MACS) center. Call **1-800-821-8204**, during normal business hours (6:00 AM to 6:00 PM Mountain Time, Monday through Friday, excluding holidays).

Software licenses

Customers must purchase a license for *each user* on an MMCX server. In other words, the maximum number of users that can be added with the **addusr** command on a server is the same as the number of end user licenses purchased for that server. You can purchase additional end user licenses by calling your Lucent Technologies account representative.

Viewing the MMCX documentation with Acrobat Reader

Lucent Technologies ships the *MMCX Technical Reference* in electronic form, on the MMCX CD shipped with each server. Using Adobe Acrobat Reader, you can read these documents on a Windows PC, on a Sun Solaris workstation, or on an HP-UX workstation. Acrobat Reader displays high-quality, print-like graphics on both UNIX and Windows platforms. It provides scrolling, zoom, and extensive search capabilities, along with online help. A copy of Acrobat Reader is included with the documents.

Running Acrobat on HP and Sun workstations

1 To view the documentation, enter **acroread mainmenu.pdf**

acroread resides in ***installation_directory*/bin** where ***installation_directory*** is the directory in which you installed the Acrobat Reader.

mainmenu.pdf resides in the **mmcxdocs** directory.

2 Select **Tools | Search | Indexes.** The index titled **MMCX Master Index** should be the only index in the available list. If it is not listed, select **Add.** Add the file **index.pdx**. This file is in the **mmcxdocs** directory.

Running Acrobat on a Windows PC

1 To view the electronic documentation, double click the Acrobat Reader icon or execute **acroread.exe** in the directory in which you installed the reader. After the reader opens, open the file **mainmenu.pdf**, which is located in the **mmcxdocs** directory.

2 Select **Tools | Search | Indexes | Add.** Add the file **index.pdx.** This file is in the **mmcxdocs** directory.

Setting the default magnification

You can set your default magnification by selecting **File | Preferences | General**. We recommend the **Fit Page** option.

Adjusting the window size

On HP and Sun workstations, you can control the size of the reader window by using the **-geometry** argument. For example, the command string **acroread -geometry 900x900 mainmenu.pdf** opens the main menu with a window size of 900 pixels square.

Hiding and displaying bookmarks

By default, the document appears with bookmarks displayed on the left side of the screen. The bookmarks serve as a hypertext table of contents for the chapter you are viewing. You can control the appearance of bookmarks by selecting **View | Page Only** or **View | Bookmarks and Page.**

Using the button bar

The button bar can take you to the book's Index, table of contents, main menu, and glossary. It also lets you update your documents. Click the corresponding button to jump to the section you want to read.

Using hypertext links

Hypertext-linked text appears in blue, italics, and underlined. These links are shortcuts to other sections or books.

Navigating with double arrow keys

The double right and double left arrows (◄◄ and ►►) at the top of the Acrobat Reader window are the go-back and go-forward functions. The go-back button takes you to the last page you visited prior to the current page. Typically, you use ◄◄ to jump back to the main text from a cross reference or illustration.

Searching for topics

Acrobat has a sophisticated search capability. From the main menu, select **Tools | Search.** Then choose the **MMCX Master Index.**

Displaying figures

If lines in figures appear broken or absent, increase the magnification. You might also want to print a paper copy of the figure for better resolution.

Printing a paper copy

If you would like to read the *MMCX Electronic Documentation* in paper form rather than on a computer monitor, you can print all or portions of the online screens to any postscript printer. The files **ugprint.pdf** and **trprint.pdf** contain the whole user guide and technical reference, respectively. These files have been formatted to include 2 screens per page so that you do not waste paper.

You can also order the printed documents by calling the Lucent Technologies publications center at 1-800-457-1235. Ask for the *MMCX Electronic Documentation.* The order code is 555-027-811. These documents will be in the same format as if you printed them from the CD.

To print the technical reference or the user guide, do the following.

1. Select **File | Open**. Select **trprint.pdf** or **ugprint.pdf**.
2. Select **File | Print**.
3. Enter the page range you want to print, or select **All**. Note that the print page range is different from the page numbers on the documents (they print two to a page).
4. Close the file. Do not leave this file open while viewing the electronic documents.

Changes in this issue

The *MMCX Technical Reference* covers Release 2.0M of the MMCX server. This issue documents new server administration commands, support for H.323-compliant endpoints, and the optional Multimedia Applications Server Interface (MASI) to Lucent's DEFINITY® ECS.

1 Introduction

The Lucent Technologies MultiMedia Communications eXchange (MMCX) lets users communicate using simultaneous voice, video, and data applications, all with the convenience of a phone call. Yet MMCX users can still make and receive ordinary voice telephone calls from the public switched telephone network (PSTN).

MMCX consists of a server and client software linked by local area networks (LANs) and wide area networks (WANs). By connecting multiple MMCX servers you can support multimedia communications between users located anywhere that has ISDN access to the public switched telephone network.

Figure 1 shows a representative MMCX network. An MMCX network is defined as a set of interconnected MMCX servers and their client workstations configured to communicate via an extension-number dialing plan. Three MMCX servers, Denver1, Denver2, and NJ1, have been configured to communicate with each other. Denver1 and Denver2 communicate via an Ethernet LAN and ISDN PRI connections to a PBX. Denver1 and Denver 2 communicate with NJ1 via ISDN PRI to a PBX and a public toll switch. MMCX clients can make and receive multimedia calls via any of the multimedia workstations shown in the figure. They can also make and receive voice calls to telephones on the public switched network.

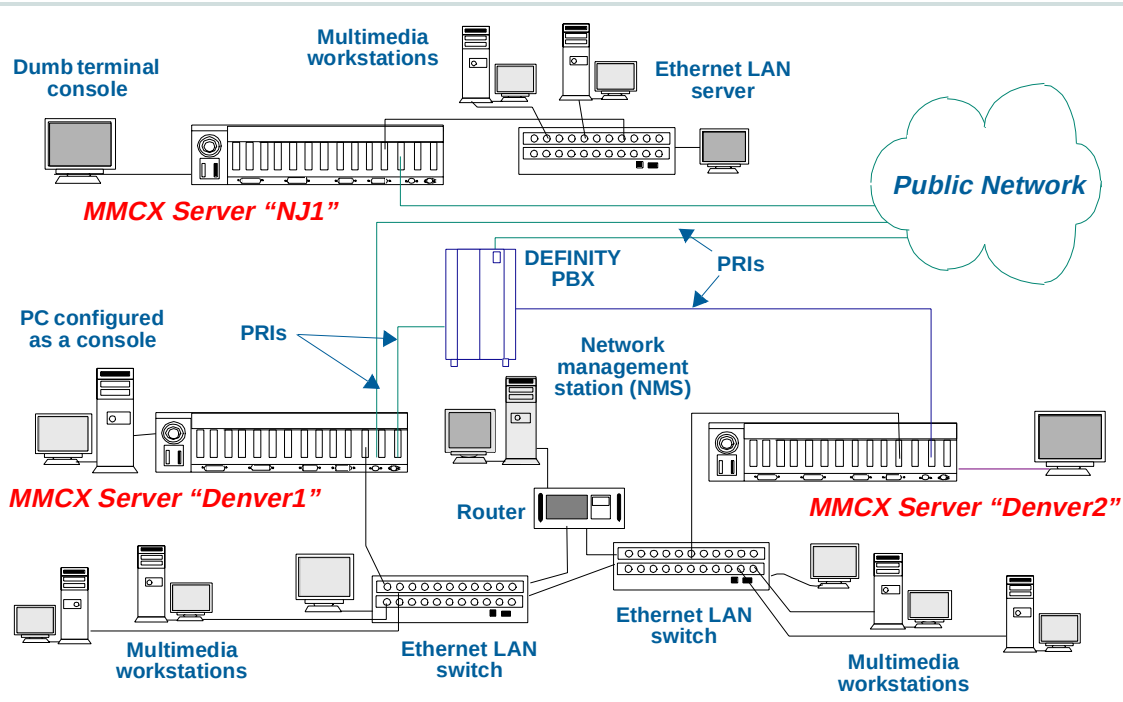


Figure 1. Sample MMCX network

Examples

Following are some examples of the types of calls that can be made in *Figure 1*, all with the convenience of making a telephone call:

- A user on any workstation can make a voice call to any other user on any other workstation in this figure. This assumes the workstations are equipped with either speaker-phones or headsets. One user contacts the other by dialing an extension number, just as if they were all located on a PBX private network.
- Once connected, the users can add video and/or data applications to the call and subsequently drop these media selectively. Users can share data applications, such as simultaneously working on a CAD drawing.
- The connected parties can decide to add additional callers, forming a conference of up to 6 parties. Again, selected media can then be added to or dropped from the conference.
- A call to a user can be redirected to another user and connected. If the other user answers, video and data applications can be added and dropped as described above.
- A user at one of the workstations can make or receive a voice call to/from any telephone accessible over a connected PBX or the public network. This call can be added to any MMCX conference.

MMCX server hardware

Figure 2, *Figure 3*, *Figure 4*, and *Figure 5* show the MMCX server hardware. The MMCX server is an industrial-grade PC using a Pentium-based CPU. It can be set on a table or mounted in a standard 19” rack. Following are the primary components in the server:

- CPU
- Ethernet card for connections to an IP LAN/WAN.
- ATM card for connections to an IP LAN/WAN
- ISDN PRI card for connections to a circuit switch (PBX or Central Office)
- WILD card for packet bus-to-TDM bus interface, conferencing, and echo cancellation
- Remote maintenance board (RMB) for remote maintenance by Lucent technical support personnel.
- VGA video card
- 1.44 Mb Floppy drive.
- 2 Gb Hard Disk Drive
- 350-Watt Power Supply

Name	
1	PRI Cards
2	Remote Maintenance Board
3	CPU Card
4	NIC (Network Interface Cards—ATM or Ethernet)
5	VGA video or NIC
6	WILD Cards
7	Card Clamp
8	Power Supply
9	Floppy Disk Drive
10	Hard Disk Drive
11	Filter
12	Fans

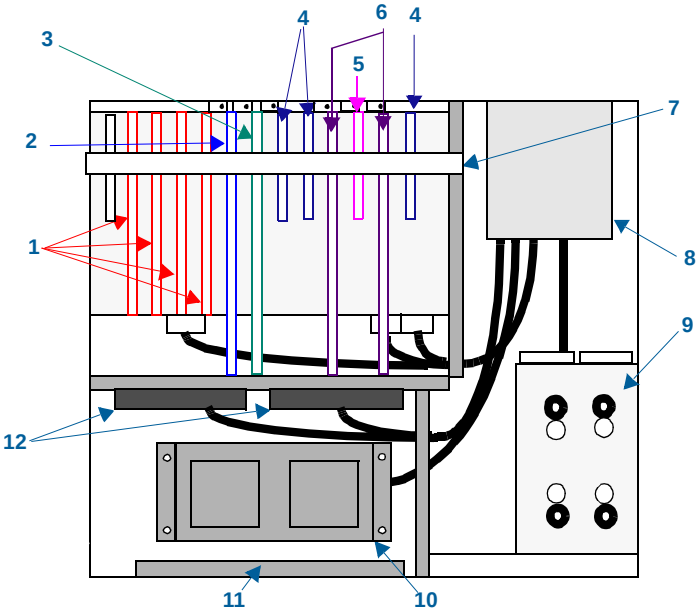


Figure 2. MMCX server hardware, top view

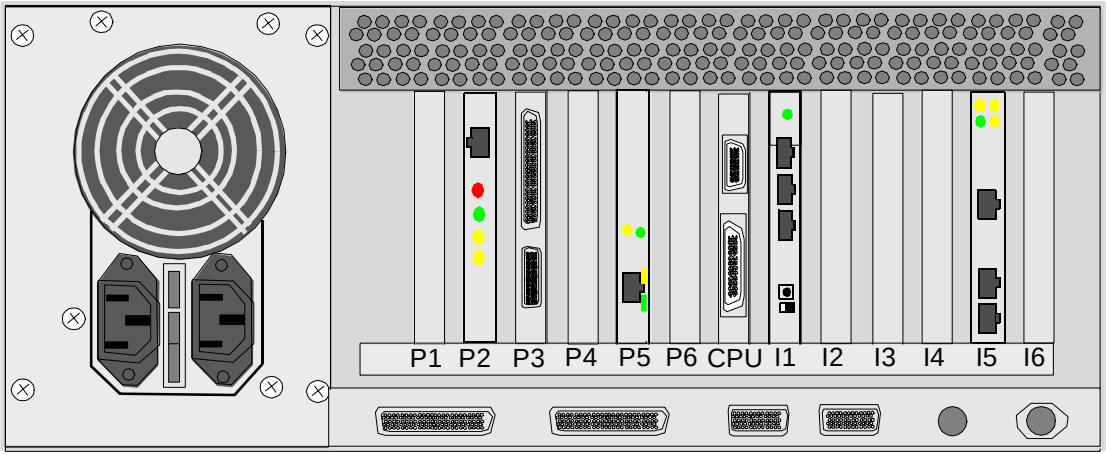


Figure 3. MMCX server, rear view

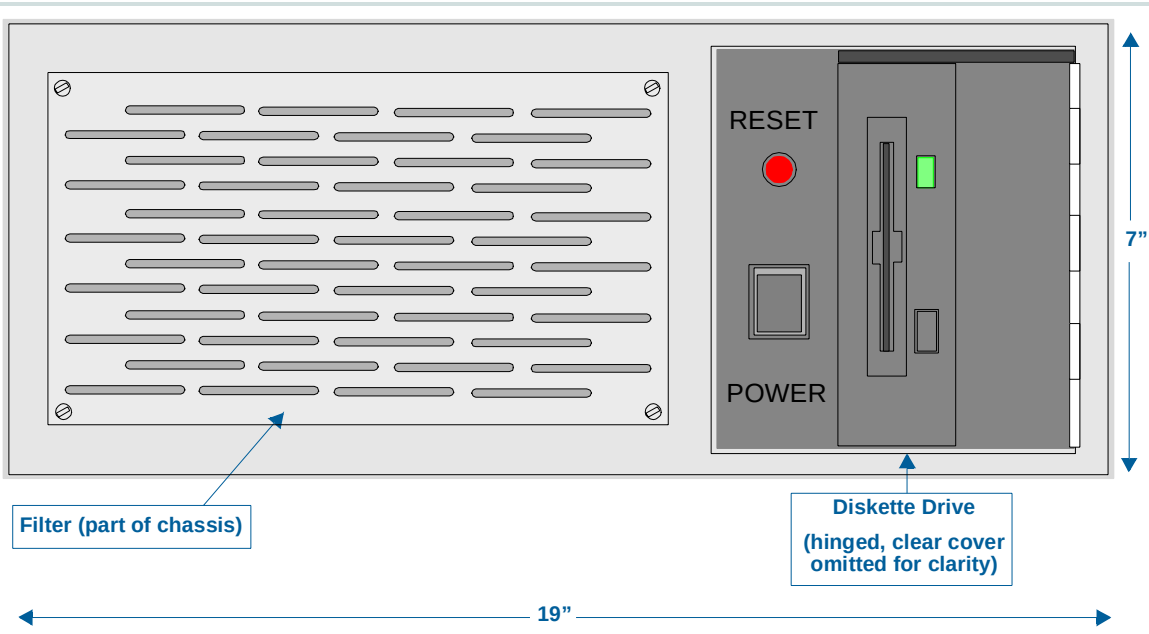


Figure 4. MMCX server, front view

Server circuit cards

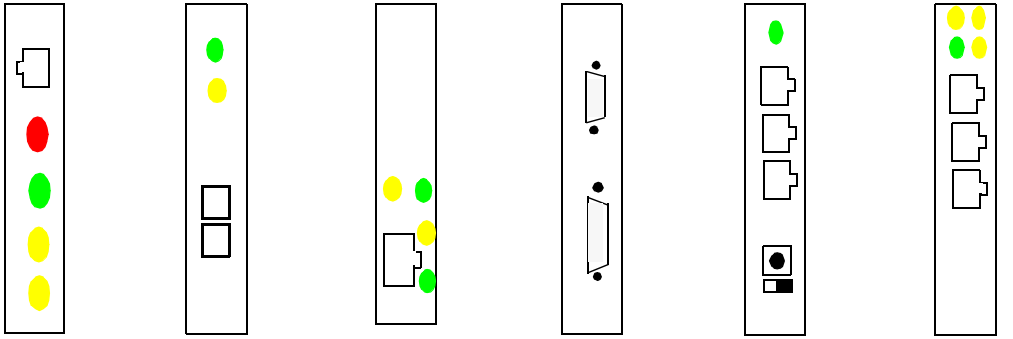


Figure 5. MMCX server circuit cards

How MMCX works

During an MMCX session, one user typically dials up another and sets up a multimedia call, adding video and shared data after the call is connected. Either user can then add callers to the call. Data and signalling can follow different paths, depending on how the server is administered. Consider the following.

Example 1

1. Ms. Blue and a coworker, Mr. Grey, log onto their local *MMCX server, Denver1*, from their *Multimedia workstations*, via the local area network (LAN). The MMCX client and server software sets up a TCP connection from *Ms. Blue*'s workstation, through her *Ethernet LAN switch*, to the Ethernet card on the Denver1 MMCX server. It does the same for *Mr. Grey*.
2. Ms. Blue dials Mr. Grey's extension number.
3. Call processing and system management software running on Denver1's CPU locates Mr. Grey using information stored in a *dial plan table*. The server finds that both parties are on Denver1.
4. Denver1 alerts Mr. Grey, and he answers the call.
5. Denver1 establishes an audio connection between Ms. Blue and Mr. Grey.
6. Mr. Grey offers video and a shared application to Ms. Blue, and Ms. Blue accepts. The video and data streams, like the audio, travel over the LAN without passing through the server.

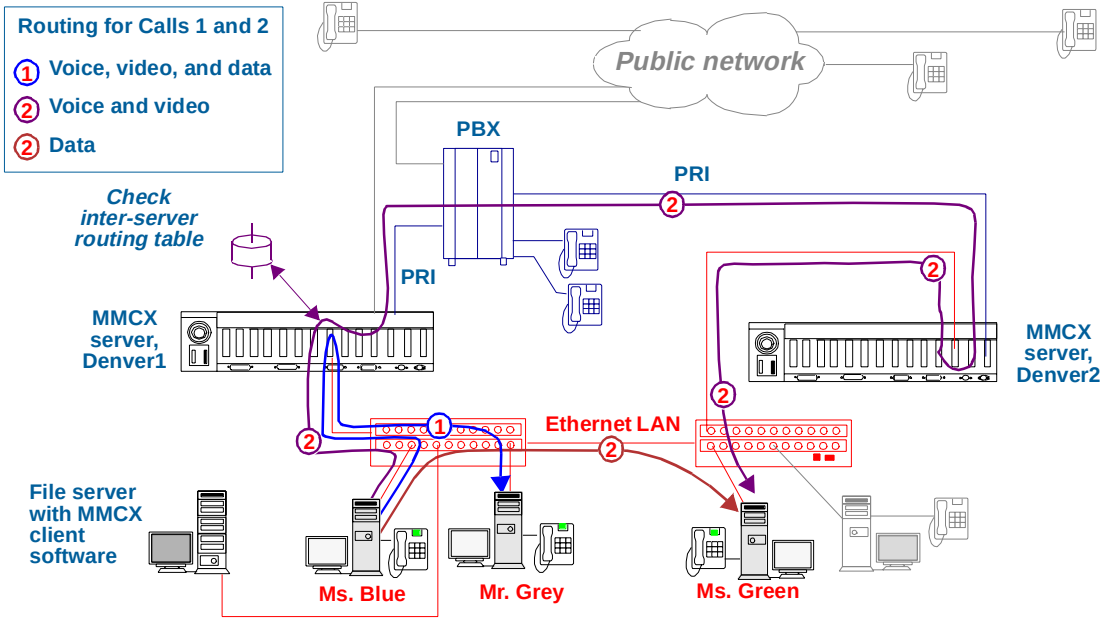


Figure 6. Routing multimedia calls with MMCX

Example 2

In the preceding example, audio, video, and data travel over the LAN once the call is established. But, to conserve Ethernet bandwidth, the Denver1 and Denver2 system managers could administer the server to send audio and video over the ISDN PRI and data and signalling over the LAN.

1. This time Ms. Blue and *Ms. Green* log into MMCX from their workstations. The MMCX client and server software sets up a TCP connection between Ms. Blue and the Denver1 server and between Ms. Green and her local *MMCX server, Denver2* via the Ethernet LAN.
2. Ms. Blue dials Ms. Green.
3. By checking the dial-plan, Denver1 finds that Ms. Green is on Denver2. Denver1 therefore calls the MMCX interserver routing software.
4. The routing software establishes a common signalling link between Denver1 and Denver2 using information provided by an *interserver routing table*.
5. The servers establish an audio connection between Ms. Blue and Ms. Green. Using information provided by the interserver routing table, Denver1 sets up the connection through the local PBX and an ISDN PRI B-channel.
6. Ms. Blue adds video to the call. Denver1 consults the interserver routing table and sets up a PPP connection over the ISDN PRI. It allots one or more B channels for the video stream (the system administrator sets the maximum number of B channels per video call during server setup and configuration).
7. Ms. Blue adds application data to the call. Denver1 again checks the interserver routing table and then sends the data over the Ethernet LAN.

WILD cards

The WILD card routes media streams travelling between the server's packet bus and the TDM (time-division multiplexing) bus on the switched network. Thus, any media over an ISDN PRI from an end-point on the LAN to an end-point on another server goes through the WILD Card. WILD cards also handle conferencing and echo cancellation for audio travelling from the LAN to the PRI (intraserver LAN calls need no echo cancellation).

Routing of customer IP traffic

The MMCX server does *not* route or otherwise process any non-MMCX media streams.

Basic features

The following table lists the major features of the MMCX system. For details, refer to the page indicated by clicking on the entry. For information on how to use these features, see the *MMCX User Guide.*

Two-party audio calling

This is the basic MMCX feature. All calls to or from an MMCX user begin with a two-party voice call. You add video, bring in other parties, and use other MMCX features *after* the two-party audio connection has been established.

MMCX uses the familiar telephony model for making calls: extension numbers and public network telephone numbers. In addition, MMCX provides DTMF tone generation and echo cancellation.

MMCX can originate and receive the following types of two-party audio calls.

- **Intraserver calls** between two users on the same MMCX server
- **Interserver calls** between two users on different MMCX servers (audio can travel over the LAN or over the ISDN PRI, depending on the configuration)
- **Voice Interworking calls** between an MMCX user and a non-MMCX telephone accessible through a PBX or central office switch connected to the MMCX server

Directory

Directory lets each user store names and telephone numbers in a personal directory. The user can search this directory and make a call by selecting an entry.

Conference

The Conference feature lets up to 6 parties share the same multimedia call. Any party on a call can add another party's audio. The new party's video can then be added if the called party is on the MMCX network. If the called party is a voice interworking telephone, you can only add their audio to the conference.

Call coverage

Call Coverage redirects calls to predefined extensions or public network numbers when you do not answer the call.

Call forward

The Call Forward feature also redirects calls if you do not answer. But unlike Call Coverage, Call Forward redirects calls to a single destination. If that destination does not answer, Call Coverage takes over and redirects the call.

Video

The Video feature lets any party to an audio call send their video to the other parties on the call. You can send, pause, and stop video transmission, and you can receive video from other parties.

SHARE

SHARE lets MMCX users share applications with the other MMCX users on a call.

WhiteBoard

Whiteboard supports image loading and editing. All multimedia-capable parties to a call are able to view and manipulate graphics files as if the images were drawings on a white board in a conference room. Whiteboard is a distributed data application, rather than an application sharing feature like SHARE.

SendFile

SendFile lets you send a file to any other MMCX user on the conference call. This feature is especially useful in conjunction with the SHARE feature. For example, the owner of the shared application can save the file and then use the SendFile feature to send the file to the other participants on the call.

Bandwidth management

The Bandwidth Management feature lets your network manager adjust server parameters to improve performance.

Performance monitoring

The Performance Monitoring lets the network manager monitor the performance of the network.

Multimedia Applications Server Interface (MASI)

MASI is an optional extension to MMCX that lets your server take advantage of the sophisticated call processing capabilities of the Lucent DEFINITY switch. With MASI enabled, you can track MMCX calls using DEFINITY call detail recording. You can use the DEFINITY switch's multipoint call redirection and call coverage to supplement the MMCX server's simple, single-point coverage. You can also lower costs and increase efficiency by using DEFINITY World Class Routing (AAR/ARS) for multimedia calls. This feature determines the optimal path through the private and public network for each call. MASI makes AUDIX® and INTUITY voice messaging features available to MMCX clients. Finally, MASI lets you assign DEFINITY trunk access codes to the ISDN interfaces that link your MMCX servers to each other and to the public switched telephone network. With these codes, the DEFINITY server can monitor traffic over these interfaces.

H.323 endpoint support

You can use MMCX 2.0M with H.323 clients. The MMCX server supports video and audio calls between H.323 endpoints, such as Microsoft® NetMeeting, and audio calls between an MMCX endpoint and an H.323 client or an H.323 client and a PBX extension or public-network telephone. H.323 clients can use the MMCX call coverage feature to forward calls to another number when they are busy or logged off. If you have purchased the optional MASI feature, you can also make use of some of the telephony features available on the DEFINITY switch. These include call blocking and advanced call routing. Release 2.0M does not support AUDIX on H.323 endpoints, however.

2 Pre-installation design and planning

This chapter covers the information you need to design and plan an MMCX network installation. Before you receive the MMCX shipment, you must do the following:

- Design your MMCX network to meet your needs
- Order the correct MMCX equipment based on your design
- Prepare your site(s) so that you will not interrupt the installation process after the shipment arrives

The table below lists the sections covering each of these tasks.

Designing an MMCX network

Before you can determine the equipment to order, you must design the MMCX network. Lucent Technologies technical support personnel perform all MMCX network designs. Your Lucent account representative will help you design your network.

Following are the prerequisite requirements for integrating MMCX into an existing network:

- The MMCX server connects to an Internet Protocol (IP) LAN.
- The connection to the IP LAN must be an Ethernet switch or an ATM switch, not a shared LAN hub.
- If you use an Ethernet switch, it must be either 10BaseT or 100BaseT.
- MMCX traffic should not travel through a router because the router can introduce unacceptable delays.
- If you use an ATM switch, the ATM network must be running LAN emulation as defined by the ATM Forum.
- An MMCX server supports either A-law or Mu-law companding but not both.

- The installation location must meet the environmental requirements specified in the following table.

	Operating	Non-Operating
Temperature	0-55 degrees C (32-131 degrees F)	0-70 degrees C (32-158 degrees F)
Humidity	5% to 95% non-condensing	5% to 95% non-condensing
Shock	5G at 10ms duration	10G at 10ms duration
Vibration	.5G at 5-100 Hz	5G at 5-100 Hz
Altitude	0 to 15,000 ft. (4572 meters)	0 to 50,000 ft. (15,240 meters)

Power requirements

The power supply is a 350 Watt auto-switching supply. It automatically adjusts to either of two allowed voltage ranges:

- 90 to 132 VAC (volts, alternating current) at 47 to 63 Hz
- 180 to 264 VAC at 47 to 63 Hz

Ordering equipment

After designing your MMCX network, you can order the MMCX equipment. Your Lucent Technologies account representative will determine the contents of the order based on the design.

Refer to the table below for the ordering codes for server components. Following are the guidelines for ordering parts:

- If a server component fails and it is no longer under warranty and you do not have a service contract with Lucent, contact the MACS. The MACS will assist you in identifying the parts you must order. If you have identified the failed component, you can contact the National Parts Service Center without first calling the MACS. Call 1-800-288-7278.
- If you want to add additional parts to the server to increase its capacity, contact your Lucent account representative.

Part Description	PEC	Comcode
Chassis, 3513P with 350W PS, FD Cable, no CPU		407579994
Chassis, Power Supply, 350W		407561661
Card, CPU P5120, 0 Mb, Custom BIOS		407515204
Card, Ethernet Network Interface	46001	407553254
Card, ATM Network Interface	46002	407553288
Cable Assembly, MVIP		601813082

Part Description	PEC	Comcode
Card, WILDCARD	46003	107560039
SIMM, 8 Mb, CPU (2 required for 16 Mb)		407416908
Card, PRI, PRI-ISA48 (T1)	46004	407562065
Drive, Floppy, 1.44Mb		406832584
Drive, Hard, SCSI, 2GB		407596857
Card, Remote Maintenance Board V1		406969238
Card, Remote Maintenance Board V2	46006	107725467
Cable Assembly, EMI Suppression, RMB		407265529
SIMM, 16 Mb, CPU (2 required for 32 Mb)		407420116
Cable Assembly, SCSI, Hard Drive		601813652
Cable Assembly, Floppy Drive		407561109
Cable Assembly, Ethernet NIC, Looparound		601813660
Cable Assembly, PRI, Looparound		601813751

Installation site planning

You should prepare for the MMCX installation well before the MMCX order arrives. If you do not do this, you might significantly delay the installation process. The following sections describe the steps you should take before starting the installation process.

Preparing and delivering installation documents to the site

The *MMCX Technical Reference* and the following documentation should be on site before begin the installation.

- A diagram of the MMCX network showing connectivity of MMCX components and your existing network
- A list of all MMCX users, their login IDs, their assigned international telephone numbers, and their proposed extensions. Each MMCX user must have a unique international telephone number. You can purchase a block of these numbers from the *central office* or *CO* (your ISDN service provider). If the server connects to a PBX, you can use an available block of numbers from the PBX.
- A list of the IP addresses for all MMCX servers and all hosts or servers with which the MMCX must communicate (such as the file server for the MMCX client software and the Network Management Station)
- Proposed PPP addresses for all inter-MMCX server connections.
- A copy of your MMCX contract showing the components you ordered

Checking network connectivity

Be sure that all eventual MMCX users are properly connected to the network by pinging several endpoints on the network. Type **ping *IP address* RETURN**.

If ping is successful with a few endpoints (at least two) then you can install the server hardware. If ping is unsuccessful, do not install the server.

Each MMCX workstation must have an IP route to the local MMCX server in its IP routing table. In addition, each workstation must have a route to IP subnetworks connected across the ISDN PRI. The best way to do this is to put an entry in the workstation's IP routing table that routes packets destined for these remote subnetworks to the local MMCX server.

Provisioning and testing ISDN PRI facilities

You have to provision all PRI facilities and services, either from the public network, from the PBX, or from both, depending on your connectivity. Some key elements of ISDN PRI provisioning are listed below.

- The ISDN PRI facilities must be able to provide both voice and data service. If your server connects to a PBX, you must use the correct trunk type on the PBX. If the server connects to a central office switch, you must provision the proper service. For example, if the server connects to AT&T, you should provision Software Defined Data Network.
- All PRI trunks that communicate with other MMCX servers must be PRI end-to-end to the other server.

- All tandem switches, such as CO switches or PBXs must pass the full calling party number. This number can sometimes be 15 digits or more. If the tandem switch truncates this number, MMCX will not communicate with remote servers. If you use a Lucent DEFINITY PBX, for example, you must configure the trunk group form to pass the calling party number.
- You must configure all tandem switches to pass 64 Kbps unrestricted data. If you use a Lucent DEFINITY PBX, for example, you have to set this parameter in the routing pattern form.
- You should test the PRI before receiving the server at the installation site.

Checking PBX administration

If the server connects to a PBX, make sure that all PRI and call routing administration is correct on the PBX. If you do not administer the PBX correctly, your MMCX will not work properly.

Install console terminal

You must have a dumb terminal or PC and suitable connectors available at the site for use as an MMCX console. You cannot install and start the server without a console terminal. If you wish to use a dumb terminal, you must build the connectors for the console-to-MMCX server cable.

Workstation system requirements

MMCX client workstations must meet the following requirements.

Platform	Intel-compatible personal computer (PC)
Processor speed	
audio and data only	100-MHz 486DX4 or better
video, audio, and data	100-MHz Pentium or better
Operating system	Microsoft Windows 95 or Windows NT 4.x
Required peripherals	
audio	full-duplex sound card
video	video capture device for QCIF video (176 x 144 pixels)
network	a network interface card (NIC): • an Ethernet card • or an ATM card with LAN emulation

Checking the installed LAN emulation packages (ATM networks only)

If you have an ATM network instead of an Ethernet, you must use LAN emulation. Be sure that you have installed the correct LAN emulation packages on all client workstations on the MMCX network. Make sure that you have installed the correct LAN emulation server on the IP network.

3 Installing and starting MMCX

This chapter guides you through setup, testing, and configuration of the MMCX server hardware. The following quick reference table provides an overview and can be printed for use as a checklist.

Lucent Technologies includes a range of customized installation services in its Installation, Software Engineering, and Network Integration offerings. You can purchase these services by contacting your Lucent representative. The service offering codes appear in the right hand column of the installation checklist table**. I** stands for Installation offering, **SE** for Software Engineering offering, and **NI** for Network Integration offering. **C** indicates a task that most customers can perform without special assistance.

Installation checklist and quick reference

	Task	Reference	Offer
	1 Unpack the server and make sure all components are present.	*Unpacking the server*	C, I
	2 Mount the server on a table or rack.	*Mounting the server*	C, I
	3 Connect loop plugs to the following connectors. • 10BaseT/100BaseT (item 11, *Figure 1*) or AUI (item 9, *Figure 1*). • T1/E1A (item 24, *Figure 1*). • T1/E1B (item 25, *Figure 1*)	*Hooking up the console, page 34*	C, I

Installation checklist and quick reference

	Task	Reference	Offer
	4 Connect a fiber patch cord to the ATM card (if so equipped)	*Hooking up the console, page 34*	
	5 Connect the console to the server	*Hooking up the console, page 34*	C, I
	6 Connect the RMB to a working analog telephone line.	*Connecting the RMB to an analog line, page 41*	C, I
	7 Connect power cord. Turn the power on. Observe the memory test, RMB initialization, and hard disk test.	*Powering up, page 42*	C, I
	8 Make sure that the RMB connection is working by calling its number from any telephone and listening for a modem answer tone.	*Checking the RMB connection, page 44*	C, I
	9 Boot the server to the ready-for-service state, and check the looparound tests.	*Booting the server to the ready-for-service state, page 45*	C, I
	10 Login to the server as **sysadm** using the default password.	*Logging in to the server, page 46*	

Installation checklist and quick reference

	Task	Reference	Offer
	11 Remove loop-around plugs and connect Ethernet, ATM, and PRI cards to the LAN and WAN networks.	*Connecting the server to the LAN and WAN, page 46*	C, I
	12 Set the IP configuration parameters.	*Assigning an IP address and server name, page 47*	C, I
	13 Configure the SNMP agent.	*Setting SNMP agent parameters, page 56*	C, I
	14 Assign a server number.	*Assigning a server number, page 58*	C, I
	15 Ping the IP addresses of endpoints and servers to check connectivity.	*Pinging MMCX endpoints and servers, page 59*	C, I
	16 Boot the server to the ready for service state, and log in.	*Booting the server to the ready-for-service state, page 45*	C, I
	17 Call MACS and request that your MMCX user licenses be enabled. Provide the MACS with the RMB dial-in number. Enable INADS.	*Enabling the end-user licenses, page 60*	C, I

Installation checklist and quick reference			
	Task	**Reference**	**Offer**
	18 Configure the server.	*Configuring MMCX parameters, page 61*	C, SE
	19 Backup the server software.	*Backing up server system files, page 318*	C, SE
	20 Boot the server to the full service state**.**	*Booting the server to the full-service state, page 61*	C, SE
	21 Wait for 5 minutes and check for alarms.	*Clearing alarms, page 62* (if needed)	C, SE
	22 Install the MMCX client software on the customer file server.	*Installing MMCX client software, page 62*	C
	23 Run the client software startup script and test features.	Refer to the *MMCX User Guide*.	C

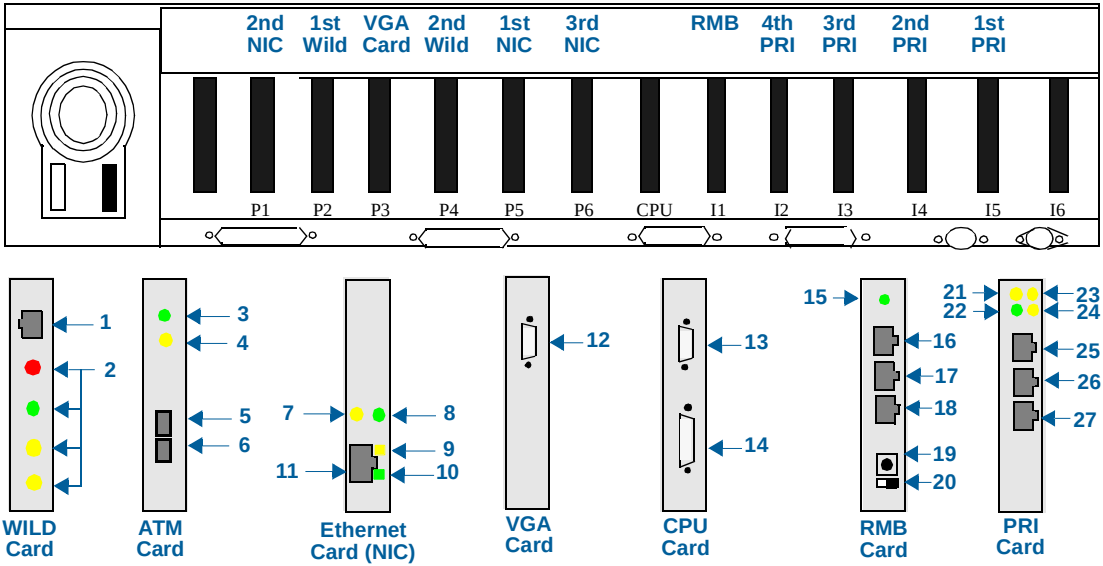


Figure 1. Server rear panel, details

Key to *Figure 1*	
1 Diagnostic and Status Connector	**2** WILD Card Indicators
3 Incoming Link Indicator	**4** Status Indicator
5 ATM Fiber Transmit Connector	**6** ATM Fiber Receive Connector
7 Full/Half Duplex Indicator	**8** 10/100 Mbps Indicator
9 Network Activity Indicator	**10** Link Integrity Indicator
11 10BaseT/100BaseT, RJ45 Connector	**12** Video monitor connector
13 Serial Port 1 Connector	**14** Parallel Port Connector
15 Status LED	**16** UPS Connector
17 Alarm Connector	**18** Modem Connector
19 SCSI Power Chain Connector	**20** Reset Switch
21 T1/E1A Indicator	**22** RUN Indicator
23 T1/E1B Indicator	**24** SYSFAIL Indicator
25 PRI Port B (port 2)	**26** PRI Port A (port 1)
27 Serial Diagnostic Connector	

Unpacking the server

To unpack the server, do the following.

1. Inspect the shipping container for signs of damage.
2. Open the shipping container from the top.
3. Remove the server and hardware.
4. Inspect the server for damage.
5. Check the contents against the shipping order. Make sure that all circuit cards are in their correct slots. For example, the first network interface card (either Ethernet or ATM) must be located in slot P5, the second NIC must be located in slot P1, etc. See *Figure 1* for these assignments. *If the specified components are not all present and correct, stop the installation*, and contact your Lucent Technologies account team representative.

Mounting the server

You can place the server on a table or mount it in a standard 19”- wide rack. If you specified a rack-mount version in your order, the server comes with telescoping slides and hardware. Follow the appropriate procedure below.

DANGER:
Before installing the server, make sure the power is off, and disconnect all power cords.

Table mounting

Place the server on a table with at least 2 inches of clearance above the vents for proper air flow. Make sure that the back of the server is readily accessible. ***Do not set other equipment on the server.*** Place a backup power supply nearby.

Rack mounting

WARNING:
Do not mount the server to the rack by hanging it from its front panel. Use the rails supplied with the unit.

To rack mount the server, proceed as follows.

1. Attach the glides of the telescoping mounting (supplied with the server) to the sides of the server case.
2. Attach the fixed rails to the rack.
3. Slide the server and glides into the rails on the rack.

The standard slides are 20 inches long. If your rack is deeper than 20 inches, attach standard extenders (available from General Devices Company, Inc., 1410 Post Rd., Indianapolis, IN 46239 317-897-7000, and from other vendors).

Hooking up the console

Once the looparound plugs are in place, connect the console, a VT100 or VT220 dumb terminal or a PC running VT100 or VT220 emulation, to the server's CPU. *You must have a console because boot-time status information is not displayed on remote terminals.*

VT100/VT220 terminals

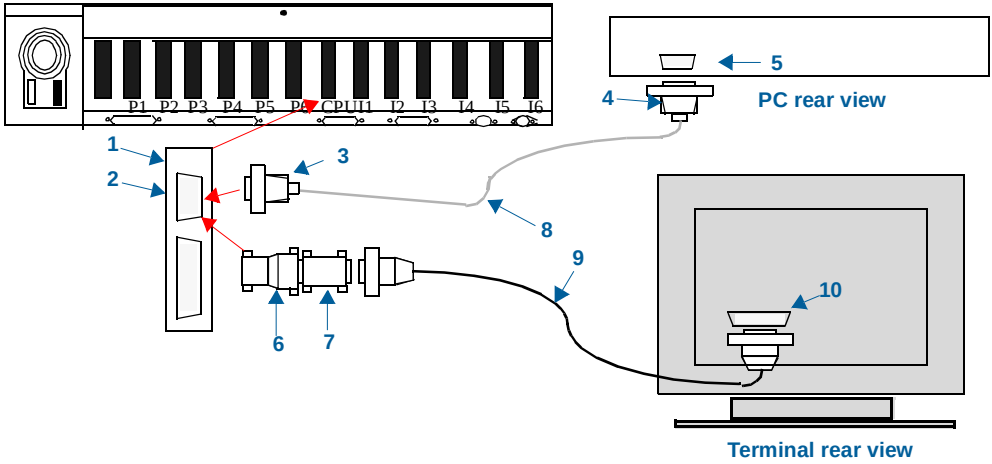
To connect a VT100 0r VT220 terminal, proceed as follows (consult *Figure 2*).

1. Build the necessary cables using the specifications in *Figure 3* and *Figure 7*.
2. Connect the 9-pin adapter (item **5**) to the null modem adapter (item **6**).
3. Connect the RS232 cable (item **9**) to the null modem adapter.
4. Connect the 9-pin adapter (item **5**) to the serial port connector (item **2**) on the CPU card.
5. Connect the other end of the RS-232 cable to the 25-pin connector (item **10**) on the terminal.
6. Set the baud rate on the terminal to **19,200** and set the bit rate for **8-bits**, **1 stop bit**, **no parity**.

Personal computers

To connect a PC with terminal emulation, proceed as follows (see *Figure 2*, *3*, and *7*):

1. Connect the CPU 9-pin plug (item **4**) to the serial port 1 connector (item **2**) on the CPU card.
2. Connect the PC 9-pin connector (item **7**) to the PC communications port (item **11**).



1 MMCX CPU card	**2** MMCX serial (COM) port 1
3 modular 9-pin MMCX serial adapter	**4** PC serial adapter
5 PC serial (COM) port	**6** 9-pin to 25-pin adapter
7 null modem adapter	**8** custom *D8W cable*
9 standard 25-pin RS-232 cable	**10** dumb terminal's 25-pin RS-232 interface

Figure 2. Connecting a PC or terminal to the server

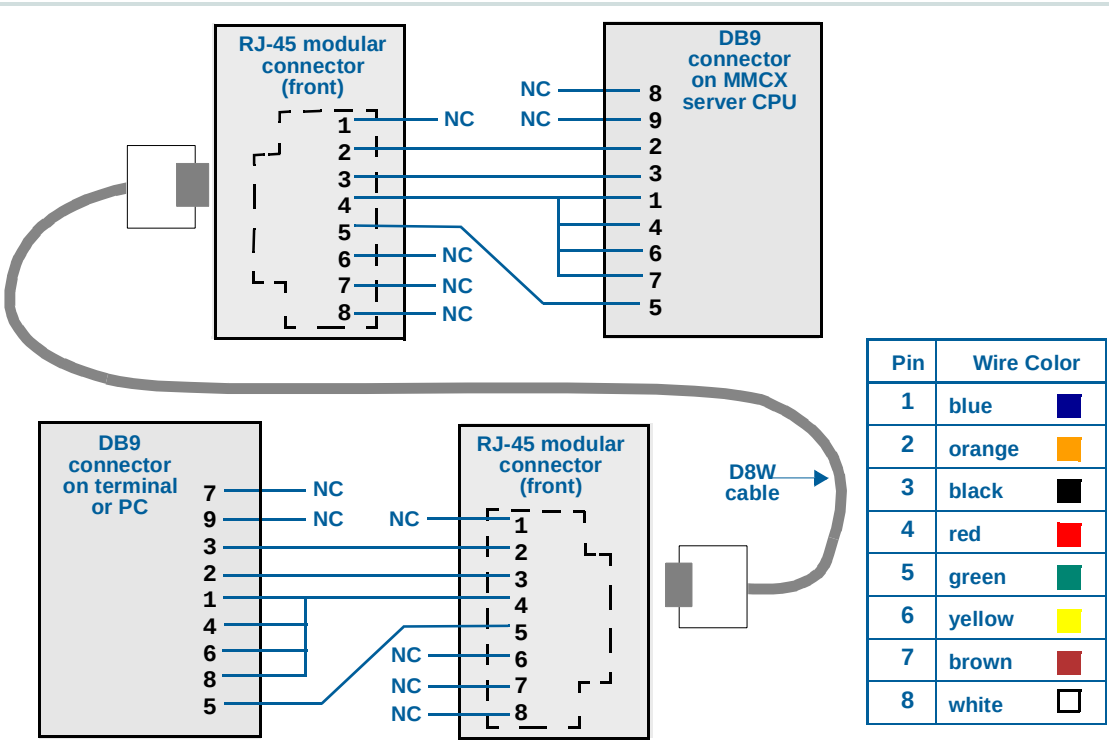


Figure 3. Adapters for connecting a console with RJ45 connectors & D8W cable

Installing external looparound plugs

After mounting the server, install external looparound plugs. Looparound plugs test the external interface of the card by sending data out the interface, through the plug, and back into the interface. When the plugs are in place, the server automatically performs tests of the external interface on the card during the startup process.

Lucent ships external looparound plugs for each Ethernet and PRI card supplied with the server. ATM-card looparounds are standard fiber-optic patch cords that you have to provide. Representative ATM patch cords and Ethernet and PRI looparounds are shown in *Figure 4*.

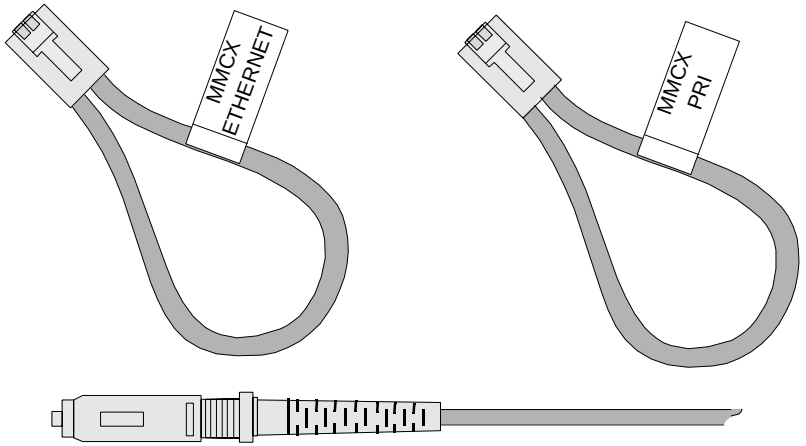


Figure 4. Ethernet and PRI looparound plugs and connector end of an ATM patch cord

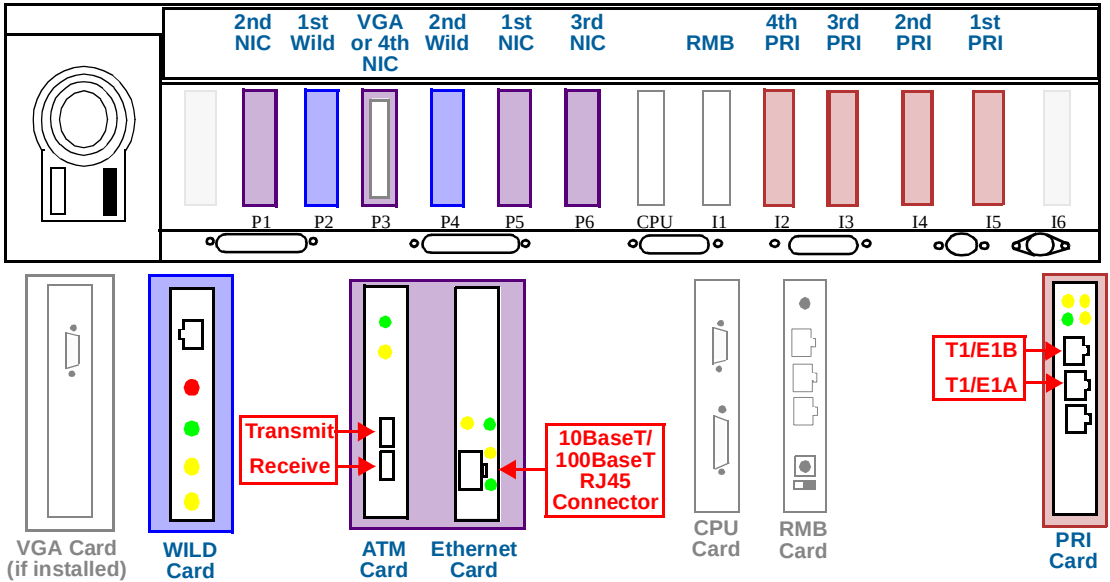


Figure 5. MMCX server backplane and card locations

Installing the looparounds

To install and use looparound plugs, proceed as follows.

1. Plug the Ethernet external loop plugs into the *10BaseT/ 100BaseT RJ45 Connector* on the Ethernet cards (unless your Ethernet card uses AUI connectors—most do not, but if yours does, follow the instructions in *Figure 6*).
2. Plug the PRI external loop plugs into the *T1/E1A* and *T1/E1B* interface connectors on the PRI cards.
3. Obtain a fiber-optic patch cord fitted with SC connectors (*Figure 4*). Connect one end to the *Transmit* connector on the ATM card and connect the other end of this same cord to the *Receive* connector on the same card. *Remember that fiber-optic patch cords are standard telecommunications cables. They are not supplied with MMCX servers.*
4. Restart the server. Type **reset level=cold2 ENTER**.
5. Check the alarm log for problems. Type **showalarm ENTER**. Perform the repairs specified in the alarm messages, if any.

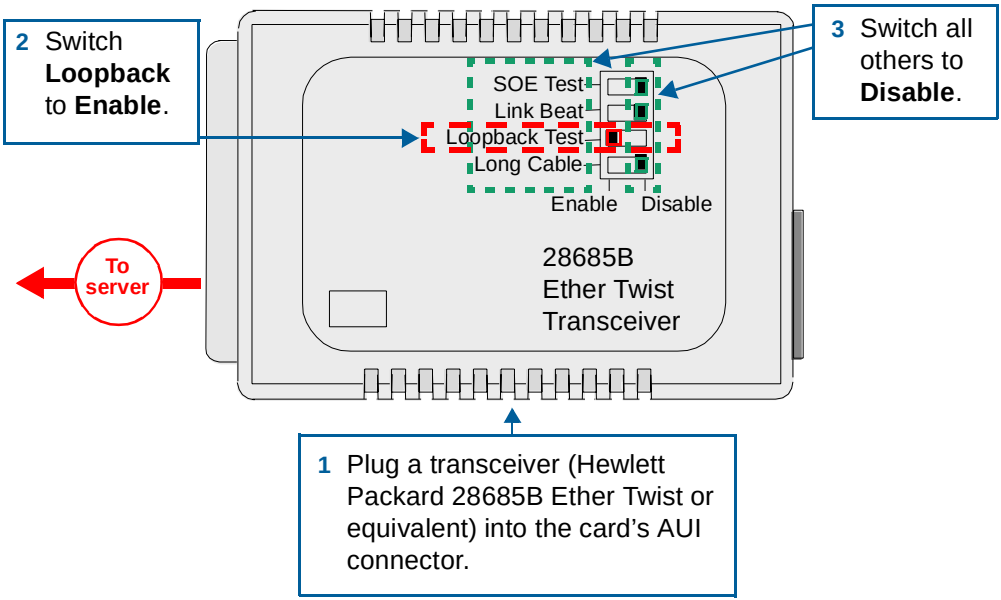


Figure 6. Ethernet transceiver looparound test

Connecting the RMB to an analog line

After you connect the console to the server, you should connect a telephone line to the Remote Maintenance Board (RMB). This line lets Lucent Technologies activate your software licenses and perform remote technical support.

Connect an analog line to the modem connector on the RMB (item 17 in *Figure 1*).

Powering up

WARNING:
Never apply power to the server without an operational console terminal connected! You cannot power-down the server properly without a console.

After connecting the console and RMB, turn on the power to the server using the procedure below. This initiates the startup sequence. If errors occur, refer to *Server startup problems, page 131*, for diagnostic and repair information.

1. Plug the server power cord into the Uninterruptible Power Supply (UPS).
2. Turn the power switch to **ON**.

   The startup sequence begins. A BIOS copyright notice appears and a memory test runs.
3. After the memory test is complete, the RMB modem initializes, and the console asks you to select **D** for **Diagnostics** or **C** for **Continue**. ***Press neither!*** Wait.

   After about 10 seconds, the bootup process continues. The following display appears.

```
Booting
Adaptec AIC-7850 BIOS v1.11
(c) 1994 Adaptec, Inc. All Rights Reserved.
Press <Ctrl><A> for SCSI Select (TM) Utility!
SCSI ID # - AT&T 1GB DPES 407340959 - Drive C: (80h)
BIOS Installed Successfully!
LynxOS preboot Version 2.3.0
Copyright (C) 1987, 1995 Lynx Real-Time Systems, Inc.
Command <b a0a /lynx.os>
```

Figure 7. Console display during bootup

4 Watch the results of the looparound tests on the console (*Figure 8*).

```
AHA 2940 Found! Bus 0 Dev1!
Waiting for boot device . . .
Installing WILD cards...
Core tests PASSED for WILD card in slot P2
Core tests PASSED for WILD card in slot P4
PRI Version 5.0 I/O 100..10f, Int 5, Mem cc000..cffff
PRI Version 5.0 I/O 110..11f, Int 7, Mem d4000..d7fff
PRI Version 5.0 I/O 120..12f, Int 5, Mem d8000..dbfff
PRI Version 5.0 I/O 140..14f, Int 7, Mem dc000..dffff
IA 5515 /dev/aal5_6: bus 0, device 15, slot 6, interrupt 14
LynxOS 386/486/Pentium PC-AT Version 2.3.0
Copyright 1987,1995 Lynx Real-Time Systems Inc.
All rights reserved.
LynxOS (lynxos) created Thu Oct  3 15:09:54 1996
LynxOS Startup:  a
Date set to  Wed Oct  9 08:12:34 MDT 1996
mounting all filesystems
atm6: flags=63<UP,BROADCAST,NOTRAILERS,RUNNING>
      inet 135.9.95.21 netmask ffffff00 broadcast 135.9.95.255
dec5: flags=23<UP,BROADCAST,NOTRAILERS>
      inet 135.9.155.73 netmask ffffff00 broadcast 135.9.155.255
add net default: gateway 135.9.155.254
hostname is mmcs01
inetd started
```

Figure 8. Results of looparound tests, LynxOS startup, and network initialization

After the server deletes old installation backups, it give you 10 seconds to enter the software administration menu.

5 Press the space bar key within 10 seconds.

If you miss this opportunity, let the server boot to the point where a user name prompt appears. Then log in to the server (see *Logging in to the server, page 46* for instructions**)**, and type **reset level=menu ENTER** to bring up the software administration menu manually.

The server displays the following menu.

```
1.  System Parameters - Configure the install time System Parameters
2.  System Backup - Perform a System backup of system files.
3.  System Restore - Restore the system files from backup.
4.  Software Installation Management - Software installation functions
5.  Continue booting of the software to full service state.
6.  Continue booting of the software to ready for service.
7.  Quit without booting - quit the menu but do not continue to boot
8.  Escape to LYNX-OS
9.  Help
Enter choice:
```

Figure 9. Software administration menu

Checking the RMB connection

Check the RMB connection by calling its number from a telephone. Listen for a modem answer tone. If the RMB does not answer, refer to *Server startup problems, page 131*, correct the problem, then return to *Powering up*.

Booting the server to the ready-for-service state

After you check the RMB, boot the server to the ready-for-service state. The ready-for-service state means that all server processes are up and running but the LAN interfaces are disabled (it is equivalent to the out-of-service state, **OOS**, that appears in many status messages). This prevents users from making MMCX calls while an administrator or technician performs actions on the server. Proceed as follows

1. From the software administration menu, type **6 ENTER** to select **Continue booting of the software to ready for service**.

   If errors occur, see *Operating system startup phase, page 143* or *Application startup phase, page 149* for diagnostics and repair information.

   If all is well, the server runs self-tests and displays their results.
2. Make sure that the server finds all cards physically present during self-test. If the server does not report all cards, refer to *Operating system startup phase, page 143* for repair procedures. After correcting the problem, return to *Powering up, page 42*.
3. The internal looparound tests (see *Looparound testing, page 338*) must pass before you can completely start the server. If any of the tests fails, the server logs an alarm (see *Viewing and interpreting alarm messages, page 156*).

   When booting is complete, the console displays the message **New Run Level: Active. System is initialized but will remain OOS as requested.** A login prompt or shell prompt appears, depending on how you reached the software administration menu.
4. If the system does not reach the Active:OOS state in a reasonable period of time, refer to *Application startup phase, page 149*. Then return to *Powering up, page 42*.

5 If the system state is **OOS FAULT** instead of **ACTIVE**, an internal looparound test probably failed. Refer to *Viewing and interpreting alarm messages, page 156*. From this section, diagnose the problem and follow the repair procedures and then return to *Powering up, page 42*.

Logging in to the server

SECURITY ALERT:

After you have finished installing the server, change the default password immediately. See *Maintaining system administrator accounts, page 71*.

Log in to the server as follows.

1 At the user name prompt, type **sysadm** and press **ENTER.**

2 At the password prompt, enter the default password for the sysadm login. This password is **sysadmpw.**

Connecting the server to the LAN and WAN

After booting to the ready-for-service state, you must leave the console and connect the server to the LAN and WAN.

1 Remove the external loop plug from the Ethernet card (item **9** or **11** in *Figure 1*).

2 Remove the external loop plug from the PRI card (items **24**, **25** in *Figure 1*).

3 Remove the ATM fiber cable from the transmit and receive connectors on the ATM card (items **5** and **6** in *Figure 1*).

4 Connect one end of a fiber patch cord with SC connector to the transmit connector on the ATM card. Connect the other end of this same cord to the receive connector on the LAN switch.

   Lucent Technologies does not ship fiber patch cords with the MMCX server. These are standard cables you must purchase from your LAN equipment vendor.

5 Connect an Ethernet cable to the 10BaseT/100BaseT connector on the NIC card or to the AUI connector (if so equipped). Connect the other end to the LAN switch.

6 Connect the PRI channel A cable to the T1/E1A Interface (Port 1) connector on the PRI card. Connect the other end to the Channel Service Unit (CSU).

7 Connect the PRI channel B cable to the T1/E1B Interface (Port 2) connector on the PRI card. Connect the other end to the CSU.

Assigning an IP address and server name

After you connect the server to the LAN and WAN, you need to configure the system to work with the network. You must set the initial IP address of the server and assign it a server name.

WARNING:
The IP address entered here has to match the IP address entered in the MMCX client software post-installation screen.

Configuring an Ethernet LAN

The procedure described in this section assumes you have an Ethernet card installed in slot **P5**. If you are using an ATM card, see *Configuring ATM networks, page 51* for the correct procedure.

1 Type **reset level=menu ENTER** to bring up the software administration menu.

2 At the prompt, press **1 ENTER** to select **System Parameters - Configure the install time System Parameters**.

The *System configuration menu* appears.

```
1.  IP Configuration
2.  SNMP Agent Configuration
3.  Set Server Number for Current Release
4.  Return to previous menu
5.  Help
```

Figure 10. System configuration menu

3 Type **1 ENTER** to select **IP Configuration**.

The *IP configuration menu* appears.

```
1. Configure Network Interface Cards
2. Configure Default IP Route
3. Define System Server Name
4. Return to previous menu
5. Help
```

Figure 11. IP configuration menu

4 Press **1 ENTER** to **Configure Network Interface Cards**.

The *NIC configuration menu* appears. The notation **p5:1** means slot P5, port 1. The term **dec5** is the driver software's name for the Ethernet card in slot P5.

```
The following prompts request information for configuration of the network
interface cards on the system.  The requested information is only enough to
allow the system to bring up the interface to a state usable by the system.
MMCX configuration management should be used for any additional required
configuration information. Entering "q" will quit the process and return to
the previous menu. Entering"?" will display help for the particular prompt.

Select a network interface card (NIC) to configure

1.  p5:1  (dec5)
q.  Quit current process and return to previous menu
?.  Help

Please enter a selection (Default - 1):
```

Figure 12. NIC configuration menu

5 At the prompt, press **ENTER.**

The system prompts you for an IP address and net mask.

6 At the prompt, enter the server's IP address. Although you can have up to 4 NICs in the server, *configure only the card in slot **p5***.

You will configure your additional Ethernet cards from the command prompt after installation is complete.

7 At the prompt, enter the IP netmask.

The server displays the IP information you entered.

8 Check the information you entered. If correct, press **Y ENTER** to return to the *NIC configuration menu*. Otherwise press **N ENTER** to start over.

9 At the prompt, press **Q ENTER** to return to the *IP configuration menu*.

10 At the prompt, press **2 ENTER** to select **Configure Default IP Route**.

11 At the, enter the ***IP-router-address*** for the server.

The server displays the new router address. *Note that this is just the default. To define other IP router addresses, see Configuring the IP routing table, page 116*.

12 Check the router address information. If correct, press **Y ENTER** to save the changes and return to the *IP configuration menu*. Otherwise, press **N ENTER** to go back.

13 At the prompt, press **3 ENTER** to define the system server name.

The server prompts you for a server name.

14 At the prompt, enter the name of the server, and press **ENTER**.

The system prompts you for a corresponding NIC card.

15 At the, prompt, press **ENTER**.

The server displays the server name information.

16 Check the server name. If correct, press **Y ENTER** to return to the *IP configuration menu*. Otherwise press **N ENTER** to start over.

17 Press **4 ENTER** to return to the *System configuration menu*.

Configuring ATM networks

If you have an ATM card in slot P5 instead of an Ethernet card, you must configure several additional parameters.

1. Type **reset level=menu ENTER** to bring up the software administration menu.
2. At the prompt, press **1 ENTER** to select **System Parameters - Configure the install time System Parameters**.

   The *System configuration menu* appears.

```
1.  IP Configuration
2.  SNMP Agent Configuration
3.  Set Server Number for Current Release
4.  Return to previous menu
5.  Help
Enter choice:
```

Figure 13. System configuration menu

3 Type **1 ENTER** to select **IP Configuration**.

The *IP configuration menu* appears.

```
1.  Configure Network Interface Cards
2.  Configure Default IP Route
3.  Define System Server Name
4.  Return to previous menu
5.  Help
```

Figure 14. IP configuration menu

4 At the *IP configuration menu* prompt, press **1 ENTER** to configure the network interface cards.

The default *Network configuration menu* appears.

```
1.  Configure Network Interface Cards
2.  Configure Default IP Route
3.  Define System Server Name
4.  Return to previous menu
5.  Help
Enter Choice:
```

Figure 15. Network configuration menu

5 Press **1 ENTER** to **Configure Network Interface Cards**.

The *NIC configuration menu* appears. The notation **p5:1** means slot P5, port 1.

```
The following prompts request information for configuration of the network
interface cards on the system.  The requested information is only enough to
allow the system to bring up the interface to a state usable by the system.
MMCX configuration management should be used for any additional required
configuration information. Entering "q" will quit the process and return to
the previous menu. Entering"?" will display help for the particular prompt.

Select a network interface card (NIC) to configure

1.  p5:1  (atm5)
q.  Quit current process and return to previous menu
?.  Help

Please enter a selection (Default - 1):
```

Figure 16. NIC configuration menu

6 At the prompt, press **ENTER.**

The system prompts you for an IP address and net mask.

7 At the prompt, enter the server's IP address.

8 At the prompt, enter the IP netmask.

The server now asks you to select **Manual** or **Automatic** configuration of LAN emulation .

9 Type **Manual ENTER** (the default is "Auto").

The server prompts you to **Please enter the LAN emulation server ATM address (Default - none (the "well-known LECS address))":**

10 Enter the LAN emulation server ATM Address.

A typical LAN emulation server address: **0000a0a0a0f03456000567002340505a00000000**

11 The server prompts you to **Please enter name of emulated LAN (Default - none):** Do so.

The display now looks something like that in *Figure 17*.

```
IP configuration information for p5:1  (atm5).
IP Address:               135.9.144.116
IP Network Mask:          255.255.255.0
ATM Configuration Mode:   Manual
ATM Address for LES:      0000a0a0a0f03456000567002340505a00000000
LES Emulated LAN Name:    LAN2

Save configuration [y or n]? y
```

Figure 17. Configuring LAN emulation

12 Check the information you entered. If correct, press **Y ENTER** to return to the *NIC configuration menu*. Otherwise press **N ENTER**, and start over.

The server now displays the new configuration and returns to the NIC configuration menu.

```
atm5: flags=23<UP,BROADCAST,NOTRAILERS>
      inet 135.9.144.20 netmask ffffff00 broadcast 135.9.144.255
```

Figure 18. Configuring LAN emulation

13 At the prompt, press **Q ENTER** to return to the *IP configuration menu*.

14 Press **2 ENTER** to select **Configure Default IP Route**.

15 Enter the ***IP-router-address*** for the server.

The server displays the new router address. *Note that this is just the default. To define other IP router addresses, see Configuring the IP routing table, page 116*.

16 Check the router address information. If correct, press **Y ENTER** to save the changes and return to the *IP configuration menu*. Otherwise, press **N ENTER** to go back.

17 At the prompt, press **3 ENTER** to define the system server name.

The server prompts you for a server name.

18 At the prompt, enter the name of the server, and press **ENTER**.

The system prompts you for a corresponding NIC card.

19 At the prompt, press **ENTER**.

The server displays the server name information.

20 Check the server name. If correct, press **Y ENTER** to return to the *IP configuration menu*. Otherwise press **N ENTER** to start over.

21 Press **4 ENTER** to return to the *System configuration menu*.

Setting SNMP agent parameters

Next you set the SNMP agent parameters. Proceed as follows.

1. At the *System configuration menu*, type **4 ENTER** to select **SNMP Agent Configuration**.
   The server displays a warning and asks for confirmation.
2. Press **y ENTER** to continue.
   The console prompts you for the server location.
3. Type ***server-location*** **ENTER**.
   The console displays community string information and the *Community string menu*.
4. Type ***server-contact-name*** **ENTER**.
   The console asks for the name of the contact person who will be responsible for the server.

```
Gathering community string configuration information.
Current community string list:

      public 0.0.0.0     read         0
      mmcx   0.0.0.0     write        2

Community string list commands:
a.  Add new community string entry.
d.  Delete current community string entry.
m.  Modify current community string entry.
x.  List complete.
q.  Quit.
?.  Help.
```

Figure 19. Community string menu

5 At the prompt, press **a ENTER** to select **Add new community string entry**.

The console prompts you to **Please enter a community string name**. Community strings are a security mechanism that protects the server's system management function. For example, you typically have to give NMS software the ability to execute read and write system management commands. Using community strings, the NMS can execute these commands without being logged onto the server.

6 Type ***NMS-name*** **ENTER**.

You are prompted for an IP address for the new community string name.

7 Type ***IP-address-for-NMS*** **ENTER**.

You are asked to assign access privileges for the new community string name.

8 At the prompt, type **write ENTER**.

The server displays the new community string information and asks you to confirm it.

9 If correct, press **y ENTER**. Otherwise press **n ENTER** to roll back the changes.

The *Trap community list commands* menu appears.

```
Trap community list commands:
a.  Add new trap community entry.
d.  Delete current trap community entry.
m.  Modify current trap community entry.
x.  List complete.
q.  Quit.
```

Figure 20. Trap community list commands

Traps generate the alarms that appear in the alarm log. Alarms are always logged locally, on the server. But you could write an application that could interpret SNMP trap messages for an NMS. In this case, you could have the server send traps to the NMS as well.

10 Press **x ENTER** to display the current community trap list. ***NMS-name*** should appear.

11 Press **q ENTER** to exit to the previous menu.

Assigning a server number

CAUTION:
The server number entered here must be the same server number as entered in the MMCX Client Software post-installation screen.

Now you have to assign a unique number to distinguish the new server from all others on the network. To assure its uniqueness, use an international telephone number. Proceed as follows.

1 Reserve the first number in the first block of international numbers you purchased for use with MMCX. This will be the server number.

In the United States, the international number is equivalent to a direct inward dial (DID) number prepended with the U.S. country code (1).

2 From the *System configuration menu*, press **3 ENTER** to select **Set Server Number for Current Release**.

The server displays the following warning (*Figure 21*) and asks for confirmation.

```
****  WARNING WARNING WARNING WARNING  ****

Changing the server number will WIPE OUT your database!!!!!
This will REQUIRE re-entry of all system management commands
used to build this database.  Restoration from a previous backup
will not restore these commands to the database with the new
server number.

Are you sure you wish to continue [y or n]?
```

Figure 21. Server number warning

3 press **y ENTER** to continue.

The server echoes several commands and then prompts you for the server number.

4 Type in the international telephone number that you reserved in step 1 of this section. Press **ENTER**.

The server rebuilds the MMCX database and returns you to the previous menu.

5 Enter 4 at the system parameters sub menu to return to the Startup Administration menu.

6 If you have a multiserver MMCX network, also assign the new server number as the interserver routing telephone number (see *Assigning interserver routing numbers, page 99*).

Pinging MMCX endpoints and servers

After you have set all system parameters, test for connectivity between MMCX endpoints and servers.

1 From the System Administration menu, type **8 ENTER** to select **Exit to LynxOS**.

2 Log in as **sysadm**.

3 Type **ping *IP-address* ENTER** for each of the following values of ***IP-address***.

- ***Server-IP-Address***
- ***Endpoint-IP-Addresses*** for all users of MMCX.

  Do not continue installing the server until these machines can be pinged successfully.
- ***MMCX-server-IP-Addresses*** for all connected MMCX servers

  Do not continue installing the server until these machines can be pinged successfully.
- ***Machine-IP-Addresses*** for the Network Management Station, file servers, and all other devices that this server connects with over the LAN.

4 Type **exit ENTER** to return you to the software administration menu.

Booting the server to the ready-for-service state

After you have checked IP network connectivity, proceed as follows.

1 Return to the software administration menu.

2 Type **6 ENTER** to boot the server to the ready-for-service state.

3 Log in.

Enabling the end-user licenses

Call Lucent Technologies' Multimedia Application Customer Support (MACS) at 1-800-821-8204 to enable your end-user software licenses.

Configuring MMCX parameters

At this point, the server is in the active out of service (OOS). Now use the server's system management command line interface to configure the server. Proceed as follows.

1. Go to *Configuration Management, page 70*, and perform all the listed tasks.
2. Then return to this step to continue server installation.

Backing up server system files

After you configure the server with the configuration management commands, backup of the software.

1. Go to *Backing up server system files, page 318*.
2. Return here to continue with installation.

Booting the server to the full-service state

When the server reaches the full-service state, all processes are all up and running, and the LAN interfaces are enabled. This state is the normal operational state of the server. Proceed as follows.

1. Type **reset level=menu ENTER** from the shell prompt.

   The server displays the nine-item software administration menu.
2. Type **5 ENTER** to select **Continue booting of the software to full service state**.

   If all is well, the server reports **New Run Level: ACTIVE**, **New System State: IS**. If errors occur, go to *Server startup problems, page 131*.

Clearing alarms

After booting the server to the full service state, you should clear any alarms that have been logged. See *Viewing and interpreting alarm messages, page 156*.

Installing MMCX client software

Once the installation of the server is complete, install the client software. Proceed as follows.

1 Make sure the PC meets the system requirements listed here. A video capture card is optional.

Platform	Intel-compatible personal computer (PC)
Processor speed audio and data only video, audio, and data	 100-MHz 486DX4 or better 100-MHz Pentium or better
Memory (RAM)	32 Mb
Disk space	about 30 Mb
Operating system	Microsoft Windows 95 or Windows NT 4.x
Audio	full-duplex sound card
Network	network interface card (Ethernet or ATM with LAN emulation)
Video (needed for video conferencing)	video capture device for QCIF video (176 x 144 pixels)

2 If you are using Windows NT, log in as the administrator (you must have administrator privileges to install software under NT).

3 Close all other applications.

4 Insert the MMCX client software CD into the CD ROM drive.

5 From the task bar, open the **Start** menu.

6 Select **Run**.

7 Enter **CD drive:\setup**.

The setup program initializes and displays a **Welcome** screen.

8 Click **Next**.

Setup warns you to close all other programs.

9 Enter the server number and the host name, and click **Next**.

Setup prompts you for an MMCX installation folder and suggests a default.

10 Most users should accept the default folder by clicking **Next**. If you want to specify a different directory, click **Browse**, enter the directory name, then click **Next**.

The setup application checks for installed copies of NetMeeting™ and asks if you want to install it or overwrite an existing installation.

11 To ensure that you have the version of NetMeeting for MMCX, click **Yes**.

If you click **No** and do not have an existing copy of the correct version of NetMeeting, MMCX installation stops. If you have NetMeeting installed already, the setup application automatically configures it to work with MMCX.

12 When prompted, click **Yes** if you want to launch MMCX each time you log on to your PC.

A bar graph shows the progress of the MMCX installation. When the setup program tells you it is finished, click **OK**.

NetMeeting installation begins.

13 Click **OK** to install NetMeeting.

14 Click **Yes** to continue installing NetMeeting.

15 Click **Yes** to accept the License Agreement.

If you do not, the NetMeeting installation stops at this step.

16 NetMeeting setup asks if you want to install in the default directory. Most users should click **OK**. If you want to specify a different directory, click **Browse**, enter the directory name, and then click **OK**.

Setup asks if it can create a NetMeeting directory if one does not already exist.

17 Click **yes**.

Installation begins. A bar graph records the progress of the setup process.

18 Setup displays a **NetMeeting installed successfully** message. Click **OK**.

NetMeeting may or may not ask you to restart Windows.

19 Restart Windows.

We recommend that you always restart windows after installing software, even if you are not forced to do so. This ensures that new applications are fully initialized.

20 MMCX client software is now installed on your PC. Make sure your administrator has installed the MMCX server software and set up your user account, or you will not be able to use MMCX.

The first time you launch MMCX, you have to enter registration information before you can use the product.

MMCX client documentation installation procedure

1. Insert the *MMCX Electronic Documentation* CD into the CD ROM drive on your PC.
2. Connect to the CD ROM drive in the File Manager. The electronic documentation is located in the **document** directory.
3. Select the **document** directory.
4. Copy the directory **mmcxdocs** and all its files and subdirectories to your PC hard drive.
5. In **c:\ acrosrch\disk1**, double-click the **setup.exe** file. This installs the Acrobat Reader in a directory you specify and adds it to your **Start** menu. During installation, when the program asks you to install the next disk, double-click that **disk** file in **c:\acrosrch**.
6. To view the electronic documentation, double-click the Acrobat Reader icon or select **Start | Programs | Adobe Acrobat | Acrobat Reader 3.0**. (Your customizing may place Acrobat Reader in a different place in **Start**.) Open **c:\ mainmenu.pdf** to display the MMCX Electronic Documentation main menu.
7. To use the Acrobat search index tool, select **Tools | Search | Indexes | Add.** Click **OK** to add the file **index.pdx,** located in the **mmcxdocs** directory. In the next window, select **MMCX Search Index** and click **OK**.

4 Using the MMCX command line

You start, configure, monitor, and troubleshoot MMCX servers from the MMCX command line. The MMCX command line interface runs from the Lynx shell on the server. You access system management functions by logging into the server and typing commands.

MMCX command-line system management is based on the Simple Network Management Protocol (SNMP). The management information base (MIB) combines standard SNMP MIB objects with objects developed specifically for MMCX. In keeping with the International Standards Organization's (ISO) Open System Interconnect (OSI) model of system management, MMCX supports security, configuration, performance, and fault management. But it does not currently support OSI accounting management.

Logging in

The login process protects the MMCX server from unauthorized or untrained users. Authorized system administrators identify themselves by entering user names and passwords. Since the server grants system administrator privileges to all users, anyone who can log in can also execute system management commands. For this reason, you should not allocate logins to persons who lack specific administrative responsibilities.

To login, follow the procedure below.

At the console

To log in to the server from the attached console, proceed as follows.

1 Make sure that the console terminal is connected and turned on.

   The server prompts you for a **user name**.

2 Enter your user name.

   The server prompts for a **password**.

3 Enter your password.

   If you enter incorrect information, the server notifies you and again prompts you for a valid user name.

   If you have logged in successfully, the server displays a shell prompt of the form ***<servername-login_ID>***

From a network workstation

With one exception, you can administer the MMCX server across a network just as you would from the attached console. The exception is rebooting: if you reboot from a remote location, you do not see the status messages that normally accompany system restarts. The server sends these messages only to the console.

To log in to the server over a network, proceed as follows.

1 Open a UNIX terminal-emulation window on your network PC or a shell on your network workstation.

2 At the shell prompt, enter **rlogin *server-name*** or **telnet *server-name***

   The server prompts you for a **user name:**

3 Enter your user name.

   The server prompts you for a **password:**

4 Enter your password.

If you enter incorrect information, the server notifies you and again prompts you for a valid user name.

If you have logged in successfully, the server displays a shell prompt of the form ***<servername-login_ID>***

Over a dialup connection

You can also log in from a dialup connection. You should realize, however, that there are security implications to this approach. If you still want to administer your server this way, proceed as follows.

1 Make sure that a modem is attached to the RS232 port on the MMCX server's CPU card and to a telephone line.

2 From a modem-equipped, VT100 terminal or PC, dial up the MMCX server.

When the call connects, the server prompts you for a **user name:**

3 Enter your user name.

The server prompts you for a **password:**

4 Enter your password.

If you enter incorrect information, the server notifies you and again prompts you for a valid user name.

If you have logged in successfully, the server displays a shell prompt of the form ***<servername-login_ID>***

Executing system management commands

You execute system management commands by typing a command line at the Lynx shell prompt and pressing **ENTER**. All commands share a common syntax:

command_name keyword1=parameter1_value ... keywordn=parameterN_value

For example, you add an Ethernet connection at slot p2 with an IP address of 135.9.144.92 and a subnet mask of 255.255.255.0 with the following command:

addenet slot=p2 port=1 ip=135.9.144.92 mask=255.255.255.0

Note that some parameters are optional and that default values are defined for most commands.

Using MMCX commands with the LynxOS shell

System management commands are, in effect, Lynx shell commands. You can use existing shell commands to filter or otherwise process system management commands. For instance, **showenet data=cfg | grep p1** displays the settings for the Ethernet card in slot p1, while **showenet data=cfg | more** displays output for all cards a page at a time.

Getting help with command syntax

To check the syntax of a specific command, refer to the *Manual Pages, page 425* or issue the UNIX **man** command with the appropriate command name.

5 Configuration Management

As the MMCX system administrator, you are responsible for configuring the server to work with your organization's telecommunications network. This chapter explains how you manage server security and how you set up the MMCX server to work with your local area network (LAN), your PBX, and the public switched telephone network (PSTN).

Using a shell script

Configuration management is much easier if you save your configuration commands as a shell script. If you accidentally erase your settings, you can then restore the server configuration with a single command, the name of your executable shell-script file.

System parameters & configuration commands

You configure the server by assigning values to the arguments of the configuration administration (CFGADM) commands. You enter the sequence ***command parameter =value*** at the system prompt. Most (but not all) parameters accept both string and numerical values. String and numerical values can appear together, with the numerical part in parentheses. For example, the line-compensation parameter can be specified as a single digit in the range 1 to 5 or as a corresponding string. All of the following set line compensation to 300 ft.

- **chgpri lcomp=3**
- **chgpri lcomp=length266to399ft.**
- **chgpri lcomp=length0to133ft(1).**

Maintaining system administrator accounts

Security should be your first consideration when configuring your server. You secure your system by assigning passwords to all authorized system administrators. MMCX servers are shipped with a superuser login, **sysadm,** and a corresponding default password, **sysadmpw**. This lets you get started.

SECURITY ALERT:

The default superuser password, sysadmpw, is not secure. Change it as soon as possible. Then change it again at reasonable intervals, in keeping with accepted system-security practices.

The MMCX superuser, sysadm

To add or modify administrative accounts on the server, you must log in as the superuser, **sysadm**. Other system administrators (those that sysadm adds using the procedures listed below) can control most of the server's calling and networking functions, but they cannot add administrators or change passwords (including their own).

Changing a password

You change passwords with the **chgsapasswd** command. Proceed as follows.

1. Log in as **sysadm**.
2. Type **chgsapasswd login=*old_login*** **ENTER**.

   The server prompts you for the current password for ***old_login***.
3. Enter the current password.

The server prompts you for a new password.

4 Enter the new password.

The server asks you to confirm the new password by entering it again.

5 Re-enter the new password.

If you type the password correctly, the server makes the change. Otherwise, the it asks you to try again.

Displaying currently authorized system administrators

If you need to see who currently has system administrator privileges, you can display a table of login names and corresponding personal names. Proceed as follows.

Type **showsa RETURN.**

Adding a new system administrator

SECURITY ALERT:

MMCX system administrators have considerable power over your communications system. For this reason, you should not set up server accounts for anyone whose job responsibilities do not require it. All accounts should be assigned passwords.

You can add new MMCX system administrators by creating new logins.

1 Log in to the server as **sysadm**.

Only the superuser, sysadm, can add accounts.

2 Type **addsa login=*new_login* name="*FirstName LastName*" id=*nnnn* ENTER.**

Be sure to enclose the name string in quotation marks. Assign an unused number between 100 and 5000 to the **id** argument.

When you press **ENTER**, the server asks you if you want to assign a password.

3 When the server asks if you want to assign a password, always type **Y RETURN**.

The LynxOS operating system offers you the option of skipping passwords for new administrators. *Always opt for the password.* If you were to choose not to assign a password, the new administrator would gain access to the server simply by typing her login. Since login names are often semi-public information, this would seriously compromise the security of your system.

4 Enter a password.

When you enter the new password, the server asks you to confirm it by re-entering it.

5 Re-enter the new password.

If you type it correctly, MMCX makes the change. Otherwise, the server asks you to try again.

6 If you typed the new password incorrectly in the preceding step, *carefully* retype it.

Be careful. This time the LynxOS operating system accepts whatever you type as the new password. If you make another mistake, the password may not be what you think it is.

7 Log out, and log back in as the new administrator. Test her password to make sure you typed it correctly.

8 If the new password fails, log back in as **sysadm**, remove the new account, and start over with step 1. See *Removing an administrator account*.

Removing an administrator account

You can also remove logins. This might be appropriate when an employee leaves your group or no longer has administrative responsibility for the server. If a password were compromised by a hacker, you might want to delete the entire login and start over. In these cases, proceed as follows.

1. Log in to the server as **sysadm**.
2. Type **rmsa login=*expired_login* RETURN**.

   The server asks you to confirm the deletion.
3. Type **Y RETURN** to delete the account, **N RETURN** to abort.

Multiple logins

Several system administrators can use the command line at the same time. But they have to coordinate their activities. MMCX commands execute sequentially. So each administrator can unintentionally countermand or contradict the instructions of the others.

Maintaining MMCX user accounts

Every user of MMCX client software has to have an account on the server. This section covers adding user accounts (client logins) and making changes to existing accounts.

Displaying MMCX users

To display account information for all MMCX users on this server, type **showusr RETURN.**

The server displays something like *Figure 22*.

```
LOGIN    STATUS          EXT     NAME
aegean   loggedOut(2)    4101    Aegean01, 01Harold
avery    loggedOut(2)    4102    Avery01, 01Averill
blatz    loggedOut(2)    4103    Blatz01, 01Earl
carlson  loggedOut(2)    4104    Carlson01, 01Carl
lsd      loggedOut(2)    4125    Davos01, 01Larry
```

Figure 22. Output of the showusr command

Adding MMCX users

To add a new user and extension to the MMCX server, proceed as follows.

1. Add the new user to the dial plan table. See *Adding information to the dial plan table*.
2. Give the user a user login on the server. Type **addusr login=*user_login* last=*last_name* ext=*new_extension* pass=*password* [first=*first_name*] [cvr=*covering_number*]**

   Enter a temporary password for the user, and have her change it when she logs in for the first time.

   The optional parameter ***covering_number*** tells the server where to route a call when ***new_extension*** is unavailable (users can configure this for themselves; see *Enabling the call coverage feature*).

Changing user passwords

The administrator, through the command can change the password for a given user at any time.

1. Login as sysadm
2. Type **chgpasswd login=*user_login_name* RETURN.**

   The server prompts you for the new password.
3. Type the new password.

   The server asks you to confirm the password by re-entering it.
4. Re-enter the new password.

   If you type it correctly, MMCX makes the change. Otherwise, the operation fails and the server returns you to the command prompt.

Moving users from one server to another

You can move MMCX users from one server to another without changing their extension numbers if the following conditions are met.

- The affected users continue to use the same international telephone numbers.
- If they connected with the public network via a PBX, they continue to connect via the same PBX (if the new server connects with a different PBX, users can keep their old extensions for internal calls but cannot receive incoming calls).

To move a user to a new server, you make changes to the dial plan. So, if necessary, refer to *Working with MMCX dial plan tables*. Then proceed as follows.

1. Remove the user from the old server. Type **rmusr login=*login_id* RETURN.**
2. On the old server, create a new **internal** entry in the dial plan table for the user. Type **adddp dial=*extension* srv=*new_server* dir=internal add=*digits_to_add***

3 On the new server, create a new **internal** entry in the dial plan table for the user. Type **adddp dial=*extension* dir=internal add=*digits_to_add***

4 Give the user a login on the new server. Type **addusr login=*user_login* last=*last_name* ext=*new_extension* [pass=*password*] [first=*first_name*] [cvr=*covering_number*]**

The optional parameter ***covering_number*** tells the server where to route a call when ***new_extension*** is unavailable. For more information, see *Enabling the calling directory feature*.

5 If the user connects to the public network via a PBX, configure the PBX dial plan so that it directs calls for the user's international telephone number to the new server, rather than the old one. Make any additional configuration changes specified in the documentation for your PBX.

User Licenses

Remember that you cannot add more users than the number of licenses you have purchased. If you get an error message that indicates this is the problem, you must purchase more licenses before proceeding.

Managing your MMCX telephone network

The MMCX server has some of the basic functions of a PBX (private branch exchange). It can route calls between your internal extensions and between internal extensions and the public telephone network. It also provides a basic call coverage capability. You set up these PBX-like functions by defining an *extension length*, *access codes*, and a *dial plan*.

Understanding MMCX call handling

This section explains the basics of call handling on MMCX servers. It defines the terms and concepts that underlie specific call-configuration procedures described in subsequent sections.

How MMCX identifies users

Each MMCX user has to have a valid international telephone number (a telephone number of the form ***n-nnn-nnn-nnnn***). The server uses this number to uniquely identify every user. You buy a block of these international numbers from your local telephone service provider. Then you assign them to your users and configure the dial plan table accordingly.

Types of MMCX calls

MMCX handles three types of calls. *Internal* calls connect MMCX users on the same MMCX server or network. *Incoming voice-interworking* calls connect a voice-grade telephone, FAX, or modem that is somewhere on the public switched telephone network and/or on a PBX with an MMCX user's workstation. *Outgoing voice-interworking* calls connect an MMCX user to an external telephone, FAX, or modem. Only internal calls can make use of MMCX multimedia calling features.

How MMCX processes dialed numbers

The MMCX server dial plan table translates between the international telephone number (the unique identifier for public network endpoints) and the digit string that callers actually dial in particular situations. For internal calls, MMCX expands the dialed digits into the corresponding international telephone number. For incoming voice-interworking calls, the server truncates the dialed digits to produce the extension of the called user. The server then uses the dial plan table to convert this extension to the unique, international telephone number for that extension (note that you do not convert the incoming digits directly into an international telephone number; you *always* convert the incoming digits to an extension first).

Displaying call-related system parameters

To see how call handling is configured on your server, type **showsys ENTER.**

```
   SERVER_NAME:      mmcs01
        SERVER_NUMBER:      13035384100
          DESCRIPTION:      Lucent MultiMedia Communications eXchange
(MMCX) Server
             LOCATION:      Planet Earth
              CONTACT:      Unknown
       SYSTEM_UP_TIME:      000:04:08:07
    EXTENSION_LENGTH:       4
SEC_BEFORE_COVERAGE:        10
    PSTN_ACCESS_CODE:       9
     PBX_ACCESS_CODE:       8
```

Figure 1. Displaying call-handling parameters

Setting or changing the extension length

MMCX lets you define the number of digits that you want to use for the extension numbers administered by your server. You *must* make all the extensions on a given MMCX server the same length, and you should make all the extensions on a given MMCX network the same length as well.

To define the number of digits in the extensions on your MMCX server, proceed as follows.

1. Remove all users. For each user, type **rmusr login=*user_login*** command.
2. Type **chgsys extlen=*n*** where ***n*** is a number between 3 and 7.
3. Add the users you removed. For each user, type

   addusr login=*user_login* last=*last_name* ext=*new_extension*
   [pass=*password*] [first=*first_name*] [cvr=*covering_number*]

   The optional parameter ***covering_number*** tells the server where to route a call when ***new_extension*** is unavailable. For more information, see *Enabling the calling directory feature*.

Defining PBX & PSTN access codes

The access code tells the MMCX server to apply the next string of dialed digits to the PBX or to the public switched telephone network (PSTN). To call a number on your PBX, you dial the code before dialing the extension number. To dial a number on the public network, you dial a different code before dialing the telephone number.

Optimizing PBX access codes

For internal calls, you can minimize the number of digits that your users have to dial by making the PBX access code the same as the leading digit of the extension. Since all PBX extensions start with the same digit, ***N*** (often **8**), you can use this digit as the PBX access code. You can then reach any

extension by dialing ***Nnnnn***. To dial an external call, you dial an arbitrary PSTN access code (9 is often used), followed by the telephone number.

Setting & changing access codes

The access codes can be 1- to 3-digit numbers or the asterisk character, ***,** followed by a single digit (*9, for example). To change your server's access codes for the PBX (**pbxac**) and public network (**pstnac**) for your server, proceed as follows.

Type **chgsys pbxac=*n_1* pstnac=*n_2* RETURN.**

Working with MMCX dial plan tables

This section explains how MMCX dial plan tables process dialed digits and route calls. Then it outlines the basic dial-plan configuration tasks that the administrator has to perform.

How dial plan tables work

The dial plan table (*Figure 2*) defines how the MMCX server interprets dialed digits and routes calls. It performs two tasks. First, it identifies a dial plan rule that applies to the kind of input it has received. Then it applies the rule and translates the dialed input into a corresponding extension or public network telephone number.

The server starts by categorizing calls according to their direction with respect to the MMCX network. Calls can be **internal** (between endpoints on the MMCX network), **in** (incoming to an MMCX endpoint from the public network or PBX), or **out** (outgoing to the public network or PBX from an MMCX endpoint).

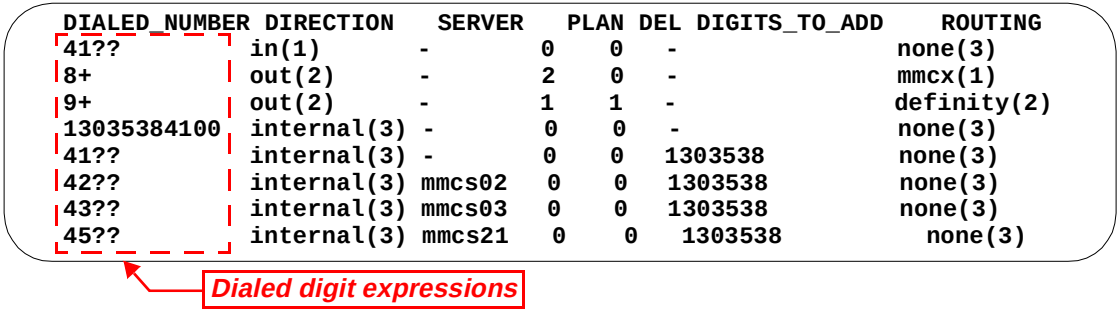


Figure 2. A simple dial plan table

When it receives dialed input from an MMCX user, the server first sees if the destination is also an MMCX user. It identifies all rows in the table that describe **internal** calls and searches these rows for the *dialed digit expression* that best describes the actual input. If it cannot find such an expression, it decides that the call is destined for an external, non-MMCX user. It evaluates the dialed digit expressions that describe calls of type **out**. When the dialed input comes from a public network trunk group rather than from an MMCX endpoint, the server evaluates the dialed digit expressions that describe calls of type **in**. If the server cannot find any dialed digit expression for the input, it notifies the caller that the call cannot be completed as dialed.

The server evaluates dialed digit expressions using the following criteria. A complete match is obviously the best. For example, if the server receives the digits 85006, **85006** is a better match than **8500?** or **8500+**. If the server cannot find a complete match, it selects the pattern that most closely matches the length of the string. So, if the server receives the digits 85006, **dial=8????** is a

better match than **dial=8+** or **dial=8500+**. If two rows satisfy both of the preceding requirements, the server selects the row that matches the greatest number of digits. So **dial=850+** is a better match for 85006 than **dial=85+**. Similarly, **dial=850??** is a better match than **dial=85???**.

Once it has found the best dialed digit expression for the input, the server generates an extension or external telephone number by adding or deleting digits from the input string. Its exact behavior is governed by the direction of the call and the *translation rules* specified in the remaining fields of the dial plan table. The MMCX server then passes the call and the appropriate number of dialed digits to the endpoint defined by the translated number.

Displaying the dial plan table

To view the dial plan table, type **showdp RETURN**.

Adding information to the dial plan table

To add basic dial plan information to the table, type the following.

adddp dial=*dialed_number_expression* dir=*direction* numdel=*num_to_delete*
add=*digits_to_add* [plan=*pri_routing_plan*] RETURN

- The **dial** and **dir** parameters are the conditions (the types of dialed input) to which the rule applies. The remaining parameters, **numdel** and **add**, tell what the server should do when the specified conditions are met.
- The ***dialed_number_expression*** is a sequence of 1 to 15 digits (including * and #) and, perhaps, wildcard characters (**?** or **+**) that define the pattern that will trigger the new dial-plan rule. The **+** wildcard character means any digit string. The **?** wildcard character means any

single digit. For example, if **dial=85001,** the new rule will apply to only one string of dialed digits, 85001. But if **dial=8500?**, the rule will apply to 85000, 85001... 85009. When **dial=8+**, 8 followed by any digit string satisfies the rule.

- The ***direction*** defines the type of call that triggers the new rule. It can have one of three values: **internal**, **in**, or **out**.
- The ***num_to_delete*** is the number of digits (1 to 15) that the server should discard from a string of dialed digits that matches the ***dialed_number_expression***. For example, if **dial=53850??, dir=in**, and **numdel=2**, then, starting with the first digit dialed, the server truncates the external telephone number 5385044 to get the internal extension 85044.
- The 1- to 15-digit string ***digits_to_add*** specifies the digits that the server should place at the start of any dialed input string that matches the ***dialed_number_expression***. For example, if **add=130353**, the server translates the dialed input 85044 to the international telephone number 1-303-538-5044.
- The ***pri_routing_plan*** value is a number in the range 1 to 32. It refers the server to a separate routing plan that administers the server's Primary Rate Interface (PRI) with the public switched telephone network. This parameter applies only to outbound calls. See *Removing a PRI trunk group* for more information.

Examples:

The following sample dial plan rules convert internal numbers for a hypothetical server.

adddp dial=850?? dir=internal add=130353

adddp dial=851?? dir=internal add=130353

adddp dial=740?? dir=internal add=1908957

These sample dial plan rules convert incoming numbers.

adddp dial=53850?? dir=in numdel=2

adddp dial=850?? dir=in

These rules convert outgoing numbers.

adddp dial=9??????? dir=out numdel=1 priplan=1

adddp dial=9+ dir=out numdel=1 priplan=2

adddp dial=911 dir=out priplan=1

adddp dial=9911 dir=out numdel=1 priplan=1

adddp dial=8+ dir=out add=53 priplan=3

Changing the dial plan table

To update or modify a dial plan entry, proceed as follows.

1. Remove each user affected by the change. For each user, type **rmusr login=*login_id* ENTER.**

   If you wanted to change the dialed digit expression **850+** to **850?? dir=internal**, for example, you would have to remove all users whose extensions started with 850**.**

2. Remove the entry. Type **rmdp dial=*dialed_digit_expression* dir=*direction* ENTER.**

   Dial plan entries are identified by their direction and dialed digit expression.

3. Add the new entry. Type **adddp dial=*dialed_number_expression* dir=*direction* numdel=*num_to_delete* add=*digits_to_add* [plan=*pri_routing_plan*] RETURN**

   See *Adding information to the dial plan table* for detailed instructions.

4. Add the users you removed. For each user, type **addusr login=*user_login* last=*last_name* ext=*new_extension* [pass=*password*] [first=*first_name*] [cvr=*covering_number*]**

The optional parameter ***covering_number*** tells the server where to route a call when the ***new_extension*** is unavailable. For more information, see *Enabling the calling directory feature*.

Enabling the call coverage feature

Individual users cannot configure call coverage for their workstations until you enable the coverage feature on the server. To enable call coverage, you tell the server how long it should ring an extension before diverting the call to the corresponding coverage point (the default is 0 seconds—no coverage).

Displaying the server-side call-coverage parameter

To view the current server-side call coverage parameter, proceed as follows.

1. Type **showsys ENTER.**
2. In the on-screen display, look for the value labeled **SEC_BEFORE_COVERAGE**.

Changing the server-side call-coverage parameter

To set the server-side coverage parameter to ***n*** seconds (where ***n*** is a number from 1 to 99), type **chgsys befcvr=*n* ENTER.**

Enabling the calling directory feature

The MMCX client software includes a directory feature that lets users record commonly called numbers. The client software builds its calling directory from an initial listing of all MMCX users. You have to build this default calling directory on the server. To create the directory file and enable the calling directory feature, proceed as follows.

1 To create a directory of all users, type **mkpersdir file=userdir.txt RETURN.**

   This command creates a file that contains each MMCX user's name and extension. The output file has to be named **userdir.txt**.

2 Copy mmcx.dir from the server to the directory where the MMCX client software is installed. See *Installing MMCX client software, page 62* for details.

Connecting MMCX to other telephone networks

MMCX uses a circuit-switched telephone network—either the public switched telephone network (PSTN) or a PBX—for all calls. It connects with the PBX or PSTN using an ISDN Primary Rate Interface. One or more onboard PRI cards link the server to the ISDN interface (for detailed discussion, see *PRIADM, page 521*).

Provisioning requirements for data and voice service

When you order ISDN PRI service from the public network or your PBX, be sure that it provides both data and voice service. In the U.S., Canada, and Japan, you must use the T1 bit-rate option if you are connecting to the public network over public facilities. In most other countries, you have to use the E1 bit rate over public facilities. If you directly connect to another server or PBX, you can use either option as long as both ends of the span are the same.

Understanding line coding

Line coding is the data format that lets either end of a communications channel correctly interpret messages from the other. Line coding systems specify the voltage levels and patterns that represent binary digits (1s and 0s). These specifications are based on the requirements of the transmission network. The AT&T network has two major requirements. It demands that the net voltage on the line equal 0 volts DC. It also requires a minimum *ones density.* Every stream of 15 consecutive bits must contain at least one binary 1, because long strings of uninterrupted 0s cause the network to lose *timing*—the receiving end in effect loses its place in the incoming bit stream.

All MMCX PRI trunks use Alternate Mark Inversion (AMI) coding. AMI represents the first 1 in a transmission as +3 volts, the second as -3 volts, the third as +3 volts, and so on. A zero is always represented as 0 volts. The reversed polarity of the 1s ensures that the net voltage is always 0. But it does not guarantee the correct ones density, so additional coding is generally required. The following, supplementary line-coding schemes are available.

- Alternate Mark Inversion with Zero Code Suppression (ZCS)

  ZCS line coding substitutes a 1 for the second least-significant bit of every all-zero byte in the AMI-encoded data. This has no effect on voice communications, but ***it corrupts digital data***. In MMCX communications, ZCS corrupts the ISDN D channel.

- Alternate Mark Inversion with Bipolar 8 Zero Substitution (B8ZS)

  B8ZS line coding substitutes a mix of 1s and 0s for every group of eight consecutive 0s in the AMI transmission stream. The encoded string contains consecutive ones with the same polarity. These intentional *bipolar violations* of the AMI coding scheme let the receiving end identify, decode, and restore the long zero strings in the original message. B8ZS line coding does not corrupt digital data.

  B8ZS is commonly used with T1 lines.

- Alternate Mark Inversion with High Density Bipolar 3-Bit Substitution (HDB3)

  HDB3 line coding is similar to B8ZS in some ways. It replaces every 4 consecutive zeros with either of two sequences. If there has been an even number of 1s since the last substitution, it substitutes the pattern **1 0 0 BipolarViolation**, where **BipolarViolation** is a 3-volt pulse (a **1**) of the same polarity as the preceding 3-volt pulse. If there has been an odd number of 1s since the last substitution, HDB3 coding substitutes the pattern **0 0 0 BipolarViolation** for the 4-zero string. This system does not corrupt binary data.

  HDB3 is commonly used with E1 lines.

Restricted and unrestricted facilities and data

A *restricted facility* is a T1 or E1 span, including the interface cards at each end, that performs zero code substitution (ZCS) at some point in the span. These facilities restrict the type of information that you can send, because they corrupt digital data.

An *unrestricted facility* is a T1 or E1 span that uses non-ZCS line coding (B8ZS or HDB3).

Unrestricted data is information that has to be sent over unrestricted facilities. Such data as to be protected from ZCS.

MMCX voice, video, and application data can travel over either type of facility, because the server takes care of the ones density requirement while preparing the data for transmission.

Configuring PRI cards

Lucent ships each server with a PRI card in slot i5. You can also choose to install additional PRI cards. The discussion below includes only the most commonly useful options. For a full discussion, see *PRIADM, page 521*.

Displaying PRI configuration information

To display the configuration of every PRI card in the server, type **showpri data=cfg RETURN.**

The output looks something like *Figure 3*.

```
 PRI CONFIGURATION
       =================
ST PT CRC    LCOMP              FRAME      LCODE    IDLE COMP     TIME
i5 1  off(1) length0to133ft(1)   ds1ESF(3)  b8zs(2)  255  muLaw(2)
incoming(129)
i5 2  off(1) length399to533ft(4) ds1ESF(3)  b8zs(2)  255  muLaw(2)
incoming(129)
ST PT INTF          CONN       PEER           VERS             SIDE
i5 1  user(1)       network(2) noPeerProto(1) a
noPeerProto(1)
i5 2  user(1)       pbx(3)     noPeerProto(1)
a               noPeerProto(1)
ST PT TERM             CNTRY              CIRCUIT-ID
i5 1  notApplicable(1) usa(1)             Denver1_Pub_Net
i5 2  notApplicable(1) usa(1)             Denver1_PBX
```

Figure 3. Viewing PRI configuration information

Changing PRI configuration information

To reconfigure an installed PRI card, type

chgpri slot=i*n* port=*port_num* lcomp=*line_length* lcode=*line_coding*
time=*clock_source* conn=*connection_type*

- ***n*** is the number of the ISA slot where the card is installed. It can be **5, 4, 3,** or **2**.
- ***port_num*** can be **1** or **2**. Each PRI card has two ports. Port 1 (labeled A on the card) and port 2 (labeled B). Connect the interface at slot i5, port 1 to the remote interface that is the best clock source. For example, if one PRI connects to a PBX and the other connects to a Lucent Technologies 5ESS central office, connect slot i5, port 1 to the 5ESS, the better of the two clock sources.
- ***line_length*** lets the server compensate for pulse distortions caused by the propagation characteristics of the cable that connects the MMCX server to the first channel service unit (CSU) on the PRI span. Set it to the value below that is closest to the *length* of your cable (the distortions are largely dependent on distance). If your cable is connected to another interface that also performs line compensation, choose the value that is closest to one half the length of the cable.

  length0to133ft (1) **length133to266ft(2)**

  length266to399ft(3) **length399to533ft(4)**

  length533to655ft(5)

  length0to133ft (1) is the default. T1 circuit packs adjust the outgoing signal so that it arrives at the far end without distortion. You do not need to adjust the **lcomp** parameter if you are using the E1 bit rate.

- ***line_coding*** can be **zcs(1)**, **b8zs(2)** (the default), **basic(3)**, or **hdb3(4)**, depending on the coding scheme used at the far-end of the T1 or E1 span (both sides must use the same scheme). Use **b8zs** on T1s that are **unrestricted**. Use **zcs** on T1s that are **restricted**. On E1 interfaces, use **hdb3** if possible. The **basic** option does not supply any 1s density protection.
- ***clock_source*** can be **incoming(3)**, **external(129)**, or **internal(130)**, depending on the location of the clock source for MMCX timing. If the PRI slot i5, port 1 connects to an external timing source such as a PBX or central office switch, set **time=incoming** (the default). Set all other interfaces to **external**. The first i5 interface then serves as the clock source for all the others. The **internal** setting is a fallback for cases where external timing is lost.
- ***connection_type*** is **network(2),** if the PRI connects to the public switched telephone network, or **pbx(3)**, with pbx(3) as the default.

Adding PRI cards

To configure a new PRI card, type the following.

chgpri slot=i*n* port=*port_num* lcomp=*line_length* lcode=*line_coding*
time=*clock_source* conn=*connection_type*

- ***n*** is the number of the ISA slot where the card is installed. It can be **5, 4, 3,** or **2**.
- ***port_num*** can be **1** or **2**. Each PRI card has two ports. Port 1 (labeled A on the card) and port 2 (labeled B). Connect the interface at slot i5, port 1 to the remote interface that is the best clock source. For example, if one PRI connects to a PBX and the other connects to a Lucent Technologies 5ESS central office, connect slot i5, port 1 to the 5ESS, the better of the two clock sources.

- ***line_length*** lets the server compensate for the length of the cable that connects the server to the channel service unit. Set it to the value below that is closest to the length of your cable. If your cable is connected to another interface that also performs line compensation, choose the value that is closest to one half the length of the cable. **(1)** is the default.

  length0to133ft (1) **length133to266ft(2)**

  length266to399ft(3) **length399to533ft(4)**

  length533to655ft(5)

  You need to adjust the **lcomp** parameter if you are using the T1 bit rate, but not if you are using E1.
- ***line_coding*** can be **zcs(1)**, **b8zs(2)** (the default), **basic(3)**, or **hdb3(4)**, depending on the coding scheme used at the far-end of the T1 or E1 span (both sides must use the same scheme). Use **b8zs** on T1s that are **unrestricted**. Use **zcs** on T1s that are **restricted**. On E1 interfaces, use **hdb3** if possible. The **basic** option does not supply any 1s density protection.
- ***clock_source*** can be **incoming(3)**, **external(129)**, or **internal(130)**, depending on the location of the clock source for MMCX timing. If the PRI slot i5, port 1 connects to an external timing source such as a PBX or central office switch, set **time=incoming** (the default). Set all other interfaces to **external**. The first i5 interface then serves as the clock source for all the others. The **internal** setting is a fallback for cases where external timing is lost.
- ***connection_type*** is **network(2),** if the PRI connects to the public switched telephone network, or **pbx(3)**, with pbx(3) as the default.

Removing a PRI card

To remove a PRI routing plan, type **rmpri slot=i*slot_num* port=*port_num* RETURN**.

Working with PRI trunk groups

Each PRI B channel on the MMCX server is a *trunk*. The B channels on one or more PRI interfaces constitute a *trunk group*. All B channels in this trunk group terminate at the same public switch, PBX, or MMCX server. Trunk groups let you apportion the server's total PRI bandwidth among the various functions that the server has to perform. For instance, you might assign one trunk group to voice-interworking calls that connect via the public telephone network and another to interserver routing.

Displaying PRI trunk group information

To display the current trunk group configuration for the server, type **showptg data=cfg RETURN.**

The console output looks something like *Figure 4*.

```
PRI TRUNK GROUP CONFIGURATION
=============================
TG AUD VID APP NFAS INTERFACE_ LIST
1 40 20 20 off i5: 1, i5: 2, -, -, -, -, -, -
2 0 0 0 i2: 1, i2: 2, i3: 1, i3: 2, -, -, -, -
3 100 0 0 i4: 1, -, -, -, -, -, -, -
PRI TRUNK GROUP COUNTS
======================
TG CUR_OUT_AUD CUR_OUT_VID CUR_OUT_APP CUR_IN_AUDCUR_IN_OTH BCHAN
1  0           0           0           0          0          0
2  1           2           3           4          5          6
3  0           0           0           0          0          0
TG MAX_OUT_ AUD MAX_OUT_VID MAX_OUT_APP MAX_IN_AUD MAX_IN_OTH
1  0           0           0           0          0          0
2  1           2           3           4          5          6
3  0           0           0           0          0          0
TG TOT_OUT_AUD TOT_OUT_VID TOT_OUT_APP TOT_IN_AUDTOT_IN_OTH
1  0           0           0           0          0          0
2  1           2           3           4          5          6
3  0           0           0           0          0          0
```

Figure 4. Viewing trunk group information

Adding a PRI trunk group

To add a PRI trunk group, type the following.

addptg tg=*trunk_group_num* intf=*intf_list* aud=*percent_audio*
vid=*percent_video* app=*percent_applications* RETURN.

- ***trunk_group_num*** is a trunk group number in the range 1 to 8.

- ***intf_list*** is a comma-delimited list of 1 to 8 interface/port combinations, each of the form **i*n*$_x$:*port*$_x$**. The full list takes the form **i*n*$_1$:*port*$_1$,i*n*$_2$:*port*$_2$, ... i*n*$_8$:*port*$_8$**.

  ***n*$_x$** is an ISA slot number in the range 2 to 5

  ***port*$_x$** is a port number, either 1 or 2.
- ***percent_audio*** is the percentage of the available bandwidth that the server should reserve for audio communications.
- ***percent_video*** is the percentage of the available bandwidth that the server should for video conferencing.
- ***percent_applications*** is the percentage of the available bandwidth that the server should reserve for shared and distributed applications and for MMCX signalling.

  Always reserve at least one B channel for MMCX interserver signalling.

When the values assigned to the **aud**, **vid**, and **app** parameters add up to less than 100, MMCX meets any unmet demands for bandwidth with the remaining, unreserved capacity. Make sure that the percentages you assign here are consistent the server's per-call bandwidth allocations. See *Allocating bandwidth per call*.

Changing a PRI trunk group

To change a PRI trunk group, type the following.

chgptg tg=*trunk_group_num* intf=*intf_list* aud=*percent_audio*
vid=*percent_video* app=*percent_applications* RETURN.

- ***trunk_group_num*** is a trunk group number in the range 1 to 8.
- ***intf_list*** is a comma-delimited list of 1 to 8 interface/port combinations, each of the form **i*n*$_x$:*port*$_x$**. The full list takes the form **i*n*$_1$:*port*$_1$,i*n*$_2$:*port*$_2$, ... i*n*$_8$:*port*$_8$**.

n_x is an ISA slot number in the range 2 to 5

$port_x$ is a port number, either 1 or 2.

- ***percent_audio*** is the percentage of the available bandwidth that the server should reserve for audio communications.
- ***percent_video*** is the percentage of the available bandwidth that the server should for video conferencing.
- ***percent_applications*** is the percentage of the available bandwidth that the server should reserve for shared and distributed applications and for MMCX signalling.

  Always reserve at least one B channel for MMCX interserver signalling.

When the values assigned to the **aud**, **vid**, and **app** parameters add up to less than 100, MMCX meets any unmet demands for bandwidth with the remaining, unreserved capacity. Make sure that the percentages you assign here are consistent the server's per-call bandwidth allocations. See *Allocating bandwidth per call*.

Removing a PRI trunk group

To remove a PRI routing plan, type **rmptg tg=*trunk_group_num* RETURN**.

Working with PRI routing plans

PRI routing plans direct outgoing voice-interworking and interserver calls to the correct trunk groups. The server sends each call to the trunk group specified in the PRI routing plan listed by the dial plan table and interserver routing table (see *Working with MMCX dial plan tables* and *Changing interserver routing numbers*). If the PRI routing plan specifies more than one trunk group, the server sends the call to the first available trunk group in the list. This arrangement lets you allow for trunk groups that are busy, out of service, or out of bandwidth.

Displaying PRI routing plans

To display the current PRI routing plan, type **showprp data=cfg RETURN**.

The console output should look something like *Figure 5*.

```
        PRI ROUTING PLAN CONFIGURATION
        ==============================
PLAN TRUNK_GROUPS
1     2,1
2    1,2
```

Figure 5. A PRI routing plan

Adding a PRI routing plan

To add a PRI routing plan, type **addprp plan=*plan_num* tg=*trunk_group_list* RETURN**.

- ***plan_num*** is an identifying number in the range 1 to 32.
- ***trunk_group_list*** is a comma-delimited list of trunk group numbers, each of which is in the range 1 to 8. The list has the form $n_1,n_2, \ldots n_8$.

  The server assigns calls to trunk groups in the order determined by ***trunk_group_list***.

Changing a PRI routing plan

To change a PRI routing plan, type **chgprp plan=*plan_num* tg=*trunk_group_list* RETURN**.

- ***plan_num*** is an identifying number in the range 1 to 32.

- ***trunk_group_list*** is a comma-delimited list of trunk group numbers, each of which is in the range 1 to 8. The list has the form n_1,n_2, ... n_8.

  The server assigns calls to trunk groups in the order determined by ***trunk_group_list***.

Removing a PRI routing plan

To remove a PRI routing plan, type **rmprp plan=*plan_num* RETURN**.

Assigning interserver routing numbers

The interserver routing number is the international telephone number that uniquely identifies your MMCX server. When an MMCX user dials the extension of a user on another server in the same MMCX network, the originating server sets up a PPP connection between the two servers by dialing the interserver routing number of the remote server. Each server must have at least one interserver routing number (servers can have more: for example, server A might have one number for communications with server B and another for communications with server C. For more information, see *CFGADM, page 458*.

Delivered digits

Although the interserver routing telephone number is an international number (country code plus national number), you usually assign only the *delivered digits* that remote servers need to dial when trying reach your server.

Displaying interserver routing numbers

To display the interserver routing number for your server, type **showisrnum RETURN.**

The output looks something like *Figure 6*.

```
ISR_PHONE_NUMBER
5385000
85000
```

Figure 6. Viewing routing numbers

Choosing an interserver routing telephone number

The best and easiest way to choose an interserver routing telephone number is to make it exactly the same as the server number. This assumes you set the server number to an international telephone number, as described in *Assigning a server number, page 58*. Trunk groups that receive interserver routing telephone calls must be ISDN PRI end-to-end between any two servers in the MMCX network. If you do not follow this rule, internal MMCX calls will not work. For example, if the server connects to a PBX, the trunk group to the PBX must be PRI and the trunk groups from the PBX to the remote server must be PRI.

Adding interserver routing numbers

To add an interserver routing number, type **addisrnum phone=*delivered_digits* RETURN.**

- ***delivered_digits*** is a list of the digits the server expects to see for calls to the interserver routing telephone number.

  If you have multiple trunk groups delivering different digits, you must configure each pattern. When a call comes in to the server, it checks the incoming digits. If these digits exactly match one of the configured **phone** numbers, the server sends the call to the interserver communications software. It sends all other calls to the dial plan software.

Changing interserver routing numbers

To add an interserver routing number, type **addisrnum phone=*delivered_digits* RETURN.**

- ***delivered_digits*** is a list of the digits the server expects to see for calls to the interserver routing telephone number.

  If you have multiple trunk groups delivering different digits, you must configure each pattern. When a call comes in to the server, it checks the incoming digits. If these digits exactly match one of the configured **phone** numbers, the server sends the call to the interserver communications software. It sends all other calls to the dial plan software.

Removing interserver routing numbers

To remove an interserver routing number, type **rmisrnum phone=*delivered_digits* RETURN.**

- ***delivered_digits*** is a list of the digits the server expects to see for calls to the interserver routing telephone number.

Setting up the interserver routing table

If you have an MMCX network composed of interconnected MMCX servers, you must configure the interserver routing table. This table lets the different servers and users on the MMCX network communicate with each other. See *ISRADM, page 490*.

How interserver routing works

If user A on server 1 makes an internal call to user B on server 2, call routing might work as follows.

1. A dials B's extension.
2. Server 1 consults its dial plan table and finds that B is on server 2.

3 Server 1 consults its interserver routing table and locates the server number for server 2, the IP address for the NIC on server 2, and the interserver routing number, the digits it must dial to set up a WAN connection with server 2.

4 Server 1 puts the digits of the interserver routing number into an ISDN message and sends the message out over the trunk group designated in the applicable PRI routing plan.

5 Server 2 receives the delivered digits and recognizes its interserver routing telephone number. It answers the call.

6 Server 1 and server 2 set up a PPP connection using one or more of the available B channels, depending on the bandwidth allocated to video and data.

7 Video travels over the PPP interface. Audio uses a separate B channel. The shared and distributed applications travel over the LAN that links server 1 and server 2. MMCX control signalling travels over the LAN.

Displaying the interserver routing table

To display the interserver routing table for a given server, type **showisr RETURN.**

The output looks something like *Figure 7*.

```
SERVER   SRVNUM          AUD VID APP SIG
Denver2  13038385100     wan wan lan lan
NJ1      19089574000     wan wan wan wan

SERVER   IP_ADDRESSES
Denver2  135.9.155.62, -, -,
NJ1      135.8.144.12, -, -,, -, -, -

SERVER   NEAR_PPP_ADDR   FAR_PPP_ADDR    ISR_PHONE_NUM   PLAN
Denver2  222.111.111.1     222.111.111.2   5385100          3
NJ1      222.111.111.3     222.111.111.4   9574000          3
-              -               0
```

Figure 7. Viewing the interserver routing table

Adding an entry to the interserver routing table

To add an entry to the interserver routing table, type

addisr name=*server_name* srvnum=*server_ID_num* ip=*server_IP_address*
nearppp=*nearPPP_IP_address* farppp=*farPPP_IP_address*
isrnum=*interserver_routing_num* plan=*PRI_routing_plan*
audio=*audio_route* video=*video_route* app=*application_route*
signal=*signalling_route*

- ***server_name*** is an 8-character alphanumeric string that identifies the server. You can display the server name by running **showsys** on the server you want to add.

- ***server_ID_num*** is a 1- to 15-digit server identification number. You can display the server number by running **showsys** on the server you want to add.
- ***server_IP_address*** is the IP address of the NIC (Ethernet or ATM card) in the remote server. If more than one NIC is present, you can list some or all IP addresses with a comma-separated list: **ip=135.8.144.12, 135.8.144.13.** Multiple IP address listing increase performance. You can display the IP addresses by running **showenet** and **showatm** on the server you want to add**.** You can omit the server IP address if you do not have a LAN connection to the remote server.
- ***nearPPP_IP_address*** is an IP address that you assign for the local server's PPP interface with the server you want to add. You can assign any IP address that is not already in use on your network.

  Pass a value for this parameter if you have a WAN (PRI-trunk) connection with the remote server. If your server communicates by LAN-only, do not supply a value for this parameter. To display the current PPP addresses, run **showisr** on the server you want to add.
- ***farPPP_IP_address*** is an IP address that you assign for the local server's PPP interface with the server you want to add. You can assign any IP address that is not already in use on your network.

  Pass a value for this parameter if you have a WAN (PRI-trunk) connection with the remote server. If your server communicates by LAN-only, do not supply a value for this parameter. To display the current PPP addresses, run **showisr** on the server you want to add.
- ***interserver_routing_num*** is the 1- to 15-digit dialed number that accesses the interserver routing telephone number for the server you want to add.

This parameter applies to interserver connections over the WAN. The dial plan does not process the digits entered here. The server puts these digits directly into the ISDN called-party number. The public network or PBX has to convert these digits into the digit string that the remote server expects.

- ***PRI_routing_plan*** is a 1- to 32-digit number that identifies the PRI routing plan that governs interserver calls to the server you wish to add.
- ***audio_route*** is either **lan** or **wan**. **lan** sends audio streams to the LAN whenever possible. **wan** sends audio over the WAN.
- ***video_route*** is either **lan** or **wan**. **lan** sends video streams to the LAN whenever possible. **wan** sends video over the WAN.
- ***application_route*** is either **lan** or **wan**. **lan** sends shared and distributed application streams to the LAN whenever possible. **wan** sends them over the WAN.
- ***signalling_route*** is either **lan** or **wan**. **lan** routes signalling over the LAN whenever possible. **wan** sends it over the WAN.

Configuring the Multimedia Applications Server Interface

The Multimedia Applications Server Interface (MASI) is an optional extension of MMCX that lets your MMCX network use your DEFINITY Enterprise Communications Server for call processing. DEFINITY switches offer sophisticated call coverage, tracking, and routing optimization features, as well as support for AUDIX and INTUITY voice messaging. Your DEFINITY system administrator handles most of the administration for MASI. But there are a couple of things you need to do on the MMCX side.

Enabling MASI on the MMCX server

Before your users can take advantage of DEFINITY ECS capabilities, you have to update your server configuration and enable the MASI feature. Proceed as follows.

1. Contact your DEFINITY system administrator, and ask him to be sure that MASI is enabled on the DEFINITY **System Parameters Options Form**.
2. Enable MASI by typing the following.

   chgmasi state=enabled [arsfac=*ars-access-code*] [nearpath=*near-path-number*] [farpath=*far-path-number*] [tscnum=*tsc-phone-number*] [slot=*tsc-slot* , port=*tsc-port*] [plan=*pri-routing-plan*] ENTER

   - ***ars-access-code*** is the ARS facility access code (FAC) that lets MMCX users access the DEFINITY Automatic Route Selection feature. It looks much like a dial-plan access code: three digits, of which the first may be replaced by an asterisk (*****). **9** is commonly used.
   - ***near-path-number*** is the *near-end* (local) number that DEFINITY dials for calls to your MMCX server. The MMCX server's MASI ***near-path-number*** is always the DEFINITY server's MASI ***far-path-number***.

- ***far-path-number*** is the *far-end* (remote) number that your MMCX server dials for calls to your DEFINITY ECS. The MMCX server's ***far-path-number*** is always the DEFINITY server's ***near-path-number***.
- ***tsc-phone-number*** is the near-end phone number that DEFINITY uses when setting up a Temporary Signaling Connection (TSC) to the MMCX. TSC signalling uses a portion of the D channel of an ISDN PRI.
- ***tsc-slot, tsc-port*** defines the slot and port location of the PRI that MMCX uses for the MASI (Temporary Signaling Connection).
- ***pri-routing-plan*** is the PRI routing plan number that MMCX uses when connecting the Temporary Signaling Connection.

3 Make an MMCX dial plan that conforms to the dial plan used on the DEFINITY side of the MASI link. At the MMCX command line prompt, type the following.

adddp dial=*access-code*+ dir=out
plan=*plan-num* numdel=*length(access-code)* rtgopt=definity

- ***access-code*** is a dial-plan access code. It is *not* the ARS feature access code. Even though they may appear to have the same value (often **9**), the codes have different meanings and must be processed differently (see **numdel** below).
- **dir=out** because, on the MMCX side, MASI routing only makes sense for outbound calls. DEFINITY routes the inbound calls, and MMCX routes the outbound calls only as far as the DEFINITY server (see the discussion of **rtgopt** below).
- **numdel** has to be set to ***length(access-code)*** **because** MASI passes the ARS facility access code (**arsfac**) value with the dialed input that it sends to DEFINITY. If you do not strip the dial-plan access code first, both codes get sent to DEFINITY ARS, and DEFINITY ARS fails to recognize the input.

- The **rtgopt=definity** parameter identifies this dial plan as a MASI plan. When this plan is in effect, MMCX defers *all* routing decisions to the DEFINITY server's ARS facility.
- For a more detailed explanation of dial plan administration, see *Working with MMCX dial plan tables* and *Defining PBX & PSTN access codes*.

4 Provision a PRI facility for the link between your MMCX server and the DEFINITY ECS.

To use MASI, your MMCX server has to be directly connected to the DEFINITY ECS. In *Figure 8*, only MMCX servers ***A*** and ***C*** could use MASI. B does not connect directly with the DEFINITY server.

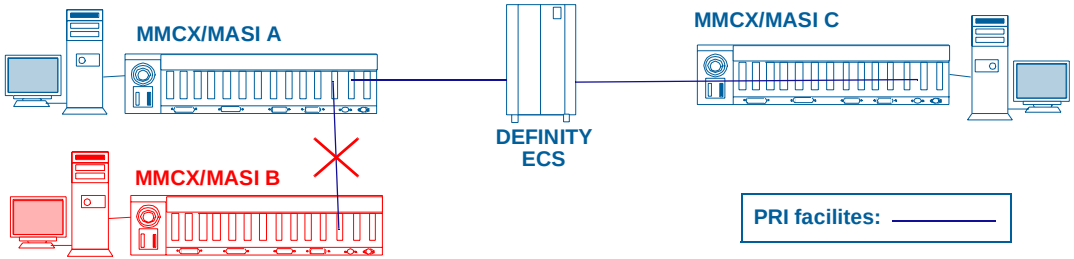


Figure 8. Possible and impossible MASI connections

5 Allocate a PRI interface for MASI. Type the following.

addpri slot=*slot-num* port=*port-num* time=*clock-source* RETURN

Review *Configuring PRI cards* if necessary.

6 Set up a PRI trunk group for MASI. Type the following.

addptg tg=*trunk-group-num* intf=*slot-num*:*port-num* aud=*percent-audio*
vid=*percent-video* app=*percent-applications* RETURN

Review *Working with PRI trunk groups* if necessary.

7 Set up a PRI routing plan for MASI. Type the following.

addprp plan=*plan-num* tg=*trunk-group-num* RETURN

Review *Working with PRI routing plans* if necessary.

8 Check to be sure no users are logged in. Type **who ENTER** to view currently logged-in users. To identify unfamiliar logins, type **showusr login=*login-id* ENTER**.

9 Restart the server so that the changes can take effect. Type **reset level=cold1 ENTER**.

The server resets, and the changes take effect.

Disabling MASI

Proceed as follows.

1 At the MMCX command line prompt, type the following.

chgmasi state=disabled [arsfac=*access-code*] [nearpath=*near-path-number*]
[farpath=*far-path-number*] [tscnum=*tsc-phone-number*]
[slot=*tsc-slot* , port=*tsc-port*] [plan=*pri-routing-plan*] ENTER

See *Enabling MASI on the MMCX server* for descriptions of the optional parameters.

2 Check to be sure no users are logged in. Type **who ENTER** to view currently logged-in users. To identify unfamiliar logins, type **showusr login=*login-id* ENTER**.

3 Restart the server so that the changes can take effect. Type **reset level=cold1 ENTER**.

The server resets, and the changes take effect.

Viewing the MASI configuration of the MMCX server

To see the current MASI configuration, type the follwing at the MMCX command line.

showmasi ENTER

Connecting with your local area network

MMCX is also a LAN server. To make MMCX operational, you have to configure MMCX to work with your Ethernet and/or Asynchronous Transfer Mode (ATM) network.

Configuring Ethernet network interface cards

Servers ship with the first network interface card (ATM or Ethernet) installed in slot p5. If you configured an Ethernet card for this slot during installation (see *Assigning an IP address and server name, page 47*), you do not need to configure it again. But if you wish to change this card's configuration or if you need to add other Ethernet cards to the server, use the procedures below.

Displaying the current Ethernet configuration

To display the Ethernet card configuration for a server, type **showenet data=cfg RETURN.**

```
ETHERNET CONFIGURATION
======================
SLOT   PORT   HARDWARE   IP_ADDRESS       NETMASK_VALUE    CAPACITY
P5     1      YES        135.9.155.73     255.255.255.0    10
```

Figure 9. Viewing the Ethernet configuration

You see something like *Figure 9*. The **HARDWARE** field shows that card is inserted.

Determining the correct MMCX traffic capacity

MMCX Ethernet card interfaces automatically work at the speed of your network, either 10 Mbps (10BaseT) or 100 Mbps (100BaseT). So you do not need to configure the interface speed. But you do have to set the traffic *capacity*, the maximum speed of MMCX data crossing the interface. Capacity has to be less than the rated speed of the interface. Otherwise, packet collisions slow the network's overall data-transfer rate to an unacceptable degree (if you need more throughput, add an Ethernet card. *Do not* increase the capacity parameter to its maximum).

You set the capacity of each Ethernet interface using the **cap** parameter of the **chgenet** and **addenet** commands.

Note that the default capacity, 10 Mbps, is too fast for a 10BaseT network (it would suffer too many packet collisions). A capacity of 7 would be better.

Reconfiguring an existing Ethernet card

To change the configuration of an Ethernet card, type

chgenet slot=p*n* port=*port_number* ip=*ip_address*
mask=*ip_subnet_mask* cap=*capacity* RETURN.

- ***n*** is identifying number for the card's PCI slot (in the order **5**, **1**, **3**, **6**).

  Note that slot p3 is usually not available, because it is occupied by a VGA video card on most systems.
- ***port_number*** is **1** (for cards with only one interface) or the data port for the interface you wish to configure (if the card carries more than one interface).

- ***ip_subnet_mask*** can range from **0.0.0.0** to **255.255.255.255**.
- ***capacity*** can range from **0** to **100**.

Adding Ethernet cards

Proceed as follows.

1. If it has not already been done, insert the Ethernet card using the procedure described in *Installing the Ethernet card, page 369*.
2. Type **addenet slot=p*n* port=*port_number* ip=*ip_address* mask=*ip_subnet_mask* cap=*capacity* RETURN.**
   - ***n*** is identifying number for the card's PCI slot (in the order **5**, **1**, **3**, **6**).

     Slot p3 is usually not available, because it is occupied by a VGA video card on most systems.
   - ***port_number*** is **1** (for cards with only one interface) or the data port for the interface you wish to configure (if the card carries more than one).
   - ***ip_subnet_mask*** must fall in the range **0.0.0.0** to **255.255.255.255**.
   - ***capacity*** can range from **0** to **100**.

Configuring ATM network interface cards

Your MMCX system is compatible with ATM networks if it meets all of the following conditions.

- The server is running LAN-emulation client (LEC) software that complies with the ATM Forum standard.
- All client workstations on the MMCX network run LAN emulation client software.

- The ATM network connects to a server running LAN-emulation server (LES) software.

The LAN-emulation client software lets MMCX supply the information that the LAN-emulation server uses to connect the MMCX server with MMCX client workstations.

Servers ship with the first network interface card (ATM or Ethernet) installed in slot p5. If you configured an ATM card for this slot during installation (see *Assigning an IP address and server name, page 47*), you do not need to configure it again. But if you wish to change this card's configuration or if you need to add other ATM cards to the server, use the procedures below.

Displaying the ATM configuration

To display the current configuration for all ATM cards in the server, type **showatm data=cfg RETURN.**

The server display looks something like *Figure 10*.

```
ATM CONFIGURATION
=================
SLOT PORT HARDWARE IP_ADDRESS      NETMASK_VALUE   CAPACITY
p5   1    yes(1)   135.9.155.73    255.255.255.0   155

LOC  CONFIG_MODE  LAN_TYPE       FRAME_SIZE     CTL CNT TIM
p5:1 manual(1)    aflane8023(2)  max1516(2)     120 1   1

LOC  VCC_IDLE   RTRY AGE FORW RESP FLSH CONN LAN_NAME
p5:1 1200       1    300 15   1    4    4    -
LOC  SERVER_ADDRESS p5:1 -
```

Figure 10. Viewing the ATM configuration

Reconfiguring an existing ATM card

To change the configuration of an ATM card, type

chgatm slot=p*n* port=*port_number* ip=*ip_address* mask=*ip_subnet_mask*
cap=155 mode=*operating_mode* name=*lan_emulation_name*
addr=*lecs_address* RETURN.

- ***n*** is identifying number for the PCI slot where the card is installed (install cards in the order **5**, **1**, **3**, **6**).

  Note that slot p3 is usually not available, because it is occupied by a VGA video card on most systems.
- ***port_number*** is **1** (for cards with only one interface) or the data port for the interface you wish to configure (if the card carries more than one).
- ***ip_subnet_mask*** must fall in the range **0.0.0.0** to **255.255.255.255**.
- ***capacity*** is any number greater than 0, but you should always use the default, 155 Mbps (Since ATM networks do not suffer packet collisions, they can run at maximum speed).
- ***operating_mode*** can be **automatic(1)** or **manual(2)**.

  Use **automatic** mode if your ATM network uses a LAN emulation configuration server (LECS). Use **manual** mode when your ATM network uses a LAN emulation server without a LECS.
- ***lecs_address*** is a hexadecimal number up to 40 digits long.

  The **addr** parameter passes the address of the LAN emulation server in **manual** mode. It passes the address of the LAN emulation configuration server (LECS) in **automatic** mode. You must supply this address if you are using **manual** mode. You can omit it in **automatic** mode, but, if you do, the MMCX server tries to contact the LECS at the *well-known address* specified in the ATM Forum standard.

- ***lan_emulation_name*** can be any unique, alphanumeric string up to 32 characters long. It is the LAN name that designates the MMCX network on the LAN emulation server.

Adding an ATM card

Proceed as follows.

1. If it has not already been done, insert the ATM card using the procedure described in *Installing the ATM card, page 373*.
2. Type **addatm slot=p*n* port=*port_number* ip=*ip_address* mask=*ip_subnet_mask* cap=155 mode=*operating_mode* name=*lan_emulation_name* addr=*lecs_address* RETURN**.
   - ***n*** is the identifying number for the PCI slot where the card is installed (cards can be inserted in the order **5**, **1**, **3**, **6**).
   - Slot p3 is usually not available, because it is occupied by a VGA video card on most systems.
   - ***port_number*** is **1** (for cards with only one interface) or the data port for the interface you wish to configure (if the card carries more than one).
   - ***ip_subnet_mask*** must fall in the range **0.0.0.0** to **255.255.255.255**.
   - ***capacity*** is any number greater than 0, but you should always use the default, 155 Mbps (ATM networks do not suffer packet collisions at maximum speed).
   - ***operating_mode*** can be **automatic(1)** or **manual(2)**.
   - Use **automatic** mode if your ATM network uses a LAN emulation configuration server (LECS). Use **manual** mode when your ATM network uses a LAN emulation server without a LECS.
   - ***lecs_address*** is a hexadecimal number up to 40 digits long.

- The **addr** parameter passes the address of the LAN emulation server in **manual** mode. It passes the address of the LAN emulation configuration server (LECS) in **automatic** mode. You must supply this address if you are using **manual** mode. You can omit it in **automatic** mode, but, if you do, the MMCX server tries to contact the LECS at the well-known address specified in the ATM Forum standard.
- ***lan_emulation_name*** can be any unique, alphanumeric string up to 32 characters long. It is the LAN name that designates the MMCX network on the LAN emulation server.

For the full range of available configuration parameters, see *ATMADM, page 437*.

Configuring the IP routing table

MMCX cannot communicate with IP addresses that are not on its own subnetwork unless you tell it how to route the network traffic. This is the function of the IP routing table (for additional details, see *IPADM, page 483*). The table lists an IP router address for each destination address. When the server gets a packet, it looks for the packet's IP address in the **DESTINATION** field of the IP routing table. If it finds the address, the server sends the packet to the router specified in the **NEXTHOP** field for that destination. If the IP address is not explicitly listed in the **DESTINATION** field, the server sends it to the router specified by the NEXTHOP field of the default destination. The default destination is indicated by a dash (**–**).

Displaying IP routing information

To display the IP routing data for the server, type **showip data=route RETURN**.

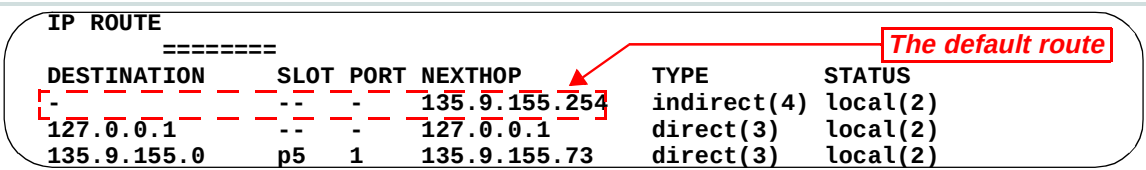


Figure 11. Viewing IP routing information

Changing IP routing information

To change the IP routing for a given destination, type the following.

chgip dest=*destination_address* nexthop=*router_address* RETURN

The routing information for the default destination has to match the information entered from the startup administration menu (see *Assigning an IP address and server name, page 47*). The ***destination_address*** for the default destination is always **0.0.0.0**

Adding IP routing information

To add IP routing for a given destination, type the following.

addip dest=*destination_address* nexthop=*router_address* RETURN

The default route is the only route you should need to add for the MMCX server.

Enabling H.323 endpoints

Starting with Release 2.0M, MMCX servers support H.323-compliant endpoints along with standard, MMCX clients. The MMCX server supports video and audio calls between H.323 endpoints, such as Microsoft® NetMeeting, and audio calls between an MMCX endpoint and an H.323 client or an H.323 client and a PBX extension or public-network telephone.

H.323 clients are handled much like MMCX clients. However, they may not have MMCX logins or passwords and may not be able to use H.323 registration and authentication. So MMCX identifies them by their MMCX extension numbers and IP addresses, logs them in automatically, and keeps them logged in. For this reason, H.323 clients are called *IP users*. The IP-user administrative tasks are otherwise similar to those for their MMCX counterparts.

Adding an IP user

To add a new IP user, type the following.

addipusr ext=*extension* ipaddr=*ip-address* last=*last-name*
[first=*first-name*] [cvr=*covering-number*] ENTER

Changing IP user information

If a user's extension, IP address, name, or coverage number changes, you can update her record. Type the following.

addipusr ext=*extension* [ipaddr=*ip-address*] [last=*last-name*]
[first=*first-name*] [cvr=*covering-number*] ENTER

Removing an IP user

To remove an IP user record, type the following.

rmipusr ext=*extension* ENTER

Displaying IP user records

To display IP user information, type the following.

showipusr [ext=*extension*] ENTER

Logging in an IP user manually

To log in an IP user, type the following.

loginipusr ext=*extension* ENTER

Forcing an IP user to log off

To force an IP user to log off, type the following.

termipusr ext=*extension* ENTER

Managing bandwidth

Video and multimedia communications require careful management, because they can rapidly consume limited network bandwidth and workstation CPU cycles. This section outlines the steps that you can take to maximize the efficiency of multimedia communications.

Maximizing efficiency with video multicasting

You can configure your MMCX server to *multicast* video streams for multimedia conference calls originated on your server. Multicasting saves bandwidth on the LAN and reduces workstation processor time. Normally, each party sends a separate video stream to each of the other 2 parties and receives a separate video stream from each party (*unicasting*). With multicasting, each party still receives two video streams but sends only one—a major saving.

For example, in *Figure 12*, each unicasting endpoint processes 4 video streams (2 incoming and 2 outgoing), for a total of 12 video streams on the LAN. With multicasting, this drops to 3 video streams (2 incoming and 1 outgoing) per endpoint or 9 for the LAN overall.

In general, if there are ***m*** parties on the MMCX multimedia conference call and if each video stream consumes ***n*** bandwidth in bits/second, then each unicast endpoint processes **2(*m*-1)** video streams and consumes **2(*m*-1)*n*** bits/sec of bandwidth. Each multicast endpoint processes only ***m*** video streams and consumes only ***mn*** bits/sec of bandwidth.

Limitations of multicasting

Multicasting does have limitations. Multicasting does not work across ISDN PRI connections. Multicasting can also cause video delays on ATM networks. Disable multicasting if this occurs.

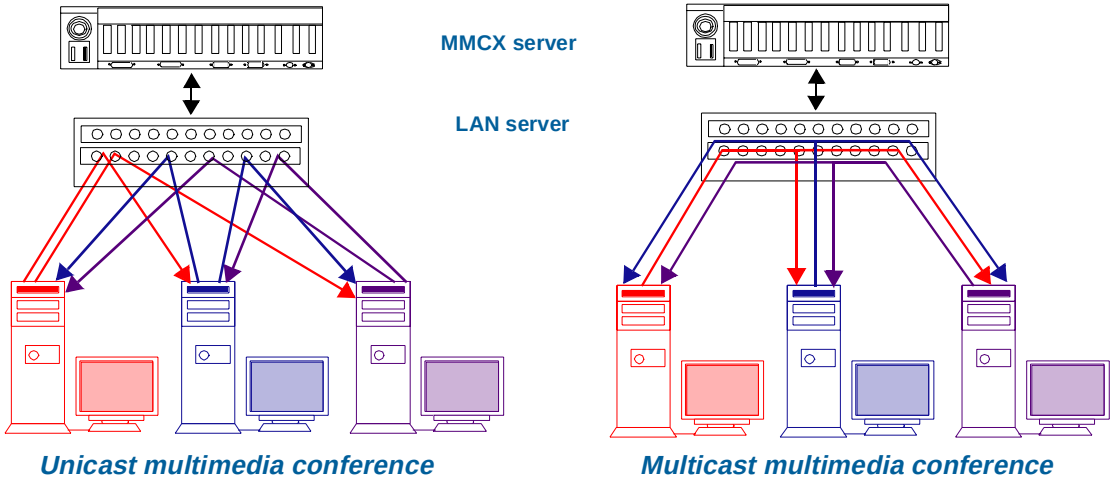


Figure 12. Unicasting vs multicasting

Configuring routers for multicasting

You must configure any routers that pass MMCX video streams for multicasting support.

Displaying multicasting configuration information

To display the current multicast configuration, type **showmcast RETURN.**

You should see something like *Figure 12*.

```
            BLOCK_NUMBER:    4
           BASE_UDP_PORT:    5000
           ROUTER_EXTENT:    0
             STATUS_FLAG:    enabled(1)
           FIRST_ADDRESS:    239.0.1.44
FIRST_UDP_PORT_IN_BLOCK:     5300
              BLOCK_SIZE:    100
           REQUEST_COUNT:    3
              FAIL_COUNT:    0
              FREE_COUNT:    0
           CURRENT_COUNT:    3

         MULTI-CAST ALLOCATION
         =====================
ALLOC_IP_ADDRESS ASSIGN_IP_ADDRESS UDP_PORT
239.0.1.44       135.9.144.88      5300
239.0.1.45       135.9.144.90      5301
239.0.1.46       135.9.144.85      5302
```

Figure 13. Multicasting parameters

- **ALLOC_IP_ADDRESS** is the multicast IP address that the server allocates.
- **ASSIGN_IP_ADDRESS** is the IP address.
- **UDP_PORT** is the UDP (User Datagram Protocol) port number for the call.

  The User Datagram Protocol is a TCP/IP protocol that routes messages from the network to applications running within the host computer. The UDP port serves as the logical address of the application that is receiving data from a TCP/IP network.

Changing the multicast configuration

To change multicast parameters, type

chgmcast blk=*num_address_blocks* udp=*udp_port_num*
route=*route_num* stat=*use_multicasting*

- ***num_address_blocks*** can be any number from 0 to 32. It is the number of IP addresses, in groups of 100 (a *block*), that the server should reserve for multicasting. The default, 0, disables multicasting.

  When the server determines that video should be multicast, it assigns the next available address in the current block. All multicast-capable workstations on the conference then listen on this address. The block number must be unique to each server on the MMCX network. *Multicast blocks must not duplicate any other IP addresses on your IP network or MMCX network.*

- ***udp_port_num*** can be any number in the range 5000 to 32000. The server reserves 3200 UDP (User Datagram Protocol) ports, 100 per block, starting at this number (if you choose 7000, MMCX reserves UDP ports 7000 to 7099 for block 1, 7100 to 7199 for block 2, **...** and 10100 through 10199 for block 32).

  When the server determines that video should be multicast, it assigns the next available UDP port in the current block. *Set the same value for all servers in the MMCX network. Do not use any UDP ports in this range for any other applications on your IP network.*

  The User Datagram Protocol is a TCP/IP protocol that routes messages from the network to applications running within the host computer. The UDP port serves as the logical address of the application that is receiving data from a TCP/IP network.

- ***route_num*** can be any number in the range 0 through 25 (0 is the default). This value is the number of routers through which multicast datagrams may pass.

- ***use_multicasting*** is either **enabled(1)** or **disabled(2)**. When you disable multicasting using the **stat** parameter, the server transmits and receives video using unicast addresses.

Allocating bandwidth per call

You can specify the amount of bandwidth allocated to each interserver video call, shared application, and distributed application. Bandwidth is always measured in kilobits per sec (Kbps). One audio call (one B-channel) takes up 64 Kbps. Each PRI interface supports 23 (T1) or 30 (E1) B-channels. Each server supports up to eight PRI interfaces, for a maximum possible bandwidth of 15,360 Kbps per server.

Determining the minimum bandwidth required

To allocate per-call bandwidth, you must first determine the minimum bandwidth required by your users. This requirement is determined by the way your organization uses MMCX. Video consumes more bandwidth than audio and data alone. Applications that transfer large volumes of data demand more bandwidth than those that are less communications intensive. So you have to apportion the available bandwidth according to specific use cases.

If, for example, your server has one PRI card, your total available bandwidth is 23x64 Kbps=1472 Kbps. Assume that your users typically make a minimum of one 3-party video call, with 128 Kbps of bandwidth for shared applications, and one concurrent, 3-party audio call, with 16 Kbps of bandwidth for distributed applications. For both kinds of calls, 2 users are on the originating server, and 1 user is on a remote server. You first have to allocate bandwidth for the bare-bones call:

- a B channel for the audio on the SHARE call and a B channel for audio on the distributed application call: 64 Kbps + 64 Kbps = 128 Kbps
- a B channel for signalling between the 2 servers: 64 Kbps

Then you assign bandwidth for the applications and data.

- bandwidth for applications on the SHARE call: 128 Kbps
- bandwidth for applications on the distributed applications call: 16 Kbps

For this scenario, you need 192 Kbps for audio and signalling plus 144 Kbps for shared and distributed applications. This adds up to 336 Kbps.

We can now determine the level of video service (and the amount of video bandwidth) that we can allot to video. After allowing for audio and signalling, you have 1136 Kbps left on your single PRI span (1472 Kbps - 336 Kbps). Since 2 of your 3 video conferees will always be on the local server, you need to allocate video bandwidth for 2 concurrent video streams going to the conferee on the remote server (the return video stream from the remote server can use the channels we reserve for the outbound video). MMCX servers can allocate 1, 2, or 3 B Channels per call for video. One 64-Kbps B Channel supports basic video on the endpoints: a *capture rate* of around 5 frames/sec with a *video quality* index of 5 (on a scale of 1 to 9). Three 64-Kbps B Channels support 5 frames/sec with quality set to 9, 10 frames/sec with quality set to 7, or 15 frames/sec with quality set to 5. This translates into the following bandwidth requirements.

- lower video quality: (64 Kbps/B Channel) x 1 channel/stream x 2 streams = 128 Kbps
- medium video quality: (64 Kbps/B Channel) x 2 channels/stream x 2 streams = 256 Kbps
- highest video quality: (64 Kbps/B Channel) x 3 channels/stream x 2 streams = 384 Kbps

In the example, the 1136 Kbps available after allowing for audio, signalling, and data is enough to support all three levels of video quality.

Displaying current per-call bandwidth allocations

To view the current bandwidth allocation, type **showbw**.

The console output of this command looks something like *Figure 14*.

```
BANDWIDTH IN KBPS
              VIDEO MAXIMUM:     2048
         SHARED APP INITIAL:     128
      SHARED APP SUBSEQUENT:     128
    DISTRIBUTED APP INITIAL:     128
DISTRIBUTED APP SUBSEQUENT:     128
```

Figure 14. Output of the showbw command

Changing per-call bandwidth allocations

To set the maximum bandwidth for video calls or the initial and subsequent bandwidth for shared and distributed applications, type the following.

chgbw data=***data_type*** **max**=***maximum_bandwidth***
[**init**=***initial_bandwidth***] [**sub**=***subsequent_bandwidth***]

- ***data_type*** is the scope of the change. You can apply the new bandwidth allocation to one of three call types: **video** (video conference call), **share** (shared application), or **dist** (distributed application).
- ***maximum_bandwidth*** is the maximum bandwidth that any one video call can consume. If **data <> video**, this parameter is ignored.

On T1 interfaces, ***maximum_bandwidth*** is a number between **0** and **12096** (the equivalent of 8 PRIs with 24 channels at 64 Kbps per channel minus one channel for the D channel, one channel for MMCX signalling, and one channel for audio).

- ***initial-bandwidth*** is the bandwidth allocated to shared or distributed applications on their first call to a remote server on the WAN. If **data = video**, this parameter is ignored.

  On T1 interfaces, ***initial_bandwidth*** is a number between **128** (equivalent to 1 B channel for MMCX signalling and1 B channel for audio) and **12096** (the equivalent of 8 PRIs with 24 channels at 64 Kbps per channel minus one channel for the D channel, one channel for MMCX signalling, and one channel for audio)**.**

- ***subsequent_bandwidth*** is the bandwidth allocated to shared or distributed applications for second and subsequent calls to the remote server. If **data = video**, this parameter is ignored.

  On T1 interfaces, ***subsequent_bandwidth*** is a number between **128** (equivalent to 1 B channel for MMCX signalling and1 B channel for audio) and **12096** (the equivalent of 8 PRIs with 24 channels at 64 Kbps per channel minus one channel for the D channel, one channel for MMCX signalling, and one channel for audio)**.**

6 Performance management

MMCX network performance is highly dependent on the server and endpoint configurations that you have chosen. If performance does not seem to be optimal, you have to monitor and, where possible, reconfigure server software and hardware. This chapter highlights performance-related configuration issues. But for a full discussion of the individual commands and procedures, you should refer to Chapter 6, *Configuration Management*.

Monitoring server performance

You check server performance using the **show-** commands listed in the table below.

Parameters to monitor	Commands
Server and application up-time	**showsys**
Use of multicasting	**showmcast data=count**
Performance of PRIs, including failed and successful call attempts, current active calls, and link status	**showpri data=stat** **showpri data=perf** **showprp data=count** **showwan data=stat**
Media usage on PRI trunk groups (number of active calls by type)	**showptg data=count**

Parameters to monitor	Commands
Media usage system-wide	**showcall**
Ethernet statistics, counts, and collisions	**showenet data=stat** **showenet data=coll** **showintf data=count** **showintf data=stat**
ATM statistics and counts	**showatm data=stat** **showatm data=count** **showatm data=vcc** **showintf data=count** **showintf data=stat**
PPP statistics and counts	**showintf data=count** **showintf data=stat**
Internet Protocol (IP) counts	**showip data=count**
Internet Control Message Protocol	**showicmp**
Simple Network Management Protocol (SNMP)	**showsnmp**
Transport Control Protocol (TCP) counts	**showtcp data=count**
User Datagram Protocol (UDP)	**showudp data=err**

Improving performance

The performance of the MMCX system varies depending on the exact configuration of your server and network. To optimize the server for your situation, try various combinations of the adjustments listed below, compare the results, and readjust until you arrive at the best combination of settings.

Things to try	Further information
At each user workstation, adjust the settings in the **Video Setup** window of the **Video Controls** window.	See the *MMCX User's Guide*.
Vary the percentage of the trunk-group bandwidth allotted to audio, video, shared data, and distributed applications.	See *Working with PRI trunk groups, page 94*.
Adjust the amount of bandwidth allotted to shared distributed applications on a single call.	See *Allocating bandwidth per call, page 124*.
Have the server send video to multicast addresses wherever possible.	See *Changing the multicast configuration, page 123*.
On MMCX networks with two servers connected by a LAN and ISDN PRI, try sending some media streams over the ISDN PRI instead of sending all media streams over the LAN.	See *Setting up the interserver routing table, page 101*.
Increase LAN capacity by installing more NIC cards on the IP subnetwork.	See *Connecting with your local area network, page 110*.

7 Server startup problems

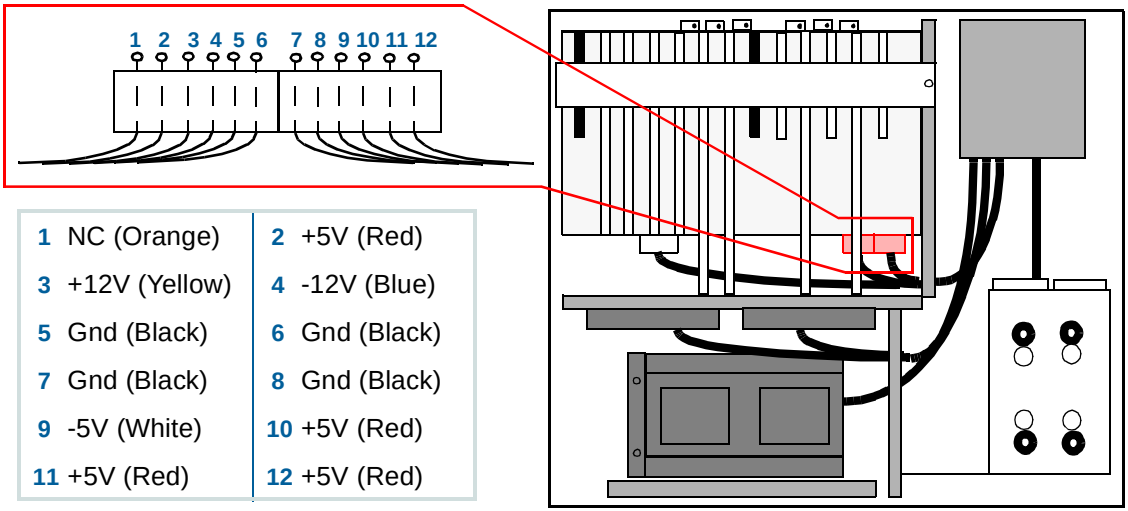
Sometimes the startup process stops before it is complete. The server is not yet in an **Active** state and the MMCX command line interface is not yet running. Identify the causes and correct the problem using the troubleshooting method described in this chapter. The method has four parts, each keyed to a specific phase in the starting sequence. Work through the parts in the order specified.

1. Check *Power-up phase, page 132* to identify problems that arise after the system powers up and before any output appears on the server console.
2. Procedures in *Self-test phase, page 134* isolate errors that occur after the system powers up and before the console displays the message **Lynx preboot Version**.
3. *Operating system startup phase, page 143* locates problems that happen after the console displays **Lynx preboot Version** and before it tells you to **Press any key to enter the software administration menu**.
4. *Application startup phase, page 149* isolates problems that happen after you are told to **Press any key to enter the software administration menu** but before the **Active** message appears.

Power-up phase

During this phase, the console display is not enabled. So you have to observe LEDs on the circuit cards and chassis for signs of trouble. Use the diagnostic chart below as a guide.

If	Then
1 The power LED is not ON.	A power cable is not connected correctly. Go to *Checking cables, page 394*.
2 The diskette drive LED does not come ON during the memory test.	A diskette-drive cable is not connected correctly. Go to *Checking cables, page 394*.
3 The 3 yellow LEDs are OFF on *all* PRIs.	Check the connections and measure the output voltages of the power supply input and output cables. Go to *Figure 1*, *Power supply voltage checks* for a list of the output values.
4 The 3 yellow LEDs are OFF on some PRIs.	A cable is loose or the board is not properly seated. Go to *Checking cables, page 394* and *PRI card maintenance, page 362* for instructions on handling these components.
5 The hard-drive LED is OFF.	Go to *Checking cables, page 394*.
6 All LEDs are on.	The startup sequence is progressing normally. Go to *Self-test phase*.



1	NC (Orange)	2	+5V (Red)
3	+12V (Yellow)	4	-12V (Blue)
5	Gnd (Black)	6	Gnd (Black)
7	Gnd (Black)	8	Gnd (Black)
9	-5V (White)	10	+5V (Red)
11	+5V (Red)	12	+5V (Red)

Figure 1. Power supply voltage checks

Self-test phase

CAUTION:
You *must attach a console* to the server before you go any farther. You cannot power down the server correctly without one and might lose setup information. See *Hooking up the console, page 34* if necessary.

Once the power-up phase is complete, you can monitor the progress of the startup on the console. During this part of the sequence, the system performs a series of self tests covering memory, the CPU, BIOS, the hard drive, and the diskette drive. See the following sections in the order specified.

1. *Interpreting console output, page 135*
2. *Checking diskette drive LEDs, page 137*
3. *Identifying CPU errors, page 138*
4. *Interpreting the hard drive test, page 139*
5. *Interpreting the diskette drive test, page 140*
6. *Handling RMB errors, page 142*

Interpreting console output

The first sign of a self-test failure is usually an abnormality in the console output. To isolate the problem, consult the troubleshooting chart below.

If	Then
1 You still do not see anything on your console several minutes after the power-up phase completed.	The console may not be connected correctly. See *Checking cables, page 394* and *Hooking up the console, page 34*.
2 You have checked the console cabling, but you still see nothing on the console.	Try to load the factory default values for the CPU BIOS into CMOS RAM. Go to *Restoring the BIOS configuration, page 406*.
3 You could not load the BIOS defaults or you reloaded the BIOS defaults but still see nothing on the console.	Replace the CPU. See *CPU card maintenance, page 356* for instructions.
4 Console output looks abnormal. The screen does not look like *Figure 2*.	Go to *Interpreting console output*.
5 Console output looks normal, like *Figure 2*.	This phase of the startup is progressing normally. Go to *Checking diskette drive LEDs*.

```
Lucent Technologies, Inc.
Copyright (C) 1985-1989 Phoenix Technologies Ltd.
Copyright (C) 1991 Texas Microsystems, Inc.
All Rights Reserved
The P5120C 120 MHz Industrial Computer BIOS, Version x.x.x.
640K Base, xxxxxx Extended, 256K External Cache
Adaptec AIC-7850 BIOS v1.11
(c) 1994 Adaptec, Inc. All Rights Reserved.
Press <Ctrl><A> for SCSISelect(TM) Utility!
SCSI ID # - T&T 1GB DPES 407340959  - Drive C: (80h)
BIOS Installed Successfully!

LynxOS preboot Version x.x.x
```

Figure 2. Console output of a normal self test

Checking diskette drive LEDs

If the console output looks like that in *Figure 3*, wait approximately 10 seconds, then check the floppy drive LED.

If	Then
1 The diskette drive LED is *not* lit.	Go to *Checking cables, page 394*.
2 The diskette drive LED is lit.	The startup sequence continues. Go to *Identifying CPU errors*.

```
Lucent Technologies, Inc.
Copyright (C) 1985-1989 Phoenix Technologies Ltd.
Copyright (C) 1991 Texas Microsystems, Inc.
All Rights Reserve
The P5120C 120 MHz Industrial Computer BIOS, Version x.x.x.
640K Base, XXXXXXK Extended, 256K External Cache
```

Figure 3. Console output when a diskette drive is faulty

Identifying CPU errors

Next, the startup process tests the CPU. Each test is identified by a number. If the CPU encounters a failure, testing stops, and the test number and an associated error message are sent to the console. Watch the console, and consult the chart below.

If	Then
1 A test failed, and testing stopped.	Look up the error code in Appendix B and proceed to *CPU card maintenance, page 356*.
2 Testing terminated normally with **BIOS Successfully Installed**.	The startup sequence continues. Go to *Interpreting the hard drive test*.

Interpreting the hard drive test

If the CPU passes all its self tests, the startup sequence checks the disk drives. Observe the console output, and consult the chart below.

If	Then
1 The error message in *Figure 4* appears and the hard drive LED *does not light* at all.	A hard disk cable may be loose or faulty. Go to *Checking cables, page 394*.
2 The error message in *Figure 4* reappears and the hard drive LED does not light *after* you have checked the cables.	The hard disk may be faulty. Go to *Hard disk drive maintenance, page 377* and *Recovering from a hard disk failure, page 416*.
3 The error message in *Figure 4* appears and the hard drive LED *is lit continuously*.	The BIOS is faulty. Go to *Restoring the BIOS configuration, page 406*.
4 No error message appears and the hard drive LED lights up normally.	Go to *Interpreting the diskette drive test*.

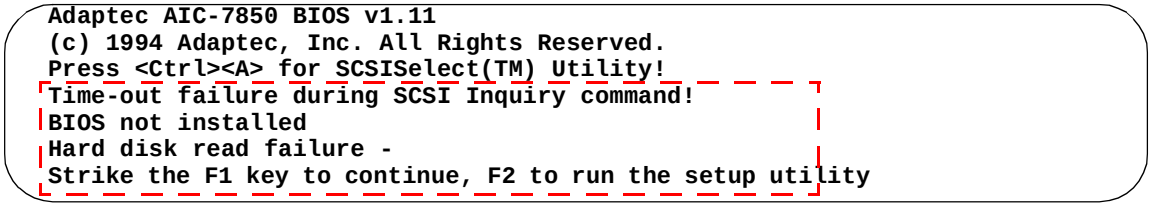


Figure 4. Console output during a hard-disk test failure

Interpreting the diskette drive test

Next the self-test process checks the diskette drive for configuration problems and read errors.

Diskette drive configuration errors

The diskette drive test begins by checking for configuration errors. Watch the console output, and consult the diagnostic chart below.

If	Then
1 You see the error message in *Figure 5*.	A cable may be loose or faulty. Go to *Powering down, page 403*.
2 The error message in *Figure 5* reappears after you have checked the cables.	The floppy disk drive may be faulty. Go to *Hard disk drive maintenance, page 377*.
3 No error message appears.	Go to *Diskette drive read errors*.

```
** Configuration Error: Floppy Drive(s) found do not match setup
** Configuration Error: Floppy Drive(s) found do not match setup
Adaptec AIC-7850 BIOS v1.11
(c) 1994 Adaptec, Inc. All Rights Reserved.
Press <Ctrl><A> for SCSISelect(TM) Utility!
SCSI ID # - T&T 1GB DPES 407340959  - Drive C: (80h)
BIOS Installed Successfully!
Strike the F1 key to continue, F2 to run the setup utility
```

Figure 5. Diskette drive configuration error

Diskette drive read errors

Next the system performs a disk-read test. Observe the console output and consult the diagnostic chart below.

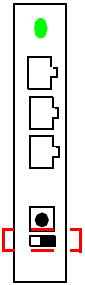
If	Then
1 You see the error message in *Figure 6*.	A cable may be loose or faulty. Go to *Checking cables, page 394*.
2 The error message in *Figure 6* reappears after you have checked the cables.	The diskette disk drive may be faulty. Go to *Diskette drive maintenance, page 381*.
3 No error message appears.	Go to *Handling RMB errors*.

```
Diskette drive A failure
Adaptec AIC-7850 BIOS v1.11
(c) 1994 Adaptec, Inc. All Rights Reserved.
Press <Ctrl><A> for SCSI Select(TM) Utility!
SCSI ID # - T&T 1GB DPES 407340959  - Drive C: (80h)
BIOS Installed Successfully!
Strike the F1 key to continue, F2 to run the setup utility
```

Figure 6. Diskette drive read error

Handling RMB errors

Startup now checks the remote maintenance board (RMB). Observe the console output, and consult the diagnostic chart below.

If	Then	RMB reset switch
1 The error message in *Figure 7* appears, *and startup stops*.	Press RESET on the remote maintenance board. Then press RESET on the front of the server.	
2 After a reset, the error message reappears *and startup stops again*.	Go to *Removing the remote maintenance board, page 387*.	
3 The server continues with the startup sequence.	Go to *Operating system startup phase*.	

```
KickStart 3
Version 1.16.4
Created 9-September-1994
RMB Problem
Adaptec AIC-7850 BIOS v1.11
(c) 1994 Adaptec, Inc. All Rights Reserved.
Press <Ctrl><A> for SCSISelect(TM) Utility!
SCSI ID # - T&T 1GB DPES 407340959  - Drive C: (80h)
BIOS Installed Successfully!
LynxOS preboot Version x.x.x
```

Figure 7. RMB error message

Operating system startup phase

This section covers problems that arise while the LynxOS operating system is loading. Loading begins when you see the message **LynxOS preboot Version** on the console. It ends with the message **Press any key to enter the software administration menu**. If errors occur at this point, the startup sequence stops. To isolate problems, see the following sections in the order specified.

- *Checking the hard drive LED, page 144*
- *Checking the PRI and ATM card tests, page 145*
- *Interpreting errors at the command prompt, page 146*
- *Isolating Ethernet card faults, page 148*

Checking the hard drive LED

When you first see the message **LynxOS preboot Version** check the hard drive LED and consult the diagnostic chart below.

If	Then
1 The hard drive LED is *not* lit.	Go to *Recovering from a hard disk failure, page 416*.
2 The hard drive LED *is* lit.	Observe the output on your console, and go to *Checking the PRI and ATM card tests*

Checking the PRI and ATM card tests

As it loads, the operating system looks for installed PRI and ATM cards. Observe the output on the console (a representative display is shown in *Figure 8*), and consult the chart below.

If	Then
1 The console reports numbers and types of cards other than those actually installed.	Go to *PRI card maintenance, page 362* and/or *ATM card maintenance, page 371*.
2 The console reports correct numbers and types of cards.	Go to *Interpreting errors at the command prompt*.

```
Loading..\loaded
Installing WILD cards...
Core tests PASSED for WILD card in slot P2
PRI Version 5.0 I/O 100..10f, Int 5, Mem cc000..cffff
PRI Version 5.0 I/O 110..11f, Int 7, Mem d4000..d7fff
pri2 not found at I/O address 120 (3 of 4)
pri3 not found at I/O address 140 (4 of 4)
IA 5515 /dev/ia0: bus 1, device 15, slot 4, interrupt 11
LynxOS 386/486/Pentium PC-AT Version x.x.x
Copyright 1987,1995 Lynx Real-Time Systems Inc.
All rights reserved.
```

Figure 8. Typical results of the PRI and ATM card check

Interpreting errors at the command prompt

To isolate faults that appear during the next part of the startup sequence, observe the console output and consult the chart below.

If	Then
1 Startup stops at the **Command?** prompt.	Press **B ENTER** to continue.
2 Startup again stops at the **Command?** prompt.	Press **RESET** on the front of the server.
3 Startup stops at the **Command?** prompt yet again.	Reinstall the software. Go to *Recovering from a hard disk failure, page 416*.

```
AHA 2940 Found! Bus 0 Dev1!
Waiting for boot device . . .
Loading . .\loaded
LynxOS 386/486/Pentium PC-AT Version x.x.x
Copyright 1987, 1995 Lynx Real-Time Systems, Inc.
All Rights Reserved.
LynxOS (lynxos) created Fri Nov 10 21:07:40 1995
LynxOS Startup: a
Date set to Fri Jan 8 14:40:28 MST 1993
mounting all filesystems
hostname is mmcs01
ifconfig: ioct1 (SIOCGIFFLAGS) : no such interface
ifconfig: ioct1 (SIOCGIFFLAGS) : no such interface
add not default: gateway cisco2: Network is unreachable
inetd started
```

Figure 9. Network interface card error

Isolating Ethernet card faults

Observe the console output, and consult the chart below.

If	Then
1 Set up stops. The prompt, **user name:** does not appear.	The CPU or Ethernet card may not be seated in the static board. Reseat them. Type **reset level=boot ENTER**.
2 The startup sequence stops at the same place after you reseat cards and reset the server.	Request technical support. Go to *Repair Number 0 - Escalate to MACS, page 162*.
3 The CPU and Ethernet cards are installed correctly, but startup again stops without displaying the **user name:** prompt.	The Ethernet card is faulty. Replace it using the procedure in *Ethernet card maintenance, page 367*.
4 Startup continues normally. The login prompt, **user name:**, appears.	Go to *Application startup phase*.

Application startup phase

This section describes the procedure for isolating faults that occur while the MMCX application is starting, after the server has powered up and the operating system has loaded. MMCX starts to load when the console displays the message, **Press any key within 10 seconds**. It ends when **Active IS** (in-service) or **OOS-FLT Active** (out-of-service due to a fault) appears on the console. If there is an error, the system stops before it reaches the **Active** state.

At this stage, faults are detected during a series of internal and external *looparound tests*. These tests make sure that the application can find the NIC, WILD and PRI cards installed on the server. *Internal* looparound tests log errors and generate alarms. External looparound tests do not.

If the system fails an internal looparound test, startup is incomplete, and the server logs an alarm or error.

Circuit card checks

When the MMCX application starts, it first locates and identifies all PRI, WILD, NIC, and ATM circuit cards installed on the system. See *Figure 10* for a typical example of the test output.

If	Then
1 The list of installed cards does not include all cards that are physically present.	Go to *Operating system startup phase*.
2 All physically installed cards are listed in the test output.	Go to *Looparound Tests*.

```
Grandma: Starting Mom...
user name:Booting MMCS SoftwareRelease1.0
New Run Level: BOOT
Installed WILD Cards found:
Slot: P2 Port: 1
Installed PRI Interfaces found:
Slot: I5 Port: 1 Type: DS1   Slot: I5 Port: 2 Type: DS1
Installed Ethernet Interfaces found:
Slot: P5 Port: 1
Installed ATM Interfaces found:
```

Figure 10. Typical output of the circuit-card location test

Looparound Tests

MMCX performs both *external* looparound tests that check the interface between the card and the network and *internal* looparound tests that check the internal circuitry of the cards. *Figure 11* shows what a typical display looks like. If one or more tests fail, consult the chart below.

If	Then
1 Both internal and external looparound tests fail.	Go to step 4, *The internal looparound test fails and startup stops.*
2 The external looparound test fails (see *Figure 12*). A looparound plug is not installed.	Install the loop plug. Go to *Installing the looparounds, page 341*.
3 All looparound plugs are installed, but the external test still fails (see *Figure 12*).	Replace the card that failed. Go to *Ethernet card maintenance, page 367* or *PRI card maintenance, page 362*.
4 The internal looparound test fails and startup stops.	**a** Get the repair number and error code for the failure. Type **showalarm data=hw-long ENTER.** **b** See *Viewing and interpreting alarm messages, page 156*. Perform indicated repair.
5 Both internal and external looparound tests end successfully.	Go to *Check processes*.

```
Hardware Test Results:
PASS  Internal Switch Fabric Test
  Wild       Slot: P2    Port: 1
  PRI        Slot: I5    Port: 1
PASS  External Switch Fabric Test
  Wild       Slot: P2    Port: 1
  PRI        Slot: I4    Port: 2
PASS  Ethernet Internal Looparound
  Ethernet   Slot: P5    Port: 1
PASS  Ethernet External Twisted Pair Looparound
  Ethernet   Slot: P5    Port: 1
Results of Analyzing Internal Switch Fabric Test
Nothing indicted in analysis
See Alarm Log for any alarms if any of the tests failed
Results of Analyzing External Switch Fabric Test
Nothing indicted in analysis
See Alarm Log for any alarms if any of the tests failed
New Run Level: ACTIVE
New System State; IS
```

Figure 11. Typical output of a looparound test

```
FAIL or LOOPAROUND NOT INSTALLED
Ethernet External Twisted Pair Looparound
        Ethernet   Slot: P5 Port: 1
```

Figure 12. Output of a failed external looparound test

Check processes

The server completes the boot process and displays its current state.

If	Then
1 **New Run Level: ACTIVE** and **New System State: IS**.	Type **showstatus ENTER** to see what processes are running.
2 Fewer than 17 MMCX processes are running.	Note the number of processes listed. Wait about 5 minutes and type **showstatus ENTER** again.
3 More processes are now running than were in Step 2.	Wait another 5 minutes and type **showstatus ENTER** again.
4 The same number of processes are running as in Step 2.	Reset the server. Type **reset level=boot ENTER**, and go back to Step 1.
5 Some processes still do not start after the server has been reset.	Reset the server again. Type **reset level=boot ENTER**. Wait about 15 seconds. Press the **Reset** switch on the front of the server.
6 Some processes still do not start after the hardware reset.	The application is not loading. Re-install the software. See *Installing MMCX server software, page 345*.

If	Then
7 The server goes to **OOS-FLT Active** state when you request **Active IS**.	Look for alarms. Go to *Viewing and interpreting alarm messages, page 156*.
8 All 17 MMCX processes are listed as running.	Troubleshooting is complete. If a fault persists, go to *Unusual problems*.

Unusual problems

If you encounter startup problems that are not covered elsewhere in this chapter, follow the steps in the table below. Perform each task in the order shown. Stop as soon as a step corrects the problem, and do not carry out the remaining steps. If the problem persists after step 4, contact customer support representative (see *Repair Number 0 - Escalate to MACS, page 162*).

1	Cycle power OFF and ON or press the RESET switch.
2	Restore the server software from a back-up copy. See *Restoring server system files, page 347*.
3	Rebuild the database from a back-up copy. See *Restoring server system files, page 347*.
4	Restore all software on the hard drive. See *Recovering from a hard disk failure, page 416*.

8 Repairs

Once the MMCX server is running, the server records errors in an alarm log. If errors occur more frequently than the *threshold database entry* for that error type allow, the server logs an *alarm*.

- For instructions on how to display and interpret alarm log information, see *Viewing and interpreting alarm messages, page 156*.
- For a list of repair numbers, see *Repair numbers, page 158*.
- For basic troubleshooting instructions, see *Using the diagnostic charts, page 161*.
- To prepare for a support call, see *Repair Number 0 - Escalate to MACS, page 162*.

Viewing and interpreting alarm messages

To view the alarm log using the following procedures (for usage details, see *ALARMMON, page 429*):

- Type **showalarm data=hw-long state=active | more ENTER** to view *current* hardware alarms.
- Type **showalarm data=sw-long state=active | more ENTER** to see *current* software alarms.
- Type **showalarm data=hw-long | more ENTER** to retrieve *all* hardware alarms.
- Type **showalarm data=sw-long | more ENTER** to see *all* software alarms.

To identify the error and the corresponding repair procedure, you need a *repair number* and an *error code*. The repair number specifies the type of repair and the code identifies the specific steps you take within that procedure. To retrieve this information, proceed as follows.

1 In the first part of the report, locate the **Seq#** (sequence number) and **Code** of the error. Write them down.

The ***sequence number*** identifies a particular event in the log. You use it as an index when looking for the repair number (see the next step).

2 Scroll down to the second part of the alarm log. Find the **Seq#** from the preceding step. Note the corresponding **RPR** (repair) code.

3 Look up the repair number in the *Repair numbers, page 158*. Use the error code to navigate within the repair procedure.

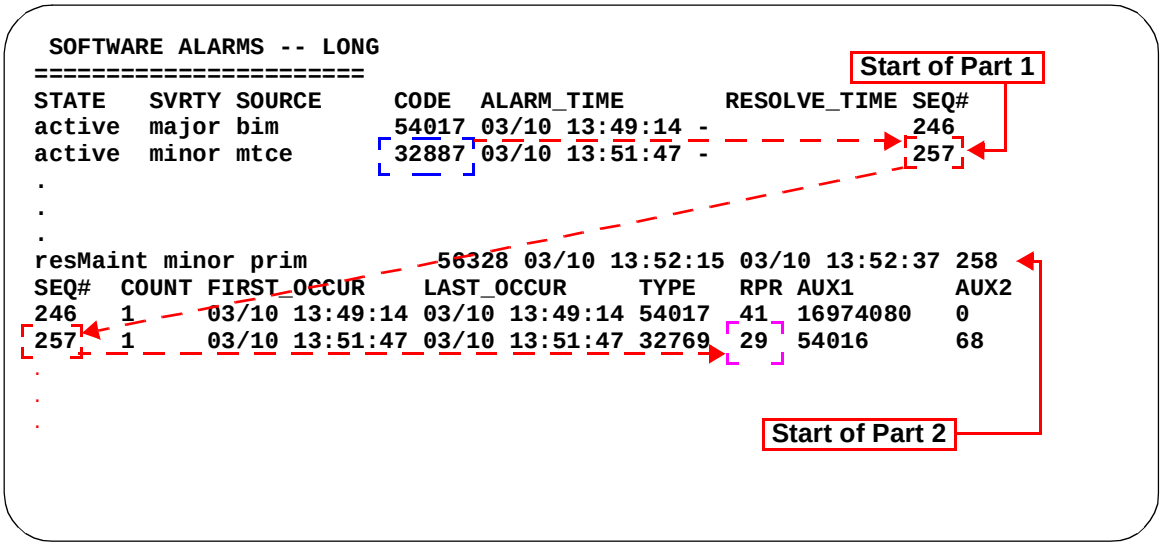


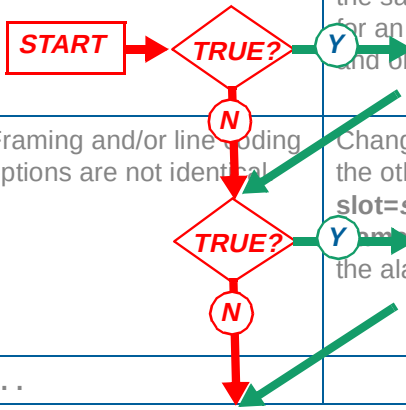
Figure 1. Typical output of the command showalarm data=sw-long

Repair numbers

Using the diagnostic charts

The diagnostic charts follow the if/then format familiar to anyone who has serviced an automobile or major appliance. To use the charts, start with the first row in the left column. When the condition described in this **If** column is *true*, move across to the righthand (**Then**) column, and perform the specified action. Then go down to the left (**If**) column of the next row. When the condition described in the **If** column is *false*, move down to the next row. Repeat the process until you reach the end of the table or are told to stop or go elsewhere.

If	Then
1 A segment is suspect.	Make sure that the devices at each end of the segment share the same framing and line-coding options. To view the options for an MMCX PRI card, type **showpri** at the system prompt, and observe the **FRAME** and **LCODE** fields of the display.
2 Framing and/or line coding options are not identical.	Change the options for one device so that they match those of the other. To change an MMCX PRI card setting, type **chgpri slot=*slot-number* port=*port-number* lcode=***line-coding** **fram=***framing*. Then use the **showalarm** command to see if the alarm is resolved.
3 . . .	



Repair Number 0 - Escalate to MACS

You cannot fix this problem without the help of the Lucent Multimedia Applications Customer Support (MACS) center. Make a note of the error code that you retrieved from the alarm log. Then proceed as follows.

1. Gather the information that MACS will need. See *Preparing for the call*.
2. Prepare a detailed description the error condition, when it arises, and how it can be reproduced. See *Preparing a scenario*.
3. Go to *Making the call*.

Preparing for the call

Before you call MACS, gather the following information.

1. Your customer number
2. The installation location (IL) number
3. The name of a contact person at the location
4. The number of the analog line to the remote maintenance board (RMB)
5. The MMCX server number
6. Number of MMCX servers in the network
7. Number of endpoints available for user login
8. LAN connectivity of the server
9. WAN connectivity of the server
10. A detailed description (see *Preparing a scenario*)

Preparing a scenario

Whenever possible, put together a detailed description of the problem, when it occurs, and how it can be reproduced. The more detailed the report, the better. Even endpoint mouse and key selections are useful. If you cannot reproduce the problem, do the following.

1. Describe the state of the server at the time of the failure. Include the following:
   - An estimate of the number of users logged on
   - An estimate of the number of users on calls
   - The media that the various callers were using
   - Unusual events or conditions, if any (abnormally heavy data traffic on the LAN, etc.)
   - Error logs for the connected switches
   - Any aberrant behavior reported by users prior to the failure
2. Then characterize normal server usage at the location. For example, do *typical* users make audio-only calls? Do they usually add other parties? Do they use video for less than 5 minutes, work with shared graphics for 20 minutes, or carry on an extended multimedia work session involving several people? Do all parties disconnect at about the same time?
3. Go back to *Repair Number 0 - Escalate to MACS*, or proceed to *Making the call*.

Making the call

When you have the necessary information and supporting documentation at hand, call the Multimedia Applications Customer Support (MACS) center at **1-800-821-8204**.

MACS is open during normal, Lucent business hours (6:00 AM to 6:00 PM Mountain Time, Monday through Friday, excluding holidays).

Repair Number 1 - PRI Physical Layer Facility Problems

A problem has arisen in the ISDN Primary Rate Interface (PRI) hardware. Make a note of the error code that you retrieved from the alarm log in case you need to call for technical support (see *Viewing and interpreting alarm messages*). Then, in the chart below, find the error code that you retrieved from the alarm log, and perform the associated repair.

Code	Repair	Corresponding alarm
4096	*Repair Action 1 - 1*	PRI Line A Yellow Alarm
4098		PRI Line A Red Alarm
4099		PRI Line B Yellow Alarm
4101		PRI Line B Red Alarm
4097	*Repair Action 1 - 2*	PRI Line A Blue Alarm
4100		PRI Line B Blue Alarm

Understanding PRI facility alarms

These alarms warn you that there is a problem with the ISDN Primary Rate Interface (PRI) hardware. There are three alarm types:

- Red alarms indicate that the equipment reporting the problem is not receiving a signal. *Isolate the fault immediately.*
- Yellow alarms mean that the far-end (the equipment that terminates the facility) has notified the near-end (the equipment reporting the problem) that it is not receiving a signal. *Isolate the fault immediately.*
- Blue alarms tell you that the equipment reporting the problem has detected maintenance actions underway on the facility or endpoints. No action is necessary unless an alarm persists for many hours.

PRI facility alarms often result from incorrect wiring or incompatible *Framing and line-coding options* in one or more of the following network elements:

- The MMCX server
- The PRI cards
- Terminating equipment, including nearby channel service units (CSUs), DEFINITY or 5ESS switching systems, transmission equipment (DACS or multiplexers), test equipment (DS1 test sets), and other MMCX servers

Framing and line-coding options

Framing and line-coding options tell a network device how to interpret an incoming data stream. The *framing* format specifies the features that identify the individual data elements (*frames* or *packets*) in the data stream, much as spaces and punctuation do in written text. If the originating equipment specifies ESF framing, it cannot communicate with a terminating device set up for a different frame size and format, such as D-4. *Line-coding* format prevents ambiguities that arise when too many successive zeros are sent over the publicly switched telephone network. A device that is using B8ZS line coding cannot talk to equipment that is configured for ZCS coding.

Repair Action 1 - 1

Study the layout of the network using a simple diagram (*Figure 2*). Identify segments that could be implicated in the failure. Then go to *Diagnosing incompatible framing and line-coding*.

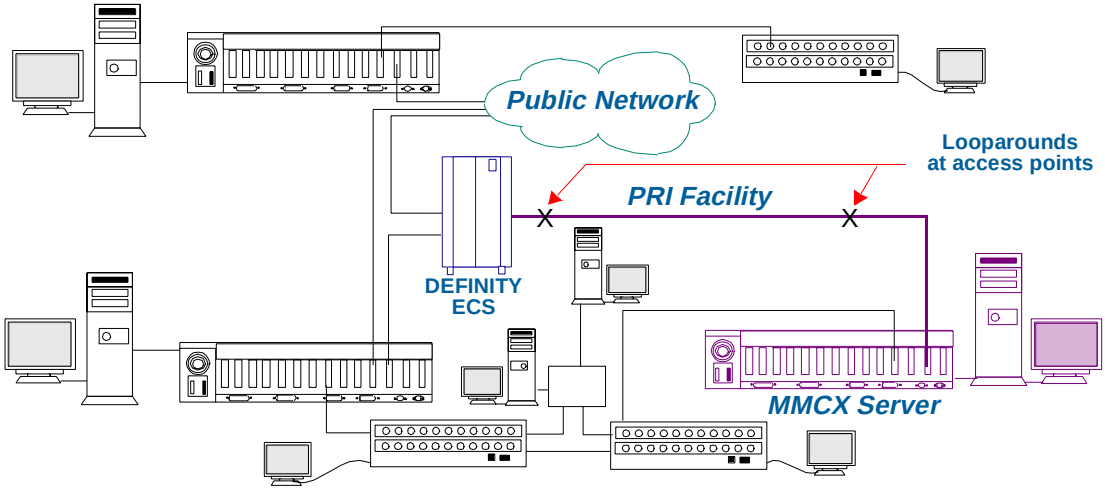


Figure 2. Sample facility connection map

Diagnosing incompatible framing and line-coding

Consult the chart below.

If	Then
1 A segment is suspect.	Make sure that the devices at each end of the segment share the same framing and line-coding options. To view the options for an MMCX PRI card, type **showpri** at the system prompt, and observe the **FRAME** and **LCODE** fields of the display.
2 Framing and/or line coding options are not identical.	Change the options for one device so that they match those of the other. To change an MMCX PRI card setting, type **chgpri slot=*slot-number* port=*port-number* lcode=*line-coding* frame=*framing* ENTER**. Then use the **showalarm** command to see if the alarm is resolved.
3 The alarm is resolved.	You are finished. Stop here.
4 The alarm persists when the options are identical.	Go to *Identifying PRI hardware failures*.

Identifying PRI hardware failures

If adjusting the framing and line-coding options fails to correct the alarm condition, proceed with hardware testing on the segment terminated by the server.

1 Look at the T1/E1 indicator LEDs, and consult *Figure 3* and the table below.

If	Then
1 T1/E1A or T1/E1B indicator ON	Check the physical distance between the board in question and the first DSX1-level termination.
2 The distance to the first DSX-1 termination is greater than 1000 feet for an E1 ISA-64 board (655 feet for an ISA-48 T1 card).	Shorten cabling, and reposition equipment if necessary.
3 The distance to the first DSX-1 termination is within the allowed range	Make sure that the PRI ***line-compensation*** (**LCOMP**) parameter is correct. Type **showpri ENTER**.
4 LCOMP is correct and the T1/E1 indicator is still ON.	**a** Attach external looparounds or loop at the Channel Service Unit (CSU). **b** Restart the server, and see if the problem resolves itself. Type **reset level=cold2 ENTER.** Then use **showalarm** to see if the alarm is resolved.
5 The problem persists (LED is ON or looparound test fails).	Go to Step 2, below.

2 Observe the RUN and SYSFAIL indicators (see *Figure 3*), and consult the chart below.

If	Then
1 RUN indicator OFF	Replace the PRI card. Go to *PRI card maintenance, page 362*.
2 SYSFAIL indicator ON	Replace the PRI card. Go to *PRI card maintenance, page 362*.
3 RUN indicator is ON, and SYSFAIL indicator is OFF, but alarms are still reported by **showalarm**.	Go to Step 3, below.

3 Check the status of the PRI trunk groups. See if the B channels that handle voice calls are up. Type **showptg ENTER**. Examine the **BCHAN** field. Then consult the table below.

If	Then
1 Fewer than 23 B channels are in service.	The server automatically audits and administers B channels, so the problem is usually at the far end. To confirm this, force an immediate audit by releasing the trunk group. Type **rlspri slot=*slot-number* port=*port-number* data=dchan ENTER**.
2 The alarm persists.	Ask the administrator at the far end to be sure that B channels are up.

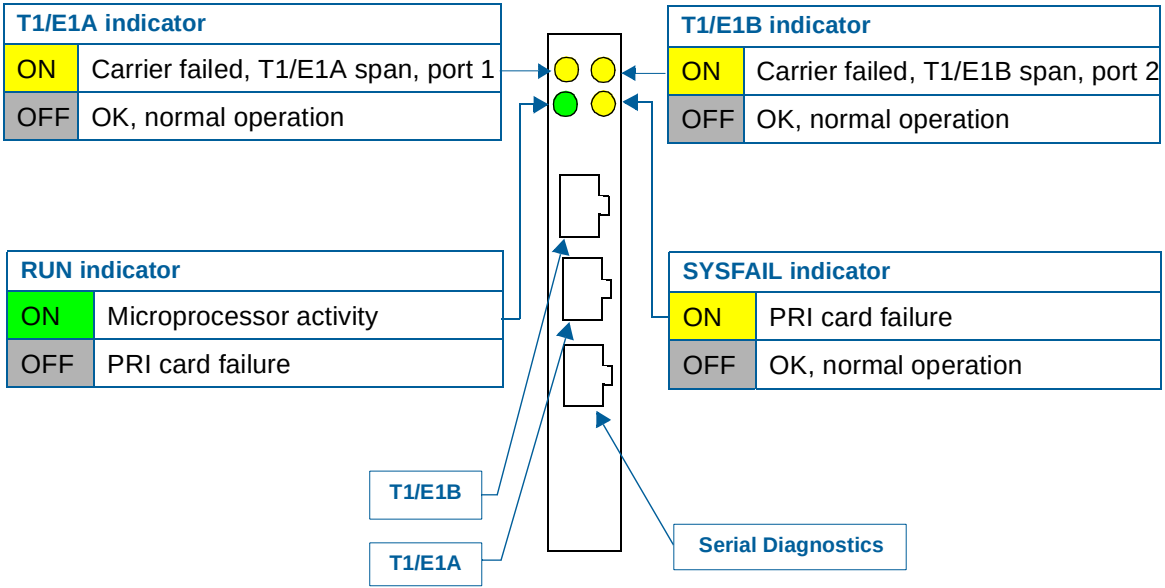


Figure 3. PRI card LED indicators

Repair Action 1 - 2

This is a blue alarm that tells you that the PRI facility is overdue for maintenance. Consult the chart below.

If	Then
1 The alarm resolves itself after a reasonable period of time.	Do nothing. The ISDN service provider may be doing maintenance.
2 The alarm persists for an extended period.	Contact the service provider for advice.

Repair Number 2 - PRI Configuration Problems

The PRI configuration parameters in the file cw.ini are not being read or are not being interpreted correctly. Make a note of the error code that you retrieved from the alarm log in case you need to call for technical support. Then, in the chart below, find the error code, and perform the associated repair.

Codes	Repair
56320-23	*Repair Action 2 - 1*

Repair Action 2 - 1

Check and, if necessary, repair ***cw.ini***. Proceed as follows.

1. Log in to the server.
2. Type **cd etc ENTER**.
3. Type **more cw.ini ENTER**.
4. Press **SPACE** to scroll down to the **[PRIM]** section (*not* [prim]). Check the **HWIDS** line against the values in *HWIDS settings*. For a sample [PRIM] section, see *Figure 4*.

If	Then
1 HWIDS settings in cw.ini file differ from those specified in *HWIDS settings*.	Force the server to rebuild cw.ini by changing the server number. See *Assigning a server number, page 58*.
2 The cw.ini file appears to be correct or has been rebuilt, but the alarm persists.	Call for technical support. Go to *Repair Number 0 - Escalate to MACS*.

HWIDS settings

The HWIDS (***hardware IDs***) line of cw.ini assigns a decimal number and an eight-digit hexadecimal equivalent to each combination of PRI slot, port, and channel. The first two digits of the eight-digit hexadecimal specify the bus (00 for ISA, so it does not show up in cw.ini). The next two represent the slot. The third pair identifies the port. The last two define the channel. See the chart below (hexadecimal equivalents are shown in the righthand columns, decimals in the left).

Slot-Port	T1 decimal	E1 decimal	T1 hexadecimal	E1 hexadecimal
I5-1	327960	327952	00050118	00050110
I5-2	328216	328208	00050218	00050210
I4-1	262424	262416	00040118	00040110
i4-2	262680	262672	00040218	00040210
i3-1	196888	196880	00030118	00030110
I3-2	197144	197136	00030218	00030210
I2-1	131352	131344	00020118	00020110
i2-2	131608	131600	00020218	00020210

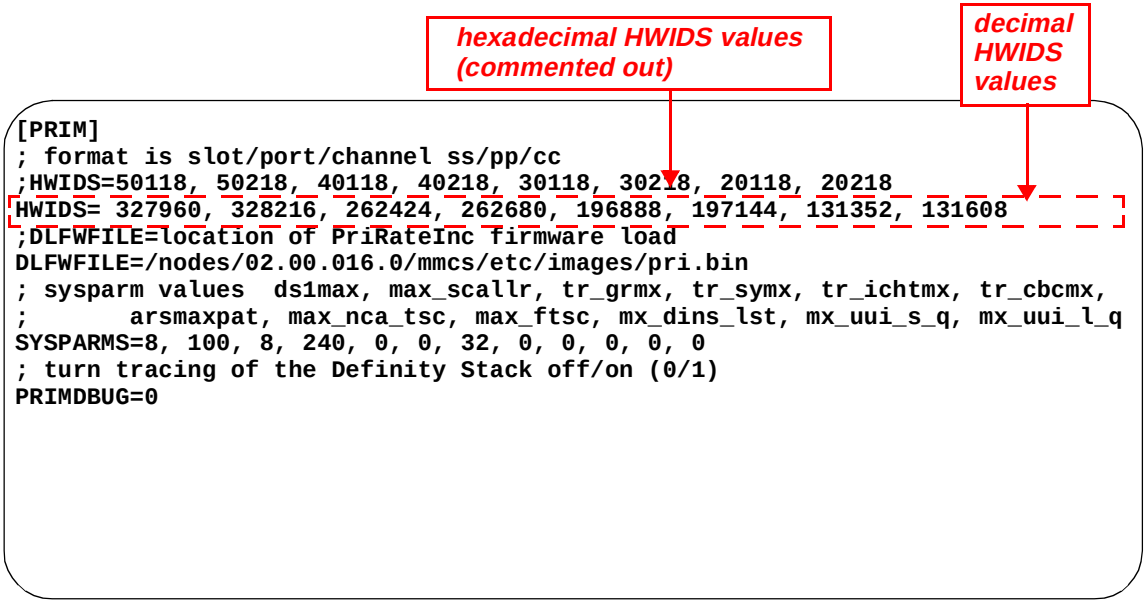


Figure 4. [PRIM] section of a sample cw.ini file

Repair Number 3 - PRI Download Info Access Errors

Make a note of the error code that you retrieved from the alarm log in case you need to call for technical support. Then, in the chart below, find the error code, and perform the associated repair.

Codes	Repair Action
56324-25	*Repair Action 3 - 3*
56326-27	*Repair Action 3 - 2*
56420	*Repair Action 3 - 1*

Repair Action 3 - 1

The MMCX software may not see the PRI device and/or its driver. Consult the table below.

If	Then
1 Repair Action 3-1 is indicated.	Type **drivers | more** to see if the driver is installed. Look for **PRI** in the **name** field.
2 The PRI driver was not found.	Driver information may be in an inconsistent state. Restart the server. Type **reset level=boot ENTER**.
3 The alarm persists after a reset.	Backup the system files. Go to *Restoring server system files, page 347*. Then return here by clicking the on-screen ◄◄ button.
4 You have backed up the system files.	Reinstall the MMCX application software. Go to *Restoring server system files, page 347*. Then return here by clicking the on-screen ◄◄ button.
5 The PRI driver was found.	Type **devices ENTER** for a list of recognized devices. Look for output like that in *Figure 5*.
6 The PRI card was not found or the driver was still not found.	The card may not be communicating with the driver software. Be sure the DIP switch settings on the card match the assigned I/O base address for the card. Go to *Configuring the replacement PRI card, page 364*.

If	Then
7 DIP switch settings are correct, but the server still cannot see the card.	Connections may be faulty. Reseat the card. Go to *Removing the suspect PRI card, page 362*.
8 All connections are sound, but the server still cannot see the card.	Replace the card. Go to *Removing the suspect PRI card, page 362*.
9 The server cannot find the new PRI card.	Call for technical support. Go to *Repair Number 0 - Escalate to MACS*.

```
id type  driver     use count start     size  name
0  char  0          16        0         0     null device
1  char  1          4         0         0     memory
2  char  2          0         0         0     ctrl dev
3  char  3          3         db2da3e0  0     kdconsole
4  char  4          0         (no dev)  0     com 1
5  char  4          11        db2dd678  0     com 2
6  char  5          0         (no dev)  0     raw HD 0-1
7  char  7          0         db2de258  0     raw Floppy 0-3
8  char  9          0         db2de550  0     SIM2940 RAW SCSI
9  char  11         4         db2f0770  0     pty 0
.
.
.
27 stdev 22         0         0         0     pri
```

A zero in the start *field for the PRI card shows that the card or driver was not found.*

Figure 5. Output of the devices command

Repair Action 3 - 2

The software cannot open the **DLFWFILE** specified by the cw.ini file. Check the path and filenames using the following procedure.

1. Login as **mmcs**.
2. Type **cd etc ENTER** to change directory to /mmcs/etc.
3. Type **more cw.ini ENTER** to list the contents of the cw.ini file, and press **SPACE** to scroll down to the **[PRIM]** section (see *Figure 4* for a sample). Consult the table below.

If	Then
1 **more** reports that it cannot open the file cw.ini, or there is no **DLFWFILE=** line in the **[PRIM]** section of cw.ini.	Contact technical support. Go to *Repair Number 0 - Escalate to MACS*.
2 The **DLFWFILE=** line exists.	Be sure that the specified file and path exist. a Type **cd images ENTER** to change the current directory to /mmcs/etc/images. b Then type **ls pri.bin ENTER**.
3 **cd** reports “not found” or **ls** reports that “File or directory doesn't exist.”	Contact technical support. Go to *Repair Number 0 - Escalate to MACS*.
4 The pri.bin file exists.	Restart the server. Type **reset level=cold2 ENTER**.

Repair Action 3 - 3

MMCX could not initialize. A disk error may have occurred. Consult the chart below.

If	Then
1 Repair Action 3-3 is indicated.	Press the POWER button on the front of the server to power down and force a file system check.
2 The file system repairs itself during the file system check.	The problem is resolved. Take no further action.
3 The problem persists or recurs after the file system check.	Call for technical support. Go to *Repair Number 0 - Escalate to MACS*.

Repair Number 4 - PRI Card Communication Errors

MMCX and/or operating system software cannot contact the PRI card. The card may not have initialized. Make a note of the error code that you retrieved from the alarm log in case you need to call for technical support. Then, in the chart below, find the error code, and perform the associated repair.

Codes	Repair Action
56425-27 56435-36 56472	*Repair Action 4 - 1*

Repair Action 4 - 1

Consult the chart below.

If	Then
1 Repair Action 4-1 is indicated.	**a** Type **reset level=cold2 ENTER** to reinitialize the PRI hardware. **b** Then use **showalarm** to see if the alarm is resolved.
2 The alarm condition has cleared.	Take no further action.
3 The alarm persists.	Replace the PRI card. Go to *PRI card maintenance, page 362*.

Repair Number 5 - System Resources & Lynx OS Errors

The system appears to be out of memory or reports operating system errors. Make a note of the error code in case that you retrieved from the alarm log you need to call for technical support. Then, in the chart below, find the error code, and perform the associated repair.

Codes	Repair Action
22674 26659 26659 53760-63 54018 54023 54137-38 55433-36 55468-73	*Repair Action 5 - 1*
55475 55482 55488	*Repair Action 5 - 2*

Repair Action 5 - 1

Consult the chart below.

If	Then
1 Repair Action 5-1 is indicated.	**a** Reset the server. Type **reset level=cold1 ENTER**. **b** Then use **showalarm** to see if the alarm is resolved.
2 The alarm condition persists.	Contact technical support. Go to *Repair Number 0 - Escalate to MACS*
3 The problem is solved.	Do nothing further for now. But for future reference, make a note of the conditions that led up to the error.

Repair Action 5 - 2

The swap (virtual-memory) file may be missing. Consult the chart below.

If	Then
1 Repair Action 5-2 is indicated.	Look for the swap file. Type **ls -l /.swap ENTER** (be sure to enter a space between **l** and **/**).
2 The swap file is not found.	**a** Reset the server. Type **reset level=cold1 ENTER**. **b** Then use **showalarm** to see if the alarm is resolved.
3 The swap file is found (see *Figure 6*).	Check the available memory. Type **ps -ax ENTER** (see *Figure 6*).
4 The server reports no free virtual memory.	**a** Reset the server. Type **reset level=cold1 ENTER**. **b** Then use **showalarm** to see if the alarm is resolved.
5 The server returns a single-digit value for either virtual or physical memory.	Call technical support. Go to *Repair Number 0 - Escalate to MACS*.

```
<mmcs>ls -l /.swap
+rw-r--r--   1 root      32624640     Apr 23 14:12/.swap
<mmcs>
<mmcs>ps -ax
.
.
.
13376K/81716K free physical/virtual, 22248K used (in this display)
```

Figure 6. Typical .swap file and free memory

Repair Number 6 - PRI Layer 2 (D channel) Errors

PRI signalling and call-data transmission are malfunctioning. Make a note of the error code that you retrieved from the alarm log in case you need to call for technical support. Then, in the chart below, find the error code, and perform the associated repair.

Codes	Repair Action
56338 56421	*Repair Action 6 - 1*
56430-33 56438 56441 56443	*Repair Action 6 - 2*

Repair Action 6 - 1

The PRI data channel is not functioning (D channels handle signalling for voice transmissions over B channels). Check the log for hardware alarms and address any PRI physical layer problems that appear (refer to *page 166*). Then consult the chart below.

If	Then
1 The alarm persists after PRI physical layer problems have been addressed or ruled out.	Make sure the D channel has not been purposely taken out of service (busied out) either on MMCX or on an attached PBX. a Type **showcard | more**. b Examine the **DCHAN_STAT** fields of the **PRI INTERFACE STATUS** section.

If	Then
2 When you type **showpri ENTER**, **showpri** reports that the D channel is down (see *Figure 7*).	a Busyout the D channel by typing **busypri slot=*slot-number* port=*port-number* data=dchan ENTER**. b Then release the D channel by typing **rlspri slot=*slot-number* port=*port-number* data=dchan ENTER**. Note that this action prevents new calls but does not interfere with active calls.
3 When you type **showptg ENTER**, the console reports (see *Figure 8*) fewer than 23 B channels in service on one of the T1 interfaces in the trunk group or fewer than 30 on an E1.	Release the B channels by typing **rlspri slot=*slot-number* port=*port-number* data=tg ENTER**.

```
PRI CONFIGURATION
.
.
.
PRI STATUS
SLOT   PORT   BIT_RATE    DCHAN_STAT   SERVICE_STATE   INTF_STATUS
       ADMIN_STAT
i5     1      t1(24)      D down(2)    inService(2)    inService(11)
       inService(2)
i5     2      t1(24)      down(2)      inService(2)    inService(11)
       inService(2)

PRI COUNTS
SLOT   PORT   IN_ATTEMPT  IN_COMPLETE  IN_ABANDON  IN_FAIL  LINK_DOWNS ACTIVE
i5     1      11          11           0           0        1          0
i5     2      7           0            0           7        2          0
SLOT   PORT   OUT_ATTEMPT OUT_COMPLETE OUT_ABANDON OUT_FAIL
i5     1      29          23           4           2
i5     2      0           0            0           0
```

Figure 7. showpri shows that the D channel is down.

```
 PRI TRUNK GROUP CONFIGURATION
============================
TG  AUD  VID  APP  NFAS   INTERFACE_LIST
1   20   60   20   off(2) i5:1, -, -, -, -, -, -, -
2   20   60   20   off(2) i5:2, -, -, -, -, -, -, -
PRI TRUNK GROUP COUNTS
======================
TG  CUR_OUT_AUD CUR_OUT_VID CUR_OUT_APP CUR_IN_AUD CUR_IN_OTH BCHAN
1   0           0           0           0          0          23
2   0           0           0           0          0          23
TG  MAX_OUT_AUD MAX_OUT_VID MAX_OUT_APP MAX_IN_AUD MAX_IN_OTH
1   2           5           3           0          9
2   0           0           0           0          0
TG  TOT_OUT_AUD TOT_OUT_VID TOT_OUT_APP TOT_IN_AUD TOT_IN_OTH
1   12          5           12          0          11
2   0           0           0           0          0
```

Figure 8. B channels in service

Repair Action 6 - 2

A PRI board-control error has occurred. Consult the chart below.

If	Then
1 Repair Action 6-2 is indicated.	a Type **reset level=cold2 ENTER**. b Then use **showalarm** to see if the alarm is resolved.
2 The alarm persists after you reset the server.	Replace the PRI card. Go to *PRI card maintenance, page 362*.
3 Resetting the server clears the alarm.	Take no further action.

Repair Number 7 - Internal PRI Card Diagnostics

The PRI card has caused the internal switch fabric test to fail or has failed its own on-board diagnostics. Make a note of the error code that you retrieved from the alarm log in case you need to call for technical support. Then, in the chart below, find the error code, and perform the associated repair.

Codes	Repair Action
4197	*Repair Action 7 - 2*
56329	*Repair Action 7 - 1*

Repair Action 7 - 1

A hardware error has occurred. Consult the chart below.

If	Then
PRI-card on-board diagnostics report an internal error.	Replace the PRI card. Go to *PRI card maintenance, page 362*.

Repair Action 7 - 2

The PRI interface has failed the internal switch fabric (internal looparound) test during initialization. The PRI card or one of its cables is faulty. Consult the table below.

If	Then
1 Repair Action 7-2 is indicated.	Test the MVIP cable (see *Checking cables, page 394*).
2 The MVIP cable is bad.	Replace the cable.
3 The MVIP cable is not the problem.	Replace the PRI card. Go to *PRI card maintenance, page 362*.

Repair Number 8 - Network Data Inconsistencies

The circuit-switched network is not providing incoming call information that the server needs. Make a note of the error code that you retrieved from the alarm log in case you need to call for technical support. Then, in the chart below, find the error code, and perform the associated repair.

Code	Repair Action
53310	*Repair Action 8 - 1*

Repair Action 8 - 1

The circuit-switched network is incorrectly configured. Consult the chart below.

If	Then
The circuit-switched network does not supply the calling number for the incoming call.	Contact the administrator of the circuit-switched network, and ask that he or she set up the network to pass the server number plus three digits of the calling party number. ***The server number must be 7 to 15 digits long*** (a network that passes 18 digits should always work).

Repair Number 9 - cw.ini File Non-existent or Corrupted

The configuration file for the MMCX server, cw.ini, is damaged or missing. You can consult the chart below for a more precise diagnosis. But all problems in this repair are handled in the same way: force the server to rebuild cw.ini, and call for technical support if this does not solve the problem.

Codes		Repair Action
21505-06 21564 22823 24741 32868 37890-92	21544 22788 24721 26122-33 33844	*Repair Action 9 - 1*
22850		*Repair Action 9 - 3*
23647		*Repair Action 9 - 5*
26378		*Repair Action 9 - 4*
55442-46	55497-55501	*Repair Action 9 - 2*

When you rebuild the database, you replace the existing system configuration using a backup copy of the software. *If the translations have been changed since the last backup (using addpri for instance), you lose the changes and must restore them yourself.*

Repair Action 9 - 1

The cw.ini file is either corrupted or cannot be found by the software. Consult the chart below.

If	Then
1 cw.ini is unusable or cannot be found.	Force the server to rebuild cw.ini by changing the server number. See *Assigning a server number, page 58*.
2 The problem persists.	Contact technical support. Go to *Repair Number 0 - Escalate to MACS*.

Repair Action 9 - 2

The Connection Manager (CM) parameters in the cw.ini file may be incorrect. Proceed as follows.

1. Log in as **mmcs**.
2. Type **cd etc ENTER**.
3. Type **more cw.ini ENTER**.
4. Press **SPACE** to scroll down to the **[CM]** (*not* [cm]) section.
5. Compare the parameters in cw.ini to those shown in *Figure 9* (note that most of the comment lines at the beginning of the section have been deleted in the example). Consult the table below.

If	Then
1 The **[CM]** parameters in cw.ini differ from those in the example.	Force the server to rebuild cw.ini by changing the server number. See *Assigning a server number, page 58*.
2 The **[CM]** parameters in cw.ini are identical to those in the example.	Contact technical support. Go to *Repair Number 0 - Escalate to MACS*.

```
[CM]
; MAXCONFERENCE: Value passed to WILD Cards for the max parties on
.
.
.
; CHANNEL_64KBPS_BW: WILD card 64Kbps channel
MAXCONFERENCE=7
COMPANDING=1
LOSSTABLESIZE=1
LOSSTABLE=32, 32, 25, 20, 20
WILDCODEFILES=/nodes/serial_number/mmcs/etc/images/wild2.S
WILDDATAFILES=""
CSWTCPPORT=1709
WILDAUDIOJITTER=0
.
.
.
```

[CM] parameters in cw.ini should match those shown here.

Figure 9. Sample [CM] section of cw.ini

Repair Action 9 - 3

The NAMER data in the cw.ini file may be incorrect or corrupt.

1. Log in as **mmcs**.
2. Type **cd etc ENTER**.
3. Type **more cw.ini ENTER**.
4. Press **SPACE** to scroll down to the **[NAMER]** section.
5. Consult the table below.

If	Then
1 The **[NAMER]** parameters in cw.ini differ from those shown here: **NAMER_NA=13035385400.namer_na** **NAMER_NS=13035385400.namer.ns** **NSPeerTimeOut=300**	Force the server to rebuild cw.ini by changing the server number. See *Assigning a server number, page 58*.
2 The **[NAMER]** parameters in cw.ini are identical to those shown above.	Contact technical support. Go to *Repair Number 0 - Escalate to MACS*.

Repair Action 9 - 4

The **minit** information in the cw.ini file may be incorrect.

1. Log in as **mmcs**, and type **cd etc ENTER**.
2. Type **more cw.ini ENTER**.
3. Press **ENTER** to scroll down to the [**minit]** section. Consult the table below.

If	Then
1 The **[minit]** parameters differ from those shown here: **num_threads=0** **my_vta=13035384300.minit** **udp_cmd_port=1037** **polling=enabled** **poll_interval=60** **sanity_ticks=1** **proc_kill_timeout=25** **mtce_reset_timeout=10**	Force the server to rebuild cw.ini by changing the server number. See *Assigning a server number, page 58*.
2 The **[minit]** parameters are identical to the above.	Contact technical support. Go to *Repair Number 0 - Escalate to MACS*.

Repair Action 9 - 5

The router data in the cw.ini file is not correct.

1. Log in as **mmcs**.
2. Type **cd etc ENTER**.
3. Type **more cw.ini ENTER**, and press **ENTER** to scroll down to **[PROC_TO_FAKE_CWID]**. Consult the table below.

If	Then
1 The **Router** parameter in the **[PROC_TO_FAKE_CWID]** section is set to something other than **f.9**.	Force the server to rebuild cw.ini by changing the server number. See *Assigning a server number, page 58*.
2 The **Router** parameter is correct.	Go to *Repair Number 0 - Escalate to MACS*.

Repair Number 10 - Networking Problems

MMCX cannot communicate over the Ethernet network using IP (Internet Protocol) addressing. You generally resolve this type of problem by mapping the network (*Figure 10*), testing its physical connectivity, and checking the status of the Ethernet and ATM cards. You test connectivity with the **ping** command. This command sends an echo-request packet from the IP processing layer of a system to the IP layer on another system. The remote system responds by returning the packet to the originating system. You test the Ethernet cards with **showenet** (see *ENETADM* for an in-depth description).

For specific repair instructions, scroll down through the chart below until you find the error code that you retrieved from the alarm log. Then perform the associated repair.

Codes		Repair Action
1030		*Repair Action 10 - 4*
1031,	1037	*Repair Action 10 - 5*
1032-33, 1039-42, 53764-65	1035-36 1281	*Repair Action 10 - 1*

Codes		Repair Action
26144-47 26170 26248 26624 26649 26654 26660-61 26703 26707 26725 26784 26804-06	26162-63 26181 26624 26647 26650-52 26657 26663-65 26705 26711 26784 26787-88	*Repair Action 10 - 2*
53264-65 53503-05	53280	*Repair Action 10 - 3*
53308-09		*Repair Action 10 - 7*
53558-60		*Repair Action 10 - 6*

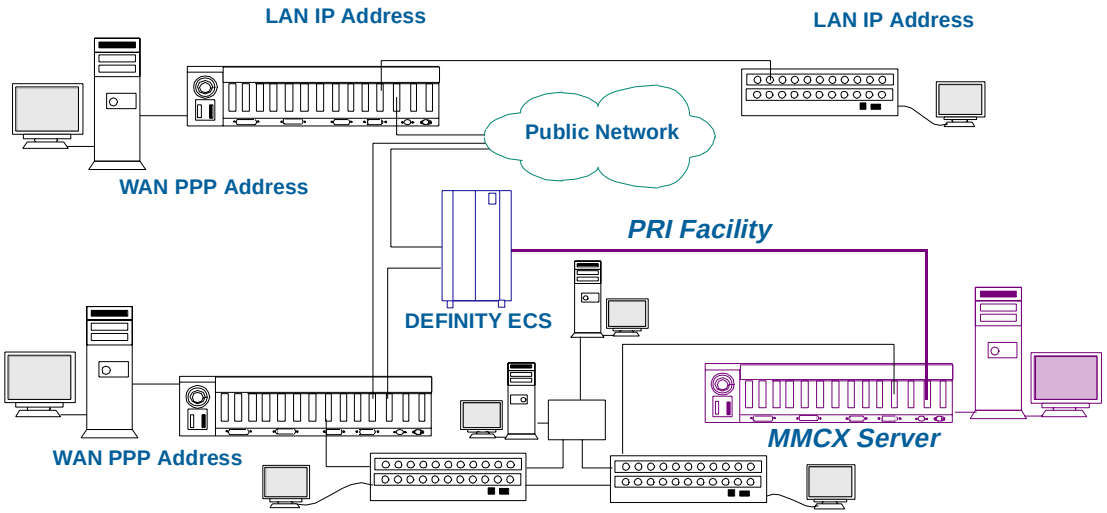


Figure 10. Typical MMCX network

Repair Action 10 - 1

There is a problem with the Ethernet network. A transmission has failed. Before proceeding further, take care of any alarms that require *Repair Number 15 - Ethernet Looparound Problems*. Then restart the server by typing **reset level=boot ENTER**, and consult the diagnostic chart below.

If	Then
1 The Ethernet card is not found during startup or the Ethernet internal looparound test fails.	Replace the Ethernet card. Go to *Ethernet card maintenance, page 367*.
2 During startup, the MMCX reports that the Ethernet card has been found and has passed the Ethernet internal looparound test.	If you are on-site, install looparound plugs, and run the external looparound test.
3 The card fails the external looparound test.	Replace the Ethernet card. Go to *Ethernet card maintenance, page 367*.
4 The card passes the external looparound test.	Ping the IP address of the next termination.
5 Pinging is successful.	Contact the network administrator.
6 Pinging is unsuccessful.	Repeat steps 4 and 5 for each succeeding termination.
7 You ping the last termination successfully. You can find no reason for the fault.	Contact technical support. go to *Repair Number 0 - Escalate to MACS*.

Repair Action 10 - 2

A connection may have failed, there may be an internal error in MMCX, or there may be a network problem. Consult the chart below.

If	Then
1 Repair Action 10-2 is indicated.	Check the configuration of the Ethernet cards by typing **showenet ENTER** (see *ENETADM, page 471* for a full description).
2 An IP address is incorrect.	Correct the address. Type **chgenet slot=*slot-number* port=*port-number* ip=*IP-address* mask=*netmask-value* ENTER**
3 An IP address is missing.	Add the address. Type **addenet slot=*slot-number* port=*port-number* ip=*IP-address* mask=*netmask-value* ENTER**
4 The card's IP address and configuration appear to be correct.	Ping distant hosts to see if the server is physically connected with other parts of the network.
5 Pinging fails.	Contact the network administrator.
6 Pinging succeeds. There is no obvious reason for the failure.	Contact technical support. Go to *Repair Number 0 - Escalate to MACS*.

Repair Action 10 - 3

Consult the chart below.

If	Then
1 Repair Action 10-3 is indicated.	Check the configuration of the Ethernet cards. Type **showenet ENTER**
2 An IP address is incorrect.	Correct the address. Type **chgenet slot=*slot-number* port=*port-number* ip=*IP-address* mask=*netmask-value* ENTER**
3 An IP address is missing.	Add the address. Type **addenet slot=*slot-number* port=*port-number* ip=*IP-address* mask=*netmask-value* ENTER**
4 The card's IP address and configuration appear to be correct.	Ping distant hosts to see if the server is physically connected with other parts of the network.
5 Pinging fails.	Contact the network administrator.
6 Pinging succeeds. There is no obvious reason for the failure.	Contact technical support. Go to *Repair Number 0 - Escalate to MACS*.

Repair Action 10 - 4

The twisted pair carrier has been lost. Consult the chart below.

If	Then
1 Repair Action 10-4 is indicated.	Check the Ethernet cards. Type **showenet ENTER** (see *ENETADM, page 471* for a full description).
2 An IP address is incorrect.	Correct the address. Type **chgenet slot=*slot-number* port=*port-number* ip=*IP-address* mask=*netmask-value*** and press **ENTER**.
3 An IP address is missing.	a Add the address. Type **addenet slot=*slot-number* port=*port-number* ip=*IP-address* mask=*netmask-value*** and press **ENTER** b Use **showalarm** to check the log for errors.
4 The card's IP address and configuration appear to be correct.	Ping distant hosts to see if the server is physically connected with other parts of the network.
5 Pinging fails.	Contact the network administrator.
6 Pinging succeeds. There is no obvious reason for the failure.	Contact technical support. Go to *Repair Number 0 - Escalate to MACS*.

Repair Action 10 - 5

A problem has arisen in an Ethernet interface. Consult the chart below.

If	Then
1 Repair Action 10-5 is indicated.	Type **showintf ENTER** to see the current status of the interface.
2 The interface is down.	Try removing and then re-adding the interface. a Type **rmenet slot=*slot-number* port=*port-number***. b Then type **addenet slot=*slot-number* port=*port-number* ip=*ip-address* mask=*subnet-mask***.
3 The problem persists.	Replace the Ethernet card. Go to *Ethernet card maintenance, page 367*.

Repair Action 10 - 6

A problem has arisen in an ATM Interface. Consult the chart below.

If	Then
1 Repair Action 10-6 is indicated.	Type **showatm ENTER** to display the current state of the ATM interface.
2 An IP address is incorrect.	Correct the address. Type **chgatm slot=*slot-number* port=*port-number* ip=*IP-address* mask=*netmask-value*** and press **ENTER**.
3 An IP address is missing. Card may not be administered.	Add the address. Type **addatm slot=*slot-number* port=*port-number* ip=*IP-address* mask=*netmask-value*** and press **ENTER**.
4 The card's IP address and configuration appear to be correct, but the problem persists.	Try removing and then re-adding the interface. **a** Type **rmatm slot=*slot-number* port=*port-number***. **b** Then type **addatm slot=*slot-number* port=*port-number***.
5 The problem persists.	Contact technical support. Go to *Repair Number 0 - Escalate to MACS*.

Repair Action 10 - 7

Low-level configuration of a network interface failed. Consult the chart below.

If	Then
1 The system could not configure the PPP/IP (Internet) interface.	Restart the server. Type **reset level=cold1 ENTER**.
2 Interface-configuration failed again during startup.	Contact technical support. Go to *Repair Number 0 - Escalate to MACS*.

Repair Number 11 - Thread and ROM Handles Problem

Needed resources are not available. MMCX is a *multi-threaded, distributed* application. A single process can execute along several parallel paths or *threads* simultaneously and can share methods (functions) with other programming objects. When a process sends the server a request for a remote object, the server assigns the request a thread and gives the desired object a unique identifier, the *Remote Object Management (ROM) handle*. The system can usually supply enough ROM handles. But threads make heavy use of system memory and operating system services. Processes thus compete for a finite number of threads. If the needed resources are temporarily unavailable, the process is *blocked* (stopped) until they are free. If the no resources become available, the process quits and logs an alarm.

Make a note of the error code that you retrieved from the alarm log in case you need to call for technical support. Then, in the chart below, find the error code, and perform the associated repair.

Codes	Repair Action
26168 26183 26268 32936 39034 55461	*Repair Action 11 - 2*
26192 26380-81 26384	*Repair Action 11 - 1*

Repair Action 11 - 1

Remote Object Management handles are not available. Consult the table below.

If	Then
1 Repair Action 11-1 is indicated.	Type **reset level=cold1 ENTER**.
2 The alarm recurs when you reset the server.	Contact technical support. Go to *Repair Number 0 - Escalate to MACS*.

Repair Action 11 - 2

The current process requires more threads or ROM handles than are currently available; all process threads are blocked. Consult the chart below.

If	Then
1 Repair Action 11-2 is indicated.	Type **reset level=cold1 ENTER**.
2 The alarm recurs when you reset the server.	Contact technical support. Go to *Repair Number 0 - Escalate to MACS*.

Repair Number 12 - Transport Connection Hangs

A connection has broken. Make a note of the error code that you retrieved from the alarm log in case you need to call for technical support. Then, in the chart below, find the error code, and perform the associated repair.

Code	Repair Action
26171	*Repair Action 12 - 1*

Repair Action 12 - 1

Occasional broken connections may not be a problem. Consult the chart below.

If	Then
1 The alarm log records excessive numbers of broken connections (>1000/day).	a Check server conditions at the time of the outages. Type **showalarm sev=12 start="*MM*/*DD*/*YY HH*:*MM*:*SS*" end="*MM*/*DD*/*YY HH*:*MM*:*SS*" | more** ENTER. b Look for problems that might cause a flurry of broken connections, such as hardware alarms and software alarms for transport processes like **prim**, **bim**, and **cm**.
2 showalarm reveals a hardware or software problem that could have caused the outages.	Resolve the hardware or software problem using the procedures specified by the repair number in the hardware or software alarm. *Stop here.*
3 No hardware or software problems could have caused the outages.	Check LAN performance. a Type **showenet | more** ENTER to view Ethernet link status. b Then ping the endpoints and any other MMCX servers with at least one hundred 64- and 4096-byte packets, and watch for packet loss.
4 Packet loss across the LAN exceeds 3% or showenet reveals an Ethernet problem.	Ask the administrator of the Ethernet network to resolve the problem. *Stop here*.

If	Then
5 The LAN seems OK.	Check WAN performance. **a** Set up a video or application connection to a distant MMCX server. **b** Type **showisr ENTER** to get the far-end PPP IP address. **c** Then ping the other MMCX server with at least one hundred 64- and 4096-byte packets.
6 Packet loss across the WAN is greater than 3%.	Ask the administrator of the PRI facility to resolve the problem. Stop here.
7 Network/PRI errors do not explain the outages.	Call for technical support. Go to *Repair Number 0 - Escalate to MACS*.

```
SERVER   SRVNUM          AUD VID APP SIG
macs1    13035385400     wan wan wan wan
mmcs01   13035385000     lan lan lan lan
.
.
.
SERVER   NEAR_PPP_ADDR   FAR_PPP_ADDR   ISR_PHONE_NUM   PLAN
macs1    125.9.5.4       125.9.4.5       5400            4
mmcs01   -               -               -               0
```

Figure 11. Sample output of showisr

Repair Number 13 - Responses Received After Time-Out

The network is excessively slow. Traffic may be heavy or outages may have reduced the available capacity. Make a note of the error code that you retrieved from the alarm log in case you need to call for technical support. Then, in the chart below, find the error code, and perform the associated repair.

Code	Repair Action
26254	*Repair Action 13-1*

Repair Action 13-1

The process timed out before it received a response from the far end. Proceed as follows.

If	Then
1 Repair Action 13-1 is indicated.	Check the condition of the server. **a** Type **showalarm sev=10 start="*MM*/*DD*/*YY* *HH*:*MM*:*SS*" end="*MM*/*DD*/*YY HH*:*MM*:*SS*" | more ENTER**.** **b** Find and repair any local problems that might produce slow performance, such as memory problems or failing network cards.
2 A local server problem could have caused time-out.	Resolve the problem. Stop here.
3 No local server problems could have caused the time-out.	Check LAN performance. **a** Type **showenet | more ENTER** to view the status of the Ethernet links. **b** Then ping the endpoints and any other MMCX servers with at least one hundred 64- and 4096-byte packets, and watch for packet loss.
4 Packet loss across the LAN exceeds 3% or showenet reveals an Ethernet problem.	Ask the administrator of the Ethernet network to resolve the problem. Stop here.

If	Then
5 The LAN seems OK.	Check WAN performance. **a** Set up a video or application connection to a distant MMCX server. **b** Type **showisr ENTER** to get the far-end PPP IP address. **c** Then ping the other MMCX server with at least one hundred 64- and 4096-byte packets.
6 Packet loss across the WAN is greater than 3%.	Ask the administrator of the PRI facility to resolve the problem. Stop here.
7 Network/PRI problems do not explain the outages.	Call for technical support. Go to *Repair Number 0 - Escalate to MACS*.

Repair Number 14 - ROM Queue Problems

An interprocess message buffer has overflowed. Make a note of the error code that you retrieved from the alarm log in case you need to call for technical support. Then, in the chart below, find the error code, and perform the associated repair.

Code	Repair Action
26262	*Repair Action 14 - 1*

Repair Action 14 - 1

You cannot increase the buffer size yourself. Proceed as follows.

If	Then
Repair Action 14-1 is indicated.	Contact technical support. Go to *Repair Number 0 - Escalate to MACS*.

Repair Number 15 - Ethernet Looparound Problems

The server has failed the internal Ethernet looparound test. An internal looparound test of Ethernet networking always executes during system initialization. The test sends data from the Ethernet driver over the PCI bus towards the Ethernet card. The startup process also performs an external looparound test if an external test loop is in place. Failed tests indicate problems with the Ethernet card or its cabling. Make a note of the error code that you retrieved from the alarm log in case you need to call for technical support. Then, in the chart below, find the error code, and perform the associated repair.

Code	Repair Action
1280	*Repair Action 15 - 1*

Repair Action 15 - 1

The Ethernet card may be faulty. Proceed as follows.

If	Then
1 The WILD card and Ethernet cards are not **found** even though they are physically installed.	A card may be loose. **a** Use the *Powering down, page 403*, to turn the server off gracefully. **b** Then make sure that all circuit cards (including Ethernet and the CPU) are fully seated in the server backplane. **c** Restart the server.
2 The alarm persists.	Replace the Ethernet card. Go to *Ethernet card maintenance, page 367*.

Repair Number 16 - WILD Card Hardware Problems

The WILD card hardware or a connection with the host has failed. Make a note of the error code that you retrieved from the alarm log in case you need to call for technical support. Then, in the chart below, find the error code, and perform the associated repair.

Codes	Repair Action
3072-73 3356	*Repair Action 16 - 2*
3073 3273 3357	*Repair Action 16 - 3*
3332 57345	*Repair Action 16 - 1*
55483	*Repair Action 16 - 5*
55494	*Repair Action 16 - 6*
57344	*Repair Action 16 - 4*

Repair Action 16 - 1

The WILD card has shut down or switch chips are not operational. Consult the chart below.

If	Then
1 Repair Action 16-1 is indicated.	Check the MVIP clock. Type **testwild slot=*slot-number* test=clock ENTER**.
2 The **testwild** clock test fails.	Go to *Repair Number 17 - MVIP Bus and Clock Sync Problems*
3 The clock test passes.	Reset the server. Type **reset level=cold2 ENTER**. See if the WILD card passes the internal looparound test.
4 The WILD card is **found** by the looparound test.	The cabling is OK. Replace the WILD card. Go to *WILD card maintenance, page 374*.
5 The WILD card is not **found** by the looparound test.	A cable may be connected incorrectly. **a** Use the *Powering down, page 403* to turn off the server. **b** Make sure that the MVIP ribbon cable is connected to the WILD-card parallel connector with the red wire towards the front of the server. **c** Then make sure that all circuit cards are fully seated in the server backplane. **d** Restart the server.

If	Then
6 The WILD card is not **found** after cabling has been checked.	The WILD card is defective. Replace it. Go to *WILD card maintenance, page 374*.
7 The WILD card is **found**, but the alarm persists.	The WILD card is defective. Replace it. Go to *WILD card maintenance, page 374*.
8 The alarm persists after the WILD card has been replaced.	Call for technical support. Go to *Repair Number 0 - Escalate to MACS*.

Repair Action 16 - 2

The WILD card controller has encountered an error. Resources may be inadequate or misallocated. Consult the chart below.

If	Then
1 Repair Action 16-2 is indicated.	Restart the server. Type **reset level=cold2 ENTER**. *This tears down all connections, so make sure users logoff before proceeding.*
2 The problem is resolved.	Take no further action.
3 The alarm persists after you reset the server.	Traffic may exceed the capacity of a single card. Install a second WILD card. Go to *WILD card maintenance, page 374*.
4 The problem recurs with two WILD cards installed.	Get technical support. Go to *Repair Number 0 - Escalate to MACS*.

Repair Action 16 - 3

WILD card hardware has failed. Consult the chart below.

If	Then
Repair Action 16-3 is indicated.	Replace the WILD card. Go to *WILD card maintenance, page 374*.

Repair Action 16 - 4

The WILD card is not communicating with the MMCX software. Consult the table below.

If	Then
1 Repair 16-4 is indicated.	Reset the server. Type **reset level=cold2 ENTER**.
2 The WILD card is **found**.	Cabling is OK. Replace the card. Go to *WILD card maintenance, page 374*.
3 The WILD card is not **found**.	**a** Use the *Powering down, page 403*, to turn off the server. **b** Make sure the MVIP ribbon cable plugs into the WILD-card parallel connector with the red wire to the front of the server. **c** Then make sure all circuit cards are fully seated. **d** Restart the server. Type **reset level=cold2 ENTER**.
4 The WILD card is not **found** after you check the cabling.	Replace the WILD card. Go to *WILD card maintenance, page 374*.
5 The WILD card is **found**, but the alarm persists.	Replace the WILD card. Go to *WILD card maintenance, page 374*.

If	Then
6 The alarm persists after the WILD card has been replaced.	Replace cards on the PCI bus one by one until you cure the problem or replace all cards. See *CPU card maintenance, page 356*, *Ethernet card maintenance, page 367*, *PRI card maintenance, page 362*, and *ATM card maintenance, page 371*.
7 The alarm persists.	Call for support. Go to *Repair Number 0 - Escalate to MACS*.

Repair Action 16 - 5

WILD card firmware did not download correctly or card did not initialize properly. Consult the chart below.

If	Then
1 Repair 16-5 is indicated.	Clear any other WILD card alarms that appear in the log.
2 The problem is resolved.	Take no further action.
3 The alarm persists after other alarms have been cleared.	Restart the server. Type **reset level=cold2 ENTER**.
4 The problem is resolved.	Take no further action.
5 The alarm persists after you reset the server.	Get technical support. Go to *Repair Number 0 - Escalate to MACS*.

Repair Action 16 - 6

The WILD card did not reset. Consult the table below.

If	Then
1 Repair 16-6 is indicated.	Do a hard restart. Type **level=halt ENTER.** Press the **RESET** button on the server.
2 The problem is resolved.	Take no further action.
3 The alarm persists after you reset the server.	Get technical support. Go to *Repair Number 0 - Escalate to MACS*.

Repair Number 17 - MVIP Bus and Clock Sync Problems

Clients and server are no longer synchronized. The Multi-Vendor Integration Protocol (MVIP) bus transfers voice, video, and data samples between WILD cards and PRI cards using clock signals provided by port 1 of the first PRI card installed, i5 (this is why the server must have a PRI card in slot i5). The best available clock source is usually attached to card i5 port 1 (for example, a 4ESS office is a better clock source than a DEFINITY PBX). When an external clock is not available, the PRI card provides free run clocks to the MVIP bus. Clock faults are typically discovered when the startup process runs **testwild slot=p2 test=clock**. But you may sometimes want to run **testwild** yourself, if, for instance, you are having intermittent problems that appear clock-related.

Make a note of the error code that you retrieved from the alarm log in case you need to call for technical support. Then, in the chart below, find the error code, and perform the associated repair.

Codes	Repair Action
3074-76	*Repair Action 17 - 1*

Repair Action 17 - 1

The WILD card reports that the MVIP 4MHz, 2MHz, or Frame Signal clock has been lost. Consult the following chart.

If	Then
1 Repair 17-1 is indicated.	Use the *Powering down, page 403*, to turn off the server. Is the MVIP ribbon cable connected to the WILD-card *and* PRI-card parallel connectors with the red wire towards the front of the server?
2 The MVIP cable is improperly connected.	Reconnect it to the PRI and/or WILD card with the red wire towards the front of the server.
3 MVIP connections are OK.	Is the clock termination jumper correctly installed on the WILD card in slot p2?
4 The WILD card jumper is improperly installed.	Install the WILD card clock jumper correctly.
5 The WILD card jumper is OK.	Are all three clock termination jumpers correctly installed on the PRI card in slot i5?

If	Then
6 The PRI card jumpers are installed incorrectly.	a Reinstall the PRI card clock jumpers. b Restart the server by typing **reset level=cold2 ENTER**.
7 PRI jumpers are OK.	Check the PRI card's DIP switches are set as in *Figure 12*.

2 of 2

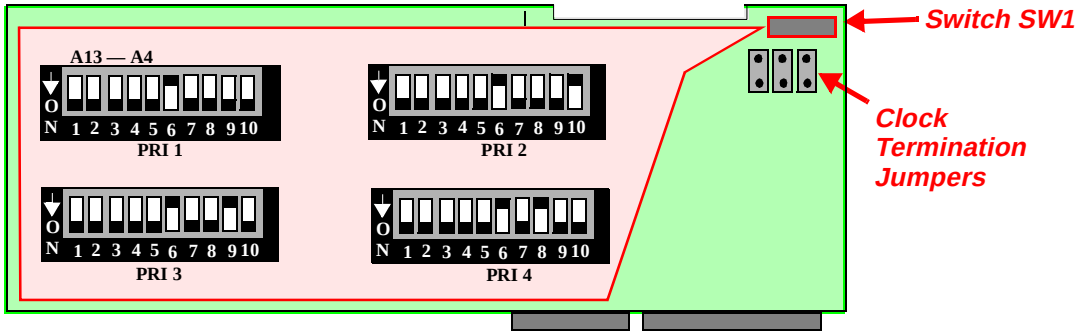


Figure 12. PRI card DIP switch location and settings

If	Then
8 PRI card jumpers are OK.	**a** Use the *Powering down, page 403*, to turn off the server. **b** Then disconnect the MVIP cable from all cards except i5 and p2. Restart the server.
9 The alarm is resolved.	Isolate the problem by powering down, reconnecting one card to the MVIP, and restarting. Repeat until the problem recurs. Then replace the offending card. Go to *PRI card maintenance, page 362*.
10 The problem recurs intermittently. **testwild** passes during startup, but fails if run thereafter.	Disconnect the PRI line from the PRI card in slot i5, and test the card using the local clock only (this recreates the startup test). Type **testwild slot=p2 test=clock ENTER**. Note the results and repeat.
11 **testwild** succeeds consistently after the PRI line is disconnected.	The external clock source is causing the problem. Connect the PRI card in slot i5 to a more reliable external timing source.
12 The alarm persists.	Call for technical support. Go to *Repair Number 0 - Escalate to MACS*

Repair Number 18 - WILD Card Receives Corrupted Data

A WILD card has detected a Cyclic Redundancy Check (CRC) violation. WILD cards use CRCs to control errors in MMCX data and video transmissions. A few CRC errors (<10/min) are no cause for concern. But higher error rates seriously reduce the quality of the transmitted information. WILD cards, MVIP cables, PRI cards, ISDN networks, and anything else that is installed in the transmission path can introduce CRC errors.

Make a note of the error code that you retrieved from the alarm log in case you need to call for technical support. Then, in the chart below, find the error code, and perform the associated repair.

Codes	Repair Action
3272	*Repair Action 18 - 1*

Repair Action 18 - 1

The receiving WILD card detected CRC errors in the incoming data from the PRI link. Consult the chart below.

If	Then
1 Repair 18-1 is indicated.	Check for network problems using the MMCX **showpri** and **showalarm** commands and any information available from other elements of the system, such as slip counts from a DEFINITY ECS PBX.
2 You notice PRI-card or PRI-trunk alarms.	Correct the problem, if possible, using the procedure indicated by the alarm.
3 You saw nothing obvious in the step above, but you have reason to suspect network problems.	Check LAN performance. **a** Type **showenet | more ENTER** to view Ethernet link status. **b** Then ping the endpoints and any other MMCX servers with at least one hundred 64- and 4096-byte packets, and watch for packet loss.
4 Packet loss across the LAN exceeds 3% or showenet reveals an Ethernet problem.	Ask the administrator of the Ethernet network to resolve the problem. *Stop here.*

To reverse the last jump, press ◄◄ on the Acrobat tool bar

If	Then
5 The LAN seems OK.	Check WAN performance. **a** Set up a video or application connection to a distant MMCX server. **b** Type **showisr ENTER** to get the far-end PPP IP address. **c** Then ping the other MMCX server with at least one hundred 64- and 4096-byte packets.
6 Packet loss across the WAN is greater than 3%.	Ask the administrator of the PRI facility to resolve the problem. Stop here.
7 The network appears to be stable.	**a** Check all server components in the path, including the MVIP cable and the cards attached to it. **b** If necessary, replace components one by one until you solve the problem or replace all the components. Go to *Checking cables, page 394*, *CPU card maintenance, page 356*, *Ethernet card maintenance, page 367*, *PRI card maintenance, page 362*, and *ATM card maintenance, page 371*.
8 The alarm persists.	You need technical support. Go to *Repair Number 0 - Escalate to MACS*.

Repair Number 19 - PRI Mngmnt Channel Enable Failed

The PRI data (D) channel is not functioning (D channels carry customer call data and handle signalling for voice transmissions over B channels). Make a note of the error code that you retrieved from the alarm log in case you need to call for technical support. Then, in the chart below, find the error code, and perform the associated repair.

Codes	Repair Action
56422	*Repair Action 19 - 1*

Repair Action 19 - 1

The PRI D channel is down. Check the log for hardware alarms and address any PRI physical layer problems that appear (refer to *page 166*). Then consult the chart below.

If	Then
1 The alarm persists after PRI physical layer problems have been addressed or ruled out.	Make sure the D channel is not busied out on purpose. a Type **showcard | more**, and examine the **ADSTAT** fields of the **INSTALLED NETWORK INTERFACE HARDWARE** and **PRI INTERFACE STATUS** sections. b Type **showpri ENTER**.
2 **showpri** reports that the D channel is down (see *Figure 7*).	a Busyout the D channel by typing **busypri slot=*slot-number* port=*port-number* scope=dchan ENTER**. b Then release the D channel by typing **rlspri slot=*slot-number* port=*port-number* scope=dchan ENTER**. *Note that this action prevents new calls but does not interfere with active calls.* c Type **showptg ENTER**.
3 **showptg** reports fewer than 23 B channels in service (see *Figure 8*).	Reinitialize by typing **rlspri data=ptg ENTER**.
4 The alarm persists.	Go to *Repair Number 0 - Escalate to MACS*.

Repair Number 20 - *number reserved for future use*

Repair Number 21 - Incomplete Hardware Equipped

The server does not appear to have the minimum hardware required by the MMCX software. Make a note of the error code that you retrieved from the alarm log in case you need to call for technical support. Then, in the chart below, find the error code, and perform the associated repair.

Codes	Repair Action
32979	*Repair Action 21 - 1*

Repair Action 21 - 1

The server has fewer than one WILD, one PRI, and one network interface (Ethernet or ATM) card installed and working properly. The server does not meet minimum system requirements.

If	Then
1 Repair 21-1 is indicated.	Restart the server. Type **reset level=cold2 ENTER**. Make sure that the required circuit cards are **found** and that they pass the hardware initialization tests.
2 The required cards are not **found** or fail initialization.	**a** Display the alarms with **showalarm**. Look for PRI, WILD, ATM, or Ethernet alarms. **b** Correct them using the procedure indicated by the specified repair number and code.
3 The alarm persists after all card-specific alarms have been cleared.	Make sure that the minimum set of circuit cards is installed. **a** Turn the server off with the *Powering down, page 403*. **b** Then make sure that PRI, WILD, and Ethernet cards are firmly seated and connected (see *Checking cables, page 394*).

If	Then
4 Required cards are missing or improperly installed.	Install them. Go to *CPU card maintenance, page 356*, *Ethernet card maintenance, page 367*, *PRI card maintenance, page 362*, and *ATM card maintenance, page 371*.
5 The required cards are physically present or **found** and correctly initialized.	You need technical support. Go to *Repair Number 0 - Escalate to MACS*.

Repair Number 22 - Name Agent Interface Problems

A software compatibility problem exists. Make a note of the error code that you retrieved from the alarm log in case you need to call for technical support. Then, in the chart below, find the error code, and perform the associated repair.

Codes	Repair Action
21504 21508	*Repair Action 22 - 1*

Repair Action 22 - 1

The server and one or more clients may be using different releases of the MMCX software. Consult the chart below.

If	Then
1 Repair 22-1 is indicated.	Restart the server. Type **reset level=cold1 ENTER**.
2 The incompatibility persists.	Make sure that the client and server are using the same version of MMCX by logging onto the client remotely.
3 The client uses an obsolete software release.	Have the remote user locate and install the correct, latest release of the client software on his or her workstation.
4 The server software is obsolete.	Install the correct, latest release. See *Installing MMCX server software, page 345* if the latest release is a full software package. If the latest release is a patch, see *Patching server software, page 348*.
5 Client and server software releases are compatible but the problem persists.	Get technical support. Go to *Repair Number 0 - Escalate to MACS*.

Repair Number 23-NameServer-NameAgent Interactions

Client-to-server communications has failed in some way. Make a note of the error code that you retrieved from the alarm log in case you need to call for technical support. Then, in the chart below, find the error code, and perform the associated repair.

Codes	Repair Action
21509 21511-14 21545 22743 22745 39032 45064 45096	*Repair Action 23 - 1*

Repair Action 23 - 1

The connection between the client and the server is failing. Consult the chart below.

If	Then
1 Repair 23-1 is indicated.	Restart the server. Type **reset level=cold1 ENTER**.
2 The incompatibility persists.	Make sure that the client and server are using the same version of MMCX by logging onto the client remotely.
3 The client uses an obsolete software release.	Have the remote user locate and install the correct, latest release of the client software on his or her workstation.
4 The server software is obsolete.	Install the correct, latest release. See *Installing MMCX server software, page 345*.
5 Client and server software releases are compatible but the problem persists.	Get technical support. Go to *Repair Number 0 - Escalate to MACS*

Repair Number 24 - Internal Data Base Problems

An internal, client-server database error has occurred. Make a note of the error code that you retrieved from the alarm log in case you need to call for technical support. Then, in the chart below, find the error code, and perform the associated repair.

Codes		Repair Action
22528-31	22533-673	*Repair Action 24 - 1*
22675	22738	
23649	24591-92	
24595	24597-99	
24661	32896-903	
32905-22	32925-32	
37889	38112-21	
38208-14	49201-09	
49212	49265-72	
49274-76	49274-76	
53258-63	49280-85	
53348-57	53266-79	
53398-415	53361-85	
53454-73	53448-52	
53506-07	53498-502	
53586-87	53509-19	

Repair Action 24 - 1

The file system may be corrupt. Consult the chart below.

If	Then
1 Repair 24-1 is indicated.	Make sure that the client and server are using the same version of MMCX by logging onto the client remotely.
2 The *client* uses an obsolete software release.	Have the remote user locate and install the correct, latest release of the client software on his or her workstation.
3 The server software is obsolete.	Install the correct, latest release. For a full release, use the procedure in *Installing MMCX server software, page 345*. For a patch, use the procedure in *Patching server software, page 348*.
4 The problem occurs when the client and server are using the same version of MMCX.	Force a file system check. **a** Turn the server OFF by pressing the **POWER** button on the front panel. **b** Turn the server back ON by pressing the **POWER** button again. Normally, you protect the file system by shutting down gracefully using the **reset** command. Since the file system is already corrupt, this is not an issue.

If	Then
5 The file system check does not resolve the problem.	Restart the server. Type **reset level=cold1 ENTER**.
6 Restarting does not resolve the problem.	Rebuild the data base. Start by typing **reset level=menu ENTER** to display the software administration menu.
7 The software administration menu appears.	At the prompt, press **1 ENTER** to select **IP Configuration**.
8 The IP configuration menu appears.	Press **3 ENTER** to select **Define System Server Name.**
9 A name-entry prompt appears.	Type ***server-name*** **ENTER**.
10 The server asks you to select a network interface card (NIC).	Press **ENTER** to accept the default.
11 The console displays the correct server information.	Press **N ENTER** to back out and start over without saving changes.
12 The console displays the correct server information.	Press **Y ENTER** to save the configuration information.

If	Then
13 The server saves the changes and displays the IP configuration menu.	Press **4 ENTER** to return to the software administration menu.
14 The software administration menu reappears.	Press **3 ENTER** to select **System Restore**.
15 The system backup menu appears.	At the prompt, press **1 ENTER** to select **Display current backup information**.
16 The console displays the date, time, status, availability, and destination of the backups.	Select the most recent available, successful backup that predates the problem. Press **2 ENTER** to select **Change restore source host and directory names**.
17 The **Enter new host** prompt appears.	Type the host name for the backup copy you selected, and press **ENTER**.
18 The server prompts you to enter a new source directory.	Type the source directory name for the backup copy you selected, and press **ENTER**.
19 The server prompts you for a user name for the restore.	Type the user name for the backup copy you selected, and press **ENTER**.

If	Then
20 The console displays the restore menu.	Type **3 ENTER** to select **Start restore**. The software warns you that it is about to overwrite the system information and asks for confirmation. Press **Y ENTER** to proceed.
21 The system performs the restore operation and returns to the restore menu.	Press **4 ENTER** to return to the software administration menu.
22 The software administration menu reappears.	**a** Press **5 ENTER** to restart the MMCX application. **b** Redo any administrative changes made since the selected restore source was backed up. **c** Reset the server, and check for alarms.
23 The problem persists.	Get technical support. Go to *Repair Number 0 - Escalate to MACS*.

Repair Number 25 - Routing Administration Problems

Network routing is not working properly. Make a note of the error code that you retrieved from the alarm log in case you need to call for technical support. Then, in the chart below, find the error code, and perform the associated repair.

Codes	Repair Action
22742 22744 40558-61 40563-66 40576-81	*Repair Action 25 - 1*

Repair Action 25 - 1

Incorrect IP address information has caused a network routing error. Consult the chart below.

If	Then
1 Repair 25-1 is indicated.	Type **showisr | more ENTER** to display routing information for all servers.
2 The console displays the server table.	Check the displayed **IP_ADDRESSES** for each server against the known addresses.
3 A displayed IP address is incorrect.	Change the IP address. Type **chgisr srv=*server-name* ip=*ip-address* ENTER**.
4 A server name and/or IP address is missing.	Add the information. Type **addisr srv=*server-name* ip=*ip-address* ENTER**.
5 A spurious server name is competing for the IP address of an actual server.	Delete the name of the non-existent server. Type **rmisr srv=*server-name* ENTER**.
6 The IP address changes cure the problem.	Take no further action.

If	Then
7 All IP addresses appear correct, but the alarm persists.	Ping the offending servers to test for physical connectivity.
8 A server cannot be pinged. There may be a network problem.	Advise the Ethernet administrator and request a list of correct IP addresses for MMCX servers.
9 All servers can be reached by pinging.	Go to *Repair Number 0 - Escalate to MACS*.

Repair Number 26 - Login, Challenge & Password Errors

Login and password validation routines are failing. Make a note of the error code that you retrieved from the alarm log in case you need to call for technical support. Then, in the chart below, find the error code, and perform the associated repair.

Codes	Repair Action
38048-50	*Repair Action 26 - 1*

Repair Action 26 - 1

Obsolete, incompatible server or client software has caused a login or password-validation error. Consult the chart below.

If	Then
1 Repair 26-1 is indicated.	Make sure that the client and server are using the same version of MMCX by logging onto the client remotely.
2 The client uses an obsolete software release.	Have the remote user locate and install the correct, latest release of the client software on his or her workstation.
3 The server software is obsolete.	Install the correct, latest release. See *Installing MMCX server software, page 345*.
4 The problem persists even though the clients and the server are all using the latest software release.	Get technical support. Go to *Repair Number 0 - Escalate to MACS*

Repair Number 27 - License File Inconsistencies

The MMCX software could not open or read a license file. Make a note of the error code that you retrieved from the alarm log in case you need to call for technical support. Then, in the chart below, find the error code, and perform the associated repair.

Codes	Repair Action
38122-29	*Repair Action 27 - 1*

Repair Action 27 - 1

A missing, unreadable, or inconsistent license file caused a login error. Consult the chart below.

If	Then
Repair 27-1 is indicated.	Contact technical support and ask the representative to download replacement license files. Go to *Repair Number 0 - Escalate to MACS*.

Repair Number 28 - Trader Received Garbled Message

An internal software error has occurred. You can generally ignore this alarm as long as it does not occur frequently. If you note many instances of these errors in the alarm log, make a note of the error code. Then, in the chart below, find the error code, and perform the associated repair.

Codes	Repair Action
24621 24641 24662	*Repair Action 28 - 1*

Repair Action 28 - 1

Internal software processes are in an inconsistent state. Consult the chart below.

If	Then
1 Errors have become frequent or chronic.	Restart the server. Type **reset level=cold1 ENTER**.
2 Restarting the server cures the problem.	This was a transient condition. Take no further action.
3 The problem persists after a restart.	Request technical support. Go to *Repair Number 0 - Escalate to MACS*

Repair Number 29 - ECS Errors Detected by Alarm Log

The alarm-processing software did not understand the alarm message and could not log it properly. In the chart below, find the error code reported in the alarm log, and perform the associated repair.

Codes	Repair Action
32885-86	*Repair Action 29 - 1*
32887	*Repair Action 29 - 2*

Repair Action 29 - 1

The alarm-processing software could not interpret the alarm message. The message may be garbled or improperly formatted. Consult the chart below.

If	Then
1 The problem occurs only occasionally.	Ignore it.
2 This is a chronic problem.	Get technical support. Go to *Repair Number 0 - Escalate to MACS*.

Repair Action 29 - 2

An undefined or unanticipated error has occurred. Consult the chart below.

If	Then
Repair Action 29-2 is indicated.	1 Choose a file name you can remember, such as **repair29.log**. 2 Then redirect the output of showalarm to the file by typing **showalarm data=sw-long > repair29.log**. This copies the alarm-log information that technical support will need. 3 Go to *Repair Number 0 - Escalate to MACS*. send them the repair-log data file.

Repair Number 30 - WILD Card to CPU Comm Problems

A problem in the WILD card hardware or the MMCX software has interrupted communications between the host computer and the WILD card. Make a note of the error code that you retrieved from the alarm log in case you need to call for technical support. Then, in the chart below, find the error code, and perform the associated repair.

Codes	Repair Action
3077 55417-20 57624	*Repair Action 30 - 4*
55478	*Repair Action 30 - 3*
55479-81 55489-93	*Repair Action 30 - 1*
57444 57524	*Repair Action 30 - 2*

CAUTION:
Some repair actions reinitialize the PRI card using the **initcard** command. When you run **initcard** against slot i5, MVIP timing is momentarily interrupted. *Sometimes* this interferes with the WILD card and results in the loss of audio. If this happens, you must restart the server by typing **reset level=cold1 ENTER** to restore service.

Repair Action 30 - 1

Code or data was lost somewhere between the WILD card and the host. Consult the chart below.

If	Then
1 Repair Action 30-1 is indicated.	Type **showalarm ENTER** to view the alarm log. Look for indications of other hardware problems, such as errors when communicating with ATM or Ethernet cards.
2 Other hardware alarms have been logged.	**a** Correct the error conditions using the procedures indicated in the alarm. **b** Return here by clicking the on-screen ◄◄ button.
3 The problem is solved.	Stop here.
4 The problem persists when no other hardware alarms are logged.	Reinitialize the card. **a** Type **busywild slot=*slot-num* ENTER**. **b** Type **initcard slot=*slot-num* ENTER**. **c** Type **rlswild slot=*slot-num* ENTER**.
5 **initcard** does not cure the problem.	Reset the server. Type **reset level=cold2 ENTER**.
6 initializing the card or resetting the server clears the alarm.	Stop here.
7 The alarm persists after resetting the server.	Get technical support. Go to *Repair Number 0 - Escalate to MACS*.

Repair Action 30 - 2

The host could send or receive messages and data. Consult the chart below.

If	Then
1 Repair Action 30-2 is indicated.	Type **showalarm ENTER** to view the alarm log. Look for other WILD-card, MVIP-bus, clock, or Ethernet alarms.
2 Other hardware alarms have been logged.	**a** Correct the error conditions using the procedures indicated in the alarm. **b** Then return here by clicking the on-screen ◄◄ button.
3 The problem is solved.	Stop here.
4 The problem persists when no other hardware alarms are logged.	Get technical support. Go to *Repair Number 0 - Escalate to MACS*.

Repair Action 30 - 3

The WILD card has failed. Consult the chart below.

If	Then
Repair Action 30-3 is indicated.	Replace the WILD card. Go to *WILD card maintenance, page 374*.

Repair Action 30 - 4

No WILD card resources are available to support the current request. Consult the chart below.

If	Then
1 Repair Action 30-4 is indicated.	See if demand is heavy enough to use up all available resources. **a** Type **showcall ENTER** to see how many audio and video calls are underway. **b** Type **showpri ENTER** to view PRI usage.
2 Traffic is heavy enough to use up the WILD-card resources.	**a** Add a second WILD card. Go to *WILD card maintenance, page 374*. **b** Then return here by clicking the on-screen ◀◀ button.
3 The problem is solved.	Stop here.
4 Demand is not heavy enough to use up WILD card resources, or the problem persists after a second WILD card has been installed.	Get technical support. Go to *Repair Number 0 - Escalate to MACS*.

Repair Number 31 - Switch Fabric Test, PRI Failure

A PRI card, WILD card, or MVIP cable has failed a looparound test. The *switch fabric* is another name for the hardware that connects the server to a service provider. Audio, video, and WAN data transmissions travel through the switch fabric. It includes WILD cards, MVIP cable, and PRI cards. During server initialization, MMCX runs *switch fabric tests* (looparound tests) that check the integrity of this hardware. Make a note of the error code that you retrieved from the alarm log in case you need to call for technical support. Then, in the chart below, find the error code, and perform the associated repair.

Codes	Repair Action
4196	*Repair Action 31 - 1*

Repair Action 31 - 1

A PRI card, WILD card, or MVIP cable may have failed. Consult the chart below.

If	Then
1 Repair Action 31-1 is indicated.	Check the alarm log for WILD- and PRI-card alarms by typing **showalarm ENTER** and examining the output.
2 WILD- and/or PRI-card are logged.	Type **testwild slot=*slot-num* test=loop** where ***slot-num*** is the slot number of the card implicated in the **AUX** field of the alarm log screen.
3 **testwild** fails.	Replace the WILD card. Go to *WILD card maintenance, page 374*.
4 **testwild** passes.	a Check the MVIP cable, and replace it if necessary. Go to *Checking cables, page 394*. a Then return here by clicking the on-screen ◄◄ button.
5 You find a defective MVIP cable.	Restart the server. See if the switch fabric test passes.
6 Switch fabric tests pass after you replace the MVIP cable.	Stop here.
7 The MVIP cable is OK, or the switch fabric tests fail again.	a Replace the PRI card. Go to *PRI card maintenance, page 362*. b Then return here by clicking the on-screen ◄◄ button. c Restart the server. See if the switch fabric test passes.

If	Then
8 The switch fabric tests pass after you replace the PRI card.	Stop here.
9 The switch fabric tests fail after you replace the PRI card.	Type **showalarm data=hw-long ENTER**. Examine the **AUX** field of the output screen.
10 AUX=**16908544** (01020100h)	Replace the WILD card in slot p2.
11 AUX=**17039616** (01040100h)	Replace the WILD card in slot p4 (if installed).
12 The alarm persists after WILD cards have been replaced.	Get technical support. Go to *Repair Number 0 - Escalate to MACS*.

Repair Number 32 - Switch Fabric Test Analysis Failures

A PRI card, WILD card, or MVIP cable has failed a looparound test. The *switch fabric* is another name for the hardware that connects the server to a service provider. It includes WILD cards, MVIP cable, and PRI cards. Audio, video, and WAN data transmissions travel through the switch fabric. During server initialization, MMCX runs *switch fabric tests* (looparound tests) that check the integrity of this hardware. Make a note of the error code that you retrieved from the alarm log in case you need to call for technical support. Then, in the chart below, find the error code, and perform the associated repair.

Codes	Repair Action
3352	*Repair Action 32 - 2*
3353-55	*Repair Action 32 - 1*

Repair Action 32 - 1

A WILD card or MVIP cable failed a looparound test. Consult the chart below.

If	Then
1 Repair Action 32-1 is indicated.	Check the alarm log for WILD- and PRI-card alarms by typing **showalarm ENTER** and examining the output.
2 WILD- and/or PRI-card are logged.	Type **testwild slot=*slot-num* test=loop** where ***slot-num*** is the slot number of the card implicated in the **AUX** field of the alarm log screen.
3 **testwild** fails.	Replace the WILD card. Go to *WILD card maintenance, page 374*.
4 **testwild** passes.	**a** Check the MVIP cable, and replace it if necessary. Go to *Checking cables, page 394*. **b** Then return here by clicking the on-screen ◄◄ button.
5 You find a defective MVIP cable.	Restart the server. See if the switch fabric test passes.
6 switch fabric tests pass after you replace the MVIP cable.	Stop here.
7 The MVIP cable is OK, or the switch fabric tests fail again.	Type **showalarm data=hw-long ENTER**. Examine the **AUX** field of the output screen.
8 AUX=**16908544** (01020100h)	Replace the WILD card in slot p2.

If	Then
9 AUX=**17039616** (01040100h)	Replace the WILD card in slot p4 (if installed).
10 The alarm persists after WILD cards have been replaced.	Get technical support. Go to *Repair Number 0 - Escalate to MACS*.

Repair Action 32 - 2

A WILD card, PRI card, or MVIP cable failed the switch fabric tests. Consult the chart below.

If	Then
1 Repair Action 32-2 is indicated.	**a** Check the MVIP cable and replace it if necessary. Go to *Checking cables, page 394*. **b** Then return here by clicking the on-screen ◄◄ button.
2 You find a defective MVIP cable.	Restart the server. See if the switch fabric test passes.
3 switch fabric tests pass after you replace the MVIP cable.	Stop here.
4 The MVIP cable is OK, or the switch fabric tests fail again.	**a** Type **showalarm data=hw-long ENTER**. Examine the **AUX** field of the output screen. **b** Using the AUX value and the list in *Figure 13*, identify the failed card. **c** Replace the PRI card. Go to *PRI card maintenance, page 362*. **d** Then return here by clicking the on-screen ◄◄ button. **e** Restart the server. See if the switch fabric test passes.

If	Then
5 The switch fabric tests pass after you replace the PRI card.	Stop here.
6 The switch fabric tests fail after you replace the PRI card.	Get technical support. Go to *Repair Number 0 - Escalate to MACS*.

2 of 2

Slot - Port	T1 hex	T1 decimal	E1 hex	E1 decimal
I5-1	50118	327960	50110	327952
I5-2	50218	328216	50210	328208
I4-1	40118	262424	40110	262416
I4-2	40218	262680	40210	262672
I3-1	30118	196888	30110	196880
I3-2	30218	197144	30210	197136
I2-1	20118	131352	20110	131344
I2-2	20218	131608	20210	131600

Figure 13. AUX Values for failed PRI cards

Repair Number 33 - Kernel Call Failed

Part of the SNMP (Simple Network Management Protocol) interface software has failed. Make a note of the error code that you retrieved from the alarm log in case you need to call for technical support. Then, in the chart below, find the error code, and perform the associated repair.

Codes	Repair Action
50320-43	*Repair Action 33 - 1*

Repair Action 33 - 1

The SNMP interface is not functioning correctly. Consult the chart below.

If	Then
1 Repair Action 33-1 is indicated.	Restart the server. Type **reset level=boot ENTER**.
2 The alarm persists after a reset.	Get technical support. Go to *Repair Number 0 - Escalate to MACS*.

Repair Number 34 - Video Driver Errors

MMCX could not start the video driver. The MMCX video driver handles video transmissions over the network (*not* the *VGA video card installation, page 370* used for console video). Make a note of the error code that you retrieved from the alarm log in case you need to call for technical support. Then, in the chart below, find the error code, and perform the associated repair.

Codes	Repair Action
55431 55440	*Repair Action 34 - 1*

Repair Action 34 - 1

The video driver would not load. Video driver files may be missing or damaged. Consult the chart below.

If	Then
1 Repair Action 34-1 is indicated.	Look for the video driver file, **video**. a Type **cd /dev ENTER**. b Type **ls video ENTER**.
2 The video driver file exists.	See if the WILD card driver is installed by typing **drivers ENTER** (the video driver is part of the WILD-card driver).
3 **drivers** does not list **WildDriver**.	Driver information may be in an inconsistent state. Restart the server. Type **reset level=boot ENTER**.
4 The alarm persists.	Backup the system files. Go to *Backing up server system files, page 318*. Then return here by clicking the on-screen ◄◄ button.
5 You have backed up the system.	Reinstall the MMCX application software. Go to *Installing MMCX server software, page 345*. Then return here by clicking the on-screen ◄◄ button.
6 You have reinstalled the server software.	Restore the server software. Go to *Restoring server system files, page 347*. Then return here by clicking the on-screen ◄◄ button.
7 The alarm recurs.	Get technical support. Go to *Repair Number 0 - Escalate to MACS*.

Repair Number 35 - WILD Card Download Errors

The WILD card did not download the firmware correctly. Make a note of the error code that you retrieved from the alarm log in case you need to call for technical support. Then, in the chart below, find the error code, and perform the associated repair.

Codes	Repair Action
55314 55333	*Repair Action 35 - 1*
55484-87	*Repair Action 35 - 2*

CAUTION:
Some repair actions reinitialize the PRI card using the **initcard** command. When you run **initcard** against slot i5, MVIP timing is momentarily interrupted. *Sometimes* this interferes with the WILD card and results in the loss of audio. If this happens, you must restart the server by typing **reset level=cold1 ENTER** to restore service.

Repair Action 35 - 1

The WILD card is in an abnormal state. Consult the chart below.

If	Then
1 Repair Action 35-1 is indicated.	Check for other WILD card/MVIP alarms that might be the ultimate cause of the problem. Type **showalarm data=hw-long ENTER**.
2 Other WILD-card errors are logged.	Perform the repairs specified by the alarm messages. Then return here by clicking the on-screen ◄◄ button.
3 No WILD-card errors are logged or the alarm persists after all other errors have been corrected.	Reinitialize the card. **a** Type **busywild slot=*slot-num* ENTER**. **b** Type **initcard slot=*slot-num* ENTER**. **c** Type **rlswild slot=*slot-num* ENTER**.
4 The problem persists after running **initcard**.	Replace the WILD card. Go to *WILD card maintenance, page 374*. Then return here by clicking the on-screen ◄◄ button.
5 The problem recurs after you replace the WILD card.	Get technical support. Go to *Repair Number 0 - Escalate to MACS*.

Repair Action 35 - 2

The WILD card could not download firmware successfully. Consult the chart below.

If	Then
1 Repair Action 35-2 is indicated.	See if the download file, **wild2rtp.S** exists, and make sure it is readable. **a** Type **cd etc/images ENTER** to get to the correct directory. **b** Type **ls -l wild2.S ENTER** to list the file attributes and permissions.
2 You do not see the download file	Ask technical support to install a usable WILD card download file. Go to *Repair Number 0 - Escalate to MACS*.

Repair Number 36 - inittab File Errors

A system file has caused a configuration problem. Make a note of the error code that you retrieved from the alarm log in case you need to call for technical support. Then, in the chart below, find the error code, and perform the associated repair.

Codes	Repair Action
33018-19 55356-57	*Repair Action 36 - 1*

Repair Action 36 - 1

Consult the chart below.

If	Then
1 Repair Action 36-1 is indicated.	The problem may be temporary. Restart the server. Type **reset level=cold1 ENTER**.
2 The alarm is cleared.	Stop here.
3 The problem persists.	Get help. Go to *Repair Number 0 - Escalate to MACS*

Repair Number 37 - ATM Internal Looparound Failure

The ATM card or PCI bus caused a looparound test failure. Make a note of the error code that you retrieved from the alarm log in case you need to call for technical support. Then, in the chart below, find the error code, and perform the associated repair.

Codes	Repair Action
2304	*Repair Action 37 - 1*

Repair Action 37 - 1

The ATM card is bad, or there is a faulty connection somewhere on the PCI bus. Consult the chart below.

If	Then
1 Repair Action 37-1 is indicated.	Check the PCI bus. **a** Move the external looparound from the cable to the socket on the backplane of the Ethernet card. **b** Reset the server by typing **reset level=cold2 ENTER.** **c** Examine the console or the log file for the results.
2 The ATM, CPU, WILD, and Ethernet cards (if installed) are **found**.	The PCI bus is functioning properly, and the cards are connected properly. *Go to step 5*.
3 The ATM, CPU, WILD, and Ethernet cards (if installed) are not **found** even though they are physically installed.	A card or cable may be loose. **a** Use the procedure in *Powering down, page 403*, to turn the server off gracefully. Then return here by clicking the on-screen ◄◄ button. **b** Make sure that all circuit cards (including Ethernet and the CPU) are fully seated in the server backplane. **c** Restart the server.

If	Then
4 The ATM, CPU, WILD, and Ethernet cards (if installed) are correctly seated and cabled but are not **found**.	Suspect a PCI bus problem. Go to *Repair Action 38 - 1*.
5 The PCI bus seems OK.	Replace the ATM card. Go to *ATM card maintenance, page 371*.
6 The problem persists after you replace the ATM card.	Contact technical support. Go to *Repair Number 0 - Escalate to MACS*.

Repair Number 38 - PCI Bus Errors

The CPU cannot communicate properly with circuit cards and peripheral devices. Data has been corrupted or lost. Make a note of the error code that you retrieved from the alarm log in case you need to call for technical support. Then, in the chart below, find the error code, and perform the associated repair.

Codes	Repair Action
3372-77 1024-29 1034 1038	*Repair Action 38 - 1*

Repair Action 38 - 1

Poor connections between circuit cards and the bus backplane, defective bus interfaces on individual cards, incorrectly set BIOS options, or software running on an installed board can all cause PCI bus errors. Consult the chart below.

If	Then
1 Repair Action 38-1 is indicated.	Turn off the server using the procedure in *Powering down, page 403*. Then return here by clicking the on-screen ◄◄ button.
2 The server is OFF.	Check the connection between the CPU card and the PCI bus. Go to *CPU card maintenance, page 356*. Then return here by clicking the on-screen ◄◄ button.
3 The CPU card is firmly seated in the PCI bus.	Check the connection between the Ethernet card and the PCI bus. Go to *Ethernet card maintenance, page 367*. Then return here by clicking the on-screen ◄◄ button.
4 The Ethernet card is firmly seated in the PCI bus, and an ATM card is installed.	Check the connection between the ATM card and the PCI bus. Go to *ATM card maintenance, page 371*. Then return here by clicking the on-screen ◄◄ button.
5 The ATM card is firmly seated, or no ATM card is installed.	Check the connection between the WILD card and the PCI bus. Go to *WILD card maintenance, page 374*. Then return here by clicking the on-screen ◄◄ button.

If	Then
6 The WILD card is firmly seated in the PCI bus.	Power up the server. Watch the initialization test results. Are the cards in the PCI bus **found**?
7 The cards installed in the PCI bus are not **found**.	**a** Turn off the server using the procedure in *Powering down, page 403*. Return here by clicking the on-screen ◄◄ button. **b** Replace the CPU card. Go to *CPU card maintenance, page 356*. Then return here by clicking the on-screen ◄◄ button. **c** Power up the server.
8 The cards installed in the PCI bus are not **found** after you change the CPU card.	**a** Turn off the server using the procedure in *Powering down, page 403*. Return here by clicking the on-screen ◄◄ button. **b** Replace the Ethernet card. Go to *Ethernet card maintenance, page 367*. Return here by clicking the ◄◄ button. **c** Power up the server.
9 The cards installed in the PCI bus are not **found** after you change the Ethernet card.	**a** Turn off the server using the procedure in *Powering down, page 403*. Return here by clicking the on-screen ◄◄ button. **b** Replace the ATM card. Go to *ATM card maintenance, page 371*. Then return here by clicking the on-screen ◄◄ button. **c** Power up the server.

If	Then
10 The cards installed in the PCI bus are not **found** after you change the ATM card.	**a** Turn off the server using the procedure in *Powering down, page 403*. Return here by clicking the on-screen ◄◄ button. **b** Replace the WILD card. Go to *WILD card maintenance, page 374*. Then return here by clicking the on-screen ◄◄ button. **c** Power up the server.
11 The cards installed in the PCI bus are **found** during initialization, and the alarm clears.	Stop here. The last card that you replaced was bad.
12 The cards installed in the PCI bus are not **found** after all cards have been replaced, and/or the alarm has not cleared.	Get help. Go to *Repair Number 0 - Escalate to MACS*

Repair Number 39 - Endpoint Errors Reported to Server

The server cannot communicate with a client. The client software notifies the user and then terminates. Make a note of the error code that you retrieved from the alarm log in case you need to call for technical support. Then, in the chart below, find the error code, and perform the associated repair.

Codes	Repair Action
65536-38	*Repair Action 39 - 1*

Repair Action 39 - 1

Consult the chart below.

If	Then
1 Repair Action 39-1 is indicated.	Tell the user to restart the MMCX client application using the procedure specified in the *MMCX User's Guide*.
2 The alarm is cleared.	Stop here.
3 The problem persists.	Get help. Go to *Repair Number 0 - Escalate to MACS*

Repair Number 40 - ATM Facility Problems

ATM communications have failed, possibly because a fiber or cable has been cut or disconnected. Make a note of the error code that you retrieved from the alarm log in case you need to call for technical support. Then, in the chart below, find the error code, and perform the associated repair.

Codes	Repair Action
2148	*Repair Action 40 - 1*

Repair Action 40 - 1

Consult the chart below.

If	Then
1 Repair 40-1 is indicated.	Make sure that both fiber-optic ATM cables are connected to the plugs in the ATM card. See *Figure 14*.
2 The alarm is cleared.	Stop here.
3 The alarm persists.	Isolate the fault with looparound tests. Install an ATM-type (fiber optic) looparound in the jacks on the back of the ATM card. Type **reset level=cold2 ENTER**.
4 The external looparound test passes.	The card is OK. The problem lies somewhere along the LAN. Inform the ATM network administrator.
5 The external looparound test fails.	The card is faulty. Replace it. Go to *ATM card maintenance, page 371*.
6 The alarm persists after you have replaced the ATM card and/or after the LAN administrator has pronounced the network OK.	Get help. Go to *Repair Number 0 - Escalate to MACS*.

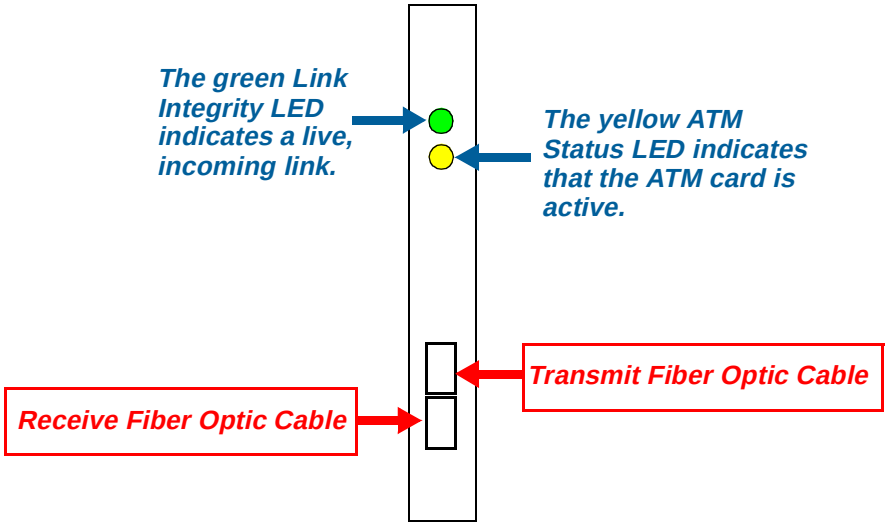


Figure 14. ATM card cable connections and LED indicators

Repair Number 41 - ATM Link & Software Configuration

An ATM software error has occurred, possibly because of a lack of free resources. Make a note of the error code that you retrieved from the alarm log in case you need to call for technical support. Then, in the chart below, find the error code, and perform the associated repair.

Codes	Repair Action
54017 54019-22 54024-31 54028 54031 54116-29 54131-36 54139	*Repair Action 41 - 1*

Repair Action 41 - 1

Consult the chart below.

If	Then
1 Repair Action 41-1 is indicated.	Check for other ATM-related alarms. Type **showalarm data=hw-long ENTER** to view the alarm log.
2 ATM-related alarms are logged.	**a** Clear these alarms first, using the procedures specified in the alarm-log entries. **b** Then restart the server by typing **reset level=cold2 ENTER**.
3 The alarm corresponding to Repair 41-1 is cleared.	Stop here.
4 The alarm corresponding to Repair 41-1 persists.	Make sure that both fiber-optic ATM cables are connected to the plugs in the ATM card. See *Figure 14*.
5 The alarm is cleared.	Stop here.
6 The alarm persists.	At the console, type **showatm ENTER** to display the current state of the ATM interface.
7 **showatm** indicates that an IP address is incorrectly specified.	Correct the address. Type **chgatm slot=*slot-number* port=*port-number* ip=*IP-address* mask=*netmask-value***, and press **ENTER**.

If	Then
8 **showatm** indicates that an IP address is missing.	Add the address. Type **addatm slot=*slot-number* port=*port-number* ip=*IP-address* mask=*netmask-value***, and press **ENTER**.
9 Correcting the IP addresses clears the alarm.	Stop here.
10 The IP addresses appear to be correct, but the problem persists.	Reinitialize by removing and then re-adding the interface. a Type **rmatm slot=*slot-number* port=*port-number***. b Then type **addatm slot=*slot-number* port=*port-number***.
11 The alarm persists.	Isolate the fault with looparound tests. Install an ATM-type (fiber optic) looparound in the jacks on the back of the ATM card. Type **reset level=cold2 ENTER**.
12 The external looparound test passes.	The card is OK. The problem lies somewhere along the LAN. Inform the ATM network administrator.
13 The external looparound test fails.	The card is faulty. Replace it. Go to *ATM card maintenance, page 371*.
14 The alarm persists.	Get help. Go to *Repair Number 0 - Escalate to MACS*.

Repair Number 42 - Initialization Errors

A software process has terminated abnormally. Make a note of the error code that you retrieved from the alarm log in case you need to call for technical support. Then, in the chart below, find the error code, and perform the associated repair.

Codes	Repair Action
39033 45065-72 45097 61440-41	*Repair Action 42 - 2*
61442	*Repair Action 42 - 1*

Repair Action 42 - 1

A process had to be restarted 1-4 times (for a minor alarm) or 5+ times (for a major alarm). Consult the chart below.

If	Then
Repair Action 42-1 is indicated.	Get help. Go to *Repair Number 0 - Escalate to MACS*

Repair Action 42 - 2

The server had to restart to recover from the abnormal termination of an MMCX process. Consult the chart below.

If	Then
1 Repair Action 42-2 is indicated.	Monitor the restart. Go to *Server startup problems, page 131*, if necessary.
2 The server does not return to the normal state, **Active IS**.	Try resetting the server again. Type **reset level=boot ENTER**.
3 The server does not return to the normal state, **Active IS**, or new alarms appear.	Get help. Go to *Repair Number 0 - Escalate to MACS*.

Repair Number 43 - Hardware busied out

A B Channel, WILD card, or PRI card has been taken out of service. Make a note of the error code that you retrieved from the alarm log in case you need to call for technical support. Then, in the chart below, find the error code, and perform the associated repair.

Code	Repair Action
18	*Repair Action 43 - 1*

Repair Action 43 - 1

Hardware may be busied out for a variety of reasons. A channel or device may have been taken out of service following a failure. Or an administrator may have simply forgotten to release it after normal maintenance. Proceed as follows.

If	Then
Repair Action 43-1 is indicated.	Search the alarm log for related alarms. Type **showalarm data=hw-long state=active | more ENTER**, and examine the output.
The log records possibly related WILD and/or PRI alarms.	Correct the alarm condition, using the repair procedure specified in the **RPR** field of the log (for information on interpreting log entries, see *Viewing and interpreting alarm messages*).
No related alarm conditions are logged.	Release the busied out hardware. • To release B Channels, **type rlspri slot=*slot-number* port=*port-number* data=tg ENTER**. • To release D Channels, type **rlspri slot=*slot-number* port=*port-number* data=dchan ENTER**. • To release a WILD card, type **rlswild slot=*slot-num* ENTER**.

9 Service, upgrade, & recovery procedures

This chapter covers routine servicing and generalized repair procedures that apply to many of the alarm and repair situations discussed elsewhere in this volume. For alarm-specific repair information, consult the preceding chapter.

Maintaining the MMCX server

This unit describes the normal, non-emergency procedures that an MMCX administrator must perform either routinely or in the course of repairs specified in *Chapter 8, "Repairs" on page 156*.

Backing up server system files

The MMCX backup process copies system files specified by a backup source file (such as ***/mmcs/backrest/backup.txt***) to a designated location. You can perform backups from the command line, using the *BACKUP* command, or from the software administration menu. Always do first-time backups from the menu, however. The backup utility on the software administration menu lets you designate the target host and directory information that command-line backups require.

WARNING:
Both backup procedures overwrite previous backup files in the target host and directory. If this is not what you want to do, backup the target files or designate a different backup target host and directory.

Backing up from the software administration menu

Proceed as follows.

1. Mount the target host file system and format backup media (diskettes, tapes, etc) as needed.
2. Type **reset level=menu ENTER** to display the nine-item software administration menu.
3. At the prompt, type **2 ENTER** to select **System Backup - Perform a System backup of system files.**
4. When the system backup menu appears, press **2 ENTER** to select the backup sub-menu.
5. From the backup menu, press **1 ENTER** to select **Display current backup information**.
   The server displays current backup information (*Figure 1*) and returns you to the backup menu.

```
Latest backup information
DATE   TIME    STATUS                  AVAILABLE   DESTINATION
01/01/93 01:38 PM SUCCEED              No          LOCAL:/mmcs/backrest
01/01/93 02:51 PM SUCCEED              No          LOCAL:/mmcs/backrest
01/01/93 03:08 PM SUCCEED              No          LOCAL:/mmcs/backrest
01/01/93 03:10 PM SUCCEED              No          LOCAL:/mmcs/backrest
01/01/93 03:15 PM SUCCEED              No          LOCAL:/mmcs/backrest
01/01/93 03:16 PM SUCCEED              No          LOCAL:/mmcs/backrest
01/01/93 03:19 PM SUCCEED              No          LOCAL:/mmcs/backrest
01/01/93 03:23 PM SUCCEED              No          LOCAL:/mmcs/backrest
01/01/93 05:49 PM SUCCEED              Yes         LOCAL:/mmcs/backrest
01/01/93 08:21 PM SUCCEED              Yes
```

Figure 1. Backup information

6 To change the target host and directory name, press **2 ENTER**. Otherwise skip to step 10.

7 At the prompt, type the new target host name, and press **ENTER**. Or just press **ENTER** to keep the default.

8 Enter the new target directory name, and press **ENTER**. Or press **ENTER** to keep the default. directory name.

9 Enter the new user name, and press **ENTER**.

The server returns you to the backup sub-menu.

10 At the prompt, press **3 ENTER** to select **Start backup**.

The server warns you that **backup will overwrite any previous backup saved on the above network site** and asks for confirmation.

11 Press **Y ENTER** to continue with the backup and return to the backup sub-menu. Or press **N ENTER** to abort, and go back to step 6.

12 When the backup sub-menu appears, press **4 ENTER** to return to the software administration menu.

13 Then press **5 ENTER** to restart the MMCX application.

The server reboots to the in-service state.

Backing up from the command line

Command-line **backup** differs from the version on the software administration menu: you can back up from the command line without stopping the MMCX application and without rebooting the server. *Note that you cannot restore system files from the command line; you must use the software administration menu.* To backup, proceed as follows.

1 At the command prompt, type **backup** **host=*hostname*** **dir=*dirname*** **user=*username***.

If you issue the command without the optional, grayed-out parameters, backup uses the defaults you set from the software administration menu. Otherwise, the parameters entered here override the defaults.

2 When backup asks you for confirmation, type **Y ENTER** to proceed or **N ENTER** to abort.

Backup copies the system files to the target.

Resetting the server

The **reset** command lets you shut down or reinitialize the system gracefully, avoiding file system corruption and consequent data loss. Proceed as follows.

However, **halt**, **menu**, **cold1**, and **cold2** cause **reset** to write cached operations to the hard drive so that the system restarts gracefully. When you call reset with the **thresh** or **mask** options, on the other hand, active sessions can continue at the endpoints.

1 Check for logged-on users, if **reset** might end their sessions. When **level=halt**, **menu**, **cold1**, or **cold2**, **reset** terminates all active sessions at the end-points and writes cached operations to the hard drive. When **level=thresh** or **mask**, **reset** does not disturb active sessions at the endpoints.

a To list logged-in users, type **who ENTER**.

b To identify unfamiliar login names, type **showusr login=*unfamiliar_login* ENTER**.

2 To reset the server, type reset **level=*reset_type* ENTER.**

reset_type is one of the following.

- **halt** forces complete reinitialization of the system. It does everything the other parameters do, and it terminates all MMCX application processes and shuts down LynxOS.

- **boot** forces the fullest initialization possible using software only. **boot** does everything that **cold2** and **cold1** do. But it also reloads BIOS, reloads the operating system, and reinitializes all system processes.
- **cold2** is actually a sub-set of **boot**. It does everything **cold1** does but also starts the system software without re-executing the BIOS and without restarting LynxOS. **cold2** executes all self-tests and downloads firmware, regardless of the current state of downloaded firmware code. It also tests the installed hardware (WILD cards, PRI Interfaces, Ethernet Interfaces, and ATM Interfaces) and reports the results to the console, debug log, and remote maintenance board (RMB) mailbox.
- **cold1** tells **reset** to do a minimum system initialization. It terminates most application processes and the system reinitializes to the in-service state. As long as vintage and integrity checks for the corresponding devices pass, **cold1** does not bother to download new copies of device firmware. If the vintage and integrity checks fail, **cold1** acts like **cold2** and resets the hardware. It reports installed hardware (WILD cards, PRI cards, Ethernet cards, and ATM interfaces) to the console, debug log, and Remote Maintenance Board (RMB) mailbox, but it does not do any hardware initialization testing.
- **menu** terminates most application processes and displays the software administration menu. If you choose to continue booting, the menu terminates, and the server reinitializes just as for **cold1**.
- **mask** changes the current selection criteria for logged events. It takes additional parameters.

  loc (“locations”) colon-delimited list of software processes (the default is all locations).

  type is an event type (the default is all types).

  enable lets you include or exclude processes from logging (default is **ON**).

The following example disables logging of trace level 3 messages from the bim process:

reset level=mask loc=BIM type=DEBUG_LVL3 enable=off ENTER.

See *SHOWMASK, page 558*.

- **thresh** changes the alarm parameters.

Administering PRI cards

PRI administration sets the options that let server hardware work with ISDN equipment.

- *Framing* defines the identifying features of the data packets (*frames*) in transmissions.
- *Line-coding* limits the number of successive zeros sent over the telephone network.
- *Line-compensation* makes up for losses caused by the cabling between the server and the nearest switching unit or repeater.
- *Companding* specifies the compression algorithm that encodes voice for PCM transmission.
- *Timing* identifies the timing source that the PRI card uses.

Other options specify switching interfaces, national protocols, error checking, etc. The chart summarizes common maintenance tasks. For fuller descriptions, see *PRIADM, page 521*.

Viewing card status/options	Type **showpri ENTER**.

Changing framing	Type **chgpri slot=*slot* port=*port* frame=*framing* ENTER**. • ***slot*** = the slot where the card is installed • ***port*** = **1** or **2** • for E1 lines, ***framing*** = **e1Basic**, **e1FEBE**, or **e1CRC** for T1 lines, ***framing*** = **ds1ESF** (default) or **ds1SFD4**
Changing line-coding	Type **chgpri slot=*slot* port=*port* lcode=*line-coding* ENTER**. • ***slot*** = the slot where the card is installed • ***port*** = **1** or **2** • ***line-coding*** = **zcs**, **b8zs** (default), **basic** (no ones density protection), or **hdb3**
Changing line compensation	Type **chgpri slot=*slot* port=*port* lcomp=*length-to-repeater* ENTER**. • ***slot*** = the slot where the card is installed • ***port*** = **1** or **2** • ***length-to-repeater*** = **length0to133ft** (default), **length133to266ft**, **length266to399ft**, **length399to533ft**, or **length533to655ft**

To reverse the last jump, press ⇐ on the Acrobat tool bar

Setting up a new PRI interface	Type **addpri slot=*slot* port=*port* ENTER**. • ***slot*** = the slot where the card is installed • ***port*** = **1** or **2** You may have to change one or more of the other options from the default values, particularly if you are administering a system outside the USA. See *PRIADM* for a detailed description of the parameters for addpri.
Removing obsolete PRI interface information	Type **rmpri slot=*slot* port=*port* ENTER**. • ***slot*** = the slot where the card is installed • ***port*** = **1** or **2**

Administering ATM cards

These operations set the parameters that let Asynchronous Transfer Mode (ATM) equipment emulate a local area network (LAN). These include IP addresses, LAN names, and time-outs. You can also change the trade-off between ATM traffic capacity and call quality using the commands covered in this section. The chart below briefly describes typical commands for performing common tasks. For a comprehensive list, see *ATMADM, page 437*.

Viewing card state or options	Type **showatm ENTER**.
Changing an IP address	Type **chgatm slot=*slot* port=*port* ip=*ip_address* mask=*ip_subnet_mask* ENTER**. • ***slot*** = the slot where the card is installed • ***port*** = the port number • ***ip_address*** = the IP address used for LAN emulation • ***ip_subnet_mask*** = the corresponding IP subnet mask
Adjusting the trade-off between line capacity and call quality	Type **chgatm slot=*slot-number* port=*port-number* cap=*capacity* ENTER**. • ***slot*** = the slot where the card is installed • ***port*** = the port number • ***capacity* = 100** Mbps (megabits per second) by default. Increasing this number improves utilization of the line while degrading call quality.

Change the LAN emulation name	Type **chgatm slot=*slot-number* port=*port-number* name=*LAN-name* ENTER**. • ***slot*** = the slot where the card is installed • ***port*** = the port number • ***LAN-name*** = a 32-character alphanumeric identifier that can be used in Configure and Join requests sent to a LAN emulation server
Changing the ATM address	Type **chgatm slot=*slot-number* port=*port-number* addr=*ATM-address* ENTER**. • ***slot*** = the slot where the card is installed • ***port*** = the port number • ***ATM-address*** = 40-digit hexadecimal number that identifies the LAN emulation client to the LAN emulation server.
Setting up a new ATM interface	Type **addatm slot=*slot* port=*port* ip=*ip-address* mask=*ip-subnet-mask* ENTER**. • ***slot*** = the slot where the card is installed • ***port*** = the port number • ***ip-address*** = the IP address used for LAN emulation • ***ip-subnet-mask*** = the corresponding IP subnet mask

To reverse the last jump, press ◄◄ on the Acrobat tool bar

Removing ATM interface information	Type **rmatm slot=*slot-number* port=*port-number* ENTER**. where: • ***slot*** = the slot where the card is installed • ***port*** = the port number Note that the IP address for this ATM interface cannot be reused until the server has been rebooted.

3 of 3

Maintaining wide area networks

Wide area networks (WANs) depend on consistent server identification and correct routing across the network. This section describes the most common administrative tasks.

Server numbers

Server numbers must uniquely identify the servers on the network. Normally, you assign a server name and server number during installation (see *Assigning a server number, page 58*).

Checking the server name and number	Type **showsys ENTER**. See *Figure 1*.

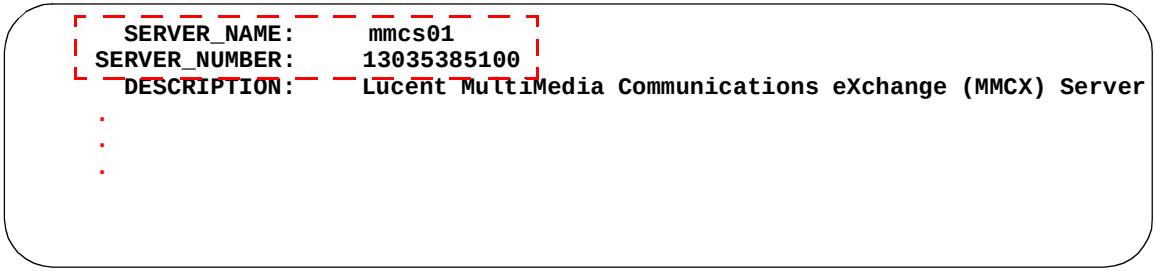


Figure 1. Typical Output of showsys

Interserver Routing Information

To communicate over the network, each server has to know the *Server numbers* of other servers and the *Interserver routing numbers* where they can be reached. For a full description, see *ISRADM, page 490*.

Checking server numbers for interserver routing	Type **showisr ENTER**. See *Figure 2*. Server numbers should be a subset of the interserver routing numbers.

```
SERVER   SRVNUM          AUD VID APP SIG
macs1    13035380100     lan lan lan lan
macs2    13035380200     lan lan lan lan
mmcs02   13035385200     wan wan wan wan
mmcs03   13035385300     wan wan wan wan
mmcs21   13035382100     lan lan lan lan
SERVER   IP_ADDRESSES
macs1    135.9.155.122, -, -, -
macs2    135.9.155.123, -, -, -
mmcs02   -, -, -, -
mmcs03   -, -, -, -
SERVER   NEAR_PPP_ADDR   FAR_PPP_ADDR    ISR_PHONE_NUM   PLAN
macs1    -               -               -               0
macs2    -               -               -               0
mmcs02   125.9.1.2       125.9.2.1       5200            1
```

Server numbers must be unique and must be used consistently.

Figure 2. Typical output of showisr

Interserver routing numbers

To contact other servers, the server has to know the ISDN telephone number (interserver routing number) that goes with each of the *Server numbers* on the network. For a comprehensive listing of ISR number commands and parameters, see *CFGADM, page 458*.

Displaying the interserver ISDN telephone numbers	Type **showisrnum ENTER**.
	A typical listing is shown at right:
	`ISR_PHONE_NUMBER`
	`5100`
	`5385100`
	`3035385100`
	`13035385100`

Adding an interserver ISDN telephone number	Type **addisrnum phone=*isr_phone_number* ENTER**. • ***isr_phone_number*** = the ISDN PRI telephone number other servers use to call this server
Removing an interserver ISDN telephone number	Type **rmisrnum phone=*isr_phone_number* ENTER**. • ***isr_phone_number*** = the ISDN PRI telephone number other servers use to call this server

Dial plans

The dial plan table defines how the server interprets dialed digit strings and translates them into valid telephone numbers. The server has to handle three kinds of dialed input: telephone numbers that come in over the PRI interface, numbers for outgoing calls, and local extension numbers that must be expanded into full telephone numbers. This section covers basic dial-plan administration. For a comprehensive list, see *DPADM, page 466*.

```
DIALED_NUMBER    DIRECTION    SERVER    PLAN DEL DIGITS_TO_ADD
5+               in(1)        -         0    0   -
81+              out(2)       -         1    1   -
83+              out(2)       -         1    1   7
9+               out(2)       -         1    0   -
13035385100      internal(3)  -         0    0   -
1??              internal(3)  macs1     0    0   13035380
2??              internal(3)  macs2     0    0   13035380
51??             internal(3)  -         0    0   1303538
521??            internal(3)  mmcs21    0    1   1303538
52??             internal(3)  mmcs02    0    0   1303538
53??             internal(3)  mmcs03    0    0   1303538
```

Figure 3. Typical dial plan

Displaying dial plan information Type **showdp ENTER**. See *Figure 3*.

Changing dial plan information	Type **chgdp dial=*number* dir=*direction* srv=*server* numdel=*leading-digits* add=*leading-digits* plan=*pri-routing* ENTER**. • ***number*** = the number dialed • ***direction*** = **in**, **out**, or **internal** (where the call originates) • ***server*** = the affected server (optional parameter, defaults to the local server if not specified) • ***leading-digits*** = leading digits to add with **add=** or delete with **numdel=** (optional, defaults to **0**) • ***pri-routing*** = the PRI routing plan number for outgoing calls (optional)
Adding dial plan information	Type **adddp dial=*number* dir=*direction* srv=server numdel=*leading-digits* add=*leading-digits* plan=*pri-routing* ENTER**. • ***number*** = the number dialed • ***direction*** = **in**, **out**, or **internal** (where the call originates) • ***server*** = the affected server (optional parameter, defaults to the local server if not specified) • ***leading-digits*** = leading digits to add with **add=** or delete with **numdel=** (optional, defaults to **0**) • ***pri-routing*** = the PRI routing plan number for outgoing calls (optional)

Removing records from a dial plan	Type **rmdp dial=*number* dir=*direction*** • ***number*** = the number dialed • ***direction*** = **in**, **out**, or **internal** (where the call originates)

3 of 3

Maintaining MMCX user accounts

This section covers common administrative chores for user accounts. See *USRADM, page 577*.

Displaying user information	Type **showusr ENTER**. The display looks something like that in *Figure 4*.
Adding users	Type **addusr login=*login-id* last=*last-name* ext=*extension*** [**first=*first-name***] [**cvr=*covering-number***] [**comment=*comment***] [**pass=*password***] **ENTER**.
Changing user information	Type **chgusr login=*login-id*** [**last=*last-name***] [**first=*first-name***] [**comment=*comment***] **ENTER**.
Adding user passwords	Type **chgpasswd login=*login-id* ENTER**.
Removing users	Type **rmusr login=*login-id* ENTER**.
Displaying user information	Type **showusr** [**login=*login-id***] [**stat=*status-flag***] **ENTER**.

1 of 2

Showing user coverage points	Type **showcvr login=*login-id***
Logging a user off	Type **termusr login**=***login-id***

2 of 2

```
LOGIN    STATUS          EXT     NAME
user1    loggedOut(2)    4802    user1, firstname1
user2    loggedOut(2)    4804    user2, firstname2
user3    loggedOut(2)    4805    user3, firstname3
user4    loggedOut(2)    4806    user4, firstname4
LOGIN    COMMENT
user1    user1-com
user2    user2-com
user3    user3-com
user4    user4-com
```

Figure 4. Typical user administration screen

Maintaining H.323 user records

This section covers common administrative chores for H.323, IP user accounts. See *USRADM, page 577*.

Displaying IP user information	Type **showipusr ENTER**. The display looks something like that in *Figure 4*.
Adding IP users	**addipusr ext=*extension* ipaddr=*ip-address* last=*last-name* [first=*first-name*]**
Changing IP user information	Type **chgipusr ext=*extension* [ipaddr=*ip-address*] [last=*last-name*] [first=*first-name*] [cvr=*covering-number*] ENTER.**
Removing IP users	Type **rmipusr ext=*extension* ENTER.**
Logging an IP user off	Type **termipusr ext=*extension* ENTER.**

```
LOGIN     STATUS          EXT      NAME
james     loggedIn(4)     557800   James Johnston
kappers   loggedOut(2)    552222   Kappers, Dennis
wlk       busy(3)         555674   Kloppman, Walter L.
<ipuser>  loggedIn(4)     557801   Swenson, Gunnar
<ipuser>  loggedIn(4)     557834   Grimsson, Ingvar
```

Figure 5. showipusr output

Performing a file system check

The file system check (**fsck**) utility finds and repairs damaged file systems. It looks for inconsistencies in the inode contents, directory structure, free inode list, and free block list and reports its findings. If it detects orphaned files in the file system, it creates a **/lost+found** directory. If a **/lost+found** directory already exists, fsck creates a new one with the name **/lost+found[*letter*]** where ***letter*** is the highest letter of the alphabet that has not yet been used. The orphaned files are named with their inode numbers.

To execute a file system check, proceed as follows.

1. Power down gracefully (if possible), using the *Powering down, page 403*.
2. Insert the boot floppy disk in the disk drive.
3. Turn the power switch **ON**.
4. When the BIOS and operating system have finished loading, the server asks you to **Please insert boot utility diskette into floppy drive**. Do so and press **ENTER**.

   A four-item menu appears.
5. At the prompt, press **3 ENTER** to select **Escape to shell (ksh).**
6. At the shell prompt, #, type **fsck *file-system-name* ENTER.**

   fsck performs the file check and echoes its progress to the console.
7. Remove the floppy disk from the floppy disk drive.
8. Type **reboot -a ENTER**.

Looparound testing

Many repairs ask you to carry out one or more looparound tests. This section describes the general procedure for performing the tests. During startup of the MMCX application, the server checks its communications circuitry with both *internal* and *external* looparound tests. The server tests the PRI, WILD, Ethernet, and ATM cards and displays the results before going to the **Active** state. Normally, only the internal test passes during startup. External tests require looparound plugs that are usually not installed on an operational server (see *Figure 7*). But, when the internal test fails, you can often isolate the source of a problem by installing looparounds at varying points on the suspect interface. When a test fails, you then examine the log for hardware alarms and perform the repair specified in the log. After you clear the hardware alarm, you restart the server with looparound plugs installed and check again for failures and alarms.

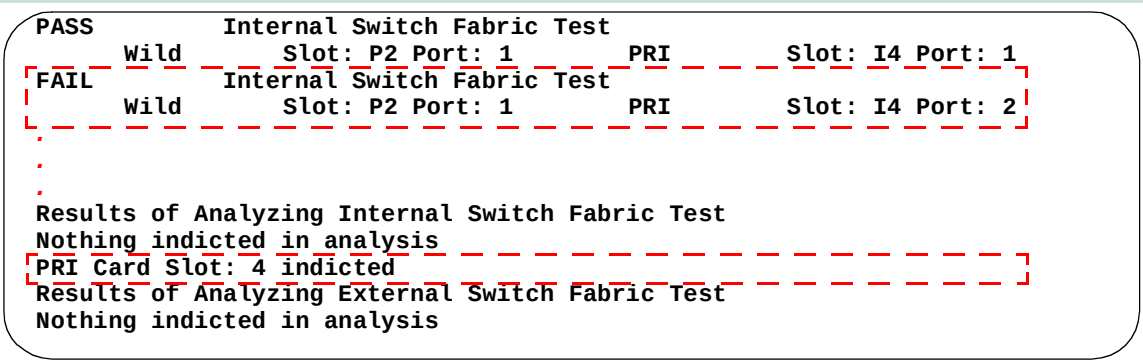


Figure 6. Results of a failed external looparound (switch fabric) test

Looparound plugs

Lucent ships external looparound plugs for each Ethernet and PRI card supplied with the server. ATM-card looparounds are standard fiber-optic patch cords that you have to provide. Representative ATM patch cords and Ethernet and PRI looparounds are shown in *Figure 7*.

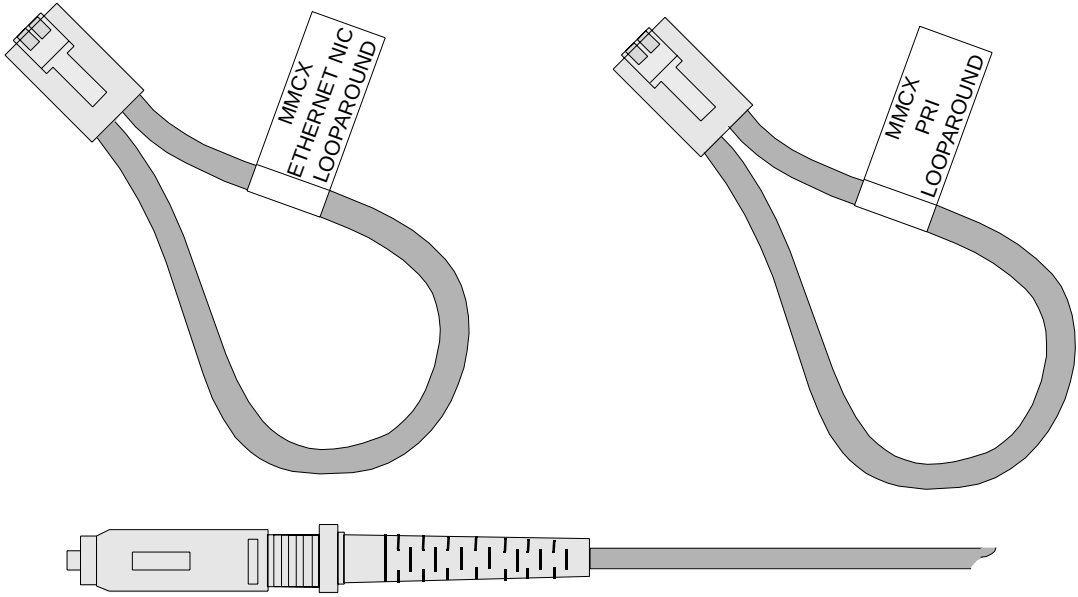


Figure 7. Ethernet and PRI looparound plugs and connector end of an ATM patch cord

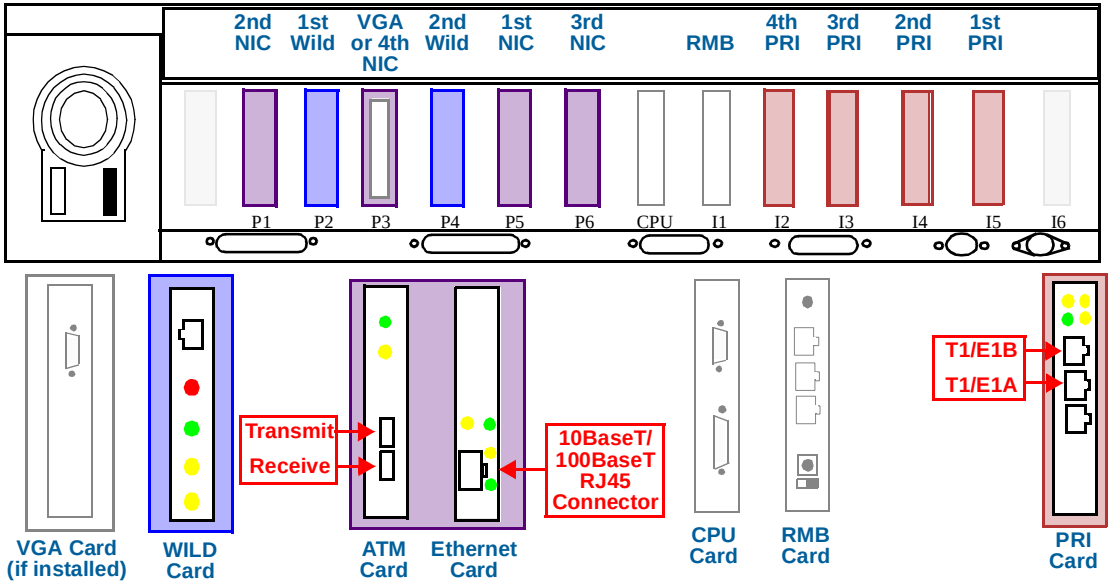


Figure 8. MMCX server backplane

Installing the looparounds

To install and use looparound plugs, proceed as follows.

1. Plug the Ethernet external loop plugs into the *10BaseT/ 100BaseT RJ45 Connector* on the Ethernet cards unless your network uses AUI connectors, in which case, follow the instructions in *Figure 9*.
2. Plug the PRI external loop plugs into the *T1/E1A* and *T1/E1B* interface connectors on the PRI cards.
3. Obtain a fiber-optic patch cord fitted with SC connectors (*Figure 7*). Connect one end to the *Transmit* connector on the ATM card and connect the other end of this same cord to the *Receive* connector on the same card. *Remember that fiber-optic patch cords are standard telecommunications cables. They are not supplied with MMCX servers.*
4. Restart the server. Type **reset level=cold2 ENTER.**
5. Check the alarm log for problems. Type **showalarm ENTER**. Perform the repairs specified in the alarm messages, if any.

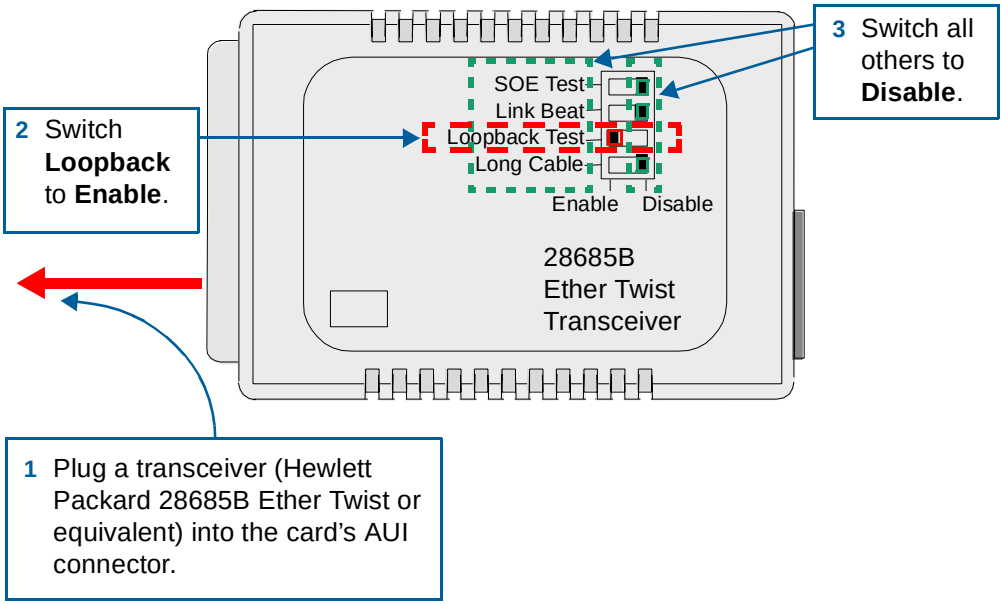


Figure 9. Ethernet transceiver looparound test

Replacing and upgrading server software

This unit explains the procedures for reinstalling software following a system failure (see *Installing MMCX server software, page 345*), loading new releases of the software, and installing patches on the current release.

Installing BIOS upgrades

Proceed as follows.

1. Before you do anything else, type **who ENTER** to see if any one is logged on to the server. *Do not proceed until all users have logged off.*
2. Power down gracefully (if possible). See *Powering down, page 403*.
3. Insert the BIOS upgrade diskette in the floppy disk drive.
4. Turn the power switch **ON** and wait about 10 seconds, and watch for the *BIOS version notice*.

```
      Lucent Technologies, Inc.
      Copyright (C) 1985-1989 Phoenix Technologies Ltd.
      Copyright (C) 1991 Texas Microsystems, Inc.
      All Rights Reserved
The P5120C 120 MHz Industrial Computer BIOS, Version 4.21.1.6
640K Base, 048128K Extended, 256K External Cache
Clearing out all of memory
```

Figure 10. BIOS version notice

When the BIOS is finished loading, the server displays the following.

```
Starting MS-DOS...
A:\>flash.exe
*      Name......P5-75/90/120C
*      Manufacturer.Intel
*      Part Number..28F002T
Flash Functions
                          ENTER: Program New BIOS
                          ESC: Abort and Reset System ;

                          *  Operation...
                          *  Address.....

                          0%            50%            100%
          Copyright (c) 1991-1995 Texas Microsystems, Inc, V1.1q
```

Figure 11. BIOS upgrade installation screen

5 Press **ENTER**.

First **Operation** changes to **ERASING** and **Address** starts updating. A progress bar displays the percentage completed. Then **Operation** changes to **PROGRAMMING** and **Address** continues to update. When the process completes, it prompts you to reboot.

6 Press any key to reboot the server. Make sure that the console displays the new BIOS version.

Installing MMCX server software

This section explains how you install MMCX software, either as part of recovery from a hard disk failure or as part of a routine software upgrade. Proceed as follows.

1. If you are trying to recover from a hard disk failure, do not proceed until you have completed the other procedures listed in *Recovering from a hard disk failure*. If you are installing a patch rather than a full release, use the procedure in *Patching server software* instead.
2. To reach the installation menu, do the following.
   a. Make sure that there are no users logged in.
   b. Type **reset level=menu ENTER**.
3. At the *System menu* prompt, press **4 ENTER** to **Install release software**.

```
WARNING:     Successful installation of a software load may
             REBOOT the system or restart the application.
Do you wish to continue [y or n]?
```

Figure 12. Software load warning

The server displays the warning **Successful installation of a software load may REBOOT the system or restart the application** and asks if you want to proceed.

4. Press **Y ENTER**.

The system prompts you for a **source host**. For a new release, this is the location of the new installation set, either a local CD-ROM or a remote FTP site.

5 Type the ***ftp-source-host-IP-address***, and press **ENTER**.

The system prompts you for a **host user name**.

6 Type the ***ftp-host-user-name***, and press **ENTER**.

The server prompts you for a **source directory**.

7 Type the ***source-directory***, and press **ENTER**.

The system displays your entries and asks if you want to continue.

8 Check the information. If correct, press **Y ENTER** to display the *MMCX software installation screen*. Otherwise, press **N ENTER** to return to step 4.

```
Make the installation directory /mnt/nodes/install
Start installation files transfer at: Wed Aug 21 19:26:18 WET 1996
FTP files from 135.9.144.64:/dr/mmcs/int7/mmcsr2p2.pj/vdsk/nodes/install to
/mnt/nodes/install
Password:
```

Figure 13. MMCX software installation screen

9 At the prompt, enter your ***password***, and press **ENTER**. The server unpacks needed files.

10 Type the ***server-number*** at the prompt, and press **ENTER**.

Watch disk activity LED to verify files are being transferred. The install process reports its progress on the console, but not immediately. You will not see anything for about 4 minutes.

When installation is complete, the server reboots to an in-service state.

Restoring server system files

When you install a new software release or reinstall software after a catastrophe, such as a hard disk failure, you lose the configuration, administration, and routing information stored in the MMCX system files. **Restore** recreates these files using copies saved during backup (see *Backing up server system files*). Proceed as follows.

1. Make sure nobody is logged on. Use the **who** and **showusr** commands.
2. Type **reset level=menu ENTER** to display the nine-item software administration menu.
3. Press **3 ENTER** to display the restore five-item menu.
4. Press **1 ENTER** to **Display current backup information** (*Figure 14*).

   The server displays the available backup sets and returns to the restore menu.

```
Latest backup information
DATE   TIME    STATUS                  AVAILABLE      DESTINATION
01/01/93 01:38 PM SUCCEED              No             LOCAL:/mmcs/backrest
01/01/93 02:51 PM SUCCEED              No             LOCAL:/mmcs/backrest
01/01/93 03:08 PM SUCCEED              No             LOCAL:/mmcs/backrest
01/01/93 03:10 PM SUCCEED              No             LOCAL:/mmcs/backrest
01/01/93 03:15 PM SUCCEED              No             LOCAL:/mmcs/backrest
01/01/93 03:16 PM SUCCEED              No             LOCAL:/mmcs/backrest
01/01/93 03:19 PM SUCCEED              No             LOCAL:/mmcs/backrest
01/01/93 03:23 PM SUCCEED              No             LOCAL:/mmcs/backrest
01/01/93 05:49 PM SUCCEED              Yes            LOCAL:/mmcs/backrest
01/01/93 08:21 PM SUCCEED              Yes
      mwick@135.9.144.64:/dr/mmcs/dev7/ws/mwick/p42bkup2.pj
```

Figure 14. Current backup information

5 If you want to use a source host name, directory name, and user name other than the defaults, press **2 ENTER**.

   a Then, at the prompt, type ***new-host-name*** **ENTER**.

   b Type ***new-directory-name*** **ENTER** to change the directory name.

   c Then type ***new-user-name*** **ENTER**.

   The server then returns to the restore sub-menu.

6 To start the restore operation, press **3 ENTER**, for **Start restore**.

   The server warns you that **This restore will overwrite any previous restore saved on the above network site** and asks for confirmation.

7 Press **Y ENTER** to start the restore process and overwrite existing files, **N ENTER** to abort.

   The server returns you to the restore menu.

8 Press **4 ENTER** to return to the software administration menu.

9 Press **5 ENTER** to restart the MMCX application.

   The server reboots to the in-service state.

Patching server software

Patches are minor upgrades or modifications to the MMCX software or LynxOS operating system. They incorporate useful or necessary changes that do not warrant a full, new release. This section explains how you install and uninstall MMCX patches. Proceed as follows.

1 Make sure no one is logged on (use **who** and **showusr**).

2 Type **reset level=menu ENTER** to display the nine-item software administration menu

3 Press **4 ENTER** to select **Install release software**.

4 Press **2 ENTER** to select **Patch a Currently Installed Release**, and go to *Installing a patch*. Or press **3 ENTER** to select **Remove a Previously Installed Patch**, and go to *Uninstalling a patch*.

Installing a patch

Selecting option **2** of the **Install release software** menu starts the patching process. Proceed as follows.

1 The server warns you that **Successful installation of a software load may REBOOT the system or restart the application** and asks you to confirm your choice. Press **Y ENTER** to proceed.

The server prompts you for a source host.

2 Type ***source-host-name***, and press **ENTER**.

If ***source-host-name*** specifies a remote host, the server prompts you for an FTP user name.

3 If the server asks for an FTP user name, type ***ftp-host-user-name*** **ENTER**.

The server prompts you for the source directory.

4 Type the ***source-directory*** **ENTER**.

The server displays the information you have entered and asks for confirmation.

5 Press **Y ENTER** to continue, **N ENTER** to abort.

If you pressed **Y**, the patch installs, reports its progress on screen, and returns to the **Install release software menu**. If there is an error, the install terminates and displays an error message. If you enter **N**, it goes straight to the menu.

6 Press **4 ENTER** to return to the software administration menu.

7 From the software administration menu, press **5 ENTER** to restart the server.

Uninstalling a patch

Option **3** of the software installation menu displays a list of currently installed patches. *You must remove patches in the order listed* (if you select **2** or **3** before removing **1**, none get removed). While the exact procedure varies, depending on the patches installed, the following example is fairly typical. There are three patches.

Before you start, the server warns you that **Successful installation of a software load may REBOOT the system or restart the application** and asks you to confirm your choice.

1 Press **Y ENTER** to continue.

A patch list appears (*Figure 15*). Your patch numbers will be different from those shown.

Figure 15. List of installed patches

2 At the prompt, type **1 ENTER** to select the first patch in the list (the last patch installed).

The patch is removed. Then the server displays a revised list.

```
1) 01.00.054.2
2) 01.00.054.1
q) Quit
?) Help
```

Figure 16. List of remaining patches

3 At prompt, press **1 ENTER** to remove the next patch.

4 Continue until you have removed all the patches that you want to uninstall.

5 Press **4 ENTER** to return to the software administration menu.

6 Press **5 ENTER** to reboot.

Activating alternative software installations

MMCX lets you keep different versions of the MMCX software installed on the server. Only one version can be active at any one time, of course. To activate a different version, proceed as follows.

1 From the nine-item software administration menu, type **4 ENTER** to select **Install release software**.

2 From the **Install release software** menu, type **4 ENTER** to select **Set another release active**.

The software load-selection menu appears (*Figure 17*). The asterisk indicates the active software release (your numbers will be different).

```
Select software load to activate (* - current active release).
1.  01.01.107.0
2.  01.01.106.0*
q.  Quit
?.  Help
```

Figure 17. Alternate software load menu

3 Press ***n*** **ENTER** where ***n*** is the item number corresponding to the release you wish to activate. The server loads the software release and reboots to the in-service state.

Maintaining and replacing server hardware

This unit covers upkeep and replacement of MMCX server components. When you carry out the procedures described below, pay special attention to ***WARNING*** and ***DANGER*** messages. Incorrect hardware maintenance can damage server components or cause serious injuries. Be especially careful to remember the following.

DANGER:

Computer power supplies are dangerous! Do not perform any maintenance on the server until you follow the procedures to power down the server. See *Powering down, page 403*.

WARNING:

Static discharge can ruin sensitive electronic components! Before attempting any maintenance on the chassis, be sure to wear a grounding wrist strap or other static-dissipating device.

Understanding the server layout

Refer to the figures below for the general layout of the MMCX server.

Component	
1	PRI Cards
2	Remote Maintenance Board
3	CPU Card
4	Network Interface Cards (ATM or Ethernet)
5	WILD Cards
6	Card Clamp
7	Power Supply
8	Floppy Disk Drive
9	Hard Disk Drive
10	Filter
11	Fans

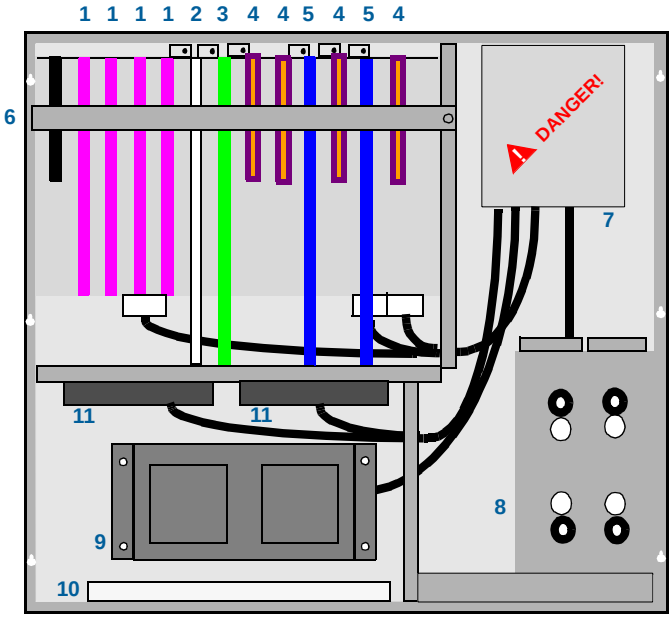
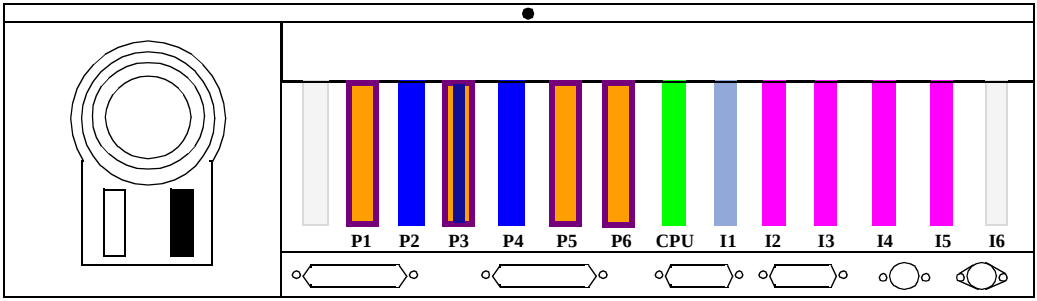


Figure 18. Server chassis, top view



Slot	Circuit card	Slot	Circuit card
P1	Network Interface Card (Ethernet or ATM)	CPU	CPU Card
P2	WILD Card	I1	Remote Maintenance Board
P3	VGA Video Card or Third NIC	I2	PRI Card
P4	WILD Card	I3	PRI Card
P5	Network Interface Card (Ethernet or ATM)	I4	PRI Card
P6	Fourth NIC	I5	PRI Card

Figure 19. Server chassis, rear view

CPU card maintenance

This section covers installation, removal, and replacement of central processing unit (CPU) circuit boards.

DANGER:
Do not perform any maintenance on the server until you follow the procedures to power down the server. See *Powering down, page 403*.

WARNING:
Before attempting any maintenance on the chassis, be sure to wear a grounding wrist strap or other static-dissipating device.

Removing the CPU card

See *Figure 18* for the location of the CPU card and associated hardware. Then proceed as follows.

1. Power down gracefully (if possible), using the *Powering down*.
2. Disconnect the dumb terminal or PC cable from the serial port on the CPU card.
3. Remove the server top cover.
   a. Loosen but do not remove the six screws on the left and right sides of the top cover.
   b. Remove the rear screw from the cover.
   c. Slide the cover towards the rear of the chassis and lift the cover away.
4. Remove the card clamp from the server chassis, and remove the screw that holds the card.
5. Disconnect the floppy controller cable from connector J6.

6 Disconnect the SCSI controller ribbon cable from connector J2.

7 Disconnect the LED drive cable from connector JP15.

8 Pull the CPU card up to disconnect it from the static board connector, and remove it.

9 See *Configuring a replacement CPU card, page 358* before replacing the CPU card.

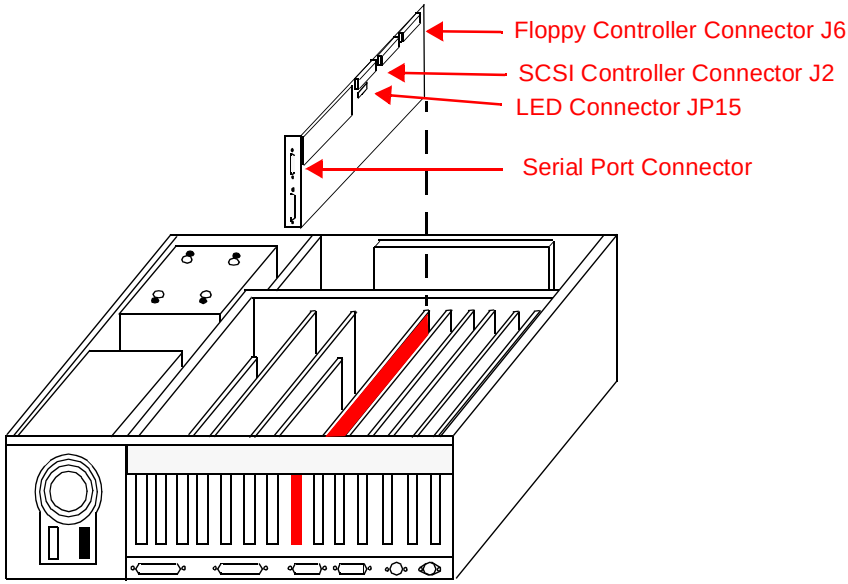


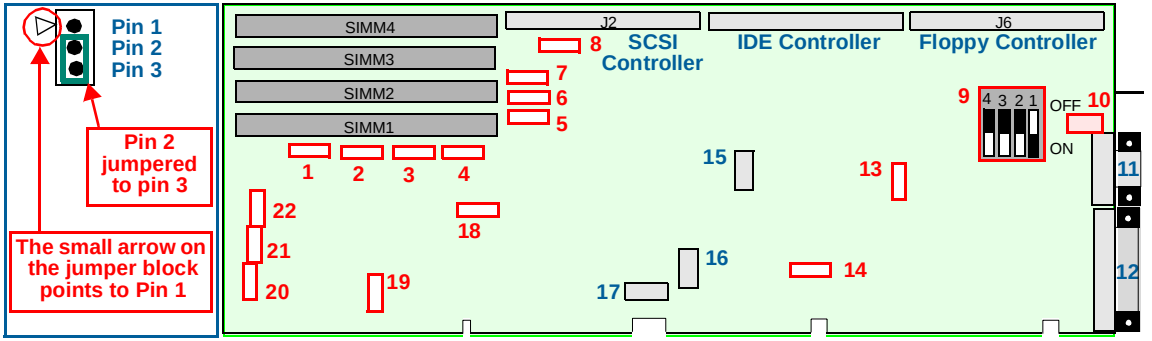
Figure 20. Replacing the CPU card

Configuring a replacement CPU card

Before installing the new CPU card, check the jumper settings and switch settings to be sure they match the specifications in the charts below. The CPU card is configured at the factory before it is shipped, and the settings should be correct. But checking now is cheap insurance. You do not want to have to repeat all your work later just because a switch was in the wrong position.

Jumper settings: see *Figure 21* for the location of the jumpers. Compare each jumper arrangement with the settings in the chart below.

Jumper	Setting	Jumper	Setting
JP1	Jumper not installed	JP10	Pin 2 jumpered to Pin 3
JP2	Jumper installed	JP11	Pin 2 jumpered to Pin 3
JP3	Jumper installed	JP12	Pin 1 jumpered to Pin 2
JP4	Pin 2 jumpered to Pin 3	JP13	Pin 1 jumpered to Pin 2
JP5-JP8	Pin 2 jumpered to Pin 3.	JP14	Pin 2 jumpered to Pin 3.
JP9	Pin 1 jumpered to Pin 2	JP15	Hard Drive LED Connector



Jumper/Switch Block	Setting	Jumper/Switch Block	Setting
1 JP5	Jumpered Pin 2 to Pin 3	2 JP6	Jumpered Pin 2 to Pin 3
3 JP7	Jumpered Pin 2 to Pin 3	4 JP8	Jumpered Pin 2 to Pin 3
5 JP12	Jumpered Pin 1 to Pin 2	6 JP11	Jumpered Pin 2 to Pin 3
7 JP10	Jumpered Pin 2 to Pin 3	8 JP15	Hard drive LED connect
9 DIP Block SW1	1 ON, 2 OFF, 3 OFF, 4 OFF	10 Serial Port 2 J7	n/a
11 Serial Port 1	n/a	12 Parallel Port	n/a
13 JP14	Jumpered Pin 2 to Pin 3	14 JP13	Jumpered Pin 1 to Pin 2
15 External Power	n/a	16 Keyboard	n/a
17 AT Keyboard J1	n/a	18 JP9	Jumpered Pin 1 to Pin 2
19 JP4	Jumpered Pin 2 to Pin 3	20 JP3	Jumpered
21 JP2	Jumpered	22 JP1	Not Jumpered

Figure 21. CPU card jumper block, DIP switch, and connector locations

DIP switch settings: see *Figure 21* for the location of switch block SW1. Be sure the four switches are set as in the chart below.

Switch	Setting
SW1-1	ON
SW1-2	OFF
SW1-3	OFF
SW1-4	OFF

Connecting the CPU card

DANGER:
Computer power supplies are dangerous! Do not reseat the CPU card until you have turned off the power using the *Powering down, page 403*.

WARNING:
Static discharge can destroy sensitive electronic equipment. Be sure to wear a grounding wrist strap or other static-dissipating device during servicing.

See *Figure 18*, *19*, and *20* for the location of the CPU card and associated hardware. Proceed as follows.

1 Place the CPU card in the CPU slot.

2. Lower the card into position and carefully push the card into the static board connectors.
3. Secure the card fastener with a screw.
4. Connect the LED hard drive cable to connector JP15 with the red wire facing the front of the chassis.
5. Connect the SCSI controller ribbon cable to connector J2 with the red wire facing the front of the chassis.
6. Connect the floppy controller cable to connector J6 with the red wire facing the front of the chassis.
7. Replace the card clamp and secure it with a screw.
8. Replace the server top cover and secure.
9. Secure the top cover with one screw on the back of the chassis and six screws on the left and right sides of the top cover.
10. Connect a dumb terminal console or PC cable to the serial port connector on the CPU card.

PRI card maintenance

PRI cards have no serviceable parts. So maintenance consists of removing the card, configuring a known good replacement, and installing the latter in the server.

Removing the suspect PRI card

DANGER:
Computer power supplies are dangerous! Do not replace PRI cards until you have turned off the power using the *Powering down, page 403*.

WARNING:
Be sure to wear a grounding wrist strap or other static-dissipating device.

See *Figure 18* for the location of the PRI card and associated hardware and *Figure 22* for PRI card details. Proceed as follows.

1. Power down gracefully (if possible) using the *Powering down, page 403*.
2. Disconnect the T1/E1B cable from the T1/E1B connector on the PRI card.
3. Disconnect the T1/E1A cable from the T1/E1A connector on the PRI card.
4. Disconnect the diagnostic cable from the serial diagnostic port connector.
5. Remove the server top cover.
   a. Loosen but do not remove the six screws on the left and right sides of the top cover.
   b. Remove the rear screw from the cover.
   c. Slide the cover towards the rear of the chassis and lift the cover away.

6 Remove the card clamp and the screw that secures the card.

7 Disconnect the MVIP ribbon cable from the MVIP connector.

8 Lift the PRI card up to disconnect it from the static board connector, and remove it.

9 Go to *Configuring a replacement CPU card*.

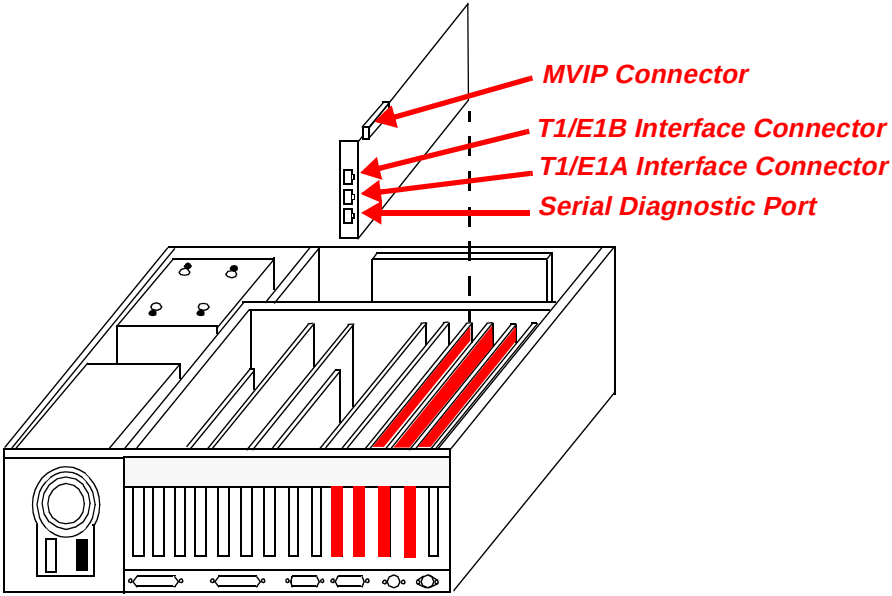


Figure 22. PRI card details

Configuring the replacement PRI card

WARNING:
Be sure to wear a grounding wrist strap or other static-dissipating device.

A single DIP switch bank (SW1) assigns the card's I/O base address. *Figure 23* shows the switch settings for PRI cards 1 through 4.

The 10 switch positions represents address bits A4 through A13. A switch in the up or OFF position represents a binary 1 and a switch in the down or ON position represents a binary 0.

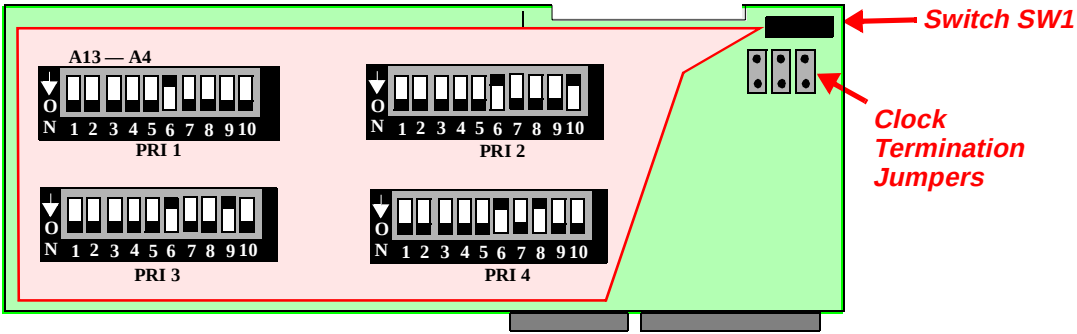


Figure 23. PRI card DIP switch location and settings

Installing the PRI card

DANGER:
Do not perform any maintenance on the server until you follow the procedures to power down the server. See *Powering down, page 403*.

WARNING:
Be sure to wear a grounding wrist strap or other static-dissipating device.

Proceed as follows.

1. Place the PRI card into its slot.
   - PRI 1 in slot I5 (First PRI)
   - PRI 2 in slot I4 (Second PRI)
   - PRI 3 in slot I3 (Third PRI)
   - PRI 4 in slot I2 (Fourth PRI).
2. Lower the card into position, and carefully push the card into the static board connector.
3. Secure the card fastener with a screw.
4. Connect the MVIP ribbon cable to the PRI card parallel connector.
5. If you are installing the PRI card in the first PRI slot (slot I5), ensure the clock termination jumpers are installed on all three jumpers.
6. Replace the card clamp and secure it with a screw.
7. Replace the server top cover. Secure it with one screw on the back of the chassis and six screws on the left and right sides of the top cover.

8 Connect the T1/E1B interface cable to the T1/E1B connector on the PRI board and the T1/E1A interface cable to the T1/E1A connector.

9 Connect the diagnostic cable to the serial diagnostic port connector on the PRI card. See *Installing the looparounds, page 341*.

Ethernet card maintenance

Ethernet cards have no serviceable parts, so maintenance consists of removing the defective unit and installing a replacement.

Removing the Ethernet card

DANGER:
Computer power supplies are dangerous! Do not perform any maintenance on the Ethernet cards until you have turned off the power using the *Powering down, page 403*.

WARNING:
Be sure to wear a grounding wrist strap or other static-dissipating device.

See *Figure 18* for the location of the Ethernet card and associated hardware and *Figure 24* for Ethernet card details. Proceed as follows.

1. Power down gracefully (if possible) using the *Powering down, page 403*.
2. Disconnect the Ethernet cable from the 10BaseT/AUI connector on the Ethernet card.
3. Remove the server top cover as follows:
   a. Loosen but do not remove the six screws on the left and right sides of the top cover.
   b. Remove the rear screw from the cover.
   c. Slide the cover towards the rear of the chassis and lift the cover away.
4. Remove the card clamp from the server chassis.
5. Remove the screw securing the card fastener.

6 Pull the Ethernet card up to disconnect it from the static board.

7 Remove the card from it's slot.

8 Go to *Installing the Ethernet card*.

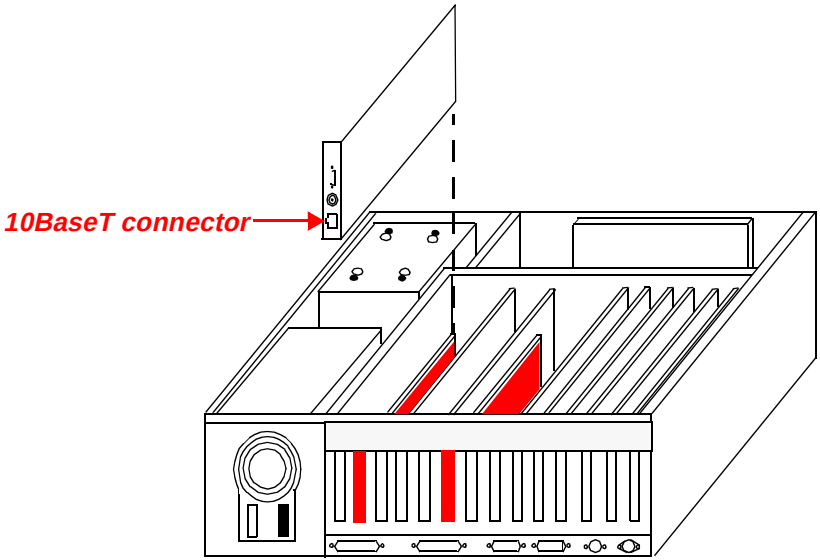


Figure 24. Ethernet card maintenance details

Installing the Ethernet card

DANGER:
Computer power supplies are dangerous! Do not perform any maintenance on the Ethernet cards until you have turned off the power using the *Powering down, page 403*.

WARNING:
Be sure to wear a grounding wrist strap or other static-dissipating device.

See *Figure 24* for the location of the Ethernet card and associated hardware.

1. Install the Ethernet card in the correct slot.

   If you are adding a card, use the next available slot, in the order **5**, **1**, **3**, **6**.

   If you are reinstalling or replacing a card, use the same slot as was used before.
2. Lower the card into position, and carefully push it into the static board connector.
3. Secure the card fastener with a screw.
4. Replace the card clamp and secure it with a screw.
5. Replace the server top cover.
6. Secure the top cover with one screw on the back of the chassis and six screws on the left and right sides of the top cover.
7. Connect the Ethernet cable to the 10BaseT connector on the Ethernet card.
8. See *Installing the looparounds, page 341*.

VGA video card installation

The normal MMCX console installation includes a VGA video card. We recommend that you install it in port P3. This displaces the third Ethernet card, if so equipped. If loss of a network card is unacceptable, contact customer support for advice (see *Repair Number 0 - Escalate to MACS, page 162*).

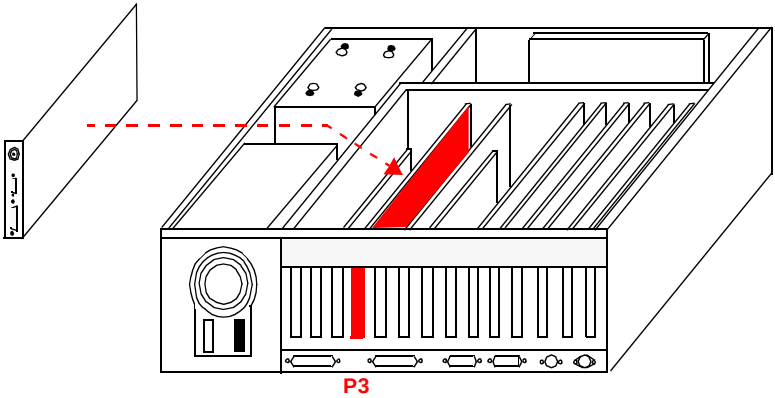


Figure 25. VGA video card installation

ATM card maintenance

Maintenance of the ATM card consists of removing a defective card and installing a new ATM card in the server.

Removing the ATM card

DANGER:
Do not perform any maintenance until you turn off the power using the *Powering down, page 403*.

WARNING:
Be sure to wear a grounding wrist strap or other static-dissipating device.

See *Figure 18* for the location of the ATM card and associated hardware and *Figure 26* for ATM card details.

1. Power down gracefully (if possible) using the *Powering down, page 403*.
2. Disconnect the fiber optic cable from the Transmit connector on the ATM card.
3. Disconnect the fiber optic cable from the Receive connector on the ATM card.
4. Remove the server top cover as follows:
   a. Loosen but do not remove the six screws on the left and right sides of the top cover.
   b. Remove the rear screw from the cover.
   c. Slide the cover towards the rear of the chassis and lift the cover away.
5. Remove the card clamp from the server chassis.

6 Remove the screw securing the card fastener.

7 Pull the ATM card up to disconnect it from the static board.

8 Remove the card from it's slot.

9 See *Installing the ATM card, page 373*.

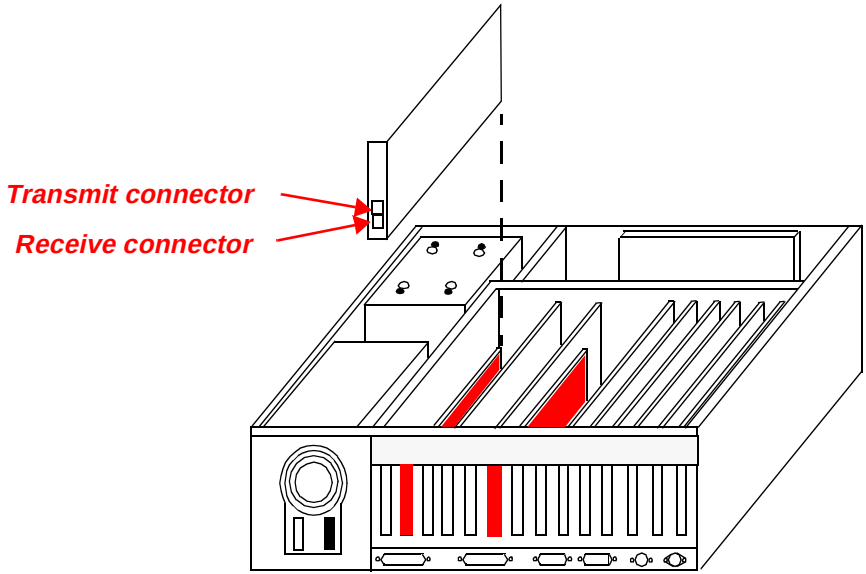


Figure 26. ATM card details

Installing the ATM card

DANGER:
Do not perform any maintenance on the server until you follow the procedures to power down the server. See *Powering down, page 403*.

WARNING:
Be sure to wear a grounding wrist strap or other static-dissipating device.

See *Figure 18* for the location of the ATM card and associated hardware and *Figure 26* for ATM card details. Then proceed as follows.

1. Install the ATM card in the correct slot.

   If you are adding a card, use the next available slot, in the order **5**, **1**, **3**, **6**.

   If you are reinstalling or replacing a card, use the same slot as was used before.
2. Lower the card into position and carefully push the card into the static board connector.
3. Secure the card fastener with a screw.
4. Replace the card clamp and secure it with a screw.
5. Replace the server top cover.
6. Secure the top cover with one screw on the back of the chassis and six screws on the left and right sides of the top cover.
7. Connect the transmit fiber optic cable to the transmit connector on the ATM card.
8. Connect the receive fiber optic cable to the receive connector on the ATM card.

WILD card maintenance

Maintenance of the WILD card consists of removing a defective card and installing a new WILD card in the server.

Removing the WILD card

DANGER:
Computer power supplies are dangerous! Do not perform any maintenance until you have turned off the power using the *Powering down, page 403*.

WARNING:
Be sure to wear a grounding wrist strap or other static-dissipating device.

See *Figure 27* for the location of the WILD card and associated hardware. Proceed as follows.

1. Power down the server gracefully (if possible), see *Powering down, page 403*.
2. Disconnect the diagnostic cable from the Diagnostic port connector on the WILD card.
3. Remove the server top cover as follows:
   a. Loosen but do not remove the six screws on the left and right sides of the top cover.
   b. Remove the rear screw from the cover.
   c. Slide the cover towards the rear of the chassis and lift the cover away.
4. Remove the card clamp from the server chassis.
5. Remove the screw securing the card fastener.
6. Disconnect the MVIP ribbon cable from the MVIP connector on the WILD card.

7 Pull the wild card up to disconnect it from the static board connector.

8 Remove the WILD card from it's slot.

9 See *Installing the WILD card, page 376*.

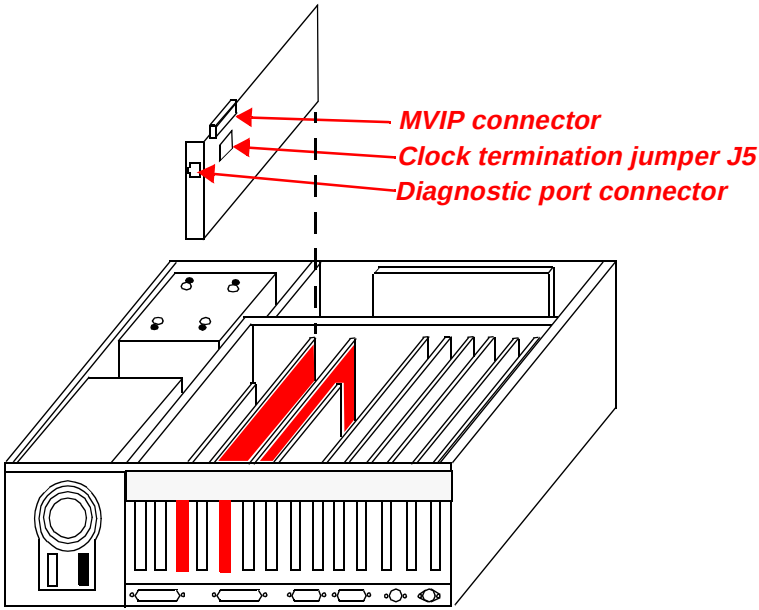


Figure 27. WILD card details

Installing the WILD card

DANGER:
Do not perform any maintenance on the server until you follow the procedures to power down the server. See *Powering down, page 403*.

WARNING:
Be sure to wear a grounding wrist strap or other static-dissipating device.

See *Figure 18* for the location of the WILD card and associated hardware. See *Figure 27* for WILD card details.

Perform the following step only if there is one WILD card in the chassis.

1. If you are installing the WILD card into slot P2, ensure the termination jumpers are installed.
2. Install the WILD card into slot P2 for WILD card number 1, or P4 for WILD card number 2.
3. Lower the card into position and push the card into the static board connector.
4. Connect the MVIP ribbon cable to the WILD card connector.
5. Secure the card fastener with a screw.
6. Replace the card clamp and secure it with a screw.
7. Replace the server top cover.
8. Secure the top cover with one screw on the back of the chassis and six screws on the left and right sides of the top cover.

Hard disk drive maintenance

Maintenance procedures for the hard drive consists of removing a faulty hard drive and replacing it with a new hard drive.

Removing the hard disk drive

DANGER:
Computer power supplies are dangerous! Do not perform any maintenance until you have turned off the power using the *Powering down, page 403*.

WARNING:
Be sure to wear a grounding wrist strap or other static-dissipating device. Back up as much data and configuration information as you can before proceeding.

See *Figure 18* for the location of the hard drive and *Figure on page 379* for hard drive details. Proceed as follows.

1. Power down gracefully (if possible) using the *Powering down, page 403*.
2. Remove the server top cover.
   a. Loosen but do not remove the six screws on the left and right sides of the top cover.
   b. Remove the rear screw from the cover.
   c. Slide the cover towards the rear of the chassis and lift the cover away.
3. Disconnect the power cable from the hard drive.
4. Disconnect the ribbon cable from the parallel connector on the hard drive.

5 Remove the four screws on the bottom of the chassis that secure the drive bracket in place.

6 Lift the bracket, with hard drive, up and out of the chassis.

7 Remove the four screws securing the hard drive to the bracket.

8 Slide the hard drive out of either side of the bracket.

9 See *Installing the hard disk drive, page 379*.

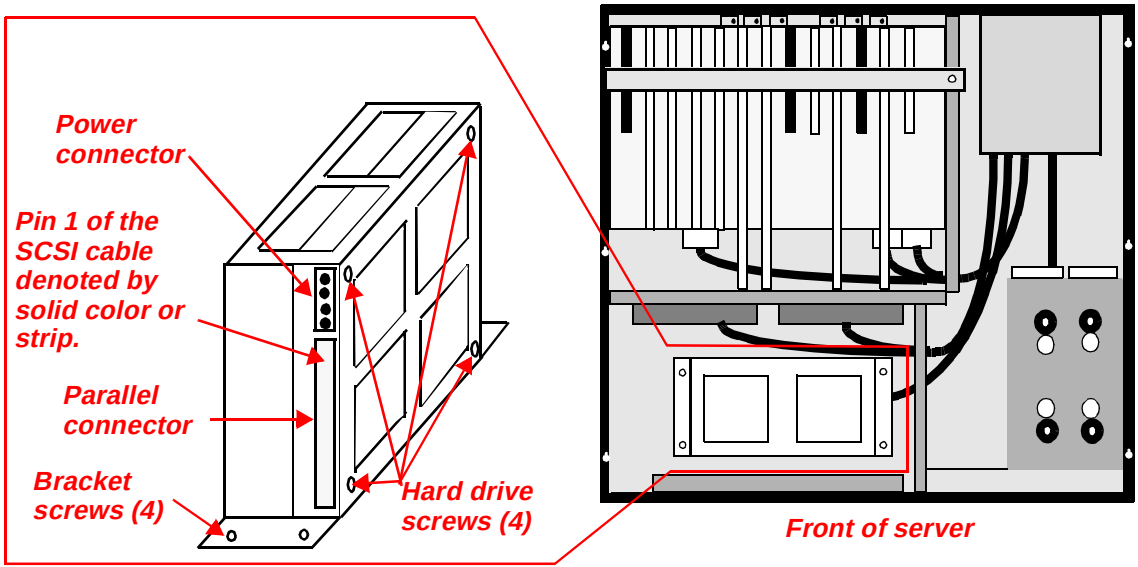


Figure 28. Hard disk details

Installing the hard disk drive

DANGER:
Do not perform any maintenance on the server until you follow the procedures to power down the server. See *Powering down, page 403*.

WARNING:
Be sure to wear a grounding wrist strap or other static-dissipating device.

See *Figure 18 on page 354* for the location of the hard drive and associated hardware and *Figure 28* for hard drive details. Proceed as follows.

1. Make sure that the SCSI ID jumper is installed correctly. See *Figure 29* for the jumper locations.

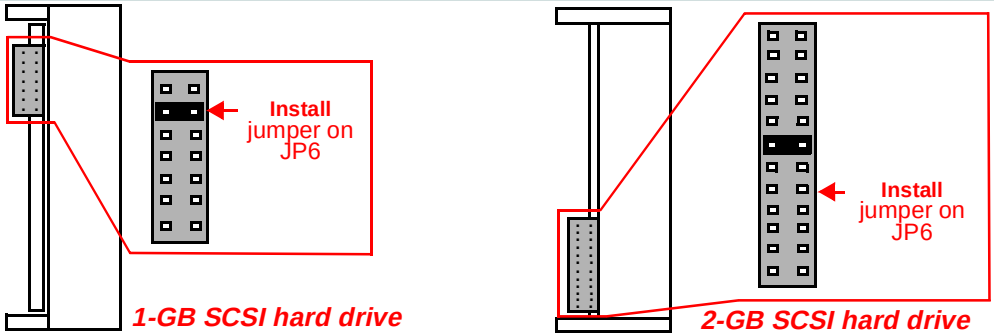


Figure 29. Hard disk jumpers

2 Slide the hard drive into the bracket from either side.

3 Secure the hard drive to the bracket with the four hard drive screws.

4 Lower the bracket, with hard drive, into the chassis.

5 Secure the hard drive bracket to the chassis with the four bracket screws.

6 Connect the ribbon cable to the parallel connector. Ensure pin 1 is closest to the power connector on the hard drive and closest to the SIMM sockets on the CPU card.

7 Connect the power cable to the power connector.

8 Replace the server top cover.

9 Secure the top cover with one screw on the back of the chassis and six screws on the left and right sides of the top cover.

10 See *Restoring server system files, page 347*.

Diskette drive maintenance

Maintenance procedures for the diskette drive consists of removing a faulty floppy drive and replacing it with a new floppy drive.

DANGER:
Computer power supplies are dangerous! Do not perform any maintenance on the server until you follow the procedures to power down the server. See *Powering down, page 403*.

WARNING:
Before attempting any maintenance on the chassis, be sure to wear a grounding wrist strap or other static-dissipating device.

Removing the diskette drive

See *Figure 30* for diskette drive location and maintenance details. Then proceed as follows.

1. Power down gracefully (if possible) using the *Powering down, page 403*.
2. Remove the server top cover as follows:
   a. Loosen the six screws on the left and right sides of the cover.
   b. Remove the rear screw from the cover.
   c. Slide the cover towards the rear of the chassis and lift the cover away.
3. Disconnect the ground wire from the floppy drive.
4. Disconnect the power cable from the power connector.
5. Disconnect the ribbon cable from the parallel connector.

6 Remove the four bracket screws on the outside wall of the chassis.

7 Slide the floppy drive and bracket away from the front of the chassis to disengage the tabs.

8 Tilt the floppy drive and bracket back so the front of the drive is facing upward.

9 Pull the floppy drive and bracket up and out of the chassis.

10 Remove the four screws securing the floppy drive to the bracket, and pull the floppy drive out.

11 See *Installing the diskette drive, page 383*.

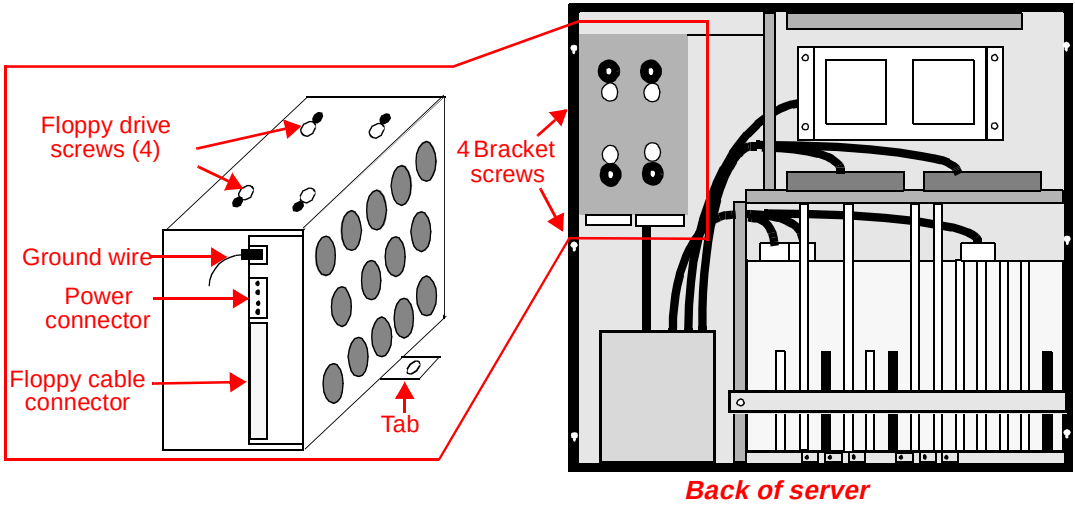


Figure 30. Diskette drive details

Installing the diskette drive

DANGER:
Power supplies are dangerous! Do not perform any maintenance on the power supply until you have turned off the electricity using the *Powering down, page 403*.

WARNING:
Be sure to wear a grounding wrist strap or other static-dissipating device.

See *Figure 30* for the location and details of the diskette drive and hardware. Then proceed as follows.

1. Slide the floppy drive into the bracket.
2. Secure the floppy drive to the bracket with the four floppy drive screws.
3. Place the floppy drive and bracket on top of the chassis.
4. Connect the power cable to the connector. (the power connector is keyed)
5. Connect the ribbon cable to the parallel connector with the red wire towards the power connector on the floppy drive and the CPU card SIMM sockets.
6. Connect the ground wire to the ground lug on the floppy drive.
7. Lower the floppy drive and bracket into place; tilt it back, then lower the front.
8. Slide the floppy drive and bracket forward into position locking it to the tab.
9. Secure the bracket to the outside wall of the chassis with four bracket screws.
10. Replace the server top cover, and secure it with one screw on the back of the chassis and six screws on the left and right sides of the top cover.

Power supply maintenance

This section explains how you remove and replace a faulty power supply.

DANGER:
Power supplies are dangerous! Do not perform any maintenance on the power supply until you have turned off the electricity using the *Powering down, page 403*.

WARNING:
Be sure to wear a grounding wrist strap or other static-dissipating device.

Removing the power supply

See *Figure 31*. Then proceed as follows.

1. Power down the server gracefully (if possible), see *Powering down, page 403*.
2. Remove the floppy drive and bracket to gain access to power switch wires. See *Removing the diskette drive, page 381*.
3. Disconnect the four spade connectors from the back of the power switch.
4. Disconnect the ground wire from the bottom of the chassis.
5. Cut or break the wire tie securing the power cable to the chassis.
6. Disconnect the hard drive power cable from the hard drive.
7. Disconnect the floppy drive power cable from the floppy drive.
8. Disconnect the power cable from the two fans.
9. Disconnect the cables from the static board connectors P9 and P8—P9 pair.

10 Remove the four power supply screws securing the power supply to the back of the chassis.

11 Remove the power supply from the chassis.

12 Go to *Installing the power supply, page 386*.

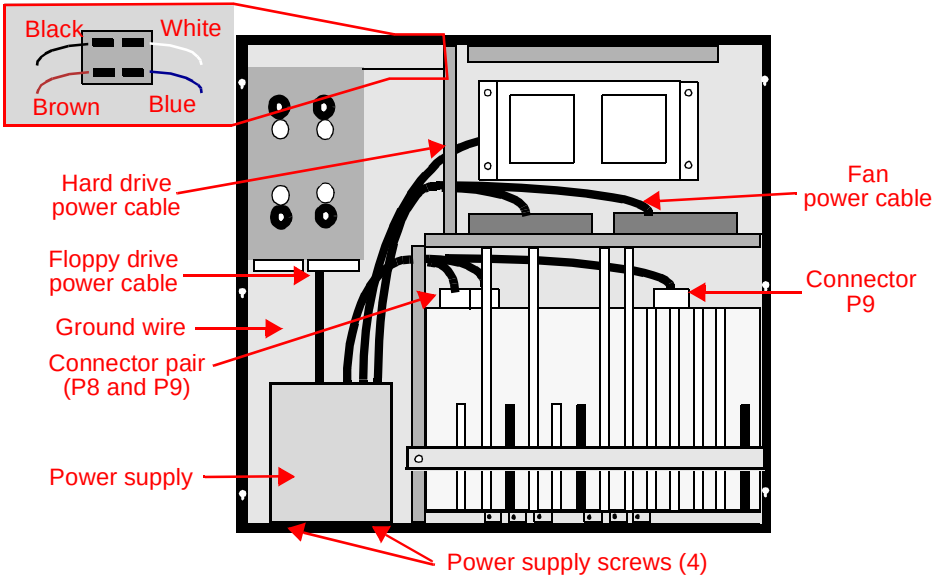


Figure 31. Power supply details

Installing the power supply

See *Figure 31* for the location of the power supply and associated hardware.

See *Figure 31 on page 385* for power supply maintenance details.

1. Position the new power supply inside the chassis.
2. Secure the power supply to the chassis with the four power supply screws.
3. Connect the three power cables to the static board connectors P9, and the P8—P9 pair. (ensure the black wires on each connector face each other)
4. Connect the power cable to the two fans.
5. Connect the hard drive power cable to the hard drive.
6. Connect the floppy drive power cable to the floppy drive.
7. Connect the green ground wire to the bottom of the chassis.
8. Connect the four spade connectors to the power switch.
9. Secure the power cable to the chassis with a tie wrap.
10. See *Installing the diskette drive, page 383* to install the floppy drive and bracket.

RMB maintenance

The remote maintenance board (RMB) lets MACS support personnel diagnose the problems you report without physically visiting your site. *The remote maintenance board is for use by factory representatives only.* Do not remove it unless you are attempting to isolate a problem.

DANGER:
Computer power supplies are dangerous! Do not perform any maintenance on the server until you follow the procedures to power down the server. See *Powering down, page 403*.

WARNING:
Before attempting any maintenance on the chassis, be sure to wear a grounding wrist strap or other static-dissipating device.

Removing the remote maintenance board

See *Figure 32* for the location of the remote maintenance board.

1. Power down the server gracefully (if possible), see *Powering down, page 403*.
2. Disconnect the analog line from the modem connector on the rear of the remote maintenance board.
3. Remove the server top cover as follows:
   a. Loosen but do not remove the six screws on the left and right sides of the top cover.
   b. Remove the rear screw from the cover.
   c. Slide the cover towards the rear of the chassis and lift the cover away.
4. Remove the card clamp from the server chassis.

5 Remove the screw securing the card fastener.

6 Pull the remote maintenance board up to disconnect it from the static board.

7 Remove the board from the slot.

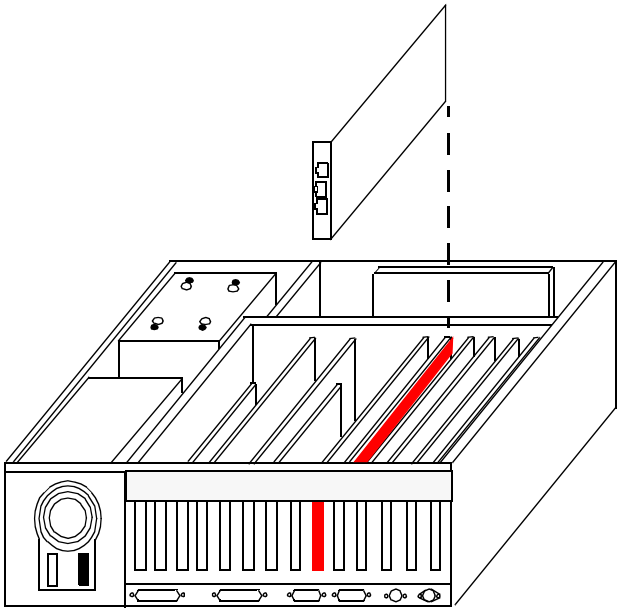


Figure 32. Remote maintenance board details

Installing the remote maintenance board

See *Figure 32*. Then proceed as follows.

1. Place the remote maintenance board in slot I1.
2. Lower the card into position and carefully push the card into the static board connectors.
3. Secure the card fastener with a screw.
4. Replace the card clamp and secure it with a screw.
5. Replace the server top cover.
6. Secure the top cover with one screw on the back of the chassis and six screws on the left and right sides of the top cover.
7. Connect the analog line to the modem connector. See *RMB cables, page 401*.

Interpreting diagnostic LEDs

PRI, WILD, ATM, and Ethernet cards have diagnostic LED displays. Interpret them as follows.

PRI Card LEDs

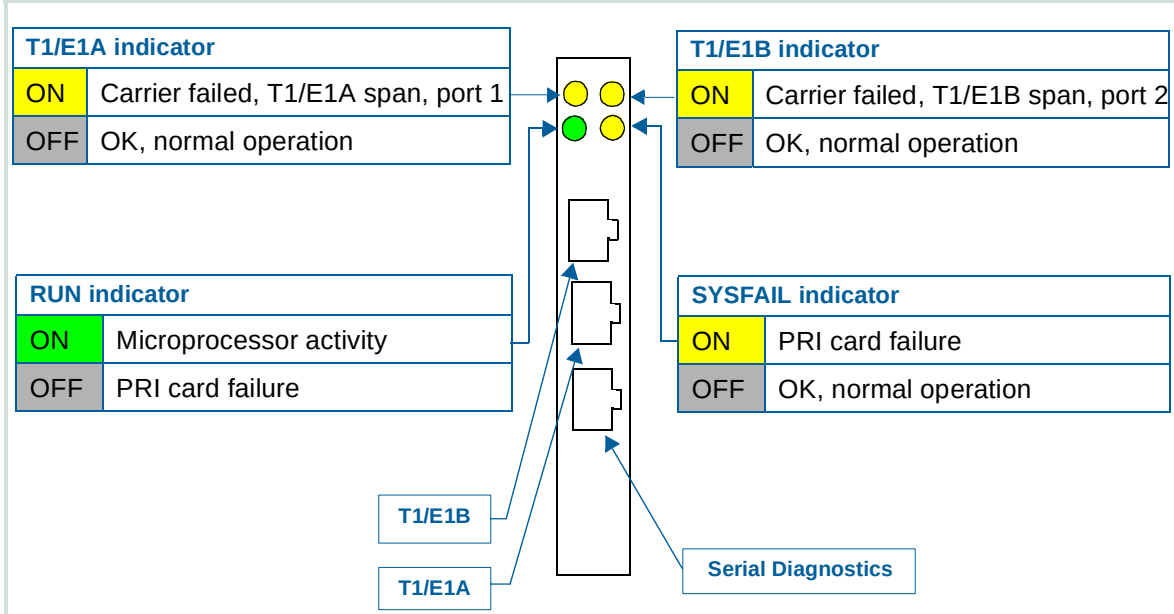


Figure 33. PRI card LED indicators

Ethernet card LEDs

Note that the position of the Ethernet card LEDs varies depending on the version of the card, but the interpretations of the LEDs remain unchanged.

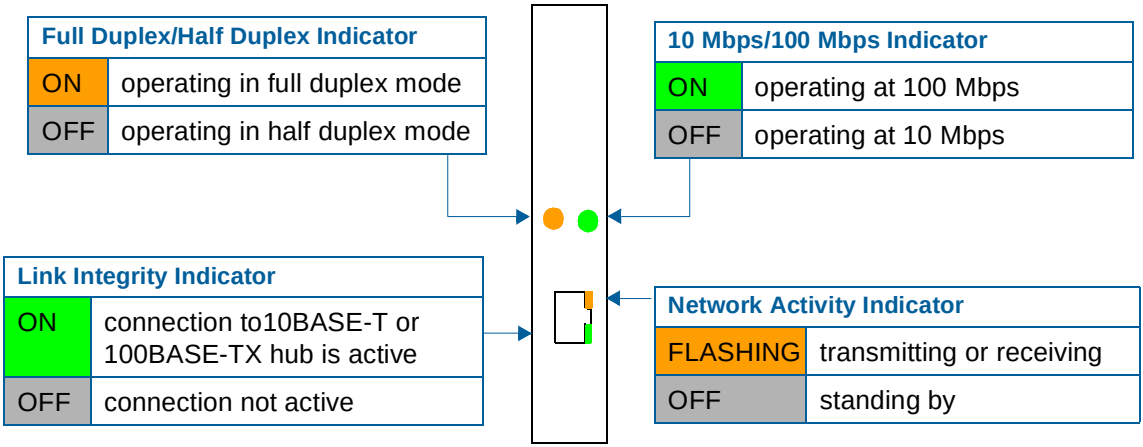


Figure 34. Network Ethernet card LED definitions

ATM card LEDs

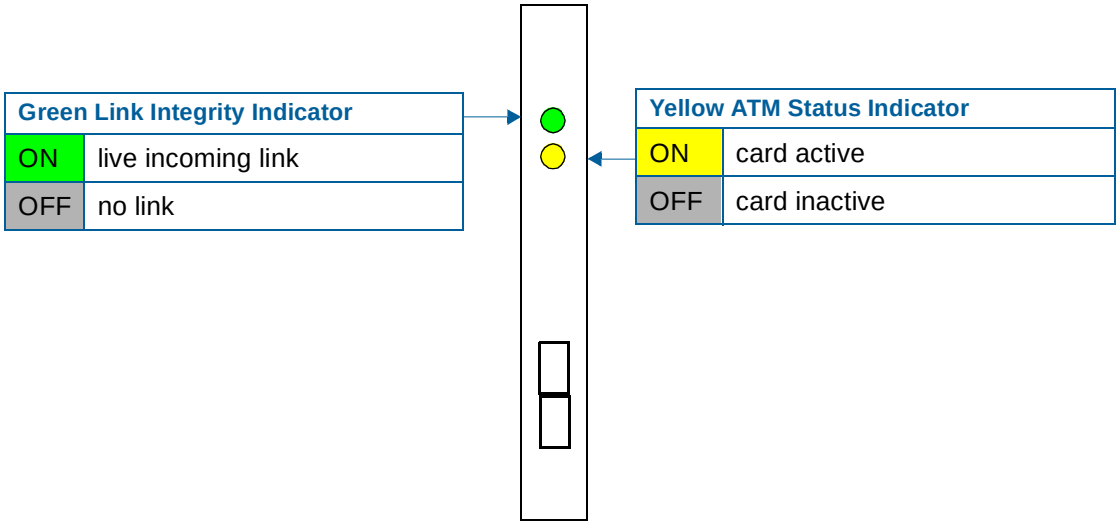
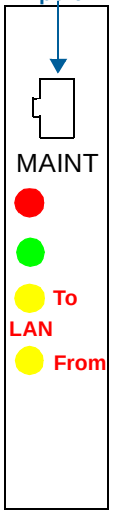


Figure 35. ATM card LED definitions

WILD card LEDs

The figure below gives the definition and status of the WILD card LEDs.



WILD card state	LED for Version 1	LED for Version 2
power-on to boot	RED and GREEN are ON	RED and GREEN are ON
pre-download self test fail	RED is ON and remains ON	RED is ON and remains ON
post download self test fail	RED is ON GREEN possibly flashing	RED is ON GREEN possibly flashing
no clocks	GREEN LED1.2 sec ON 0.4 sec OFF	GREEN LED 1.2 sec ON 0.4 sec OFF
normal operation	GREEN LED 0.4 sec ON 0.4 sec OFF	GREEN LED 0.4 sec ON 0.4 sec OFF
First Yellow	*Not used on this version*	Toggles on every LAN packet
Second Yellow	*Not used on this version*	Toggles on every LAN packet

The two YELLOW LEDs are not used on Version 1 cards

Figure 36. WILD card LED definitions

Checking cables

If a cable is suspect, you have to power down the server, check the suspect cable for continuity, and check connectors and sockets for bent or missing pins. Follow the procedure outlined below.

Working with cables

DANGER:
Computer power supplies are dangerous! Do not perform any maintenance on the server until you power down the server using the procedure described in *Powering down, page 403*. Failure to properly power down can corrupt system files on the server's hard disk.

WARNING:
Before attempting this or any other maintenance on the chassis, be sure to wear a grounding wrist strap or other static-dissipating device.

After you have read the cautions above, in *Checking cables*, proceed as follows.

1. Be sure that no one is logged-in to the server by typing **who** at the system prompt.
   The system lists all logged-in users.
2. Type **reset level=halt ENTER**.
   See *Resetting the server* for a full description of the command.
3. Wait approximately 15 seconds.
4. Turn the power switch OFF.
5. Go to *Identifying and correcting problem cabling*, below.

Identifying and correcting problem cabling

WARNING:
Do not attempt to work with cables unless you have read and understand the general cautions and procedures in *Checking cables*.

Once you have completed the general, preparatory procedure, you are ready to isolate and repair the specific problem. If you suspect a specific type of cabling, locate it in the list below. If you are still trying to identify the problem, work through each step in the list below in the order given.

1. *Hard disk drive cables, page 395*
2. *Checking cables, page 394*
3. *MVIP cable, page 397*
4. *Static board cables, page 399*
5. *CPU card cables, page 400*
6. *RMB cables, page 401*
7. *PRI cables, page 402*

Hard disk drive cables

Ensure the cables to the hard disk drive are connected, as follows:

- Ribbon cable to parallel connector with the red wire towards the power connector.
- Power cable to power connector (the connector and cable are keyed).

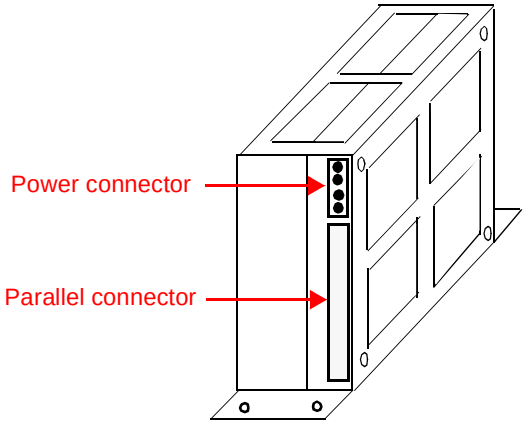


Figure 37. Hard disk drive cable connections

Diskette drive cables

Ensure the cables to the diskette drive are connected, as follows.

- Ribbon cable to the parallel connector with the red wire towards the power connector.
- Power cable to power connector (the connector and cable are keyed).
- Ground wire to the grounding stud.

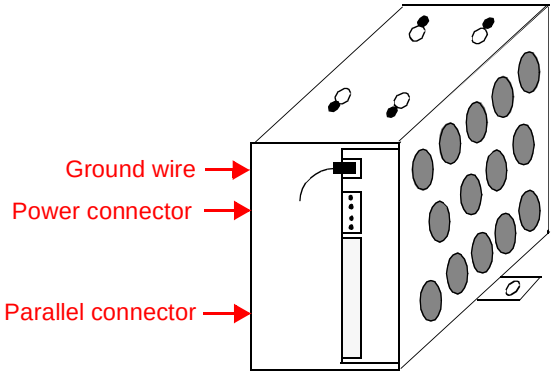


Figure 38. Diskette drive cable connections

MVIP cable

Ensure the MVIP ribbon cable is connected to the WILD card parallel connector(s) with the red wire towards the front of the server. Ensure it is connected to the PRI card parallel connectors with the red wire towards the front of the server.

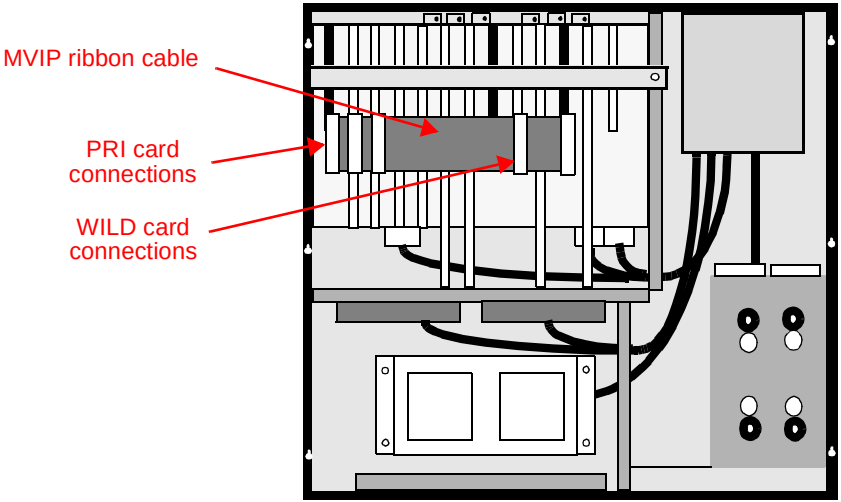
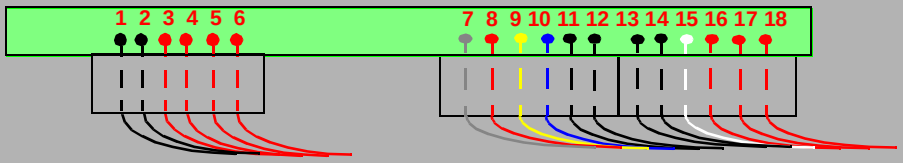


Figure 39. MVIP cable connections

Static board cables

Be sure that the three connectors on the static board are connected as shown below.



Name	Name
1 Gnd (Black)	2 Gnd (Black)
3 +5V (Red)	4 +5V (Red)
5 +5V (Red)	6 +5V (Red)
7 N.C.	8 +5V (Red)
9 +12V (Yellow)	10 -12V (Blue)
11 Gnd (Black)	12 Gnd (Black)
13 Gnd (Black)	14 Gnd (Black)
15 -5V (White)	16 +5V (Red)
17 +5V (Red)	18 +5V (Red)

Figure 40. Static board cable connections

CPU card cables

Be sure that the cables to the CPU card are connected, as follows.

- LED hard drive cable to connector JP15 with the red wire facing the SIMM socket on the CPU card.
- SCSI controller ribbon cable to connector J2 with the red wire facing the SIMM socket on the CPU card.
- Floppy controller cable to connector J6 with the red wire facing the SIMM socket on the CPU card.

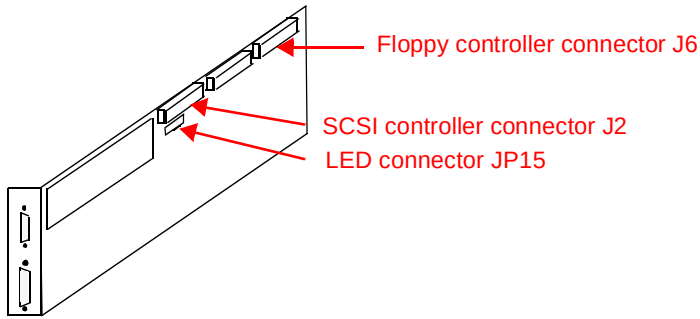


Figure 41. CPU card, cable connections

RMB cables

Be sure that the analog telephone line is connected to the RMB modem connector.

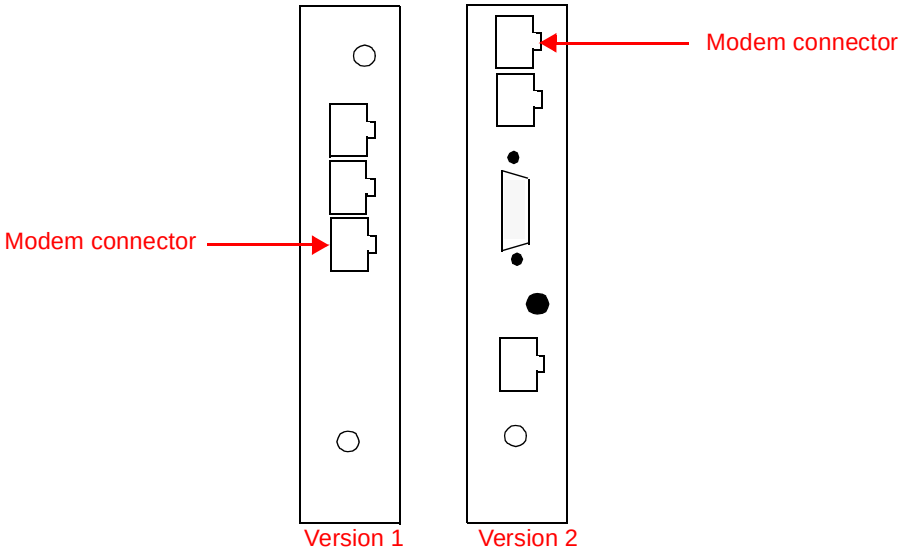


Figure 42. RMB cable connections

PRI cables

Ensure the MVIP ribbon cable is connected to the PRI parallel connector. Ensure the D8W cables are connected and connectors are wired correctly. See the table below for proper wire connections.

T1A/ E1A Pin	Signal Name	T1B/ E1B Pin	Signal Name
1	Receive Ring (A)	1	Receive Ring (B)
2	Receive Tip (A)	3	Receive Tip (B)
4	no connection	5	no connection
6	Transmit Ring (A)	7	Transmit Ring (B)
8	Transmit Tip (A)	9	Transmit Tip (B)
10	no connection	11	no connection
12	no connection	13	no connection
14	no connection	15	no connection

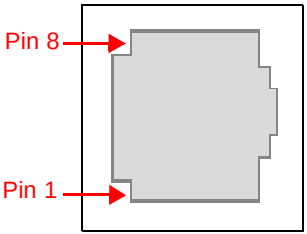


Figure 43. PRI cable connections

Powering down

WARNING:
Failure to properly power down the server can corrupt the file system.

To power down the server gracefully (without damage to files or loss of data), proceed as follows.

1. Make sure there are no users logged into the server.
   a. To view the login IDs of all logged in users, type **who ENTER**.
   b. To identify users from their logins, type **showusr login=*login_ID* ENTER**.
2. Type **reset level=halt ENTER**.
3. Wait approximately 15 seconds.
4. Turn the power switch **OFF**.

Cleaning the fan filter

The cooling fan's air filter is located at the front of the server, behind the front panel. Clean the filter at least once every year (more in dusty environments). Use the following procedure.

1. Turn the two captive screws on the filter cover until they release, lower the filter cover, and remove the fan filter.
2. Wash the filter with a mild soap-and-water solution, and dry it thoroughly.
3. Replace the filter in its original position, close the filter cover, and tighten the screws.

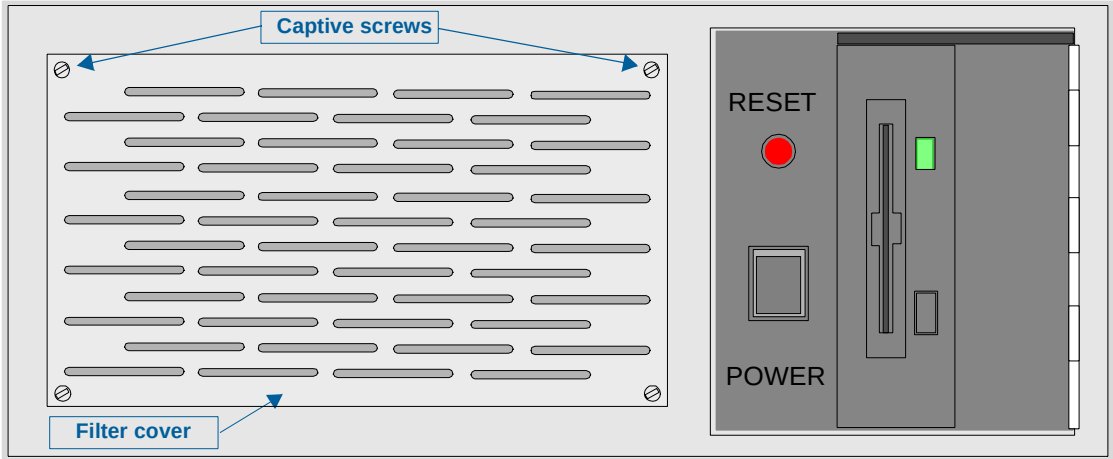


Figure 44. Fan filter cover

Checking drivers and devices

Sometimes a driver cannot open a device. When this happens, make sure the device is listed correctly in the device and driver table. Proceed as follows.

1 At the system prompt, type **devices ENTER**.

Common name	System name	Common name	System name
PRI card	pri	ATM card	ia
RMB	rmb	Diskette drive	Floppy
Ethernet card	dec21040	RMB analog line port	com1
WILD card	WILDDriver	CPU console port	com2
Hard drive	AD29040		

2 In the display, locate the device in question. System names for common devices are listed in the table above.

3 At the system prompt**,** type **drivers ENTER**.

4 In the display, locate the device in question. System names for common devices are listed in the table above.

5 If you cannot find entries for the device, type **reset level=boot ENTER**.

6 If you cannot find entries for the device, go to *Repair Number 0 - Escalate to MACS, page 162*.

Recovering from a disaster

This units tells you how to get the server running again after a catastrophic malfunction, such as a hard disk crash or major power failure. Once the server is running, you will have to follow up with the administration and configuration procedures described elsewhere in this book.

Restoring the BIOS configuration

The server stores critical system configuration information, such as I/O port and interrupt assignments, in CMOS RAM. CMOS RAM is volatile, so any interruption to the power supply results in loss of information. A catastrophic power failure involving line power, uninterruptible power supply, and onboard battery backup (if so equipped), returns CMOS RAM to a default configuration that generally does not reflect the actual hardware installation. CMOS RAM is also editable, so the configuration is vulnerable to misadministration. Finally, improper or incomplete hardware installations may make configuration changes that are not recorded in CMOS RAM. When this fundamental, BIOS configuration information is incorrect, hardware competes for CPU time and I/O addresses, with sometimes bizarre and unpredictable results. The system may lock up, hardware devices may work intermittently or not at all, and processes may generate misleading alarms.

This section outlines procedure for recovering from a CMOS RAM problem. Recovery has two parts: you restore the Lucent factory default configuration for the server and then restore the specific configuration information for the cards installed on your system. There are three ways to accomplish this, listed below in order of preferability.

1. *Restoring BIOS configuration from a backup diskette, page 407*
2. *Restoring BIOS configuration from the console, page 409*
3. *Restoring hardware-resident default BIOS configuration, page 414*

Restoring BIOS configuration from a backup diskette

Whenever possible, restore the standard MMCX configuration information from the diskette that came with your server. This is less labor-intensive and error-prone than doing the job by hand. Once the basic server configuration has been restored, you can restore any cards specific to your system manually (see *Restoring BIOS configuration from the console*). Proceed as follows.

1 Obtain BIOS configuration backup diskettes for your version of MMCX (backup diskettes came with the server and can be obtained from MACS). The BIOS version is displayed just prior to the memory test (*Figure 45*).

```
      Lucent Technologies
      Copyright (C) 1985-1989 Phoenix Technologies Ltd.
      Copyright (C) 1991 Texas Microsystems, Inc.
      All Rights Reserved
The P5120C 120 MHz Industrial Computer
640K Base, 031744K Extended, 256K External Cache
Adaptec AIC-7850 BIOS v1.11
(c) 1994 Adaptec, Inc. All Rights Reserved.
Press <Ctrl><A> for SCSISelect(TM) Utility!
SCSI ID # - T&T 1GB DPES 407340959  - Drive C: (80h)
BIOS Installed Successfully!
```

Figure 45. BIOS information displayed during boot up

2 Power down gracefully, if possible. See *Powering down*.

3 Insert the backup diskette in the floppy drive.

4 Turn the power switch **ON**. After the BIOS information appears (*Figure 45*), the BIOS configuration utility should start automatically. It looks something like *Figure 46*.

```
Starting MS-DOS...
A:\>REM Setting the CPU CMOS Parameters NOW...
A:\>echo Setting the CPU CMOS Parameters per the file LUCENT.DAT
Setting the CPU CMOS Parameters per the file LUCENT.DAT
A:\>fld_bios
Texas Micro CPU Configuration Utility for DOS, Version 1.1
Copyright (c) 1994 Texas Microsystems, Inc.
All Rights Reserved
CPU has been configured.
A:\>REM Setting the SCSI BIOS Parameters NOW...
A:\>echo Setting the SCSI BIOS Parameters per the file LUCSCSI.DAT
Setting the SCSI BIOS Parameters per the file LUCSCSI.DAT
A:\>fld_scsi
Texas Micro SCSI Configuration Utility for DOS, Version 1.0
Copyright (c) 1994 Texas Microsystems, Inc.
All Rights Reserved
SCSI drive has been configured.
A:\>
```

Figure 46. BIOS configuration utility

5 Make sure that the configuration process concludes successfully. Look for the messages **CPU has been configured** and **SCSI drive has been configured**. If configuration fails, contact technical support (go to *Repair Number 0 - Escalate to MACS, page 162*).

6 Remove the diskette from the drive, and press **RESET** on the front of the server.

Restoring BIOS configuration from the console

If you do not have access to the BIOS setup disks, or if you have extra hardware not covered by the basic MMCX configuration, you have to make changes from the console. Proceed as follows.

1. Power down gracefully, if possible. See *Powering down*.
2. Turn the power switch **ON**. While the memory test is running, press **S** to start the setup utility.
3. Set the BIOS basic options to the values listed in the chart below.

Device	Parameters	Settings
Time and Date	Time: Date: Time/Date Boot Errors:	***hh/mm/ss*** yy/mm/dd **ON**
Floppy Disks	On-board floppy controller Select Drive A: Type: Select Drive B: Type: Floppy Configuration Errors:	**ON** **3.5 Inch, 1.44MB** **Not Installed** **ON**
Fixed Disks	On-board IDE Interface: Set Hard Disk 1 Type: Set Hard Disk 2 Type:	**OFF** **SCSI Disk Installed** **Not Installed**
Video Adapter	Select Video Adapter Type: Video Configuration Errors:	**VGA/EGA** **OFF**

Device	Parameters	Settings
Keyboard	Keyboard Configuration Errors: Set Keyboard Typematic Rate:	**OFF** **NO**
Shadow RAM	Address: C000:0, Status: Address: C800:0, Status: Address: E000:0, Status: Address: F000:0, Status: *Other_ISA_Card_Address, Status:*	**SHADOW** **SHADOW** **SHADOW** **SHADOW** ***ISA_card-specific_setting***
Boot Options	Boot Drive Sequence: Keyboard Numlock at Boot:	**Drive A: then C:** **OFF**
Password Options	Password Protect Options:	**NONE**
	Password Edit:	**SKIP**

2 of 2

4 Select *Advanced Options* from the *Basic Options* screen. Select the values listed below.

Device	Parameters	Settings
Serial Ports	16550 Compatible UART 1: 16550 Compatible UART 2:	**02F8, IRQ3** **Disabled**
Parallel Ports	Select Parallel Port Address:	**Disabled**
PS/2 Mouse	On-board PS/2 Mouse Port:	**OFF**

1 of 4

Device	Parameters	Settings
Cache	Internal 16K Code/Data Cache:	**Enabled**
	Level 2 Write Back Cache:	**Enabled**
	Level 2 Cache Test:	**Disabled**
PCI Configuration	Is C800 Available to PCI?	**YES**
	Is CC00 Available to PCI?	**YES**
	Is D000 Available to PCI?	**NO**
	Is D400 Available to PCI?	**NO**
	Is D800 Available to PCI?	**NO**
	Is DC00 Available to PCI?	**NO**
	Is IRQ5 Available to PCI?	**NO**
	Is IRQ9 Available to PCI?	**NO**
	Is IRQ10 Available to PCI?	**YES**
	Is IRQ11 Available to PCI?	**YES**
	Is IRQ12 Available to PCI?	**YES**
	Is IRQ14 Available to PCI?	**YES**
	Is IRQ15 Available to PCI?	**YES**
	Integrated Adaptec PCI SCSI:	**Enabled**
	PCI Bus: Device 00:00:	**OK**
	PCI Bus: Device 00:01:	**OK**
	PCI Bus: Device 00:02:	**OK**
	PCI Bus: Device 00:0C:	**OK**
	Other_Devices_Installed:	**OK**

Device	Parameters	Settings
PCI INT/IRQ Binding	INTA IRQ Availability: INTB IRQ Availability: INTC IRQ Availability: INTD IRQ Availability:	**Automatic** **Automatic** **Automatic** **Automatic**
Memory Options	Base Memory Size: Memory Gap Block Size:	**640K** **Disabled**
System Performance	ISA Bus Speed: Guaranteed Access Time: DRAM Performance Mode: PCI Burst Mode: PCI to Memory Posting: Host to PCI Posting: DMA Performance Mode: ISA Performance Mode: 8-Bit I/O Recovery Time: 16-Bit I/O Recovery Time:	**7.5MHz** **Disabled** **Enhanced** **Enhanced** **Enhanced** **Standard** **Enhanced** **Enhanced** **6 SYSCLK** **6 SYSCLK**

To reverse the last jump, press ◄◄ on the Acrobat tool bar

Device	Parameters	Settings
Miscellaneous	Watchdog Timer Delay: ISA/PCI Option ROM Scan Order:	**1.2 sec.** **PCI ROM Scan First**
Console Redirection	COM1 Baud Rate: COM2 Baud Rate: Redirected Terminal Type: COM3 Baud Rate: COM4 Baud Rate:	NOT USED 19200 VT100 NOT USED NOT USED

4 of 4

5 Once all parameters have been specified, select **Flash It!** from the **Basic Options** menu.

This stores the current contents of CMOS memory, including the new changes, to BIOS flash memory. CMOS RAM is now restored.

Restoring hardware-resident default BIOS configuration

When all else fails, you can force the system to disregard CMOS RAM settings and reconfigure using default settings that you saved to non-volatile Flash memory during setup. These settings reflect the state of the original installation, not necessarily its current state. So you will have to proceed with *Restoring BIOS configuration from a backup diskette* or *Restoring BIOS configuration from the console* after completing the steps in this section. Follow the steps below.

1. Power down gracefully (if possible), see *Powering down, page 403*.
2. Attach a grounding wrist strap to your wrist and to the server chassis.
3. Turn BIOS switch SW1-3 **ON** (*Figure 47*).

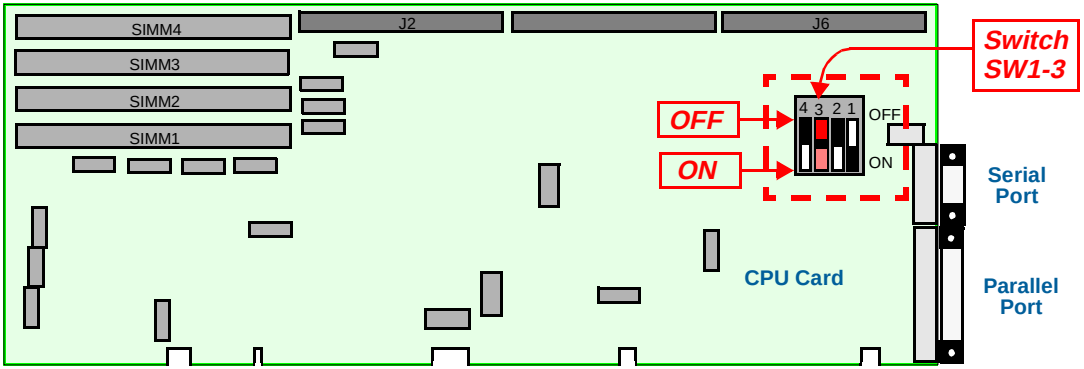


Figure 47. Location of switch SW1-3 on CPU card

4 Turn the power switch **ON**.

You should see the following message.

```
System Switch 3 is ON - Default System Configuration Loaded
```

Figure 48. Switch SW1-3 is ON

5 When the server finishes rebooting, turn the power switch **OFF**.

6 Turn switch SW1-3 **OFF**.

7 Go to *Restoring BIOS configuration from a backup diskette*.

8 If the console warns you that configuration information is invalid when you power up and asks you to run the Setup program, press **F2**, and go to *Restoring BIOS configuration from the console*.

9 When configuration is correct, type **reset level=boot ENTER**.

Recovering from a hard disk failure

This section covers reinstalling software when a hard drive is failing or has failed. Perform all of the steps below, in the order specified.

Repairing the file system

A corrupted file system can make the hard disk unbootable. So, before you go to the trouble of replacing a disk, try to repair the file system. Proceed as follows.

1. Power down gracefully (if possible) using the *Powering down*.
2. Insert the boot floppy disk in the disk drive.
3. Turn the power **ON**.

   The BIOS version number appears, and the LynxOS operating system begins to load.

4 When you are instructed to insert the boot utility diskette in the floppy drive, do so. Then press **ENTER**. The operating system displays a menu like that in *Figure 49*

```
1.  Initialize the hard disk.
2.  Install software on the hard disk.
3.  Escape to shell (ksh).
4.  Help.
```

Figure 49. LynxOS initialization menu

5 Type **3 ENTER** to escape to the shell.

6 At the # prompt, type **fsck /dev/ad2940.0a ENTER.**

FSCK repairs the file system. If it finds orphaned files, it saves them to a ***/lost+found*** directory (see *Maintaining and replacing server hardware*).

7 Remove the floppy disk from the floppy disk drive, and type **reboot -a ENTER**.

Booting from a diskette

Use the boot floppy disks to load the BIOS and LynxOS operating system.

1 Power down gracefully (if possible) using the *Powering down*.

2 Insert the first boot diskette in the floppy disk drive. It is an Ethernet or an ATM boot floppy, depending on your system.

3 Turn the power **ON**.

The BIOS version message appears and the LynxOS operating system starts to load.

4 When prompted, remove the first boot diskette from the floppy disk drive.

5 Insert the boot utility diskette in the floppy drive. Then press **ENTER**. The operating system displays a menu like that in *Figure 49*

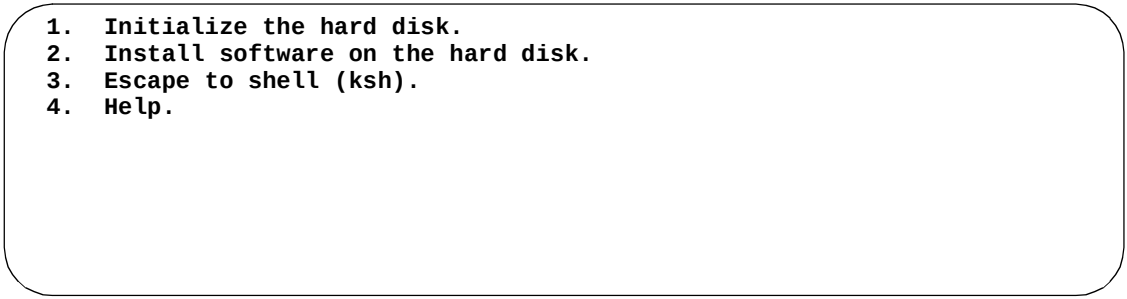


Figure 50. LynxOS initialization menu

6 Go to *Initializing the hard disk and installing boot utilities*.

Initializing the hard disk and installing boot utilities

Now you have to name the hard disk and partition and specify a file system block size. Proceed as follows.

1. Type **1 ENTER** to initialize the hard disk.

   The server asks if you want to enter a hard disk device name or use the default.
2. If the default name is correct, press **ENTER**. Otherwise, type ***drive-name*** **ENTER**.

   The server asks if you want to enter a partition name or use the default.
3. If the default partition name is correct, press **ENTER**. Otherwise, type ***partition-name*** **ENTER**.

   The server asks if you want to specify a file system block size or use the default.
4. If the default file system block size is correct, press **ENTER**. Otherwise type ***file-system-block-size*** **ENTER**.

   The server asks if you want to **Continue with device information**
5. Press **Y ENTER** to proceed.
6. When the initialization menu reappears, type **2 ENTER** to install software.
7. Remove the boot utilities floppy disk from the floppy disk drive.
8. Insert the install utilities floppy disk, and press **ENTER** to continue.

   The software installs.
9. Remove the install utilities floppy disk from the floppy drive.
10. Install the boot utilities. Insert the boot utilities floppy disk in the diskette drive, and press **ENTER** to continue.
11. Go to *Restoring the IP configuration*.

Restoring the IP configuration

At this point in the recovery process, the *System menu* appears.

```
1.  IP Configuration
2.  System Backup - Perform a System backup of system files.
3.  System Restore - Restore the system files from backup.
4.  Install release software.
5.  Continue booting of the software to full service state.
6.  Continue booting of the software to ready for service.
7.  Quit without booting - quit the menu but do not continue to boot.
8.  Escape to LYNX-OS.
9.  Help
```

Figure 51. System menu

Carry out the procedure below.

1 At the prompt, press 1 **ENTER** to select **IP Configuration**.

The *IP configuration menu* appears.

```
1.  Configure Network Interface Cards
2.  Configure Default IP Route
3.  Define System Server Name
4.  Return to previous menu
5.  Help
```

Figure 52. IP configuration menu

2 At the *IP configuration menu* prompt, press **1 ENTER** to configure the network interface cards.

The *NIC configuration menu* appears. *Note that this procedure merely sets up the minimum configuration that the server can recognize. You probably have to do additional work before the network is fully functional. See Configuration Management, page 70.*

```
Select a network interface card (NIC) to configure
1.  p5:1  (dec5)
q.  Quit current process and return to previous menu
?.  Help
Please enter a selection (Default - 1):
```

Figure 53. NIC configuration menu

3 At the prompt, press **ENTER.**

The system prompts you for an IP address and net mask.

4 At the prompt, enter the server's IP address.

5 At the prompt, enter the IP netmask.

The server displays the IP information you entered.

6 Check the information you entered. If correct, press **Y ENTER** to return to the *NIC configuration menu*. Otherwise press **N ENTER**, and go back to step 3.

7 At the prompt, press **Q ENTER** to return to the *IP configuration menu*.

8 At the prompt, press **2 ENTER** to select **Configure Default IP Route**.

9 At the, enter the ***IP-router-address*** for the server.

The server displays the new router address. *Note that this is just the default. To define other IP router addresses, see Configuring the IP routing table, page 116*.

10 Check the router address information. If correct, press **Y ENTER** to save the changes and return to the *IP configuration menu*. Otherwise, press **N ENTER**, and return to step 9.

11 At the prompt, press **3 ENTER** to define the system server name.

The server prompts you for a server name.

12 At the prompt, enter the name of the server, and press **ENTER**.

The system prompts you for a corresponding NIC card.

13 At the, prompt, press **ENTER**.

The server displays the server name information.

14 Check the server name. If correct, press **Y ENTER** to return to the *IP configuration menu*. Otherwise press **N ENTER** to start over at step 12.

15 Press **4 ENTER** to return to the *System menu*.

16 Go to *Installing MMCX server software*.

10 Responding to user-reported problems

MMCX users sometimes report problems before you see anything wrong on the server. When dealing with these problems, follow the procedure below.

If	Then
1 A user reports an audio or video problem at his workstation.	Examine the alarm log for anything that might explain the problem. To display the hardware alarms, type **showalarm data=hw-long | more RETURN**. Then, to display software alarms, type **showalarm data=sw-long | more RETURN**.
2 You see one or more alarm conditions that might explain the user's problem.	Carry out the repair action specified in the alarm table entry (see *Viewing and interpreting alarm messages, page 156*).
3 You see no significant alarms or the specified repairs did not solve the user's problem.	Find out whether other users are affected.
4 The problem occurs on a single endpoint.	Consult the *MMCX User's Guide* for diagnostic advice.
5 The problem affects every user on a particular server.	Reset the problem server. Type **reset level=cold2 ENTER**.

If	Then
6 The problem is still unresolved.	Answer the following questions. • Do intraserver calls work? • Do interworking calls work? • Do interserver calls work?
7 Intraserver and interworking calls complete, but interserver calls time-out without giving the calling party any feedback.	Interserver routing numbers may be incorrectly administered. Go to *Maintaining wide area networks, page 328*.
8 Intraserver calls work, but interworking and interserver calls fail. The calling party receives a reorder tone.	Something may be wrong with the PRI facility. Contact your service provider for assistance.
9 The problem is still unresolved.	Get help. Go to *Repair Number 0 - Escalate to MACS, page 162*.

A Manual Pages

This appendix contains the manual pages for MMCX. The following table is a cross reference to the individual manual pages.

INTRO

MMCX system management commands provide access to the SNMP (Simple Network Management Protocol) MIB (Management Information Base). SNMP is an official Internet standard for system and network management.

The SNMP MIB is an abstract or virtual database of management information. There are many standard groups and objects in the MIB that apply across systems, described in Internet RFC (Request for Comment) documents. The MIB also contains groups and objects specifically for MMCX systems, described in MMCX documentation.

Since SNMP is an official standard, several vendors provide network management systems and software applications that use it. Those systems can use the MMCX MIB to manage an MMCX system.

MMCX system management commands give a high-level application view of the MIB. They can be used for primary system management, and they serve as a backup if an external network management system fails.

With a few exceptions, each command performs one of four actions: add, remove, change, or show. The second part of the command identifies the object it acts on, for example rmusr to delete an MMCX user from the server user table, or chgpri to change the parameters of the PRI board. See the *HELP, page 477* manual page for a high-level view of all commands.

Many MIB tables contain counts: event counts, error counts, performance counts. They start at zero when the system is initialized and grow until the next system initialization. A rapidly changing count may reach its maximum, usually a ten-digit integer, and overflow to zero.

There is no concept of resetting counts in SNMP. To get a count for a specified interval, request the count at the beginning and end of the interval and subtract, allowing for overflow if necessary.

OPTIONS

A few common options appear in many MMCX system management manual pages.

slot=***slot-number*** and **port**=***port-number*** identify a network interface by its physical slot and port.

A slot number has a one-character prefix to identify the bus type: “i” for ISA or “P” for PCI. Slot numbers range from P1 - P6 and i1 - i6.

Port number is a small integer with range depending on the interface type, at most 1 - 6. Where slot and port are optional, the default is “all”.

dial=***dialed-number*** is a dialed number or an expression that represents a group of numbers. For example “dial=538+” applies the action to all dialed numbers beginning with 538.

srv=***server-name*** identifies an MMCX server by name, e.g. “mmcx3”.

plan=***pri-routing-plan*** refers to a PRI routing plan and can be from 1 to 32.

data=***data-type*** allows the user to select a subset of the available data. The data subsets and their contents vary between commands.

time=***date-and-time*** specifies a date and time in a specific format. A time specification containing blanks must be enclosed in single or double quotes, for example “time=”10/31 16:00:00””.

With all MMCX system management commands, the user may type a partial option. For example, **addpri lcomp=3** or **addpri lcomp=length266to399ft**.

Also, with all enumerated types, the user may enter either the number for that enumerated type or the corresponding string. For example, "**adddp dir=in**", and "**adddp dir=1**" are equivalent. When a parameter is displayed as the result of a show command, the string value is displayed usually followed by the numerical value in parentheses.

For example, **type** and **status** have enumerated values in the following display:

```
DESTINATION    SLOT     PORT       NEXTHOP          TYPE          STATUS
135.1.16.116   p1       1          135.2.17.144     direct(3)     netmgmt(3)
```

DIAGNOSTICS

All commands print an SNMP agent error message if a valid SNMP request fails. Other general causes of failure include: an unrecognized keyword in a ***keyword=value*** argument, an invalid value, or unknown server name. A request to add an object already present will fail. A request to show, remove or change an object will fail if that object is not found.

SEE ALSO

HELP, page 477

ALARMMON

NAME

clearalarm, **showalarm**, **showtraps** - use to clear and show hardware and software alarms, monitor ongoing alarms and traps

SYNOPSIS

clearalarm data=***data-type*** [**seq**=***sequence-number***] [**confirm**=***confirm***]

showalarm [**data=*data-type***] [**seq**=***sequence-number***] [**slot**=***slot-number***] [**port**=***port-number***] [**state**=***alarm-state***] [**sev**=***alarm-severity***] [**src**=***source***] [**start**=***start-time***] [**end**=***end-time***]

showtraps

DESCRIPTION

When an alarmable event has reached a pre-determined threshold, an alarm is registered. The system administrator (SA) can view these alarms via the **showalarm** command. Each alarm retrieved through **showalarm** will provide a suggested remedial action as well as an action code. This code correlates to an additional set of suggested maintenance actions in the maintenance documentation.

The **clearalarm** command clears one specific or all errors and alarms in the MMCX system. The default condition is to be prompted for confirmation. "**confirm=no**" will override the default condition.

The **showtraps** command provides realtime monitoring of new traps as they become registered by MMCX. It performs a “sleep and read” endless loop function which attempts to read further trap records as they become registered.

A trap is a special type of alarm. As alarms are generated and change states, MMCX software determines whether the situation is serious enough to generate a trap. If so, MMCX sends an SNMP trap to the terminal running the **showtraps** command.

This command can be terminated with a <Ctrl-C> or by killing the process.

OPTIONS

The **showalarm** command shows the current and historical set of software and hardware alarms that the system manager may use to uncover a problem condition within MMCX. If no options are used, all errors and alarms are shown.

data-type specifies the type of data requested. The options are:

- **hw-short** - short version of hardware alarms
- **hw-long** - long version of hardware alarms
- **sw-short** - short version of software alarms
- **sw-long** - long version of software alarms

The default for ***data-type*** is to show the short version of hardware alarms followed by the short version of software alarms (**hw-short**, **sw-short**). The user can override this default by specifying any data-type or combination of data-types desired.

sequence-number specifies the event that you want data on. The default is to show all sequence numbers. Sequence numbers are created for each alarmed event, so a single alarm code may appear with different sequence numbers.

slot-number consists of the prefix for the type of bus (p for PCI, and i for ISA) along with the slot number (1 to 6); for instance, slot 3 on the PCI bus is represented as p3, and slot 5 on the ISA bus is represented as i5. All Ethernet interfaces are on the PCI bus, so this field will start with a “p”. To retrieve alarms over two or more slots, use a comma separated list or use a dash, for example **slot=i5,i4** or **slot=p1-p6**. This option is ignored for software alarms.

port-number is the number of the port within that particular slot. To retrieve alarms over the full range of ports on slot 5, set **slot=p5** and leave out port. To retrieve alarms over two or more ports, use a comma separated list or use a dash, for example **port=1,2** or **port=1-4**. This option is ignored for software alarms.

source is the source of the alarm. For hardware alarms it is the name of the board where the alarm originated:

- ETHER_PT
- ATM/OC3-PT, WILD
- PRI_INTF
- CPU.

For software alarms, it is the name of the software process that created the alarm. If multiple ***sources*** are specified, then those source-types will be shown in the order of their input. The default is to show all source-types.

alarm-state is either: “**active**”, “**inactive**”, “**resMaint**” for resolved by maintenance, “**resClear**” for resolved by the clearalarm command, or “**resBoot**” for resolved by reboot. If nothing is specified, then all errors and alarms are shown.

alarm-severity is either “**none**”, “**warn**”, “**minor**”, or “**major**”. If multiple ***alarm-severities*** are specified, then those types will be shown in the order of their input. However, if no ***alarm-severity*** is specified, then all types will be shown.

start-time and ***end-time*** bracket the interval of interest. The format for these fields is “MM/DD/YY hh:mm:ss” where YY is the year, MM is the month, DD is the day, hh is the hour, mm is the minute, and ss is the second. This field should always be 17 characters, so if January is the desired month, MM should be set to 01 and not 1. Also, hh should be expressed in terms of a 24 hour clock (00-23).

If the start-time is missing, the default is the earliest time in the alarms log, If the end-time is missing, the default is the time of request. If the start-time is used, then all entries with **RESOLVE_TIME >= start** will be shown. If end-time is used, then all entries with **ALARM_TIME <= end** will be shown.

Other fields that are not options but are displayed include:

- **Alarm Time** - the time at which this event first triggered an alarm.
- **Resolve Time** - the time at which the alarm was resolved.
- **First Occur** - the time at which this event first occurred.
- **Last Occur** - the time at which this event last occurred.
- **Count** - the number of times this event has occurred.
- **Type** - the type of error event that has occurred.
- **RPR** - the repair action number for this alarm.

Note: Time fields do not display the year in order to save space. These fields appear as MM/DD.

For hardware alarms only:

- **brd** - indicates whether this alarmable error occurred in a specific board (**on** or **off**).
- **srv** - the service state of the hardware that caused the event (**in** or **out**).
- **aux** - a number that passes additional information for use with particular repairs.

For software alarms only:

- **code** - a number that identifies the source code line that generated the event.
- **aux1** - a number that passes additional information for use with particular repairs.
- **aux2** - a number that passes additional information for use with particular repairs.

The **clearalarm** command allows you to clear a specific alarm or clear all alarms.

This command takes the following options:

- ***data-type*** indicates the type of alarm(s) you want to clear. It is a required option and it can be set to: "**hw**", "**sw**", or "**total**". If you specify "**total**", then all alarms will be cleared. The option "**hw**" clears a specific hardware alarm while "**sw**" clears a specific software alarm. Both "**hw**" and "**sw**" require that a **sequence-number** be specified.
- ***sequence-number*** specifies the sequence number to clear for hardware and software alarms. It is ignored if ***data-type*** is set to total.
- ***confirm*** is a flag used to determine if a confirmation should be requested. If confirm is set to "**no**", then no confirmation message will be shown. If it is set to "**yes**" (or anything else), a confirmation message will be shown. The default for this field is "**yes**".

The **showtraps** command allows you to view traps as MMCX generates them. It is advisable to dedicate a window specifically for this purpose. The **showtraps** command takes no arguments.

EXAMPLES

To show the long version of hardware alarms of source type “WILD” which were resolved after 3:45pm on Jan 1, 1996.

```
$ showalarm data=hw-long src=WILD start=01/01/96
         HARDWARE ALARMS -- LONG
        ======================
STATE      SVRTY  SOURCE  ST PT   ALARM_TIME       RESOLVE_TIME       SEQ#
resBoot    major  WILD    i1 1    12/31 17:03:21   01/01/96 16:26:12  2
resBoot    major  WILD    i1 1    12/31 17:03:21   01/01/96 16:26:12  3

SEQ#  COUNT  RATE  FIRST_OCCUR     LAST_OCCUR      BRD SRV  CODE RPR AUX
3     12     15    12/31 17:03:21  12/31 17:06:43  on in    2    4   1
3     22     15    12/31 17:03:21  12/31 17:06:43  on in    3    5   1
```

To show the long version of all cleared software alarms which became alarms before the start of 1996.

```
$ showalarm data=sw-long state=resClear end=01/01/96
         SOFTWARE ALARMS -- LONG
        ======================
STATE      SVRTY  SOURCE  CODE   ALARM_TIME       RESOLVE_TIME       SEQ#
resClear   minor  mtce    0      12/31 17:03:21   01/02/96 17:31:20  3
resClear   minor  mtce    0      10/31 17:47:00   01/02/96 17:28:22  6
resClear   none   mtce    16384  12/31 17:00:00   01/02/96 17:28:22  7


SEQ#  COUNT  RATE  FIRST_OCCUR     LAST_OCCUR         CODE  RPR  AUX1   AUX2
```

```
3     7      2     12/31 17:03:21  12/31/95 17:06:43  3     1    12     15
6     7      0     11/01 03:30:50  11/27/95 15:11:22  6     2    13     16
7     1      0     12/31 08:07:01  01/01/96 08:07:01  16384 3    14     17
```

To monitor alarms.

```
$ showtraps
TIME              TRAP_NAME           STATE    SVRTY  SOURCE    LOC   SEQ#
02/01 12:24:36    Software Alarm      active   minor  mtce      1234  5
02/01 12:40:01    Hardware Alarm      active   major  PRI_INTF  i5:1  6
02/02 00:00:00    Authentication Fail -        -      -         -     -
```

The meaning of the headings are as follows:

- **Time** - the time that the trap was received, as determined by the server.
- **Trap_name** - the name of the trap. Values are:
  - Software alarm
  - Hardware alarm
  - Authentication fail
  - Cold start
  - Warm start
  - Link down
  - Link up
  - Unknown trap

The following fields are only valid for hardware or software alarms:

- **State** - the same as **showalarm**; however, traps will most likely be in the active state
- **Source** - the same as **showalarm**

- **Loc** - for software alarms, this is the code (software location), for hardware alarms, this is the slot and port location.
- **Seq**# - the same as **showalarm**

To clear the software alarm with sequence number 87 without confirmation.

```
$ clearalarm data=sw seq=87 confirm=no
Your request to clearalarm succeeded.
```

DIAGNOSTICS

MIB GROUPS

mmcxHWAlarmTable, mmcxSWAlarmTable, mmcxAlarmThresholdTable

SEE ALSO

INTRO, page 426

SNMPADM, page 572

ATMADM

NAME

addatm, chgatm, rmatm, showatm - administer the MMCX ATM (Asynchronous Transfer Mode) related information

SYNOPSIS

addatm slot=*slot-number* port=*port-number* ip=*ip-address* mask=*netmask-value*
[cap=*capacity*] [mode=*configuration-mode*]
[name=*LAN-name*] [addr=*ATM-address*] [control=*control-timeout*]
[count=*unknown-frame-count*] [time=*unknown-frame-time*]
[vcc=*VCC-timeout*] [retry=*max-retries*] [aging=*cache-aging-time*]
[forw=*forward-delay-time*] [resp=*ARP-response-time*]
[flush=*flush-timeout*] [conn=*connection-complete-timer*]

chgatm slot=*slot-number* port=*port-number* [ip=*ip-address*]
[mask=*netmask-value*] [cap=*capacity*] [mode=*configuration-mode*]
[name=*LAN-name*] [addr=*ATM-address*] [control=*control-timeout*]
[count=*unknown-frame-count*] [time=*unknown-frame-time*]
[vcc=*VCC-timeout*] [retry=*max-retries*] [aging=*cache-aging-time*]
[forw=*forward-delay-time*] [resp=*ARP-response-time*]
[flush=*flush-timeout*] [conn=*connection-complete-timer*]

rmatm slot=*slot-number* port=*port-number*

showatm [data=*data-type,data-type...*]
[slot=*slot- number,slot-number...*]
[port=*port-number,port-number...*]

DESCRIPTION

addatm allows a user to add an ATM LAN emulation client to the system. The valid ranges for the parameters that can be configured are:

- ***slot-number***: consists of the prefix for the type of bus (p for PCI, and i for ISA) along with the slot number (1 to 6). For instance, slot 3 on the PCI bus is represented as p3. All ATM interfaces are on PCI buses, so this field will start with a p.
- ***port-number***: valid range is dependent on the physical network card used (1-6).
- ***ip-address***: the IP address assigned to this ATM interface for LAN emulation.
- ***netmask-value***: the netmask value for this ATM interface for LAN emulation.
- ***capacity*****:** the optional estimated capacity of the ATM connection. The default is 100 Mbps (megabits per second). Increasing this parameter allows higher utilization of the connection with possible degradation of call quality.
- ***configuration mode***: automatic(1) or manual(2). Default is automatic(1). In automatic mode a client uses a LAN Emulation Configuration Server (LECS) to learn the ATM address of its LAN Emulation Server (LES). In manual mode, management tells the client the ATM address of its LES. See the description of the ATM address parameter below.
- ***LAN name***: up to 32 alphanumeric characters. In automatic configuration mode LAN name is used in the **Configure** request sent to a LECS. In manual mode it is used in the **Join** request sent to a LES.

- ***ATM address***: up to 40 hexadecimal digits (0-9, A-F), case-insensitive. This parameter is required in manual configuration mode, where it represents the ATM address of the LES which this client will use the next time it is started. In automatic mode this parameter gives the ATM address of the LECS. If the parameter is omitted in automatic mode, the system uses the well-known LECS address defined by the ATM Forum.

The user may also administer the following optional protocol parameters:

- ***control timeout***: 10-300 seconds. Default is 120 seconds. This is the timeout period for most request/response control frame interactions.
- ***max unknown frame count***: 1-10 frames. Default is 1 frame.
- ***max unknown frame time***: 1-60 seconds. Default is 1 second. Within max-unknown-frame-time seconds, a LAN emulation client will send at most max-unknown-frame-count frames to the bus for a given unicast LAN destination.
- ***VCC timeout***: 0-2147483647 seconds. Default is 1200 seconds, or 20 minutes. Zero seconds means the timeout period is infinite. A LAN Emulation Client should release any Data Direct Virtual Channel Connection (VCC) that it has not used to transmit or receive any data frames for the length of the VCC timeout period. This parameter is used only for SVC Data Direct VCS.
- ***max retry count***: 0-2 retries. Default is 1. A LAN emulation client must not retry an LE_ARP_ REQUEST message for a given frame's LAN destination more than max-retry-count times after the first request for that same frame's LAN destination.
- ***aging time***: 10-300 seconds. Default is 300 seconds. The maximum time that a LAN emulation client will maintain an entry in its LAN emulation ARP cache in the absence of a verification of that relationship.

- ***forward delay time***: 4-30 seconds. Default is 15 seconds. The maximum time that a LAN emulation client will maintain an entry for a non-local MAC address in its LAN emulation ARP cache in the absence of a verification of that relationship. Forward delay time should be less than aging time; otherwise aging time governs all ARP cache aging.
- ***ARP response time***: 1-30 seconds. Default is 1 second. The maximum time the client expects an LE_ARP_REQUEST/LE_ARP_RESPONSE cycle to take. Used for retries and verifies.
- ***Flush timeout***: 1-4 seconds. Default is 4 seconds. After an LE_FLUSH_REQUEST, the client will wait this long for an LE_FLUSH_RESPONSE before taking recovery action.
- ***Connection complete timer***: 1-10 seconds. Default is 4 seconds. During “Connection Establishment” this is the time within which either data or a READY_IND message is expected from a calling party.

chgatm allows a user to change the LAN emulation parameters described above for an ATM interface. The slot and port parameters should be specified to determine which interface to change.

rmatm allows a user to remove a row entry from the interface configuration table. A user needs to specify a valid slot number and a port number associated with that slot number for the command to succeed.

Note: When an ATM interface is removed, the IP address assigned to that interface cannot be reused until after a system reboot.

showatm is the command to view ATM related data for the optional slot number and optional port number. **data-type** can be one of the following:

- **cfg** - ATM local interface configuration parameters, one entry per ATM interface port.

- **stat** - LAN emulation interface configuration and state information.
- **count** - LAN emulation interface counts.
- **vcc** - LAN emulation VCC server connections.

If multiple data-types are specified, then that data will be shown in the order of their input. However, if no data-type is specified, then all data will be shown. The slot and port parameters let you specify which interfaces to retrieve data on. If only slot-number is specified, then the data associated with all the ports on that slot will be shown. If port-number is specified, then slot number must be specified as well. If no slot-number is specified, then data across all interfaces will be shown.

EXAMPLES

To add a row in the interface configuration table:

```
$ addatm slot=p4 port=1 ip=135.11.12.133 mask=255.255.255.0
Your request to addatm succeeded.
SLOT PORT HARDWARE IP_ADDRESS      NETMASK_VALUE   CAPACITY
p4   1    yes(1)   135.11.12.133   255.255.255.0   100
Your request to addatm succeeded.
LOC  CONFIG_MODE  LAN_TYPE       FRAME_SIZE     CTL CNT TIM
p4:1 automatic(1) aflane8023(2)  max1516(2)     120 1   1

LOC  VCC_IDLE   RTRY AGE FORW RESP FLSH CONN LAN_NAME
p4:1 1200       1    300 15   1    4    4    -

LOC  SERVER_ADDRESS
p4:1 -
```

Configuring an ATM interface modifies two tables in the server, and the system shows **request succeeded** for each one. The meaning of the headings are as follows:

- **SLOT**= the physical bus/slot that this interface resides on. The first letter indicates the bus type: p for PCI, i for ISA; the number following the bus type is the slot number.
- **PORT**= the physical port within this slot that the interface resides on.
- **HARDWARE**= whether or not the hardware for that interface is currently attached (**yes** or **no**).
- **IP_ADDRESS**= the IP address assigned to this ATM interface for LAN emulation.
- **NETMASK_VALUE**= the netmask value for this ATM interface for LAN emulation.
- **CAPACITY**= the estimated capacity of the ATM connection.
- **LOC**= abbreviated hardware location: slot and port in the form “p4:1”.
- **CONFIG_MODE**= configuration mode set in **addatm**: automatic(1) or manual(2).
- **LAN_TYPE**= LEC data frame format. In MMCX R1 this is always aflane8023(2).
- **FRAME_SIZE**= LEC data frame size. In MMCX R1 this is always max1516(2).
- **CTL**= control timeout
- **CNT**= max unknown frame count
- **TIM**= max unknown frame time
- **VCC_IDLE**= VCC timeout period
- **RTRY**= max retry count
- **AGE**= aging time
- **FORW**= forward delay time
- **RESP**= ARP response time
- **FLSH**= flush timeout
- **CONN**= connection complete timer

- **LAN_NAME**= LAN name
- **SERVER_ADDRESS**= server ATM address

To change a row in the interface configuration table:

```
$ chgatm slot=p4 port=1 cap=155
Your request to chgatm succeeded.
SLOT PORT HARDWARE IP_ADDRESS      NETMASK_VALUE   CAPACITY
p4   1    yes(1)   135.11.12.133   255.255.255.0   155
LOC  CONFIG_MODE  LAN_TYPE       FRAME_SIZE     CTL CNT TIM
p4:1 automatic(1) aflane8023(2)  max1516(2)     120 1   1
LOC  VCC_IDLE   RTRY AGE FORW RESP FLSH CONN LAN_NAME
p4:1 1200       1    300 15   1    4    4    -
LOC  SERVER_ADDRESS p4:1 -
```

The meaning of the headings is described above.

To view the ATM configuration table for all interfaces:

```
$ showatm data=cfg
ATM CONFIGURATION
=================
SLOT PORT HARDWARE IP_ADDRESS      NETMASK_VALUE   CAPACITY
p4   1    yes(1)   135.11.12.133   255.255.255.0   155
LOC  CONFIG_MODE  LAN_TYPE       FRAME_SIZE     CTL CNT TIM
p4:1 automatic(1) aflane8023(2)  max1516(2)     120 1   1
LOC  VCC_IDLE   RTRY AGE FORW RESP FLSH CONN LAN_NAME
p4:1 1200       1    300 15   1    4    4    -
LOC  SERVER_ADDRESS p4:1 -
```

The meaning of the headings is described above.

To view the LAN emulation client status table:

```
$ showatm data=stat
ATM CURRENT STATUS
==================
LOC  LEC_ID     INTF_STATE          PTC VER TOPOL LAN_TYPE    FRAME_SIZE
p4:1 0          11                  1   1   false aflane8023  max1516
LOC  CONFIG_SOURCE        PROXY  LAN_NAME
p4:1 usedWellKnownAddress false  1
LOC  LEC_CLIENT_ATM_ADDRESS
p4:1 39 00 00 00 00 00 00 00 00 00 00 00 00 77 88 71 00 00
LOC  LECS_CONFIG_SVR_ATM_ADDRESS
p4:1 47 00 79 00 00 00 00 00 00 00 00 00 00 A0 3E 00 00 01 00
LOC  LES_SERVER_ATM_ADDRESS
p4:1 47 00 79 00 00 00 00 00 00 00 00 00 00 A0 3E 00 00 01 00
```

The meanings of the headings are as follows:

- **LOC** is defined above.
- **LEC_ID**= LAN emulation client identifier assigned by the LES during the **Join** phase. The LEC ID is placed in control requests by the LE client and may be used for echo suppression on multicast data frames sent by that LE client.
- **INTF_STATE**= The current state of the LAN emulation client. This will be one of initialState(1), lecsConnect(2), configure(3), join(4), initialRegistration(5), busConnect(6), operational(7).
- **PTC**= The LAN emulation protocol which this client supports, and specifies in its LE_JOIN_ REQUEST messages.
- **VER**= The LAN emulation protocol version which this client supports, and specifies in its LE_ JOIN_REQUEST messages.

- **TOPOL**= Indicates whether the LE client is using the forward delay time instead of the aging time to age non-local entries in its LE_ARP cache. See the description of **addatm** parameters aging time and forward delay time.
- **LAN_TYPE** and **FRAME_SIZE** are defined above.
- **CONFIG_SOURCE**= Indicates whether this LE client used the LAN emulation configuration server, and if so, what method it used to establish the configuration direct VCC. Values include:
  - gotAddressViaIlmi(1),
  - usedWellKnownAddress(2),
  - usedLecsPvc(3)
  - didNotUseLecs(4).
- **PROXY**= Indicates whether this client is acting as a proxy. Proxy clients are allowed to represent unregistered MAC addresses, and receive copies of LE_ARP_REQUEST frames for such addresses.
- **LAN_NAME** is defined above.
- **LEC_CLIENT_ATM_ADDRESS**= The primary ATM address of this LAN emulation client. This address is used to establish the control direct and multicast send VCC, and may also be used to set up data direct VCC.
- **LECS_CONFIG_SVR_ATM_ADDRESS**= The ATM address of the LAN emulation configuration server, if known. If the LECS address is not known this field is blank.
- **LES_SERVER_ATM_ADDRESS**= The LAN emulation server address currently in use or most recently attempted. If no LES attachment has been tried this field is blank.

To view the LAN emulation client statistics table:

```
$ showatm data=count
```

```
ATM COUNTS
==========
LOC  REQ_OUT    REQ_IN     REP_OUT    REP_IN     FRAME_OUT  FRAME_IN SVC_FAIL
p4:1 1          0          0          1          3          3          0
```

The meanings of the headings are as follows:

- **LOC** is defined above.
- **REQ_OUT**= The number of LE_ARP_REQUESTs sent by this LE client.
- **REQ_IN**= The number of LE_ARP_REQUESTs received by this LE client. Requests may arrive on the control direct VCC or on the control distribute VCC, depending on how the LES is implemented and the chances it has had for learning. This counter covers both VCCs.
- **REP_OUT**= The number of LE_ARP_RESPONSEs sent by this LE client.
- **REP_IN**= The number of LE_ARP_RESPONSEs received by this LE client. Responses may arrive on the control direct VCC or on the control distribute VCC, depending on how the LES is implemented. This counter covers both VCCs.
- **FRAME_OUT**= The total number of control packets sent by this LE client.
- **FRAME_IN**= The total number of control packets received by this LE client.
- **SVC_FAIL**= The total number of SVC failures, including: out-going LE SVCs Sifts which this client tried, but failed, to open; incoming LE SVCs which this client tried, but failed, to establish; incoming LE SVCs which this client rejected for protocol or security reasons.

To view the LAN emulation client server VCC table:

```
$ showatm data=vcc
ATM SERVER CONNECTIONS
======================
LOC  CTL_DIR VPI VCI CTL_DIS VPI VCI MC_SEND VPI VCI MC_FORW VPIV CI
```

```
p4:1 p4:1    0   131    p4:1    0   132    p4:1    0   133    p4:1    0   134
```

The meaning of the headings are as follows:

- **LOC** is defined above.
- **CTL_DIR**= Control direct VCC interface.
- **TL_DIS**= Control distribute VCC interface.
- **MC_SEND**= Multicast send VCC interface.
- **MC_FORW**= Multicast forward VCC interface.
- **VPI**= Virtual path identifier
- **VCI**= Virtual channel identifier

VPI and VCI together represent the ATM channel number. This table shows VPI and VCI for four network interfaces associated with LE virtual channel connections (VCCs).

In MMCX R1, the four interfaces will be the same, but in future releases they may be different. The two columns following each interface give VPI and VCI for that interface. If a VCC does not currently exist, its VPI and VCI will both be zero.

To remove a row from the interface configuration table:

```
$ rmatm slot=p4 port=1
Your request to rmatm succeeded.
```

DIAGNOSTICS

addatm will fail if no parameters are specified or if invalid parameters are specified.

rmatm will fail if invalid slot or port numbers are specified, or if no parameters are specified.

MIB GROUPS

LAN emulation client MIB (ATM Forum LAN Emulation Client Management: Version 1.0).

GLOSSARY

ARP Address Resolution Protocol

ATM Asynchronous Transfer Mode

BUS Broadcast and Unknown Server

LE LAN Emulation

LEC LAN Emulation Client

LECS LAN Emulation Configuration Server

LES LAN Emulation Server

MAC Media Access Control, a 6-byte hardware address unique for every interface card.

SVC Switched Virtual Channel

VCC Virtual Channel Connection

VCI Virtual Channel Identifier

VPI Virtual Path Identifier

IP Internet Protocol

ISA

LAN Local Area Network

PCI

multicast messages sent to multiple recipients

unicast messages sent to exactly one recipient

SEE ALSO

INTRO, page 426

INTFADM, page 479

IPADM, page 483

BACKUP

NAME

backup - start a system backup

SYNOPSIS

backup [**host=*hostname***] [**dir=*dirname***] [**user=*username***] [**prompt=*y/n***]

DESCRIPTION

This command allows the caller to start a backup of specific MMCX system files to a specific site. Parameters for the backup can come from the command line, read from a configuration file (such as **/mmcs/backrest/config.dat**) or taken from system defaults.

The system backup reads lines from a backup file (such as **/mmcs/backrest/backup.txt**) that lists the files and directories that should be backed up. Processing copies the files and directories to a backup staging area until it can be sent to the designated output device.

This command can be executed from a command line or from a user supplied script using **prompt=n**. However, the MMCX environment must be setup for proper execution.

OPTIONS

host=***hostname***: Overrides the default or configured target host device name for this backup. The hostname must be a valid foreign host (e.g. an IP address in dot notation), LOCAL (indicating the backup is done to a local directory) or FLOPPY (indicating the backup is done to a correctly formatted diskette in the server's floppy drive). The default is LOCAL, overridden by the Host= value in the configuration file.

dir=***dirname***: Overrides the default or configured target directory name for this backup. The dirname must be a fully qualified path on the target host device. The default is /mmcs/backrest, overridden by the dir= value in the configuration file.

user=***username***: Overrides the default or configured target host user name. The ***username*** is only used when backing up to a foreign host (e.g. some host in the network) and provides access to the foreign host for the backup. The default is mmcx, overridden by the **User**= ***value*** in the configuration file.

prompt=***y***|***n***: This parameter indicates whether the command should prompt for target information verification prior to starting the backup or go ahead without verification. The default is "***y***". Use of the "***n***" option is recommended when executing this command from a script in the background.

The log information is saved in a log file called ***BR.log*** in the directory defined by the LOGROOT environmental variable or the standard system logfile also located in the same area.

EXAMPLES

To backup a system with default or configured target information:

```
example% backup
```

To backup a system and override the default/configured target information:

```
example% backup host=121.21.212.1 dir=/mmcs/backup user=jdoe
```

To backup a system to a diskette in the server's floppy drive:

```
example% backup host=FLOPPY dir=/
```

To backup a system to a local server directory:

```
example% backup host=LOCAL dir=/tmp
```

WARNINGS

Any previous backup to the same target host and directory combination will be overwritten by the current successful backup process. Backups to the same floppy device but different floppy disks will indicate that previous backups to that device are unavailable when issuing a display from the administration menu.

Of course, the backup archive on the disk is very much available. Care must be taken to manage floppy disk backups so that if a restore is done, it is done using the intended backup version.

Any foreign device used to read from or write to for this process must have been previously mounted prior to invoking the command. Any floppy disk backups require the floppy disk be correctly formatted prior to the backup.

Restorations from a backup are only allowed from the administration menu. Please refer to other documentation for correct entry methods to the administration menu.

FILES

/mmcs/backrest/config.dat

/mmcs/backrest/backup.txt

SEE ALSO

RESET, page 544

BUGS

No known bugs.

BWADM

NAME

chgbw, **showbw** - change and view system-wide bandwidth parameters

SYNOPSIS

chgbw data=***data-type*** [**max**=***maximum-bandwidth***] [**init**=***initial-bandwidth***] [**sub**=***subsequent-bandwidth***]

showbw

DESCRIPTION

Bandwidth administration allows the system manager to adjust system-wide priorities for access to PRI bandwidth resources. All bandwidth parameters are in units of KBPS (kilobits per sec), and 64-kbps equates to one B-channel or one audio call. If PRI usage is low enough that bandwidth is not a scarce resource, these commands are unnecessary. But if PRI bandwidth is used heavily the system manager may want to adjust priorities.

Each PRI interface supports 23 (T1) or 30 (E1) B-channels. There may be up to eight PRI interfaces in a MMCX server, for a maximum of 15,360 kbps bandwidth per server. Of course, the actual bandwidth available will depend on the server's configuration.

chgbw sets the maximum bandwidth for video calls as well as the initial and subsequent bandwidths for shared and distributed applications.

The ***data-type*** parameter indicates what media to change bandwidth parameters for. The three applicable types are:

- **video** - set maximum video bandwidth
- **share** - set initial and subsequent bandwidth for shared applications
- **dist** - set initial and subsequent bandwidth for distributed applications

If ***data-type*** is set to '**video**', then only the ***maximum-bandwidth*** parameter is applicable. It signifies the maximum bandwidth that any one video call on the server can use. The other parameters, if specified, will be ignored. Likewise, if ***data-type*** is set to '**share**' or '**dist**', then either ***initial-bandwidth*** or ***subsequent-bandwidth***, or both, can be set.

Maximum-bandwidth, if specified, will be ignored. ***Initial-bandwidth*** indicates the bandwidth allocated to all shared or distributed applications on their first call to a remote server connected via the Wide Area Network. ***Subsequent-bandwidth***, on the other hand, indicates the bandwith for second and subsequent calls to that remote server.

showbw shows the current setting of the bandwidth parameters described above.

EXAMPLES

To show the current setting of the system-wide bandwidth parameters:

```
$ showbw
BANDWIDTH IN KBPS
                VIDEO MAXIMUM:     0
            SHARED APP INITIAL:    128
         SHARED APP SUBSEQUENT:    128
       DISTRIBUTED APP INITIAL:    128
    DISTRIBUTED APP SUBSEQUENT:    128
```

To update video maximum bandwidth to allocate 512 kbps for video calls:

```
$ chgbw data=video max=512
Your request to chgbw succeeded.
BANDWIDTH IN KBPS
                VIDEO MAXIMUM:     512
           SHARED APP INITIAL:     128
        SHARED APP SUBSEQUENT:     128
      DISTRIBUTED APP INITIAL:     128
   DISTRIBUTED APP SUBSEQUENT:     128
```

To improve response time of subsequent application connections by increasing the subsequent-percentage parameter for shared applications:

```
$ chgbw data=share sub=192
Your request to chgbw succeeded.
BANDWIDTH IN KBPS
              VIDEO MAXIMUM:     512
         SHARED APP INITIAL:     128
      SHARED APP SUBSEQUENT:     192
    DISTRIBUTED APP INITIAL:     128
 DISTRIBUTED APP SUBSEQUENT:     128
```

DIAGNOSTICS

MIB GROUPS

mmcxBandwidth

SEE ALSO

INTRO, page 426

PRIADM, page 521

PRPADM, page 534

PTGADM, page 538

CFGADM

NAME

addisrnum, **chgsys**, **rmisrnum**, **showsys**, **showstor**, **showdev**, **showdsk**, **showisrnum** - administer system-wide parameters, show host resource configuration and status

SYNOPSIS

addisrnum phone=***isr-phone-number***

chgsys [**extlen**=***extension-number-length***] [**befcvr**=***seconds-before-coverage***] [**atcvr**=***seconds-at-coverage***] [**pstnac**=***pstn-access-code***] [**pbxac**=***pbx-access-code***]

rmisrnum phone=***isr-phone-number***

showsys

showstor

showdev

showdsk

showisrnum

DESCRIPTION

addisrnum is the command to add a number to the PRI phone number list. This is the list of phone numbers for which other servers can call this server over ISDN PRI.

rmisrnum will remove the specified number from the list, while **showisrnum** shows the current list of PRI phone numbers.

chgsys is the command to change certain system-wide parameters. The parameters that can be changed are:

- ***extension-number-length*** - number of digits in user extension numbers; all users will have extensions of the same length, which can be from 3 to 7 digits; (3-7). Note the ***extension-number-length*** field can not be changed after a user has been configured. Also, no user can be configured until this field is first set.
- ***seconds-before-coverage*** - number of seconds of ringing before calls go to coverage (1-99, default=10)
- ***seconds-at-coverage*** - number of seconds of ringing at each coverage point (1-99, default=10)
- ***pstn-access-code*** - the access code for connecting to the pstn (public switched telephone network); this access code is from 1 to 3 digits, the first of which can be an asterisk (*).
- ***pbx-access-code*** - the access code for connecting to a pbx; this code is from 1 to 3 digits, the first of which can be an asterisk (*).

To change things like server name, location, or contact, you must use the maintenance menu. Either execute the reset command (**reset level=menu**), or access the maintenance menu on the next reboot.

The ***cfgadm* show** commands report configuration and status of system resources, such as:

- system-wide parameters
- operating system
- data storage
- devices such as processors, network interfaces, and disks.

showsys prints the system-wide parameters. In addition to those fields listed above under **chgsys**, the following fields are shown:

- ***server-name*** - the hostname of the server, as determined by the LynxOS startup scripts
- ***server-number*** - the unique number assigned to this server (1-15 digit number, country and location dependent)
- ***description*** - textual description of the server
- ***location*** - the physical location of this server
- ***contact*** - the contact person for this server, together with information on how to contact this person
- ***system_up_time*** - total time the MMCX system has been running (DDD:HH:MM:SS, where DDD is days, HH is hours, MM is minutes, and SS is seconds)
- ***current_date_time*** - the current date and time as kept by the server
- ***host_up_time*** - total time the host/server has been running (DDD:HH:MM:SS, where DDD is days, HH is hours, MM is minutes, and SS is seconds)
- ***active_users*** - the current number of active system administrator users logged on the system
- ***active_processes*** - the current number of active processes
- ***maximum_processes*** - the maximum number of processes on this server

- ***initial_load_parm*** - the initial load parameter
- ***initial_load_device*** - the initial load device of the server

showstor prints information about data storage devices, with an entry for each logical area of storage that is allocated and has fixed resource limits.

showdev prints the status of installed devices, for example CPU, network interfaces, and disks. Output includes a table for all device types.

showdsk prints detailed information on the disks including the disk storage information, partitions and file systems. The ***data-type*** argument can be used to specify the data of interest. The default is to show all 3 tables.

The options are:

- **stor** - storage table
- **part** - partition table
- **fs** - file system table

EXAMPLES

```
$ addisrnum phone=13035384000
Your request to addisrnum succeeded.
ISR_PHONE_NUMBER
13035384000

$ chgsys pstnac=9
Your request to chgsys succeeded.
      EXTENSION_LENGTH:     4
   SEC_BEFORE_COVERAGE:     10
```

```
       SEC_AT_COVERAGE:     10
      PSTN_ACCESS_CODE:     9
       PBX_ACCESS_CODE:     8

$ showsys
          SERVER_NAME:    mmcx01
        SERVER_NUMBER:    13035384214
       DESCRIPTION:    Lucent Multimedia Communications eXchange (MMCX) server
             LOCATION:    Planet Earth
              CONTACT:    Unknown
       SYSTEM_UP_TIME:    023:12:14:34
     EXTENSION_LENGTH:    4
  SEC_BEFORE_COVERAGE:    10
      SEC_AT_COVERAGE:    10
     PSTN_ACCESS_CODE:    9
      PBX_ACCESS_CODE:    8
    CURRENT_DATE_TIME:    03/26/96 09:23:21
         HOST_UP_TIME:    023:13:46:54
         ACTIVE_USERS:    2
     ACTIVE_PROCESSES:    35
    MAXIMUM_PROCESSES:     1024
    INITIAL_LOAD_PARM:     a0a
  INITIAL_LOAD_DEVICE:     SCSI Disk

$ showstor
TYPE                    UNITS      SIZE       USED       DESCRIPTION
hrStorageRam            4096       8192       7977       RAM Memory
hrStorageVirtualMemory  4096       32768      5211       Virtual Memory
hrStorageFixedDisk      512        2118112    1203386    Local Disk File System
```

The meanings of the headings are as follows:

- **Type** - the type of storage represented by this entity.
- **Units** - the size, in bytes, of the unit of data allocation for this storage type.
- **Size** - the total size of the storage allocated to this storage type.
- **Used** - the total amount of storage used by this storage type.
- **Description** - textual description of the entry shown under “TYPE.”

```
$ showdev
TYPE                        DESCRIPTION
hrDeviceProcessor           Intel Pentium processor
hrDeviceOther               PRII48D Rev5.02  95Mar24  5.0.n
hrDeviceOther               PRII48D Rev5.02  95Mar24  5.0.n
hrDeviceNetwork             Ethernet
hrDeviceNetwork             Ethernet
hrDeviceDiskStorage         SCSI Disk
hrDeviceOther               AT&T PCI Wild Card
hrDeviceOther               AT&T PCI Wild Card
```

The meanings of the headings are as follows:

- **Type** - the type of device.
- **Description** - textual description of the device, including manufacturer, revision, and optionally, serial number.

```
$ showdsk
        DISK STORAGE
        ============
DESCRIPTION             ACCESS     MEDIUM      REMOVE   SIZE(KB)
SCSI Disk               readWrite  hardDisk    false    1059072
```

```
        PARTITION
        =========
ID         SIZE(KB)   LABEL
101        4096       my_label


        FILE SYSTEM
        ===========
TYPE            ACCESS    BOOT  MOUNT_POINT            REMOTE_MOUNT_POINT
hrFSOther       readWrite false /                      -
```

For the disk storage table, relevant headings are as follows:

- **Description** - textual description of the disk storage device.
- **Access** - indication of whether device access is read-only or read/write.
- **Medium** - type of medium (hard disk, tape drive, etc) for this device.
- **Remove** - denotes whether this is a removable storage medium, such as floppy disk.
- **Size** - the total storage capacity of this device, in Kilobytes.

For the partition table, relevant headings are as follows:

- **ID** - the unique descriptor that identifies this partition to LynxOS.
- **Size** - the size of the partition, in Kilobytes.
- **Label** - textual description of this partition.

For the file system table, relevant headings are as follows:

- **Type** - the SNMP file system type for this file system (see RFC 1514 for a list of valid types)
- **Access** - indication of whether file system access is read-only or read/write.

- **Boot** - a flag indicating whether or not this is a bootable file system.
- **Mount-point** - the path name of the root of this file system.
- **Remote-mount-point** - a description of the name and/or address from which this file system is mounted, if it is remotely mounted.

DIAGNOSTICS

chgsys will fail if no parameter is specified.

MIB GROUPS

These commands provide access to the Host Resources MIB, RFC 1514 (September 1993), the System Group of MIB-II RFC 1213 (March 1991), and the mmcxConfig MIB.

SEE ALSO

INTRO, page 426

ISRADM, page 490

USRADM, page 577

DPADM

NAME

adddp, **chgdp**, **rmdp**, **showdp** - administer the MMCX dial plan table.

SYNOPSIS

adddp dial=*dialed_number_expression* dir=*direction*
numdel=*num_to_delete*add=*digits_to_add*
[plan=*pri_routing_plan*] [srv=*server-name*] [rtgopt=*pstn-routing-option*]

chgdp dial=*dialed_number_expression* dir=*direction*
numdel=*num_to_delete*add=*digits_to_add*
[plan=*pri_routing_plan*] [srv=*server-name*] [rtgopt=*pstn-routing-option*]

rmdp dial=*dialed-number-exp* dir=*direction*

showdp [dial=*dialed-number-exp*] [dir=*direction*]

DESCRIPTION

The dial plan table is a list of rules and the conditions for applying them. These rules define how the MMCX server interprets dialed digits and routes calls. When it has dialed input, the MMCX server first identifies the dial plan rule that best applies to the kind of input it has received (the condition). The server then applies the rule and translates the dialed input into a corresponding extension or public network telephone number.

When it receives dialed input from an MMCX user, the server first sees if the destination is also an MMCX user. It identifies all rows in the table that describe **internal** calls and searches these rows for the *dialed digit expression* that best describes the actual input. If it cannot find such an expression, it decides that the call is destined for an external, non-MMCX user. It evaluates the dialed digit expressions that describe calls of type **out**. When the dialed input comes from a public network trunk group rather than from an MMCX endpoint, the server evaluates the dialed digit expressions that describe calls of type **in**. If the server cannot find any dialed digit expression for the input, it notifies the caller that the call cannot be completed as dialed. The server always selects the closest match between the input and the rule. So **85006** is a better match than **8500?** or **8500+**, both of which use wild card characters.

adddp adds a record to the MMCX dial plan table. It takes the following parameters.

The **dial** and **dir** specify the digit patterns that can trigger application of the rule. The remaining parameters, **numdel** and **add**, tell what the server should do when the specified conditions are met.

- The ***dialed-number-expression*** is a sequence of 1 to 15 digits (including * and #) and, perhaps, wildcard characters (**?** or **+**) that define the pattern that will trigger the new dial-plan rule. The **+** wildcard character means any digit string. The **?** wildcard character means any single digit.
- The ***direction*** defines the type of call that triggers the new rule. It can have one of three values: **internal**, **in**, or **out**.
- The ***num-to-delete*** is the number of digits (1 to 15) that the server should discard from a string of dialed digits that matches the ***dialed-number-expression***.
- The 1- to 15-digit string ***digits-to-add*** specifies the digits that the server should place at the start of any dialed input string that matches the ***dialed-number-expression***.

- The ***pri-routing-plan*** value is a number in the range 1 to 32. It refers the server to a separate routing plan that administers the server's Primary Rate Interface (PRI) with the public switched telephone network. This parameter applies only to outbound calls.
- ***server-name*** is the target server for the command. It is the local server by default.
- ***pstn-routing-option*** determines how the server handles outbound PSTN routing when MASI is enabled. There are three possible values: **mmcx** for MMCX Voice Interworking routing, **definity** for DEFINITY ARS routing, and **none** for inbound (**dir=in**) or internal (**dir=internal**) call routing.

chgdp changes an existing rule in the MMCX dial plan table. It takes the same parameters as **adddp**. But if you do not specify a value for a parameter, it defaults to its original value.

rmdp removes the dial plan rule for ***dialed-number-expression*** and ***direction***.

showdp shows all translations with the specified ***direction*** and/or ***dialed-number-expression.*** Both default to **all** if not specified.

EXAMPLES

To drop the first two digits of any incoming seven-digit number beginning with 555:

```
$ adddp dial="538+" dir=in numdel=2
Your request to adddp succeeded.
DIALED_NUMBERDIRECTION   SERVER       PLAN        DEL DIGITS_TO_ADD ROUTING
538+         in(1)       mmcx01       -           2   -             none(3)
```

To change the above translation to drop three digits instead of two, and to prepend a "7":

```
$ chgdp dial="538+" dir=in numdel=3 add=7
Your request to chgdp succeeded.
```

```
DIALED_NUMBER    DIRECTION    SERVER    PLAN  DEL   DIGITS_TO_ADD ROUTING
538+             in(1)        mmcx01    -     3     7             none(3)
```

To remove the above translation from the table:

```
$ rmdp dial="538+" dir=in
Your request to rmdp succeeded.
```

To look at the entire dial plan table:

```
$ showdp
DIALED_NUMBER    DIRECTION    SERVER    PLAN   DEL   DIGITS_TO_ADD ROUTING
538+             in(1)        mmcx01    -      3     7             none(3)
8????            internal(3)  mmcx01    -      0     130353        none(3)
9+               out(2)       mmcx02    1      -     -             mmcx(1)
*111             internal(3)  mmcx01    -      0     5555          none(3)
```

DIAGNOSTICS

These commands follow the standard rules when validating parameters. You cannot show or change non-existent data and cannot add existing data. Valid parameters must also satisfy the following conditions.

- If **dir=out**, then ***pri-routing-plan*** must have a corresponding entry in the PRP table (see *PRPADM, page 534*); if it does not, omit it.
- If **dir=internal**, ***server-name*** defaults to the name of the local host and need not be specified. If specified, it must have a corresponding entry in the ISR table (see *ISRADM, page 490*).
- ***dialed-number-expression*** has to be a 1- to 15-character string made up of digits, *****, # , and, optionally, the wildcards **?** or **+** (but not both). The characters ***** and # cannot be used consecutively **(***#).

If **dial=internal**, ***dialed-number-expression*** has to have the following form: one or more digits [0-9], optionally followed by a **+** or by one or more **?**. Expressions with no digits (such as **+** or **??**) are valid but not generally useful.

If **dial=in**, ***dialed-number-expression*** has to have the following form: an optional *****, followed by one or more digits [0-9], optionally followed by either **+**, **#**, or one or more **?**. Expressions with no digits (such as **+** or **??**) are valid but not generally useful.

If **dial=out**, ***dialed-number-expression*** has to have the following form: a PBX or PSTN access code (see *CFGADM, page 458*), followed by one or more digits [0-9], optionally followed by either **+**, #, or one or more **?**. *Outbound patterns with no digits are never valid.*

- ***digits-to-add*** has to be a 1- to 32-digit string.
- ***num-to-delete*** has to be a 1- to 32-digit string.

MIB GROUPS

mmcxDPlanTable

SEE ALSO

INTRO, page 426

PRPADM, page 534

CFGADM, page 458

ISRADM, page 490

MASIADM, page 509

ENETADM

NAME

addenet, **chgenet**, **rmenet**, **showenet** - administer ethernet interface data

SYNOPSIS

addenet slot=***slot-number*** **port**=***port-number*** **ip**=***ip-address*** **mask**=***netmask-value*** [**cap**=***capacity***]

chgenet slot=***slot-number*** **port**=***port-number*** [**ip**=***ip-address***] [**mask**=***netmask-value***] [**cap**=***capacity***]

rmenet slot=***slot-number*** **port**=***port-number***

showenet [**data**=***data-type***] [**slot**=***slot-number***] [**port**=***port-number***]

DESCRIPTION

addenet is the command to add an ethernet interface.

The following parameters should be specified:

- ***slot-number*** - consists of the prefix for the type of bus (p for PCI, and i for ISA) along with the slot number (1 to 6); for instance, slot 3 on the PCI bus is represented as p3, and slot 5 on the ISA bus is represented as i5; all ethernet interfaces are on the PCI bus, so this field will start with a p.
- ***port-number*** - the port number of the specific interface

- ***ip-address*** - the ip address assigned to this ethernet interface, and
- ***netmask-value*** - the netmask value for this ethernet interface
- ***capacity*** is the optional estimated capacity of the ethernet connection. The default is 10 Mbps (megabits per second). Increasing this parameter allows higher utilization of the connection with possible degradation of call quality.

chgenet allows the user to change the parameters of an ethernet interface based on the slot and port parameters. The i***p-address***, ***netmask-value***, or ***capacity*** fields can be changed.

rmenet removes the ethernet interface specified by ***slot-number*** and ***port-number.*** Note: when an ethernet interface is removed, the IP address assigned to that interface cannot be reused until after a system reboot.

showenet is the command to view ethernet data such as configuration, collision, or statistics data. ***data-type*** describes the type of data being requested.

The three types of data possible are (the default is to show all three):

- **cfg** - shows current configuration for ethernet interfaces
- **stat** - show statistics that apply specifically to ethernet interfaces
- **coll** - show the ethernet collision table

The slot and port parameters let you specify which interfaces to retrieve data on. If only ***slot-number*** is specified, then the data associated with all the ports on that slot will be shown. If ***port-number*** is specified, then ***slot-number*** must be specified as well. If no ***slot-number*** is specified, then data across all interfaces will be shown.

EXAMPLES

To add an ethernet interface to slot P2, port 1:

```
$ addenet slot=p2 port=1 ip=135.2.130.12 mask=255.255.255.0
Your request to addenet succeeded.
SLOT PORT   HARDWARE  IP_ADDRESS    NETMASK_VALUE  CAPACITY
p2   1      no        135.2.130.12  255.255.255.0  10
```

To change the ethernet interface on slot P2, port 1:

```
$ chgenet slot=p2 port=1 mask=255.255.0.0
Your request to chgenet succeeded.
SLOT PORT   HARDWARE  IP_ADDRESS    NETMASK_VALUE  CAPACITY
p2   1      yes(1)    135.2.130.12  255.255.0.0    10
```

To remove the ethernet interface on slot P2, port 1:

```
$ rmenet slot=p2 port=1
Your request to rmenet succeeded.
```

To show configuration data for all ethernet interfaces, the field **HARDWARE** is an indication of whether or not the hardware for that interface is currently attached (**yes** or **no**):

```
$ showenet data=cfg
      ETHERNET CONFIGURATION
      ======================
SLOT PORT HARDWARE IP_ADDRESS      NETMASK_VALUE  CAPACITY
p2   1    yes(1)   135.2.130.12    255.255.255.0  10
```

To show the statistics for ethernet interfaces for slot p1, port 1:

```
$ showenet data=stat slot=P1 port=1
      ETHERNET STATISTICS
      ===================
SLOT   PORT   ALIGN   FCS   SCOLLFRAME   MCOLLFRAME   LATECOLL   EXCESSCOLL
p1     1      20      30    40           50           60         70
SLOT PORT  DEFERTRAN    MACTRAN     MACRCV  CARRSENSE  FRAMELONG
p1   1     80           90          11      22         33
```

The meaning of the headings are as follows:

- **SLOT**=the physical bus/slot that this interface resides on; the first letter indicates the bus type: p for PCI, i for ISA; the number following the bus type is the slot number
- **PORT**=the physical port within this slot that the interface resides on
- **ALIGN**=a count of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check
- **FCS**=a count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check
- **SCOLLFRAME**=single collision frames, a count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision
- **MCOLLFRAME**=multiple collision frames, a count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision
- **LATECOLL**=late collisions, the number of times that a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet
- **EXCESSCOLL**=excessive collisions, a count of frames for which transmission on a particular interface fails due to excessive collisions

- **DEFERTRAN**=deferred transmissions, a count of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy
- **MACTRAN**=internal MAC transmit errors, a count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error
- **MACRCV**=internal MAC receive errors, a count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error
- **CARRSENSE**=carrier sense errors, the number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular interface
- **FRAMELONG**=frame too longs, a count of frames received on a particular interface that exceed the maximum permitted frame size

To view the ethernet collision statistics for all ethernet interfaces:

```
$ showenet data=coll
      ETHERNET COLLISIONS
      ===================
SLOT  PORT      COLLCOUNT         FREQUENCY
p1    1         1                 100
p1    2         2                 50
p1    3         3                 1
```

The meaning of the headings are as follows:

- **SLOT**=the physical bus/slot that this interface resides on; the first letter indicates the bus type: p for PCI, i for ISA; the number following the bus type is the slot
- **number**=the physical port within this slot that the interface resides on
- **PORT**=the physical port within this slot that the interface resides on

- **COLLCOUNT**=the number of per-frame media collisions for which a particular collision histogram cell represents the frequency on a particular interface
- **FREQUENCY**=a count of individual MAC frames for which the transmission on a particular interface occurs after the frame has experienced exactly the number of collisions in the associated COLLCOUNT field

DIAGNOSTICS

addenet, **chgenet**, or **rmenet** fail if given slot and port do not exist, or are not ethernet slots.

addenet fails if given slot and port have already been added.

chgenet fails if given slot and port are currently running traffic.

MIB GROUPS

Ethernet-like interface MIB (RFC1643), MIB-II

SEE ALSO

INTRO, page 426

INTFADM, page 479

IPADM, page 483

HELP

NAME

help - list and describe MMCX System Management commands

SYNOPSIS

help *keyword*

DESCRIPTION

The **help** command will print a list of commands related to the keyword, with a short description of each and the name of the manual page that describes it in parentheses.

OPTIONS

help *keyword* where keyword is a word describing the general area of interest. If keyword is missing all SM commands will be included.

EXAMPLES

```
$ help add
MMCX System Management Commands related to "add" See manual page (in parentheses)
for more information. (*) indicates a command not yet implemented.
Call Server administration:
   adddp - Add a dial plan to the call server (dpadm)
   addisr - Add a server to the inter-server routing table (isradm)
```

```
Interface administration LAN:
   addatm - (*)Add an ATM interface (atmadm)
   addenet - Add an ethernet interface (enetadm)
Interface administration WAN:
   addpri - Add a new ISDN PRI interface (priadm)
   addprp - Add a PRI routing plan (prpadm)
   addptg - Add a PRI trunk group (ptgadm)
Interface administration:
   addip - Add an IP route (ipadm)
User administration:
   addsa - Add a new System Administrator account (saadm)
   addusr - Add a new end user (usradm)

$ help password
MMCX System Management Commands related to "password" See manual page (in
parentheses) for more information. (*) indicates a command not yet implemented.
User administration:
   chgsapasswd - Change a System Administrator's password (saadm)
   chgpasswd - Change an end user's password (usradm)
```

SEE ALSO

INTRO, page 426

INTFADM

NAME

chgintf, **showintf** - update the administration status of an interface, or show interface data.

SYNOPSIS

chgintf slot=***slot-number*** **port**=***port-number*** **adstat**=***administration-status***

showintf [**data**=***data-type***] [**slot**=***slot-number*** [**port**=***port-number***]]

DESCRIPTION

chgintf is used to update the administration status of a link on a slot and port basis. This could be used to bring down either an ethernet interface or an ATM interface. The valid values for ***administration-status*** are: up and down. To view what the current status is, see **showintf** ***data=stat***.

Note: A reboot will reset the status of all interfaces to their original values.

The ***slot-number*** field consists of the prefix for the type of bus (p for PCI, and i for ISA) along with the ***slot number*** (1 to 6). For instance, slot 3 on the PCI bus is represented as p3, and slot 5 on the ISA bus is represented as i5. The WILD, ENET and ATM interfaces are on PCI buses, while the PRI and RMB interfaces are on ISA buses. The ***port-number*** field specifies the port number of the specific interface to be changed.

showintf is the command to view the data that applies to interfaces such as ethernet, atm, and ppp.

data-type describes the type of data being requested. ***data-type*** can be one of the following:

- **stat** - show the status of the various links
- **count** - show the interface-related counts.

If multiple ***data-types*** are specified, then those data will be shown in the order of their input. However, if no ***data-type*** is specified, then all data will be shown.

The slot and port parameters let you specify which interfaces to retrieve data on. If only ***slot-number*** is specified, then the data associated with all the ports on that slot will be shown. If ***port-number*** is specified, then ***slot-number*** must be specified as well. If no ***slot-number*** is specified, then data across all interfaces will be shown.

Since the PPP interface does not correspond to a slot and port, no slot and port information will be shown. Slot and Port should not be specified in this case (they will be ignored if they are specified). Note: PPP interfaces are not permanent, and two successive runs of this command may yield varying output.

EXAMPLES

To change the administration-status for the interface on slot 5, port 1:

```
$ chgintf slot=p5 port=1 adstat=down
Your request to chgintf succeeded.
SLOT PORT TYPE                ADSTAT  MTU    SPEED      DESCRIPTION
p5   1    ethernet-csmacd(6)  down(2) 128    10000000   dec1
```

To see the status of the links over all interfaces:

```
$ showintf data=stat
```

```
      INTERFACE STATISTICS
      ====================
SLOT PORT  TYPE                ADSTAT  MTU    SPEED      DESCRIPTION
p5   1     ethernet-csmacd(6)  down(2) 128    10000000   dec1
-    -     ppp(23)             up(1)   256    0          ppp1
```

The meaning of the headings are as follows:

- **SLOT**=the physical bus/slot that this interface resides on; the first letter indicates the bus type: p for PCI, i for ISA; the number following the bus type is the slot number; for PPP we display the remote server name instead of slot and port.
- **PORT**=the physical port within this slot that the interface resides on.
- **TYPE**=the type of interface.
- **MTU**=the size of the largest datagram, in octets, which can be sent/received on the interface.
- **SPEED**=an estimate of the interface's current bandwidth in bits per second.
- **ADSTAT**=the requested state of the interface (up, down, or testing).
- **DESCRIPTION**=a textual string containing information about the interface.

To view the counts of the interface table for slot I2, port 1:

```
$ showintf data=count slot=p2 port=1
      INTERFACE COUNTS
      ================
SLOT  PORT  IN_U_PKT   OUT_U_PKT  IN_ERROR   OUT_ERROR
p2    1     100        50         4          2
```

The meaning of the headings are as follows:

- **SLOT** and **PORT** are defined above.
- **IN_U_PKT**=the number of subnetwork unicast packets delivered to a higher-layer protocol.
- **OUT_U_PKT**=the number of packets that higher-level protocols requested be transmitted to a subnetwork unicast address, including those that were discarded or not sent.
- **IN_ERROR**=the number of inbound packets that contained errors preventing them from being delivered to a higher-layer protocol.
- **OUT_ERROR**=the number of outbound packets that could not be transmitted because of errors.

DIAGNOSTICS

MIB GROUPS

Interfaces Group, TCP/IP MIB-II (RFC1213)

SEE ALSO

INTRO, page 426

IPADM, page 483

ENETADM, page 471

ATMADM, page 437

SHOWWAN, page 569

IPADM

NAME

addip, **chgip**, **rmip**, **showip** - administer the IP (internet protocol) interface

SYNOPSIS

addip dest=***destination-address*** **nexthop**=***nexthop-address*** [**type**=***route-type***] [**stat**=***status-type***]

chgip dest=***destination-address*** [**nexthop**=***nexthop-address***] [**type**=***route-type***] [**stat**=***status-type***]

rmip dest=***destination-address***

showip [**data**=***data-type***] [**ip**=***ip-address***]

DESCRIPTION

addip is the command to add an entry in the ip routing table. The ip routing table is used to determine the routing scheme for all interfaces that run IP (internet protocol). **addip** takes as input, the following fields:

- ***destination-address*** - the destination IP address of this route; an entry with a value of '-' is considered a default route
- ***nexthop-address*** - the IP address of the nexthop (gateway) of this route
- ***route-type*** - the type of route (**direct** or **indirect**). The default value is **indirect**.

- ***status-type*** - the status of the route (**netmgmt** or **local**). The default value is **netmgmt**. **Netmgmt** indicates that this route will be saved and will be available even on reboot. On the other hand, local routes are only active until the next reboot (or until they are removed). The above two values (**netmgmt** and **local**) are the only ones supported for this field.
- **chgip** is the command to change the entries in the iproute table given a ***destination-address.*** Any of the fields in the iproute table can be changed.
- **rmip** is the command to remove an entry from the iproute table based on the ***destination-address***.
- **showip** is the command to view IP related data.
- ***data-type*** describes the type of data being requested. ***data-type*** can be one of the following:
  - **count** - show IP related counts and parameters.
  - **addr** - show the IP address table.
  - **route** - show the IP route table.
  - **media** - show the IP net to media table.

If multiple ***data-types*** are specified, then those data will be shown in the order of their input. However, if no ***data-type*** is specified, then all data will be shown.

For all tables (addr, route, media), the ***ip-address*** field can be specified, so only those data with the given ***ip-address(es)*** are listed.

EXAMPLES

To add an IP route:

```
$ addip dest=135.1.16.116 nexthop=135.2.17.144 type=direct stat=netmgmt
```

```
Your request to addip succeeded.
DESTINATION     SLOT PORT  NEXTHOP          TYPE         STATUS
135.1.16.116    p1   1     135.2.17.144     direct(3)    netmgmt(3)
```

To change an IP route:

```
$ chgip dest=135.1.16.116 nexthop=135.2.17.145
Your request to chgip succeeded.
DESTINATION     SLOT  PORT  NEXTHOP          TYPE         STATUS
135.1.16.116    p1    1     135.2.17.145     direct(3)    permanent
```

To remove an IP route:

```
$ rmip dest=135.1.16.116
Your request to rmip succeeded.
```

To show the IP counts:

```
$ showip data=count
              FORWARD:     forwarding
           DEFAULT_TTL:    40
            IN_RECEIVE:    505
          IN_HDR_ERROR:    4
         IN_ADDR_ERROR:    92
         FORW_DATAGRAM:    31
```

The meaning of the headings are as follows:

- **FORWARD**=the indication of whether this entity is acting as an IP gateway in respect to forwarding of datagrams received by, but not addressed to, this entity (**forwarding** or **not-forwarding**).

- **DEFAULT_TTL**=the default value inserted into the **Time-To-Live** field of the IP header of datagrams originated at this entity, whenever a TTL value is not supplied by the transport layer protocol (integer).
- **IN_RECEIVE**=the total number of input datagrams received from interfaces, including those received in error.
- **IN_HDR_ERROR**=the number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options.
- **IN_ADDR_ERROR**=the number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity.
- **FORW_DATAGRAM**=the number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination.

To view the IP address table:

```
$ showip data=addr
      IP ADDRESS
      ==========
ADDRESS          SLOT   PORT      NETMASK         BCAST_ADDR  REASM_MAXSIZE
134.133.132.131  p1     1         255.255.255.0   1           512
```

The meaning of the headings are as follows:

- **ADDRESS**=the IP address to which this entry's addressing information pertains.
- **SLOT**=the physical bus/slot that this interface resides on. The first letter indicates the bus type: p for PCI, i for ISA; the number following the bus type is the slot number.

- **PORT**=the physical port within this slot that the interface resides on.
- **NETMASK**=the subnet mask associated with the IP address of this entry. The value of the mask is an IP address with all the network bits set to 1 and all the hosts bits set to 0.
- **BCAST_ADDR**=the value of the least-significant bit in the IP broadcast address used for sending datagrams on the (logical) interface associated with the IP address of this entry.
- **REASM_MAXSIZE**=the size of the largest IP datagram which this entity can re-assemble from incoming IP fragmented datagrams received on this interface.

To view the IP routing table:

```
$ showip data=route
      IP ROUTE
      ========
DESTINATION      SLOT PORT NEXTHOP            TYPE        STATUS
135.135.135.135  p1   1    136.136.136.136    direct(3)   permanent
134.134.134.134  p1   2    137.137.137.136    direct(3)   temporary
```

The meaning of the headings are as follows:

- **DEST**=the destination IP address of this route; an entry with a value of considered default route.
- **NEXTHOP**=the IP address of the next hop of this route (IpAddress).
- **TYPE**=the type of route (**direct** or **indirect**).
- **STATUS**=the status of the route (**netmgmt** or **local**).
- **SLOT** and **PORT** are defined above.

To view the IP net to media table:

```
$ showip data=media
      IP NET TO MEDIA
      ===============
NETADDR           SLOT   PORT     TYPE        PHYSADDR
123.123.123.123   p1     1        static(4)   -
```

The meaning of the headings are as follows:

- **SLOT** and **PORT** are defined above.
- **PHYADDR**=the media-dependent physical address (**PhysAddress**).
- **NETADDR**=the **IpAddress** corresponding to the media-dependent physical address (**IpAddress**).
- **TYPE**=the type of mapping (**other**, **invalid**, **dynamic**, or **static**).

MIB GROUPS

IP Group, TCP/IP MIB-II (RFC1213)

SEE ALSO

INTRO, page 426

INTFADM, page 479

SHOWICMP, page 555

SHOWTCP, page 563

SHOWUDP, page 567

SNMPADM, page 572

ISRADM

NAME

addisr, **chgisr**, **rmisr**, **showisr** - administer the inter-server routing table

SYNOPSIS

addisr srv=***server-name*** **srvnum**=***server-number*** **ip**=***ip-addr ...***

addisr srv=***server-name*** **srvnum**=***server-number*** **farppp**=***far-end-ppp-addr***
nearppp=***near-end-ppp-addr*** **isrnum**=***isr-phone-number*** **plan**=***pri-routing-plan***

addisr srv=***server-name*** **srvnum**=***server-number*** **ip**=***ip-addr ...*** **farppp**=***far-end-ppp-addr***
nearppp=***near-end-ppp-addr*** **isrnum**=***isr-phone-number*** **plan**=***pri-routing-plan***
[**aud**=***audio-priority***] [**vid**=***video-priority***] [**app**=***app-priority***]
[**sig**=***signal-priority***]

chgisr srv=***server-name*** [**ip**=***ip-addr ...***] [**farppp**=f***ar-end-ppp-addr***]
[**nearppp**=***near-end-ppp-addr***] [**isrnum**=***isr-phone-num***] [**plan**=***pri-routing-plan***]
[**aud**=***audio-priority***] [**vid**=***video-priority***] [**app**=***app-priority***] [**sig**=***signal-priority***]

rmisr srv=***server-name***

showisr [**srv**=***server-name ...***]

DESCRIPTION

addisr adds a record to the inter-server routing table. (To distinguish between the server being administered and the servers in its inter-server routing table, we'll refer to the former as the ***local server***, and the latter as ***remote servers***.) There must be IP address information in this table for every other MMCX server the local server has to communicate with directly.

- ***server-name***: the remote server name, a character string of up to eight alphanumeric characters.
- ***server-number:*** the number assigned to the remote server; this number uniquely identifies that server, and its length depends on the location and country, and can be from 1 to 15 digits.

Both ***server-name*** and ***server-number*** should reflect the values given from a **showsys** command executed on the remote server (see *CFGADM, page 458*).

There is one inter-server routing table, but three classes of remote servers. The first class of remote servers includes those that can only be accessed over the LAN; the first **addisr** corresponds to this case.

The remote server's IP addresses, ***ip-addr***, should be specified. The number of IP addresses that can be administered is limited by the number of LAN ports on the remote server. Also, the priority (determining which IP address to use before others) is decided by the order in which these IP addresses are specified (e.g. the first IP address specified has the highest priority, the second has the next highest priority, etc).

The second class of remote servers are those that can only be accessed over the WAN (PRI network); in this case, the following fields should be specified:

- ***far-end-ppp-addr***: the remote server's far-end IP address for its PPP interface

- ***near-end-ip-addr***: the local server's near-end IP address for its PPP interface
- ***isr-phone-num***: the remote server's ISR phone number
- ***pri-routing-plan***: the number of the PRI routing plan to use for the local server (see *PRPADM, page 534*), valid range is 1 to 32

Finally, the third addisr corresponds to the case where the remote server can be accessed by either the local network (LAN) or the PRI network (WAN). In this case, all the fields mentioned above should be specified. Additionally, the ***audio-priority, video-priority, app-priority,*** and ***signal-priority*** fields can be specified by setting them to either LAN or WAN (the default is LAN).

For example, by setting the ***audio-priority*** field to LAN (or not specifying it at all), then all audio traffic to that server will try going over the LAN before going over the WAN. On the other hand, by setting the ***audio-priority*** field to WAN, then all audio traffic to that server will try going over the WAN before the LAN.

- **chgisr** changes one or more fields in a routing record.
- **rmisr** removes server ***server-name*** from the routing table.
- **showisr** shows the routing record for a single server if ***server-name*** is specified, otherwise it shows all routing records.

EXAMPLES

To add a server to be contacted directly over the local network:

```
$ addisr srv=mmcx02 srvnum=12029991234 ip=129.30.20.126
Your request to addisr succeeded.

SERVER   SRVNUM        AUD  VID  APP  SIG
mmcx02   12029991234   lan  lan  lan  lan
```

```
SERVER   IP_ADDRESSES
mmcx02 129.30.20.126

SERVER  NEAR_PPP_ADDR   FAR_PPP_ADDR  ISR_PHONE_NUM  PLAN
mmcx02  -               -             -              -
```

To add a server to be contacted directly over PRI:

```
$ addisr srv=mmcx01 srvnum=13031119876 farppp=129.30.25.112 nearppp=129.30.26.113
isrnum=6148604931 plan=11
Your request to addisr succeeded.

SERVER   SRVNUM          AUD  VID  APP  SIG
mmcx01   13031119876     wan  wan  wan  wan

SERVER   IP_ADDRESSES
mmcx01   -, -, -, -

SERVER   NEAR_PPP_ADDR  FAR_PPP_ADDR   ISR_PHONE_NUM  PLAN
mmcx01   129.30.26.113  129.30.25.112  6148604931     11
```

To add a server to be contacted either by PRI or the local network:

```
$ addisr srv=mmcx03 srvnum=12065550000 ip=129.30.20.125 farppp=129.30.25.124
nearppp=129.30.26.125 isrnum=6148603075 plan=12 aud=lan vid=lan app=lan sig=wan

SERVER   SRVNUM          AUD  VID  APP  SIG
mmcx03   12065550000     lan  lan  lan  wan

SERVER   IP_ADDRESSES
```

```
mmcx03   129.30.20.125, -, -, -

SERVER   NEAR_PPP_ADDR  FAR_PPP_ADDR  ISR_PHONE_NUM  PLAN
mmcx03   129.30.26.125  129.30.25.124 6148603075     12
```

To change a server's far-end IP address:

```
$ chgisr srv=mmcx01 farppp=129.30.25.127

Your request to chgisr succeeded.

SERVER   SRVNUM         AUD  VID  APP  SIG
mmcx01   13031119876    wan  wan  wan  wan

SERVER   IP_ADDRESSES
mmcx01   -, -, -, -

SERVER   NEAR_PPP_ADDR  FAR_PPP_ADDR  ISR_PHONE_NUM  PLAN
mmcx01   129.30.26.113  129.30.25.127 6148604931     11
```

To remove a server from the server table:

```
$ rmisr srv=mmcx01
Your request to rmisr succeeded.
```

To show the entire server table:

```
$ showisr

SERVER   SRVNUM          AUD  VID  APP  SIG
mmcx01   12029991234     wan  wan  wan  wan
```

```
mmcx02   13031119876     lan  lan  lan  lan
mmcx03   12065550000     lan  lan  lan  lan

SERVER   IP_ADDRESSES
mmcx01   -, -, -, -
mmcx02   129.30.20.126, -, -, -
mmcx03   129.30.20.125, -, -, -

SERVER  NEAR_PPP_ADDR  FAR_PPP_ADDR   ISR_PHONE_NUM  PLAN
mmcx01  129.30.26.112  129.30.25.127 6148604931     11
mmcx02  -              -               -             -
mmcx03  129.30.26.125 129.30.25.124 6148603075     12
```

DIAGNOSTICS

chgisr and **rmisr** fail if ***server-name*** is not found in the server table.

chgisr will fail if any of the PRI-specific fields are specified for a remote server that can only be accessed over the LAN; similarly, it will fail if ***ip-addr*** is specified for a remote server that can only be accessed over the WAN.

MIB_GROUPS

mmcxIsrTable

SEE ALSO

INTRO, page 426

PRPADM, page 534

CFGADM, page 458

DPADM, page 466

MAINTENANCE

NAME

showcard, **busycard**, **rlscard**, **busypri**, **rlspri**, **initcard**, **startwild**, **testwild**, **showtest** - network interface and card maintenance functions.

SYNOPSIS

showcard [data=***data-type*****] [slot**=***slot-number*****]**

busycard slot=***slot-number***

rlscard slot=***slot-number***

busypri slot=***slot* port**=***port-number* data**=***scope***

rlspri slot=***slot-number* port**=***portnumber* data**=***scope***

initcard slot=slot-number **[confirm=...]**

testwild [**test**=***test-type***] **slot**=***slot-number***

showtest slot=***slot-number***

DESCRIPTION

These commands take network interfaces and cards out of service (busyout) and release them back into service. They also allow you to reinitialize PRI or WILD cards and to test and restart WILD

cards individually (system resets return the administrative status of *all* cards and interfaces to their original values). Each MMCX contains a subset of the cards shown in *Table 1*.

Table 1. Chassis Slots/Bus

Bus	Chassis Slots					
	1	2	3	4	5	6
PCI	LAN#2	WILD#1	Console VGA card or LAN#4	WILD#2	LAN#1	LAN#3
ISA	RMB	PRI#4	PRI#3	PRI#2	PRI#1	empty

Initialization and restart operations take 15 to 30 seconds; **initcard** only starts the operation and returns. Use **showcard data=hw** for initcard status.

showcard shows all network interface hardware installed on the system (except the RMB), even if the interfaces are not administered for the hardware. The command's input includes card **type** and administrative state. If the hardware has been reinitialized since system startup, output includes the last initialization time and the result, such as success or reason for the failure. The **slot** parameter

specifies the hardware locations for which you want to retrieve data. If you don't specify a **slot** number, the command shows you data for all hardware locations.

showcard parameters	result
all	all data (this is the default)
hw	high level view of installed hardware without interface data
wild	additional information specific to the WILD card
lan	detailed interface information
pri	detailed interface information

The administrative state of a card may be **inService** or **maintBusy**. The state of a PRI card depends on the state of the interfaces on the card. You see **inService** if at least one interface can carry traffic.

If all interfaces are down with a status of **intfBusy**, the card has a status of **maintBusy** and is available for restart or initialization.

busypri changes the administrative state of the PRI interfaces. PRI cards may be in **slot** i2 through i5. **scope** is the breadth of effect. You must always specify one interface by **slot** and **port**; the value you provide for **scope** may affect additional interfaces.

rlspri changes the administrative state of the PRI interfaces. PRI cards may be in **slot** i2 through i5. **scope** is the breadth of effect. You must always specify one interface by **slot** and **port**; the value you provide for **scope** may affect additional interfaces. When you use **rlspri**, any D-channel will go

down and then up. Run **rlspri slot=... port=... data=tg** to run the B-channel service state audit. The b-channel service state audit also runs 30 seconds after the D-channel goes into service. This audit also runs automatically every 15 minutes. Use the rlspri command with data=tg when not all the B-channels have come into service. For example, showptg shows less than the number of B-channels in the trunk group.

busypri scope	result
dchan	Affects only the D Channel of the interface you specify. It does not interrupt active calls, but the interface goes to **dchanBusy** state. No new calls are allowed on the interface. If the interface is a NFAS signalling interface, no new calls are allowed on the trunk group.
intf	Affects all channels of the interface you specify. Active calls are torn down, the D Channel is taken down, and the interface enters the **intfBusy** state. No new calls are allowed on the interface.
card	Affects all channels of the interface you specify and all other interfaces on the same card. Active calls are torn down, D Channels are taken down, and the interfaces enter the **intfBusy** state. No new calls are allowed on the card.
tg	Affects all channels of the interface you specify and all other interfaces on the same trunk. Active calls are torn down, D Channels are taken down, and all interfaces enter the **intfBusy** state. No new calls are allowed on the trunk group.

initcard reinitializes the interface card in the **slot** you specify. This clears all status information on the card, performs a hardware reset, and downloads and restarts firmware. **initcard** applies only to PRI cards. You can only reinitialize PRI cards that are in the maintBusy state.

testwild runs hardware tests on the WILD card in the **slot** you specify. **test-type** is either loop or clock; the default is both. The internal looparound is a single test with one result. The MVIP clock test has three results, one for each of the 4MHz clock, the 2MHz clock, and the frame signal clock. Each test can give a pass, fail, or not-run result. If you see a not-run result, you also see an error message explaining why. The most common explanation of a not-run result is that the card was in an abnormal state.

showtest shows the shows the most recent results of WILD card tests. The internal looparound is a single test with one result. The MVIP clock test has three results, one for each of the 4MHz clock, the 2MHz clock, and the frame signal clock. Each test can give a **pass**, **fail**, or **not-run** result. If you see a **not-run** result, you also see an error message explaining why. The most common explanation of a **not-run** result is that the card was in an abnormal state.

EXAMPLES

Show status of all hardware and interfaces.

```
$ showcard
INSTALLED NETWORK INTERFACE HARDWARE
TYPE          SLOT        PORTS       ADSTAT      LAST_INITITALIZED   INIT_STATE
ethernet(2)   p1          1           inService(1)-                   neverRun(26)
wild(4)       p2          0           inService(1)-                   neverRun(26)
atm(3)        p3          1           inService(1)-                   neverRun(26)
wild(4)       p4          0           inService(1)-                   neverRun(26)
ethernet(2)   p5          1           inService(1)-                   neverRun(26)
ethernet(2)   p6          1           inService(1)-                   neverRun(26)
```

```
pri(5)       i2          0           inService(1)-                neverRun(26)
pri(5)       i3          0           inService(1)-                neverRun(26)
pri(5)       i4          2           inService(1)-                neverRun(26)
pri(5)       i5          2           inService(1)-                neverRun(26)

LAN INTF STATUS
TYPE                     SLOT        PORTS       ADSTAT
ethernet-csmacd(6)       p1          1           up(1)
alfane8023(59)           p3          0           up(1)
ethernet-csmacd(6)       p5          1           up(1)
ehternet-csmacd(6)       p6          1           up(1)

PRI INTF STATUS
SLOT  PORT   ACT_CALLS   ADSTAT
i3    1      3           inService (1)
i4    1      0           inService (1)
i4    2      1           inService (1)
i5    1      1           dchanBusy(2)
i5    2      2           nfasBusy(3)

WILD CARD STATUS
TYPE    SLOT  ACT_CONN    ADSTAT       LAST_INITIALIZED    START_STATE
wild(4)p2     3           inService(1) 10/31/97 17:47:00   passed(1)
wild(4)p4     4           inService(1) -                   neverRun(26)
```

Field Names	Field Definitions
TYPE	The type of card or interface. LAN link status shows the interface type from the standard MIB-II if Table.
SLOT	
PORT	
ADSTAT	This is the administrative state. For LAN interfaces this is up or down, as in the standard MIB-II; it does not apply for LAN cards. For other cards the administrative state is inService or maintBusy. PRI interfaces can have an ADSTAT of dchanBusy, the D-channel is down but the B-channels are up, or intfBusy, all channels are down. An NFAS extension interface can have an ADSTAT of nfasBusy; the signaling interface of its trunk group is either intfBusy or dchanBusy. The nfasBusy state is the functional equivalent of dchanbusy.
ACT_CALLS	This shows the number of active calls using a PRI interface and helps you determine the impact of bringing down the interface.
ACT_CONN	This shows the number of connections using a WILD card and helps you determine the impact of bringing down the card. The number of active calls using the card is not larger than the number of connections.
LAST_ INITIALIZED	This is the date and time of the last reinitialization. A dash indicates that the card has not been initialized since system startup.

Field Names	Field Definitions
INIT_STATE	This is the cause of the last initialization failure, if any.
LAST_ STARTED	This is the date and time of the last restart. A dash indicates that the card has not been restarted since system startup.
START_STATE	The cause of the last restart failure, if any.

2 of 2

Show status of Wild cards only.

```
$ showcard data=wild
WILD CARD STATUS
TYPE    SLOT  ACT_CONN    ADSTAT       LAST_INITIALIZED    START_STATE
wild(4)p2     3           inService(1) 10/31/97 17:47:00   passed(1)
wild(4)p4     4           inService(1) -                   neverRun(26)
```

Busy out the PRI interface in slot **i5**, port **1**, without interrupting active calls. If NFAS is in effect for this trunk group, the other interfaces go into the **nfasBusy** state

```
$ busypri slot=i5 port=1 data=dchan
Your request to busypri succeeded.
PRI INTF      STATUS
SLOT   PORT   ACT_CALLS   ADSTAT
i5     1      1           dchanBusy(3)

$showcard slot=p2
INSTALLED NETWORK INTERFACE HARDWARE
TYPE   SLOT   PORTS       ADSTAT
wild(4)p2     0           maintBusy(2)
```

```
WILD CARD STATUS
TYPE   SLOT   ACT_CONN    ADSTAT
wild(4)p2     3           maintBusy(2)
```

Reinitialize the WILD card in slot p2. This example uses the **showcard** command to determine the outcome of the initialization operation. The first **showcard** command shows that the operation is not yet complete. The second **showcard** command shows the completed operation.

```
$ busywild slot=p2

This may interrupt active calls. Please confirm: Y
Your request to busywild succeeded.

WILD CARD STATUS
TYPE          SLOT        ACT_CONN     ADSTAT      LAST_INITIALIZED    START_ERROR
wild(4)       p2          0            inService(1)-                   none(0)

$ initcard slot=p2

Your request to initcard succeeded.

$ showcard slot=p2 data=wild

INSTALLED NETWORK INTERFACE HARDWARE
TYPE     SLOT PORTS       ADSTAT       LAST_INITIALIZED    INTI_ERROR
wild(4) p2    0           maintBusy(2) -                   inProgress(0)

WILD CARD STATUS
TYPE     SLOT ACT-CONN    ADSTAT       LAST_INITIALIZED    INTI_ERROR
wild(4) p2    3           Busy(2)      -                   none(0)
```

```
$ showcard slot=p2 data=wild

INSTALLED NETWORK INTERFACE HARDWARE
TYPE     SLOT PORTS       ADSTAT       LAST_INITIALIZEDINTI_ERROR
wild(4)  p2   0           maintBusy(1) 11/2/97 09:43:15passed(1)

WILD CARD STATUS
TYPE     SLOT PORTS       ADSTAT       LAST_INITIALIZEDINTI_ERROR
wild(4)  p2   3           Busy(2)      -               none(0)

$ rlswild slot=p2

Your request to rlswild succeeded.

WILD CARD STATUS
TYPE    SLOT  PORTS       ADSTAT       LAST_INITIALIZEDINTI_ERROR
wild(4)p2     0           inService(1) -               none(0)
```

Test the MVIP clock on the WILD card in slot p2.

```
$ testwild test=clock slot=p2

Your request to testwild succeeded.

$ showtest

WILD CARD TEST RESULTS
======================
SLOT   LOOP_TEST          FRAME_CLOCK     2MHZ_CLOCK        4MHZ_CLOCK
p2     neverRun(26)       inProgress(27)   inProgress(27)   inProgress(27)
```

```
$ showtest

WILD CARD TEST RESULTS
======================
SLOT   LOOP_TEST          FRAME_CLOCK  2MHZ_CLOCK  4MHZ_CLOCK
p2     neverRun(26)       passed(1)    passed(1)   failed(2)
```

WARNINGS

Interface cards must be installed in the order indicated in *Table 1 on page 498*, otherwise location information will be incorrect.

PRI interfaces in NFAS trunk groups depend on one interface for all their signalling. If the signalling interface in the group is in the intfBusy or dchanBusy state, all interfaces in the group are effectively dchanBusy. **showcard data=pri** will show their state as nfasBusy. Use the showptg command to find NFAS trunk groups

PRI interface i5:1 contains the MVIP clock for the entire server. Reinitializing the card in slot i5 will interrupt synchronization. The effect will last at most 30 seconds (for instance, a 3-party call on one server might lose and regain audio). If you change the administrative state on the MVIP clock interface, it will not affect other interfaces, *in most cases.* However, when you run **initcard** against slot i5, interrupted timing *sometimes* interferes with the WILD card and results in the loss of audio. When this happens, you must restart the server by typing **reset level=cold1 RETURN** to restore service.

initcard fails if the card is not in the maintBusy state. You see the status as an INIT_STATE or START_STATE of cardNotBusy in the showcard command display.

DIAGNOSTICS

initcard fails if the card is not in the maintBusy state.

Use **initcard** only on PRI and WILD cards; it fails on LAN cards.

An NFAS extension interface cannot be put in the dchanBusy state, since it does not have a D-channel. Instead, change the signalling interface of its trunk group to dchanBusy; this changes all the extension interfaces to nfasBusy.

MIB GROUPS

Interfaces Group, TCP/IP MIB-II (RFC1213); mmcxinstalled HWTable; mmcxPriStatusTable, mmcxPriPerfTable; mmcxWildStatusTable, mmcxWildPerfTable

SEE ALSO

INTRO, page 426

ATMADM, page 437

ENETADM, page 471

INTFADM, page 479

PRIADM, page 521

PTGADM, page 538

MASIADM

NAME

chgmasi, **showmasi** - administer the optional Multimedia Application Server Interface (MASI) to connect MMCX with a DEFINITY Enterprise Communications Server (ECS).

SYNOPSIS

chgmasi [state=*new-state*]
[arsfac=*access-code*] [nearpath=*near-path-number*]
[farpath=*far-path-number*] [tscnum=*tsc-phone-number*]
[slot=*tsc-slot* , port=*tsc-port*] [plan=*pri-routing-plan*]

showmasi

DESCRIPTION

These commands enable the Multimedia Application Server Interface (MASI) on the MMCX server (most actual administration is handled on the DEFINITY side).

To enable, disable, or configure MASI on your server, you pass the parameters listed below with the **chgmasi** command. Changes take effect after the next MMCX reset.

showmasi displays the MASI parameters for your server.

All MASI parameters are optional, but you must specify at least one if you want to make changes.

- ***new-state*** is the desired MASI state, either **enabled** or **disabled**.

- ***access-code*** is the Facility Access Code (FAC) that lets MMCX users access the DEFINITY Automatic Route Selection feature. It is much like a dial plan access code: three digits, of which the first may be replaced by an asterisk (*****).
- ***near-path-number*** is the *near-end* (local) path-terminating number that DEFINITY uses for calls to your MMCX server.
- ***far-path-number*** is the *far-end* (remote) path-terminating number that your MMCX server uses for calls to your DEFINITY ECS.
- ***tsc-phone-number*** is the near-end phone number that DEFINITY uses when setting up a Temporary Signaling Connection (TSC) to the MMCX. TSC signalling uses a portion of the D channel of an ISDN PRI.
- ***tsc-slot, tsc-port*** defines the slot and port location of the PRI that MMCX uses for the MASI (Temporary Signaling Connection).
- ***pri-routing-plan*** is the PRI routing plan number that MMCX uses when connecting the Temporary Signaling Connection.

EXAMPLES

```
$ chgmasi state=enabled arsfac="*7" nearpath=3035385555 neartsc=3035381234
slot=i5 port=1 plan=1

Your request to chgmasi succeeded.

               STATE:enabled(1)
 FEATURE ACCESS CODE:"*7"
NEAR-END PATH NUMBER:3035385555
 FAR-END PATH NUMBER:3035386666
    TSC PHONE NUMBER:3035381234
```

```
      TSC INTERFACE:i5:1
   PRI ROUTING PLAN:1
```

DIAGNOSTICS

The Feature Access Code must be at most three digits or one star (*****) followed by two digits.

MIB GROUPS

mmcxMasi

SEE ALSO

INTRO, page 426

CFGADM, page 458

DPADM, page 466

RESET, page 544

MCASTADM

NAME

chgmcast, **showmcast** - administer MMCX IP Multicast related information.

SYNOPSIS

chgmcast [**blk**=***block-number***] [**udp**=***first-udp-port***] [**route**=***router-extent***] [**stat**=***status-flag***]

showmcast [**data**=***data-type,data-type ...***]

DESCRIPTION

chgmcast allows a user to modify the parameters governing MMCX use of IP Multicasting. ***block-number*** and **stat** must be administered to enable Multicasting in the server. ***first-udp-port*** and ***router-extent*** can usually be left at their initial defaults.

Exceptions are described below. The valid ranges for the parameters that can be configured are:

- ***block-number***: The block number of IP Multicast addresses assigned to this MMCX server. Valid range is 0 - 32. Block number defaults to zero, meaning that no block numbers are assigned and Multicasting is disabled. Before enabling Multicasting, assign a unique block number to each MMCX server on the LAN.

- ***first-udp-port***: The number of the first UDP port to use for Multicast connections. Valid range is 5000 - 31900. The server will choose a reasonable default based on the block number. It is possible that this choice may conflict with UDP ports used by another application that performs Multicasting on the customer's LAN. In that case the network administrator must determine a block of 100 free UDP ports and set ***first-udp-port*** to the lowest port number of this block.
- ***router-extent***: The maximum number of routers through which multicast datagrams can pass. Valid range is 0 - 25, with default zero. This must be raised in order to perform Multicasting across LAN segments connected by routers. The routers must also be Multicast-capable and administered for Multicasting. Each MMCX server in all segments must have a unique block number. In general, **router-extent** should be the minimum number that spans all LAN segments with MMCX end-points. Higher numbers may generate unnecessary traffic on remote segments.
- ***status-flag***: The desired Multicast status: enabled(1) or disabled(2).
- **showmcast** is the command to view Multicast related data. ***data-type*** can be one of the following:
  - **count** - Multicast configuration and address allocation counts, used primarily for performance management.
  - **alloc** - Multicast address allocation table, used primarily for troubleshooting.

If multiple ***data-types*** are specified, then those data will be shown in the order of their input. If no ***data-type*** is specified, all data will be shown.

EXAMPLES

To enable multicasting:

```
$ chgmcast blk=13 status=enabled
Your request to chgmcast succeeded.
  BLOCK_NUMBER:     13
FIRST_UDP_PORT:     11300
 ROUTER_EXTENT:     0
   STATUS_FLAG:     enabled(1)
```

The meaning of the headings are described above.

To view the Multicast counts:

```
$ showmcast data=count
BLOCK_NUMBER:     13
FIRST_UDP_PORT:     11300
 ROUTER_EXTENT:     0
   STATUS_FLAG:     enabled(1)
FIRST_ADDRESS:     224.0.5.20
    BLOCK_SIZE:     100
 REQUEST_COUNT:     50297
    FAIL_COUNT:     0
    FREE_COUNT:     50294
 CURRENT_COUNT:     3
```

The meaning of the first four headings is described above.

- **FIRST_ADDRESS**= The first IP address in the assigned block given by **BLOCK_NUMBER**.
- **BLOCK_SIZE**= The number of sequential IP addresses in the assigned block.
- **REQUEST_COUNT**= The number of Multicast address allocation requests processed.
- **FAIL_COUNT**= The number of Multicast address allocation requests that failed.
- **FREE_COUNT**= The number of Multicast address free requests processed.
- **CURRENT_COUNT**= The number of Multicast addresses currently allocated in this server.

To view the Multicast Allocation Table:

```
$ showmcast data=alloc
```

The meaning of the table headings is as follows:

- **ALLOC_IP_ADDRESS**= A Multicast IP address that has been allocated in this server.
- **ASSIGN_IP_ADDRESS**= The IP address of the entity assigned to this Multicast address.
- **UDP_PORT**= The UDP port number on which the assigned entity listens.

DIAGNOSTICS

chgmcast will fail if no parameters are specified or if invalid parameters are specified.

MIB GROUPS

MMCX Multicast MIB

SEE ALSO

INTRO, page 426

IPADM, page 483

MSTADM

NAME

showmst, clearmst, startmst, stopmst, chgmst, resetmst, showexpr - administer Message Sequence Trace

SYNOPSIS

showmst [**data**=data-type] [**prot**=protocol, protocol ...]

clearmst

startmst [**clear**=clear-option] [**confirm**=confirmation-request]

stopmst

chgmst prot=protocol [**trace**=trace-option] [**filt**=filter-expression] [**start**=start-trigger] [**stop**=stop-trigger] [**trig**=trigger-option]

resetmst

showexpr

DESCRIPTION

showmst displays the Message Sequence Trace (MST) parameters administered by the other commands. If the trace is enable, it also shows the time it was started.

data-type - may be stat for MST status, filt for filter and trigger information, or all. Default is all.

protocol - specifies one or more protocols for which to display filter and trigger information. Default is all. If data-type is stat, protocol is ignored.

clearmst empties the trace log; any previous trace is discarded. The trace must be stopped to clear the log.

startmst initiates the trace.

clear-option - To clear the previous file use yes, otherwise use no. Default is yes.

confirmation-request - Use clear=yes to confirm; this is the default. Use confirm=no to suppress the confirmation request.

stopmst stops the trace.

chgmst changes the filter and trigger parameters that control the messages logged into the trace file. You must stop the trace to change parameters. Each protocol has its own set of filter and trigger parameters; this command affects only one protocol at a time.

protocol - select the affected protocol

trace-option - set the trace for this protocol to on or off

filter-expression - select the message traces you want traced. You can only get message traces for those messages that match the expression. See ecs_filter for expression rules.

start-trigger and **stop-trigger** - turn tracing on and off automatically. Tracing begins when a message matches the start trigger; it continues until another message matches the stop-trigger. If the start-trigger is empty, tracing begins immediately after the startmst command. If the stop-trigger is empty, tracing continues until the stopmst command.

trigger-option - is effective only if both start- and stop-triggers are specified. Valid values are once, and retrigger. If trigger-option is retrigger, the trace cycles between start- and stop-triggers until stopped manually. If trigger-option is once, it stops on the stop-trigger until started manually.

resetmst - resets all filters, triggers, and option so that the trace includes all messages.

Filter and trigger expressions may be replaced by a predefined expression provided by the system administrator. The showexpr command shows the available expressions.

EXAMPLES

```
$showmst
MESSAGE SEQUENCE TRACE PARAMETERS
MST STATUS: running(1)
START TIME: 07/08 10:22:04
STOP TIME:  -
PROTOCOL TRACING TRIGGER OPTION
q.931(1)on(1)once(1)
Q.931 FILTER:-
Q.931 START TRIGGER:@mtype 0xce
Q.931 STOP TRIGGER:@mtype 0xc7
```

To add a predefined filter named “PRI up/downlink”, stop the trace, make the change, and start again.

```
$stopmst
Your request to stopmst succeeded.
MESSAGE SEQUENCE TRACE PARAMETERS
MST STATUS:stopped(2)
START TIME:07/08 10;22:04
```

```
STOP TIME:07/08 12:17:09
PROTOCOLTRACINGTRIGGER OPTION
q.931(1)on(1)once(1)
Q.931 FILTER:-
Q.931 START TRIGGER:@mtype 0xce
Q.931 STOP TRIGGER:@mtype 0xc7
$showexpr
NAME         EXPRESSION
PRI up/downlink(@mtype 0x60 OR @mtype 0x62)
PRI level 2  (@mtype 0x6C OR @mtype 0x6D)
PRI unrecognized(@mtype 0x6E)
$chgmst prot=q931 filt="PRI up/downlink"
Your request to chgmst succeeded.
MESSAGE SEQUENCE TRACE PARAMETERS
MST STATUS:stopped(2)
START TIME:07/08 10:22:04
STOP TIME:07/08 12:17:09
PROTOCOLTRACING          TRIGGER OPTION
q.931(1)on(1)            once(1)
Q.931 FILTER: (@mtype 0x60 or @mtype 0x62)
Q.931 START TRIGGER:@mtype 0xce
Q.931  STOP TRIGGER@mtype 0xC7
```

To further restrict the filter, use xterm cut-and-paste to copy an expression from showexpr to showmst into the command line.

```
$chgmst prot=q931 filter="@source=jpsingh AND (@mtype 0x60 OR @mtype 0x62)"
Your request to chgmst succeeded.
MESSAGE SEQUENCE TRACE PARAMETERS
MST STATUS:stopped(2)
START TIME:07/08 10:22:04
STOP TIME:07/08 12:17:09
```

```
PROTOCOLTRACINGTRIGGER OPTION
q.931(1)on(1)once(1)

Q.931 FILTER:@source=jpsingh AND (@mtype 0x60 OR @mtype 0x62)
Q.931 START TRIGGER:@mtype 0xce
Q.931 STOP TRIGGER:@mtype 0xc7
$startmst
This will erase the trace log. Please confirm:y
MESSAGE SEQUENCE TRACE PARAMETERS
MST STATUS:running(1)
START TIME:07/08 10:27:38
STOP TIME:-
PROTOCOLTRACINGTRIGGER OPTION
q.931(1)on(1)once(1)
Q.931 FILTER:@source=jpsingh AND (@mtype 0x60 OR @mtype 0x62)
Q.931 START TRIGGER:@mtype 0xce
Q.931 STOP TRIGGER:@mtype 0xc7
```

MIB GROUPS

mmcxMst

PRIADM

NAME

addpri, **chgpri**, **rmpri**, **showpri** - administer and display various parameters on an ISDN PRI interface; update link status for PRI interfaces

SYNOPSIS

addpri slot=***slot-number*** **port**=***port-number*** [**lcomp**=***line-compensation***] [**lcode**=***line-coding***] [**idle**=***idle-code***] [**frame**=***framing***] [**crc**=***crc4***] [**comp**=***companding***] [**conn**=***connect-type***] [**intf**=***interface-type***] [**cntry**=***country-protocol***] [**peer**=***peer-protocol***] [**vers**=***protocol-version***] [**side**=***side***] [**time**=***timing***] [**cir**=***circuit-id***] [**term**=***term-imp***]

chgpri slot=***slot-number*** **port**=***port-number*** [**lcomp**=***line-compensation***] [**lcode**=***line-coding***] [**idle**=***idle-code***] [**frame**=***framing***] [**crc**=***crc4***] [**comp**=***companding***] [**conn**=***connect-type***] [**intf**=***interface-type***] [**cntry**=***country-protocol***] [**peer**=***peer-protocol***] [**vers**=***protocol-version***] [**side**=***side***] [**time**=***timing***] [**cir**=***circuit-id***] [**term**=***term-imp***]

rmpri slot=***slot-number*** **port**=***port-number***

showpri [**data**=***data-type...***] [**slot**=***slot-number...***] [**port**=***port-number***...]

DESCRIPTION

addpri adds a new ISDN PRI interface to the server in the specified slot and port. It creates a record for that interface with all required parameters set to default values. The default values

administer the interface as if it were connected to a central office ISDN switch in the U.S. using the Bellcore protocol. After adding PRI interfaces, the system needs to be rebooted in order for the translations to take affect. Note that PRI interfaces are not usable, until the system is rebooted.

chgpri changes the parameters in the record for the PRI in the specified slot and port.

rmpri removes the record for the PRI in the specified slot and port.

showpri displays the current settings for the interface in the specified slot and port. If no arguments are included, it displays the current settings for all interfaces on the server. If slot is specified but not port, it displays the current settings for all interfaces in that slot.

Following are the parameters, their possible values, and the default values, which are indicated by the parenthetical remarks:

- ***slot-number*** i5-i2 (default is **all** on a show) The slot in the server in which the board containing the interface is inserted
- ***port-number*** 1-2 (default is **all** on a show) The port number on the board for the interface
- ***data-type*** **cfg**, **stat**, **perf** (default is **all**) The type of data requested.

  cfg shows the current configuration parameters for PRI interfaces

  stat shows the statistics that apply specifically to PRI interfaces

  count shows the performance counts.

  For **cfg**, all interfaces that have been translated will be shown; however, for both **stat** and **count**, only those interface that have hardware will be shown.
- ***svcstat***

  1 outOfService

  2 inService

The service state that you want the specified interface to be set to. There is no default.

- ***line-compensation***

  1 length0to133ft (default)

  2 length133to266ft

  3 length266to399ft

  4 length399to533ft

  5 length533to655ft

  The length of the cable from the server to the CSU or nearest repeater on an interface. 1=0-133', 2=133-266', 3=266-399', 4=399-533', 5=533-655'.

- ***framing***

  1 e1Basic

  2 e1FEBE

  3 ds1ESF (default)

  4 ds1SFD4

  5 e1CRC

  For an E1 bit rate, framing can be **e1Basic**, **e1FEBE**, or **e1CRC**; for a T1, framing can be **ds1ESF** or **ds1SFD4**.

- ***line-coding***

  1 zcs

  2 b8zs (default)

  3 basic

4 hdb3

Line coding types are as follows:

- **ZCS** - AMI line coding with ZCS ones density protection.
- **B8ZS** - AMI line coding with B8ZS ones density protection.
- **Basic** - AMI line coding with no ones density protection.
- **HDB3** - AMI line coding with HDB3 ones density protection. HDB3 is used in some countries other than the U.S. to guarantee ones density.

- ***idle-code***

  A number in the range 0-255 (default is 255)

- ***crc4***

  1 off (default)

  2 on

  CRC4 is a 4-bit error-checking scheme in which a CRC bit is encoded as the first position of all even-numbered frames. If CRC4 is not administered, this bit position is unassigned.

- ***companding***

  1 aLaw

  2 muLaw (default)

  A-law and Mu-law are the two possible algorithms for improving the signal-to-noise ratio resulting from the pulse code modulation (PCM) on voice transmission.

- *connect-type*

  2 network

  3 pbx (default)

This is the type of switch at the other end of this interface, either a private switch (PBX, MMCX) or a public network switch.

- ***interface-type***

  1 user (default)

  2 network

  3 peerMaster

  4 peerSlave

  This field allows you to choose a user or network protocol, or a peer protocol for server-to-PBX connections.

- ***country-protocol***

  A valid country code in the range 1-99 (1)

  Valid codes are as follows:

  1 usa (default)

  2 australia

  3 japan

  4 italy

  5 netherlands

  6 singapore

  7 mexico

  8 belgium

  9 saudiArabia

10 uk
11 spain
12 france
13 germany
14 czechoslovakia
15 russia
16 argentina
17 greece
18 china
19 hongkong
20 thailand
21 macedonia
22 poland
99 etsi

Note that required tones are hardcoded for each country protocol.

- ***peer-protocol***

  1 noPeerProto (default)
  101 qsig

  The peer protocol for this interface.

- ***protocol-version***

  1 noPeerProto (default)

  2 a

  3 b

  For country-protocol **1**

  a = AT&T G3V2 protocol

  b = NI-2/Bellcore protocol

  For country-protocol **10**

  a = ETSI

  b = national protocol

  For country-protocol **12**

  a = national protocol

  b = ETSI

  For country-protocol **13**

  a = ITR6 protocol

  b = ETSI

- *side*

  1 noPeerProto (default)

  2 a

  3 b

Administering the system as side **a** means that the system is the “a” side at layer 3 in the QSIG peer protocol. Similarly, administering the system as side **b** means that it is side “b” at layer 3 in the QSIG peer protocol.

- ***timing***

  3 external

  129 incoming

  130 internal (default)

  This field refers to the clocking mechanism to use. External means that the timing for this board will be externally synchronized with the MVIP interface from the WILD board, while internal means that the timing will be synchronized internally.

- ***circuit-id*** is a string of 0-255 characters (no default) that describes the ISDN circuit to which the interface is connected.
- ***term-imp***

  1 notApplicable (default)

  2 term120ohm

  3 term75ohm

  This is the termination impedance for this PRI interface.

The rest of these fields show up in either the statistics or performance displays. Since they are display-only fields, valid values and default values are not specified.

- ***BIT_RATE*** is the type of physical interface. T1 is 1.544 mbps (24 channels, 64-kbps each). E1 is 2.048 mbps (32 channels, 64-kbps each).
- ***DCHAN_STAT*** is the operational status of the D channel for this interface.

- ***SERVICE_STATE*** is the service state of this interface.
- ***INTF_STATUS*** is the current status of this interface.
- ***LINK_DOWNS*** is the number of times this link has gone down.
- ***ACTIVE*** is the number of currently active ISDN calls.
- ***IN_ATTEMPT*** is the total number of incoming ISDN calls attempted on this interface.
- ***IN_COMPLETE*** is the total number of incoming ISDN calls completed on this interface.
- ***IN_ABANDON*** is the total number of incoming ISDN calls abandoned on this interface.
- ***IN_FAIL*** is the total number of incoming ISDN calls that failed on this interface.
- ***OUT_ATTEMPT*** is the total number of outgoing ISDN calls attempted on this interface.
- ***OUT_COMPLETE*** is the total number of outgoing ISDN calls completed on this interface.
- ***OUT_ABANDON*** is the total number of outgoing ISDN calls abandoned on this interface.
- ***OUT_FAIL*** is the total number of outgoing ISDN calls that failed on this interface.

EXAMPLES

To add port 2 of a PRI board in slot i3 and administer all default values except framing:

```
$ addpri slot=i3 port=2 frame=4

Your request to addpri succeeded.

ST  PT  CRC    LCOMP              FRAME      LCODE   IDLE COMP      TIME
i3  2   off(1) length0to133ft(1)  ds1SFD4(4) b8zs(2) 255  muLaw(2)  internal(130)

ST  PT  INTF   CONN         PEER                VERS    SIDE
i3  2   user(1)  network(2)qsig(101)            b(3)    a(2)
```

```
ST  PT  TERM             CNTRY       CIRCUIT-ID
i3  2   notApplicable(1) usa(1)      -
```

To change the setting for line coding on that same PRI interface:

```
$ chgpri slot=i3 port=2 lcode=3

Your request to chgpri succeeded.

ST PT CRC    LCOMP            FRAME       LCODE    IDLE  COMP      TIME
i3 2  off(1) length0to133ft(1) ds1SFD4(4)  basic(3)  255  muLaw(2)  internal(130)

ST PT INTF     CONN        PEER       VERS   SIDE
i3 2  user(1)  network(2)  qsig(101)  b(3)   a(2)

ST PT TERM              CNTRY   CIRCUIT-ID
i3 2  notApplicable(1)  usa(1)  -
```

To display current settings for all PRI interfaces on slot i3:

```
$ showpri data=cfg slot=i3

      PRI CONFIGURATION
      =================
ST PT CRC    LCOMP            FRAME      LCODE    IDLE COMP     TIME
i3 1  off(1) length0to133ft(1) ds1ESF(3)  b8zs(2)  255  muLaw(2) internal(130)
i3 2  off(1) length0to133ft(1) ds1SFD4(4) basic(3) 255  muLaw(2) internal(130)

ST PT INTF          CONN         PEER           VERS       SIDE
i3 1  user(1)       network(2)   qsig(101)      b(3)       a(2)
i3 2  user(1)       network(2)   qsig(101)      b(3)       a(2)
```

```
ST PT     TERM               CNTRY           CIRCUIT-ID
i3   1    notApplicable(1)   usa(1)          -
i3   2    notApplicable(1)   usa(1)          -
```

To display the statistics for all PRI interfaces:

```
$ showpri data=stat

      PRI STATUS
      ==========
SLOT PORT BIT_RATE DCHAN_STAT SERVICE_STATE   INTF_STATUS
i5   1    t1(24)   down(1)    outOfService(2) testing(10)
i5   2    t1(24)   down(1)    outOfService(2) testing(10)
```

To display performance counts for the PRI interface on slot i5:

```
$ showpri data=count slot=i5

      PRI COUNTS
      ==========
SLOT PORT IN_ATTEMPT  IN_COMPLETE  IN_ABANDON  IN_FAIL  LINK_DOWNS ACTIVE
i5   1    0           0            0           0        0          0
i5   2    0           0            0           0        0          0

SLOT PORT OUT_ATTEMPT OUT_COMPLETE OUT_ABANDON OUT_FAIL
i5   1    0           0            0           0
i5   2    0           0            0           0
```

DIAGNOSTICS

The following two tables summarize the rules of validation used for **addpri** or **chgpri**.

To encapsulate all the rules in a succinct manner, the following guidelines will be used:

- Any argument not specifically mentioned below has no restrictions.
- An argument left blank in the table may be any value.
- A word identifies a single selection for the argument. A word preceded by **!** means any selection other than the one named. A word ending in ***** means all options that start with that word.

bit	frame	code	term
t1	ds1*	zcs, b8zs	-
e1	e1*	basic, hdb3	

conn	intf	peer	vers	side	cntry
network	user	noPeerProto	noPeer Proto	noPeerProto	

conn	intf	peer	vers	side	cntry
pbx	!peer*	noPeerProto	noPeerProto	noPeerProto	
pbx	peer*	qsig	a,b	a,b	US, UK, Germany, France
pbx	peer*	qsig	noPeerProto	noPeerProto	US, UK, Germany, France

MIB GROUPS

mmcxPriTranslationTable, mmcxPriStatusTable, mmcxPriPerfTable

SEE ALSO

INTRO, page 426 *PRPADM, page 534*

PTGADM, page 538

BWADM, page 454

PRPADM

NAME

addprp, **chgprp**, **rmprp**, **showprp** - administer the MMCX PRI routing plan table

SYNOPSIS

addprp plan=***pri-routing-plan*** **tg**=***trunk-group...***

chgprp plan=***pri-routing-plan*** **tg**=***trunk-group...***

rmprp plan=***pri-routing-plan***

showprp [**data**=***data-type***] [**plan**=***pri-routing-plan...***]

DESCRIPTION

PRI routing involves two tables:

- PRI routing plan table
- PRI trunk group table.

This manual page covers the PRI routing plan table only, see *PTGADM, page 538* for information on the PRI trunk group table.

A PRI routing plan contains an ordered list of PRI trunk groups. It indicates which trunk groups should be tried, and in what order. Trunk group numbers in a PRI routing plan point to records in the PRI trunk group table. See dial plan and inter-server routing administration--*DPADM, page 466* and *ISRADM, page 490*--to see where these routing plans are used.

addprp adds the trunk group list for ***pri-routing-plan*** in the MMCX PRI routing plan table.

Pri-routing-plan is a number from 1 to 32. It is used in the dial plan table and the inter-server routing table.

Trunk-group is a PRI trunk group number which ranges from 1 to 8. It is an index into the trunk group table. A plan can contain 1 to 8 trunk group numbers.

chgprp changes the trunk group list for a given ***pri-routing-plan***.

rmprp removes the ***pri-routing-plan*** from the table.

showprp shows, by default, both the PRI routing plan configuration and the PRI routing plan counts. To see just one table, use the ***data-type*** option and set it to **cfg** for configuration, or **count** for the count information. Also, to see data on a specific routing plan, use the ***pri-routing-plan*** option. The default is to show data on all routing plans.

EXAMPLES

To add PRI routing plan 1 with trunk groups 1, 2, 3, and 4:

```
$addprp plan=1 tg=1,2,3,4
Your request to addprp succeeded.
PLAN  TRUNK_GROUPS
1     1, 2, 3, 4
```

To change PRI routing plan 3 to try trunk groups 5, 6, 1, and 4:

```
$ chgprp plan=3 tg=5,6,1,4
Your request to chgprp succeeded.
PLAN  TRUNK_GROUPS
3     5, 6, 1, 4
```

To look at the PRI routing plan configuration and counts:

```
$ showprp
        PRI ROUTING PLAN CONFIGURATION
        ==============================
PLAN   TRUNK_GROUPS
1      1, 2, 3, 4
3      5, 6, 1, 4
        PRI ROUTING PLAN COUNTS
        =======================
PLAN   NO_BCHAN    PROTO_ERROR
1      0           0
3      0           0
```

The **NO_BCHAN** column is the number of times a request was refused due to no B-channels available in the routing plan. The **PROTO_ERROR** column is the number of PRI stack protocol errors encountered on this routing plan.

DIAGNOSTICS

addprp fails if the pri-routing-plan number already exists in the table.

chgprp and **rmprp** fail if pri-routing-plan number doesn't exist.

MIB GROUPS

mmcxPriRtPlanTable

SEE ALSO

INTRO, page 426

PRIADM, page 521

PTGADM, page 538

DPADM, page 466

ISRADM, page 490

PTGADM

NAME

addptg, **chgptg**, **rmptg**, **showptg** - MMCX PRI trunk group administration and counts

SYNOPSIS

addptg tg=***trunk-group*** **intf**=***interface...*** [**nfas**=***nfas-status***] [**aud**=***audio-percentage***] [**vid**=***video-percentage***] [**app**=***application-percentage***]

chgptg tg=***trunk-group*** [**intf**=***interface...***] [**nfas**=***nfas-status***] [**aud**=***audio-percentage***] [**vid**=***video-percentage***] [**app**=***application-percentage***]

rmptg tg=***trunk-group***

showptg [**data**=***data-type***] [**tg**=***trunk-group...***]

DESCRIPTION

These commands assign PRI interfaces to trunk groups. Each PRI interface (e.g. slot-port) can belong to one and only one trunk group. These trunk groups can then be used in PRI routing plans to determine which trunk groups should be tried, and in what order.

These commands also allow the system administrator to assign bandwidth percentages to the trunk groups. Each bandwidth parameter indicates the percentage of B-channels that should be reserved for that use.

For example, if audio-percentage is set to 100%, all B-channels on all interfaces for that trunk group will only route audio calls.

addptg adds the interface list and bandwidth parameters for ***trunk-group.***

trunk-group is a number from 1 to 8. It is used in the PRI routing plan table to indicate which trunk groups belong to which routing plans.

Interface is the list of interfaces that belong to this trunk group. There can be 1 to 8 interfaces in an interface list, where each interface is a slot/port combination (e.g. i5:1, is slot 5 on the ISA bus and port 1).

audio-percentage is the percentage of B-channels on the interfaces in the interface-list that are reserved exclusively for audio calls.

video-percentage is the percentage of B-channels on the interfaces that are reserved exclusively for video calls.

application-percentage is the percentage of B-channels on the interfaces that are reserved exclusively for application calls.

The sum total of all percentages cannot be greater than 100; however, it can be less than 100, because you may choose to leave some B-channels unreserved, for incoming calls. The default for these 3 percentage fields is 0.

nfas-status is an indication of whether nfas is active or not. Valid values are:

- **on**
- **off**

chgptg changes the interface-list or the percentage parameters for a given ***trunk-group***.

rmptg removes the ***trunk-group*** from the PRI trunk group table.

showptg shows the current trunk group configuration and/or performance counts on those trunk groups.

data-type can be one of **cfg**, **count** or **all**, where **cfg** shows the configuration information and **count** shows the performance counts. The default is to show both tables. If ***trunk-group*** is specified, then only those trunk groups will be displayed, otherwise all trunk groups will be displayed.

EXAMPLES

To add trunk group 1 with interface-list: i5:1 and i5:2, and percentages set to 20, 20, 20 for audio, video and application calls, respectively:

```
$ addptg tg=1 intf=i5:1,i5:2 aud=20 vid=20 app=20
Your request to addptg succeeded.
TG  AUD  VID   APP NFAS INTERFACE_LIST
1   20   20    20  off  i5:1, i5:2, -, -, -, -, -, -
```

To change trunk group 1 to allocate 20% more bandwidth to audio calls:

```
$ chgptg tg=1 aud=40
Your request to chgptg succeeded.
TG  AUD  VID   APP NFAS INTERFACE_LIST
1   40   20    20  off  i5:1, i5:2, -, -, -, -, -, -
```

To remove trunk group 1:

```
$ rmptg tg=1
Your request to rmptg succeeded.
```

To show all PRI trunk group information:

```
$ showptg

      PRI TRUNK GROUP CONFIGURATION
      =============================
TG   AUD   VID   APP NFAS INTERFACE_LIST
1    40    20    20  off  i5:1, i5:2, -, -, -, -, -, -
2    0      0     0       i2:1, i2:2, i3:1, i3:2, -, -, -, -
3    100    0     0       i4:1, -, -, -, -, -, -, -

      PRI TRUNK GROUP COUNTS
      ======================
TG   CUR_OUT_AUD  CUR_OUT_VID CUR_OUT_APP CUR_IN_AUD CUR_IN_OTH BCHAN
1    0            0           0           0          0          0
2    1            2           3           4          5          6
3    0            0           0           0          0          0
TG   MAX_OUT_AUD MAX_OUT_VID MAX_OUT_APP MAX_IN_AUD MAX_IN_OTH
1    0            0           0           0          0          0
2    1            2           3           4          5          6
3    0            0           0           0          0          0
TG   TOT_OUT_AUD TOT_OUT_VID TOT_OUT_APP TOT_IN_AUD TOT_IN_OTH
1    0            0           0           0          0          0
2    1            2           3           4          5          6
3    0            0           0           0          0          0
```

The meaning of the headings for the trunk group counts are as follows:

- **TG**=the trunk group number.

- **CUR_OUT_AUD**=the current number of outgoing audio calls active for this trunk group.
- **CUR_OUT_VID**=the current number of outgoing video calls active for this trunk group.
- **CUR_OUT_APP**=the current number of outgoing application and shared data calls active for this trunk group.
- **CUR_IN_AUD**=the current number of incoming voice calls active for this trunk group.
- **CUR_IN_OTH**=the current number of incoming non-voice calls active for this trunk group.
- **BCHAN**=the current number of B-channels in service for this trunk group.

The next row of headings that begin with **MAX** indicate the maximum number of calls that were reached at any one time.

For example, **MAX_OUT_AUD** is the maximum number of outgoing audio calls active for this trunk group at any one time.

The final row of headings that begin with **TOT** indicate the total number of calls that were ever reached.

For example, **TOT_OUT_AUD** is the cumulative total number of outgoing audio calls for this trunk group.

DIAGNOSTICS

addptg and **chgptg** will fail if the sum of the three percentage parameters is greater than 100. It will also fail if a duplicate interface is specified in the same trunk group or in a different trunk group.

addptg will fail if the trunk-group already exists; and **chgptg** and **rmptg** will fail if the trunk-group does not exist.

MIB GROUPS

mmcxPriTrunkGrpTable, mmcxPriTrunkGrpStatusTable

SEE ALSO

INTRO, page 426

PRIADM, page 521

PRPADM, page 534

BWADM, page 454

RESET

NAME

reset - perform system initialization

SYNOPSIS

reset level=*reset_level*

reset level=mask [loc=*event_location*] [type=*event_type*] [enable=*on_or_off*]

DESCRIPTION

reset provides two system functions: graceful system initialization and changing maintenance related system parameters.

Execution of the command with ***halt, menu, cold1, cold2,*** or ***boot*** options causes the system processes to be gracefully shutdown, avoiding file system corruption and data inconsistencies. When the completion of operations is successfully made in a timeout period, the reset is considered graceful.

A graceful reset is always the best method to reset a system. Therefore use of the **reset** command is always recommended instead of power down, use of the LynxOS reboot command, depression of the chassis mounted RESET switch, or execution of the RMB commands (e.g. REBOOT) causing the chassis RESET switch equivalent depression.

Execution of the command with the **mask** and **thres** options cause the maintenance process to reset the values used for the ECS mask or threshold action tables. These options are intended for highly trained technical support people.

The following ***reset-level*** options are provided:

- **halt** gracefully terminates the MMCX application processes and halts the Lynx OS. You must either cycle the power OFF and ON or press RESET on the front of the server to restart the server.
- **cold1** Most application processes are terminated and the system will reinitialize back to an IS (In-Service) state. Full diagnostics of the hardware are not executed prior to placing the system into the IS state. If vintage and integrity checks pass (e.g. the present vintage and checksum of the FW to be downloaded match those read from the hardware), the FW is not downloaded and full diagnostics of the hardware are not executed prior to placing the system into IS. If the vintage and integrity checks fail, the reset level escalates to **cold2**.
- **cold2** The functions of **cold1** are performed after forcing both the execution of self-tests and the downloading of FW, independent of the state of the presently downloaded code.
- **boot** The currently running system is placed back into BIOS, resulting in the reloading of the operating system, and the initialization of the system processes. The system initializes with a **cold2** setting and is placed in the IS state once the hardware and software has been initialized.
- **menu** Most application processes are terminated and the software administration menu is entered. From the menu, installation, patching, system back-up and system restore can be executed. If the option is chosen to continue booting, then the menu will terminate and the system will reinitialize with a **cold1** level.

- **mask** This level is used to change the current setting of the ECS mask in the maintenance process. This mask is used to select which events are to be collected and logged by the maintenance process. Additionally, the **loc, type**, and **enable** options may also be specified to provide further granularity on these events. If **loc** is unspecified, then all locations are used. If **type** is unspecified, then all types are used except **MST**. If **enable** is unspecified, then **on** is assumed. **loc** is a colon (":") separated list of locations (typically software processes). **type** is a colon separated list of event types.
- **thres** The maintenance process will re-read threshold action table stored in the database and reset its RAM resident table. The database can be modified by the database tools and effected by executing this command and level.

If no level is specified, then **cold1** is assumed.

EXAMPLES

The following will cause the system to gracefully shutdown prior to turning off power and replacing the hardware:

```
$ reset level=halt
```

To force the system to reinitialize the hardware, execute the following:

```
$ reset level=cold1
```

To log all messages produced by the BIM process, execute the following command:

```
$ reset level=mask loc=BIM
```

To disable the logging of trace level 3 messages from BIM, execute the following:

```
$ reset level=mask loc=BIM type=DEBUG_LVL3 enable=off
```

DIAGNOSTICS

The system may not be able to load LynxOS if the hard disk is defective. If this is the case, then consult the ***MMCX Technical Reference*** Documentation for rebuilding and reloading the hard disk.

SAADM

NAME

addsa, **chgsapasswd**, **rmsa**, **showsa** - administer MMCX System Administrators

SYNOPSIS

addsa login=***login-id*** **name**=***full-name*** **id**=***user-id***

chgsapasswd login=***login-id***

rmsa login=***login-id***

showsa

DESCRIPTION

These commands administer MMCX system administrators. Any user can list the system administrators, but only the MMCX super-administrator (login **sysadm**) or the Unix super-user (login **root**) can modify administrator accounts.

addsa adds a system administrator account to **/etc/passwd** within Lynx.

login-id is a character string of up to eight alphanumeric characters. This will be the ID typed by the system administrator when logging in.

full-name This is the user's full name; it identifies the person to whom the login is assigned.

user-id This is the numerical user id that will be associated with the login-id. It must be between 100 and 5000 and must be unique for each user.

chgsapasswd prompts twice for, and changes, the password for the system administrator with login id ***login-id***.

rmsa removes a system administrator account for login ID.

showsa shows all the current system administrator accounts.

EXAMPLES

To add a system administrator:

```
$ addsa login=jjd name="John James Doe" id=101
Enter password:
```

When the administrator types the password an asterisk is echoed for each character.

```
Re-enter password:
```

The administrator types the same password again.

```
New account added for user jjd
```

To remove a system administrator record in **/etc/passwd**:

```
$ rmsa login=jjd
User jjd account removed.
```

To show all the system administrator accounts:

```
$ showsa
LOGIN     NAME
abc       Archibald Conifer
jjd       John James Doe
sysadm    MMCX System Administrator
```

DIAGNOSTICS

Exit status is 0 for any command that executes successfully, 1 for any that fails.

addsa fails if the specified login ID already exists in ***/etc/passwd***. It prompts twice for an initial user password. It fails if the responses to the two prompts differ. It also fails if a specified password does not meet Lynx's criteria for passwords. For example, minimum length, inclusion of special characters, etc.

rmsa fails if ***login-id*** is not found.

chgsapasswd fails if ***login-id*** is not found. It prompts twice for a user password. It fails if the responses to the two prompts differ. It will also fail if a specified password does not meet Lynx's criteria for passwords.

addsa, **chgsapasswd**, and **rmsa** fail if executed by anyone not logged in as either **sysadm** or **root**.

The account **sysman** may not be removed, nor its password changed. (Either **sysadm** or **root** can change the **sysadm** password using the Lynx command **passwd**.)

NOTES

This set of commands should not be confused with the MMCX commands for administering end-point user logins.

SEE ALSO

INTRO, page 426

SHOWCALL

NAME

showcall - show multimedia call counts

SYNOPSIS

showcall

DESCRIPTION

showcall shows statistics related to multimedia calls. No periodic counts, such as hourly or daily counts, are maintained. If the system manager needs such counts, she or he can write shell scripts to run this command and store the results.

TOTAL_ATTEMPTED_CALL - total number of calls attempted, where a “call” is defined as any time the user selects “call” or “conf” from the MMCX Client Software interface.

TOTAL_ALERTED_CALL - total number of calls that reached the ringing state.

TOTAL_ANSWERED_CALL - total number of calls that were answered by the remote end.

CURRENT_ACTIVE_CALL - the current number of active calls.

TOTAL_AUDIO_CONN - the total number of audio connections used, where a connection is defined as a uni-directional media bearer path.

TOTAL_VIDEO_CONN - the total number of video connections used.

TOTAL_SHARED_CONN - the total number of shared application connections used.

TOTAL_DISTRIBUTED_CONN - the total number of distributed application bearer paths used.

MAX_AUDIO_CONN - the maximum number of audio connections that existed at any one time.

MAX_VIDEO_CONN - the maximum number of video connections that existed at any one time.

MAX_SHARED_CONN - the maximum number of shared application connections that existed at any one time.

MAX_DISTRIBUTED_CONN - the maximum number of distributed application connections that existed at any one time.

CURRENT_AUDIO_CONN - the current number of audio connections.

CURRENT_VIDEO_CONN - the current number of video connections.

CURRENT_SHARED_CONN - the current number of shared application connections.

CURRENT_DISTRIBUTED_CONN - the current number of distributed application connections.

EXAMPLE

```
$ showcall
    TOTAL_ATTEMPTED_CALL:     500
      TOTAL_ALERTED_CALL:     490
     TOTAL_ANSWERED_CALL:     400
     CURRENT_ACTIVE_CALL:     5
        TOTAL_AUDIO_CONN:     500
        TOTAL_VIDEO_CONN:     300
       TOTAL_SHARED_CONN:     100
```

```
  TOTAL_DISTRIBUTED_CONN:     50
          MAX_AUDIO_CONN:     15
          MAX_VIDEO_CONN:     10
         MAX_SHARED_CONN:     5
    MAX_DISTRIBUTED_CONN:     5
      CURRENT_AUDIO_CONN:     5
      CURRENT_VIDEO_CONN:     3
     CURRENT_SHARED_CONN:     0
CURRENT_DISTRIBUTED_CONN:     1
```

SHOWICMP

NAME

showicmp - show data associated with icmp counts.

SYNOPSIS

showicmp

DESCRIPTION

showicmp is the command to show the data that applies to icmp (Internet Control Message Protocol) counts.

EXAMPLES

To see icmp counts:

```
$ showicmp
                                IN                  OUT
                           ----------          ----------
                  MSG:     1                   1
                ERROR:     1010                1010
         DEST_UNREACH:     9999999999          9999999999
            TIME_EXCD:     4                   4
            PARM_PROB:     32                  32
           SRC_QUENCH:     565789              565789
             REDIRECT:     25                  25
```

```
                ECHO:      0                    0
            ECHO_REP:      0                    0
          TIME_STAMP:      11111                11111
      TIME_STAMP_REP:      1234567890           1234567890
           ADDR_MASK:      22222                22222
       ADDR_MASK_REP:      33                   33
```

The meaning of the headings are as follows:

- **MSG**=the total number of ICMP messages which the entity received/sent
- **ERROR**=the number of ICMP messages which the entity received but determined as having ICMP-specific errors; the number of ICMP messages which this entity did not send due to problems discovered within ICMP
- **DEST_UNREACH**=the number of ICMP destination unreachable messages received/sent
- **TIME_EXCD**=the number of time exceeded messages received/sent
- **PARM_PROB**=the number of ICMP parameter problem messages received/sent
- **SRC_QUENCH**=the number of ICMP source quench messages received/sent
- **REDIRECT**=the number of ICMP redirect messages received/sent
- **ECHO**=the number of ICMP echo (request) messages received/sent
- **ECHO_REP**=the number of ICMP echo reply messages received/sent
- **TIME_STAMP**=the number of ICMP timestamp (request) messages received/sent
- **TIME_STAMP_REP**=the number of ICMP timestamp reply messages received/sent
- **ADDR_MASK**=the number of ICMP address mask request messages received/sent
- **ADDR_MASK_REP**=the number of ICMP address mask reply messages received/sent

DIAGNOSTICS

MIB GROUPS

ICMP Group, TCP/IP MIB-II (RFC1213)

SEE ALSO

INTRO, page 426

IPADM, page 483

SHOWMASK

NAME

showmask - display the current maintenance mask.

SYNOPSIS

showmask [**loc**=***event_location***] [**rows**=number]

DESCRIPTION

Use showmask to display the current setting of the ECS mask in the maintenance process. This mask is used to select events to be collected and logged by the maintenance process.

You can use the **loc** and **rows** options to limit the display. If you do not specify a **location**, the system displays all locations. The **loc** option is a list of locations separated by colons (:). If you do not request a number of **rows**, only one type header is printed. If you want more than one type header, specify the **number** of **rows** you want printed before another type header is printed.

This maintenance mask defaults to all enabled locations and all types except types DEBUG_LVL2 and DEBUG_LVL3. You can enable these two types by adding the following line under the [mtce] section in the cw.ini file:

[location] = [2,3]

Where the location is uppercase and either a 2 or a 3 may be used. A 2 enables DEBUG_LVL2 for that location and a 3 enables both DEBUG_LVL2 and DEBUG_LVL3 for that location. For example **BIM=3** would enable DEBUG_LVL2 and DEBUG_LVL3 for BIM.

You can dynamically change the mask by using the **reset level=mask** command.

EXAMPLES

To display a portion of the mask relating to the BIM location:

```
$ showmask loc=BIM
```

To display the entire mask:

```
$ showmask
```

To print a type header for every 20 lines of locations:

```
$ showmask rows=20
```

DIAGNOSTICS

The maintenance and minit processes must be running for this command to retrieve the current mask.

SEE ALSO

RESET, page 544

SHOWSTATUS

NAME

showstatus - show data associated with icmp counts.

SYNOPSIS

showstatus

DESCRIPTION

showstatus displays the current status of the system software running on the server. The output consists of 2 parts: the status of the software processes (tasks), and the state of the system.

The status of the processes is represented in 5 columns with a row for each process. The first column is the name of the process. The next column is the process instance ID (referred to as PID) and is assigned by the operating system when the **Num Aborts** field is the number of times that the process has abnormally terminated.

Note that the system recovers from a process that has abnormally terminated. The next 2 columns deal with the initialization state of a process. For a process to be fully initialized, it must be both **Ready** and **Init Done** which is denoted by having a corresponding **Y** under each column.

If a process is not **Ready** or **Init Done**, it will have an **N** under the corresponding column. For a small set of processes, **Ready** and **Init Done** does not apply and this will be denoted with a dash (**-**) for these columns.

The second piece of information is the current system state. When the system software is booting up (initializing), the state will be OOS. If the system successfully initializes, the state will be IS. A system whose state is IS will have all processes running (non-zero process ID) and fully initialized ("**Y**" for both "**Ready**" and "**Init Done**"). When a system is IS, users may log in through endpoints and establish calls. In the event that hardware cannot be successfully initialized during system booting, then the state will be OOS-FLT.

EXAMPLES

```
$showstatus
                        Num                 Init
Process          PID    Aborts   Ready     Done
-----------     ----    ------   -----     ----
MUM              518       0       Y         Y
SECMGR           535       0       Y         Y
bim              494       0       Y         Y
cm               505       0       Y         Y
commware         487       0       Y         Y
cwagt            539       0       Y         Y
diag             506       0       Y         Y
dpm              522       0       Y         Y
mediaMgr         511       0       Y         Y
mib2agt          548       0       -         -
minit            351       0       Y         Y
mtce             491       0       Y         Y
prim             499       0       Y         Y
snmpdm           536       0       -         -
t120nc           512       0       Y         Y
transagt         543       0       Y         Y
trapagt          544       0       Y         Y
```

```
System state: IS
```

DIAGNOSTICS

MIB GROUPS

SEE ALSO

SHOWTCP

NAME

showtcp - show TCP (transmission control protocol) related data

SYNOPSIS

showtcp [**data**=***data-type***]

DESCRIPTION

showtcp is the command to view TCP (transmission control protocol) related data.

data-type describes the type of data being requested. The two types of data possible are (the default is to show both):

- **count** - show TCP related counts and parameters
- **conn** - show the TCP connection table.

EXAMPLES

To view TCP counts:

```
$ showtcp data=count
    RTO_ALGORITHM:     constant(2)
          RTO_MIN:     240
          RTO_MAX:     2400
      ACTIVE_OPEN:     34
     PASSIVE_OPEN:     33
```

```
      CURR_ESTAB:     22
    ESTAB_RESET:      4
         IN_SEG:      440
        OUT_SEG:      438
    RETRANS_SEG:      2
   ATTEMPT_FAIL:      2
         IN_ERR:      20
```

The meaning of the headings are as follows:

- **RTO_ALGORITHM**=algorithm used to determine the timeout value used for transmitting unacknowledged octets (**other**, **constant**, **rsre**, **vanj**)
- **RTO_MIN**=minimum value (in milliseconds) permitted by a TCP implementation for the retransmission timeout
- **RTO_MAX**=maximum value (in milliseconds) permitted by a TCP implementation for the retransmission timeout
- **ACTIVE_OPEN**=number of times TCP connections have made a transition from **closed** to **synRcv**
- **PASSIVE_OPEN**=number of times TCP connections have made a transition from **listen** to **synRcv**
- **CURR_ESTAB**=number of TCP connections having a current state of either **established** or **closeWait**
- **ESTAB_RESET**=number of resets that have occurred (from **established** to **closed**, or **closeWait** to **closed**)
- **IN_SEG**=total number of segments received
- **OUT_SEG**=total number of segments sent

- **RETRANS_SEG**=total number of segments retransmitted
- **ATTEMPT_FAIL**=number of failed connection attempts (from **synSent** to **closed**, **synRcv** to **closed**, or **synRcv** to **listen**)
- **IN_ERR**=total number of segments received in error

To view the TCP connection table:

```
$ showtcp data=conn
      TCP CONNECTIONS
      ===============
STATE           LOCALADDRESS      LOCALPORT  REMADDRESS        REMPORT
established(5)  125.233.240.111   65535      125.211.100.101   65535
closed(1)       125.222.1.12      4          125.1.1.1         5
synSent(3)      11.11.11.11       3          22.22.22.22       3
```

The meaning of the headings are as follows:

- **STATE**=state of this TCP connection (**closed**, **listen**, **synSent**, **synRcv**, **established**, **finWait1**, **finWait2**, **closeWait**, **lastAck**, **closing**, **timeWait**, **deleteTCB**)
- **LOCALADDRESS**=local IP address for this TCP connection
- **LOCALPORT**=local port number for this TCP connection
- **REMADDRESS**=remote IP address for this TCP connection
- **REMPORT**=remote port number for this TCP connection

MIB GROUPS

TCP Group, TCP/IP MIB-II (RFC1213)

SEE ALSO

INTRO, page 426

IPADM, page 483

SHOWUDP

NAME

showudp - show UDP (user datagram protocol) related data

SYNOPSIS

showudp [**data**=***data-type***]

DESCRIPTION

showudp is the command to show UDP (user datagram protocol) related data.

data-type describes the type of data being requested. The two types of data possible are (the default is to show both):

- **err** - show UDP related errors
- **listener** - show the UDP listener table

EXAMPLES

To show UDP errors:

```
$ showudp data=err
IN_ERR:     1
```

The meaning of the headings are as follows:

- **IN_ERR**=the number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.

To view the UDP listener table:

```
$ showudp data=listener
      UDP LISTENER
      ============
LOCALADDRESS          LOCALPORT
-                     2
125.233.240.111       3
10.101.1.10           65535
```

The meaning of the headings are as follows:

- **LOCALADDRESS**=the local IP address for this UDP listener. The case of a UDP listener which is willing to accept datagrams for any IP interface associated with the node, the value '-' is used
- **LOCALPORT**=the local port number for this UDP listener

DIAGNOSTICS

MIB GROUPS

UDP Group, TCP/IP MIB-II (RFC1213)

SEE ALSO

INTRO, page 426

IPADM, page 483

SHOWWAN

NAME

showwan - show information on interserver connections that use a WAN interface (such as PPP interfaces)

SYNOPSIS

showwan [**data**=***data-type,data-type***] [**srv**=***server-name,server-name***]

DESCRIPTION

showwan is the command to view inter-server connection information for the wide area network (WAN). WAN connections are implemented through the use of a Point-to-Point Protocol (PPP) interface that is dynamically assigned as traffic requires.

Data-type describes the type of data being requested. ***data-type*** can be one of the following two:

- **stat** - show status and counts of WAN inter-server connections
- **cfg** - show configuration information for WAN inter-server connections

If multiple ***data-types*** are specified, then those data will be shown in the order of their input. However, if no ***data-type*** is specified, then all data will be shown.

Server-name refers to the MMCX remote server(s) for which you want to receive data on. If no ***server-name*** is specified, then all servers will be shown.

EXAMPLES

To see the status of WAN inter-server connections:

```
$ showwan data=stat
SERVER    WILD IN_PACKET   OUT_PACKET MP_ERROR    MAX    CUR    TOT_BCHAN   BCHAN_SEC
mmcs02    i-   0           0          0           0      0      0           -
mmcs03    i-   0           0          0           0      0      0           -
```

The meaning of the headings are as follows:

- **SERVER**=the remote server name.
- **WILD_SLOT**=the bus and slot number of the WILD card being used.
- **IN_PACKET**=accumulated total of incoming octets for the PPP interfaces that have been used.
- **OUT_PACKET**=accumulated total of outgoing octets for the PPP interfaces that have been used.
- **MP_ERROR**=the number of accumulated PPP/MP (multi-protocol) errors for links to this server.
- **MAX_BCHAN**=the maximum number of B-channels used for the connection to this server at any one time.
- **CUR_BCHAN**=the current number of B-channels in use for the connection to this server.
- **TOT_BCHAN**=the total number of B-channels ever used for the connection to this server.
- **TOT_BCHAN_SEC**=the total number of seconds of connection time of originated B-channels used for the connection to this server.

To see configuration information for WAN inter-server connections:

```
$ showwan data=cfg
SERVER     PRI_SLOT          PRI_PORT          BCHAN         ERROR
mmcx02     i2                1                 1             10
```

```
mmcx02    i2              1               3               100
mmcx03    i2              1               2               0
mmcx03    i2              1               4               0
```

The meaning of the headings are as follows:

- **SERVER**=the remote server name.
- **PRI_SLOT**=the bus type and slot number of the PRI card for the B-channel.
- **PRI_PORT**=the port number on the card for the B-channel.
- **BCHAN**=the B-channel number.
- **ERROR**=the number of errors that occurred on this B-channel for this interface.

MIB GROUPS

mmcxWanServerTable and mmcxWanServerMpTable

SEE ALSO

INTRO, page 426

INTFADM, page 479

SNMPADM

NAME

chgsnmp, **showsnmp** - enable and disable authentication-failure traps, show SNMP counts

SYNOPSIS

chgsnmp trap=***enable|disable***

showsnmp

DESCRIPTION

chgsnmp can be used to enable or disable the authentication failure traps field. This is accomplished by setting the **trap** field to **enable** or **disable**, as desired. Disabling the **trap** field means that SNMP authentication failure traps will not be generated, and thus will not be viewable through the **showalarm** command. The default for this field is enabled.

Changing the **trap** field is only effective for the current run (it will revert to the default at every reboot). If you would like to make a permament change to this field, then edit the file **$MROOT/etc/srconf/agt/snmpd.cnf.**

showsnmp is the command to view Simple Network Management Protocol (SNMP) data.

EXAMPLES

To disable the snmp authentication-failure trap:

```
$ chgsnmp trap=disable
```

Your request to chgsnmp succeeded.

AUT_FAIL_TRAP: disabled(2)

To see snmp counts:

```
$ showsnmp
```

	IN	OUT
PKT:	100	100
GET_REQUEST:	565789	565789
GET_NEXT:	9876543210	9876543210
SET_REQUEST:	90	90
GET_RESPONSE:	80	80
TOO_BIG:	5	5
NO_SUCH_NAME:	3	3
BAD_VALUE:	4	4
GEN_ERR:	32	32
TRAP:	11111	11111
BAD_VERSION:	5	
BAD_COMM_NAME:	9	
BAD_COMM_USE:	83	
ASN_PARSE_ERR:	32	
READ_ONLY:	3	
TOTAL_REQ_VAR:	44	
TOTAL_SET_VAR:	44	
AUT_FAIL_TRAP:	enabled(1)	

The meaning of the headings are as follows:

- **PKT**=the total number of messages delivered to/generated by the SNMP entity from the transport service
- **GET_REQUEST**=the total number of SNMP Get-Request PDUs which have been accepted/generated by the SNMP protocol entity
- **GET_NEXT**=the total number of SNMP Get-Next PDUs which have been accepted/generated by the SNMP protocol entity
- **SET_REQUEST**=the total number of SNMP Set-Request PDUs which have been accepted/generated by the SNMP protocol entity
- **GET_RESPONSE**=the total number of SNMP Get-Response PDUs which have been accepted/generated by the SNMP protocol entity
- **TOO_BIG**=the total number of SNMP PDUs which were delivered to/generated by the SNMP protocol entity and for which the value of the error-status field is tooBig
- **NO_SUCH_NAME**=the total number of SNMP PDUs which were delivered to/generated by the SNMP protocol entity and for which the value of the error-status field is noSuchName
- **BAD_VALUE**=the total number of SNMP PDUs which were delivered to/generated by the SNMP protocol entity and for which the value of the error-status field is badValue
- **GEN_ERR**=the total number of SNMP PDUs which were delivered to/generated by the SNMP protocol entity and for which the value of the error-status field is genErr
- **TRAP**=the total number of SNMP Trap PDUs which have been accepted/generated by the SNMP protocol entity
- **BAD_VERSION**=the total number of SNMP messages which were delivered to the SNMP protocol entity and were for an unsupported SNMP version

- **BAD_COMM_NAME**=the total number of SNMP messages delivered to the SNMP protocol entity which used a SNMP community name not known to said entity
- **BAD_COMM_USE**=the total number of SNMP messages delivered to the SNMP protocol entity which represented an SNMP operation which was not allowed by the SNMP community named in the message
- **ASN_PARSE_ERR**=the total number of ASN.1 or BER errors encountered by the SNMP protocol entity when decoding received SNMP messages
- **READ_ONLY**=the total number of valid SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is readOnly
- **TOTAL_REQ_VAR**=the total number of MIB objects which have been retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs
- **TOTAL_SET_VAR**=the total number of MIB objects which have been altered successfully by the SNMP protocol entity as the result of receiving valid SNMP Set-Request PDUs
- **AUT_FAIL_TRAP**=indicates whether the SNMP agent process is permitted to generate authentication-failure traps (enabled or disabled)

DIAGNOSTICS

MIB GROUPS

SNMP Group, TCP/IP MIB-II (RFC1213)

SEE ALSO

INTRO, page 426

IPADM, page 483

SHOWUDP, page 567

ALARMMON, page 429

USRADM

NAME

addusr, **chgusr**, **chgpasswd**, **rmusr**, **showusr**, **showcvr**, **termusr**, **addipusr**, **chgipusr**, **rmipusr**, **showipusr**, **termipusr**, **mkpersdir** - administer MMCX users, make a personal directory file from the contents of the MMCX user database.

SYNOPSIS

addusr login=***login-id*** **last**=***last-name*** **ext**=***extension*** [**first**=***first-name***] [**cvr**=***covering-number***] [**comment**=***comment***] [**pass**=***password***]

chgusr login=***login-id*** [**last**=***last-name***] [**first**=***first-name***] [**comment**=***comment***]

chgpasswd login=***login-id***

rmusr login=***login-id***

showusr [**login**=***login-id***] [**stat**=***status-flag***]

showcvr login=*login-id*

termusr login=***login-id***

addipusr ext=*extension* ipaddr=*ip-address*
last=*last-name* [first=*first-name*] [cvr=*covering-number*]

chgipusr ext=*extension* [ipaddr=*ip-address*]
[last=*last-name*] [first=*first-name*] [cvr=*covering-number*]

rmipusr ext=*extension*

showipusr [ext=*extension*]

termipusr ext=*extension*

mkpersdir [**file**=***filename***]

DESCRIPTION

MMCX supports both MMCX and H.323-compliant endpoints from other vendors.

MMCX endpoint-administration commands

The following administer users logged in through MMCX end points

addusr adds a user record to a MMCX server.

- ***login-id*** is a character string of up to eight alphanumeric characters. This will be the ID typed by the user when he or she invokes MMCX on the endpoint. It must match the user's UNIX login ID on the endpoint, but no verification is done here.
- ***extension*** is the user's three- to seven-digit extension. Its length must equal extension-number-length (See *CFGADM, page 458*).
- ***last-name*** may be up to twenty characters.
- ***first-name*** may be up to fifteen characters; it may contain initials and any other qualifiers: “John”, “John C.”, “J.C.”, “John C., Jr.”, and “Junior” are all valid.
- ***covering-number*** is the extension of another MMCX user, ordinary voice telephone, to contact if this user does not answer a call. It is the number stored in the initial path coverage for this user.

- ***comment*** is a character string of up to sixty characters, for general use by the system administrator.
- ***password*** is the user's initial password, from eight to twelve alphanumeric characters.
- If it is not specified, **addusr** prompts for a password (twice), but does not echo the characters entered to the screen. A user cannot be added without a valid password.

chgusr changes one or more fields in a user record. If any field value is not specified, it is not changed. ***login-id*** is used to find the record to change.

chgpasswd prompts twice for the password for the user with specified ***login-id***, then changes it.

mkpersdir retrieves all user records from an MMCX server's database, formats them into the form expected by the personal directory software on the MMCX endpoints, and writes them to ***file***. The system administrator can then copy ***file*** to the endpoints or to a file system accessible by the endpoints, where the copies will serve as initial personal directories. Each MMCX user will then be able to modify his or her copy of the personal directory as needed.

mkpersdir provides no support for transferring the user data to places accessible by the endpoints. It merely retrieves and formats the user data. Also, its intent is only to generate an initial personal directory file. It provides no convenient way of merging records in the user database with existing personal directories. If ***file*** is not specified, the formatted output is written to **$MROOT/etc/epdir.dat**. If ***file*** already exists and is writable, **mkpersdir** will overwrite it.

rmusr removes a user record by login ID, as well as the coverage paths for that user.

showusr shows all user records matching the specifications. The ***login-id*** defaults to **all** users. The status flag can be **logged out**, **logged in**, or **busy**.

showcvr shows the coverage point of the user specified by ***login-id***.

termusr drops user ***login-id*** from all calls he or she is involved in, and terminates his or her MMCX session.

H.323 endpoint-administration commands

The preceding commands administer users logged in through MMCX end points.The MMCX server also supports H.323-compliant end points from other vendors. Users of those end points may not have logins and passwords, so they are identified only by their MMCX extension. They are called *IP users* because the administrator has to specify the IP address of the end point they use.

IP user administration is very similar to MMCX user administration. An IP user has no login ID, password, or comment but does have an additional argument, the end point IP address, which can be changed. IP users may not be able to log in to the MMCX server using H.323 registration and authentication. So MMCX automatically logs them in and keeps them in the logged-in state. The administrator can force them to log out using **termipusr** and can log them in with **loginipusr**.

The IP user commands **termipusr** and **rmipusr** also work for MMCX users. Using these commands, you can administer your MMCX endpoints by extension rather than by login ID.

EXAMPLES

To add a user:

```
$ addusr login=bbb ext=551234 last="Bogartz" first="Bruce B." cvr=527575
Enter password:
```

The administrator types the password, and an asterisk is echoed for each character.

```
Re-enter password:
```

The administrator types the same password again.

```
Your request to addusr succeeded.

LOGIN    STATUS          EXT      NAME

bbb      LoggedOut(2)  551234   Bogartz, Bruce B.
LOGIN    COMMENT

bbb      -

COVER_NAME   STATUS
initial      enabled(1)
```

To change a user's first name:

```
$ chgusr login=bbb first="John A."

Your request to chgusr succeeded.

LOGIN    STATUS        EXT     NAME
bbb      LoggedOut(2)  551234  Bogartz, John A.

LOGIN    COMMENT
bbb      -
```

To remove a user record:

```
$ rmusr login=bbb

Your request to rmusr succeeded.
```

To see the records for all users:

```
$ showusr

LOGIN    STATUS           EXT      NAME
james    loggedIn(4)      557800   James Johnston
kappers  loggedOut(2)     552222   Kappers, Dennis
wlk      busy(3)          555674   Kloppman, Walter L.
<ipuser> loggedIn(4)      557801   Swenson, Gunnar
<ipuser> loggedIn(4)      557834   Grimsson, Ingvar

LOGIN    COMMENT
kappers  1234 Perry St., Rochester, MI 54323
wlk      RM 222
james    RM 476
<ipuser> User with fixed IP address
<ipuser> User with fixed IP address
```

To see the coverage point of login **kappers**:

```
$ showcvr login=kappers

Login kappers has the following coverage path:

COVERAGE_POINTSTATUS
559000        enabled(1)
```

To retrieve all users from the MMCX server database and write them to the file /tmp/users

```
$ mkpersdir file=/tmp/users
MMCX user records written to /tmp/users.
```

To add an IP user record:

```
$addipusr ext=557801 ip=147.3.18.168 cvr=559000 last=Swenson first=Gunnar

Your request to addipusr succeeded.

EXT    STATUS             COVER        IP_ADDRESS      NAME
557801 loggedIn(4)        559000       147.3.18.168    Swenson, Gunnar
```

To see the records for all IP users:

```
$ showipusr

EXT     STATUS          COVER   IP_ADDRESS      NAME
557801  loggedIn(4)     559000  147.3.18.168    Swenson, Gunnar
557834  loggedIn(4)     559000  147.3.18.170    Grimsson, Ingvar
```

DIAGNOSTICS

addusr fails if the specified login ID or extension already exists in the user table, or if the extension is not the right length (see *CFGADM, page 458*). If an initial user password is not specified, it prompts twice for one. It fails if the responses to the two prompts differ. It also fails if a specified password does not meet MMCX's criteria for passwords. For example, minimum length, inclusion of special characters, etc. Finally, the command fails if the number of users already in the table matches the number licensed for the server.

rmusr, **showusr**, **showcvr**, **chgusr**, and **chgpasswd** fail if ***login-id*** is not found.

chgpasswd prompts twice for a user password. It fails if the responses to the two prompts differ. It will also fail if a specified password does not meet MMCX's criteria for passwords. For example, minimum length, inclusion of special characters, etc.

NOTES

This set of commands should not be confused with the LYNX commands for administering logins to the server. MMCX users, which the commands described here administer, don't actually log into the server, but into an MMCX endpoint through which they register with the server.

MIB GROUPS

mmcxUserTable, mmcxCoverTable

SEE ALSO

CFGADM, page 458

DPADM, page 466

INTRO, page 426

RESET, page 544

B MMCX alarm codes

Normally, you look up alarm codes under the repair number specified by the alarm log entry. However, you may sometimes want more detailed information about the error than troubleshooting generally requires. Accordingly, this appendix lists all the alarm codes in numerical order.

Code	Condition	Level	On Board?
18	"PRI Interface or WILD Card busy out"	"WN"	"Off"
1024	"PCI bus error occurred"	"WN"	"Off"
1025	"PCI bus parity error detected"	"WN"	"Off"
1026	"Fatal PCI bus parity error detected"	"MJ"	"Off"
1027	"PCI bus transactaon aborted by master"	"MN"	"Off"
1028	"PCI bus transaction aborted by target"	"MN"	"Off"
1029	"Unknown PCI bus error ocurred"	"WN"	"Off"
1030	"Twisted Pair carrier lost"	"MJ"	"Off"
1031	"other transmitter failure detected"	"MJ"	"On"
1032	"receive buffer overload"	"None"	"Off"
1033	"number of frames missed due to rvc buf overflow"	"None"	"Off"

Code	Condition	Level	On Board?
1034	"rvc data lost due to blockage on PCI bus"	"WN"	"Off"
1035	"received frame too short"	"None"	"Off"
1036	"received frame too long"	"None"	"Off"
1037	"transmit carrier failed"	"MJ"	"Off"
1038	"xmt data lost due to blockage on PCI bus"	"WN"	"Off"
1039	"transmit carrier failed"	"MJ"	"On"
1040	"transmit carrier failed"	"MJ"	"On"
1041	"transmit carrier failed"	"MJ"	"On"
1042	"transmit carrier failed"	"MJ"	"On"
1280	"Alarm info 1: Ethernet Internal Looparound Test Failed"	"MJ"	"On"
1281	"Ethernet port out of service."	"MJ"	"Off"
2148	"No SUNI carrier"	"MJ"	"Off"
2304	"ATM Internal Looparound Test Failed"	"MJ"	"On"
3072	"WILD_RSRC_EV - Severe Resource Allocation Error"	"MJ"	"Off"
3073	"WILD_HDWR_ERR_EV - WILD Onboard Hardware Fault"	"MJ"	"On"

Code	Condition	Level	On Board?
3074	"WILD_MVIP_C4_CLK_EV - Lost MVIP 4 MHz Clock"	"MJ"	"Off"
3075	"WILD_MVIP_C2_CLK_EV - Lost MVIP 2 MHz Clock"	"MJ"	"Off"
3076	"WILD_MVIP_F0_CLK_EV - Lost MVIP Frame Signal"	"MJ"	"Off"
3077	"Lost interrupts on quicc3 - Reset WILD Card"	"MJ"	"Off"
3272	"WILD_HDLC_INLINE_EV - Incoming Data Errors from the PRI Link"	"MJ"	"Off"
3273	"WILD_HDLC_SHTDWN_EV - HDLC Controller Global Error Condition"	"MJ"	"Off"
3332	"Switch chips are not operational; Check MVIP cable; check PRI alarms"	"MJ"	"Off"
3352	"Internal Switch Fabric Test - WILD Card Failure"	"MN"	"Off"
3353	"WILD Card Power Up Diagnostics Failed - aux data has result of test"	"MJ"	"On"
3354	"Analysis of Internal Switch Fabric Test - WILD Card indicted"	"MJ"	"Off"
3355	"Analysis of Internal Switch Fabric Test - MVIP Bus in aux data field indicted"	"MN"	"Off"
3356	"WILD Loop Test Failed"	"MJ"	"On"

Code	Condition	Level	On Board?
3357	"Result of WILD Card Reset is FAILURE"	"MJ"	"Off"
3372	"iErrorInterrupt - wild driver detected PCI bus error"	"WN"	"Off"
3373	"iBusParityError - wild driver detected PCI bus parity error"	"WN"	"Off"
3374	"iFatalBusParity - wild driver detected fatal PCI bus parity error"	"MJ"	"Off"
3375	"iBusMasterAbort - PCI bus transaction aborted by master"	"MN"	"Off"
3376	"iBusTargetAbort - PCI bus transaction aborted by target"	"MN"	"Off"
3377	"iBusUnDefError - Unknown PCI bus error occurred"	"WN"	"Off"
4096	"PRI Line A Yellow Alarm"	"MJ"	"Off"
4097	"PRI Line A Blue Alarm"	"MN"	"Off"
4098	"PRI Line A Red Alarm"	"MJ"	"Off"
4099	"PRI Line B Yellow Alarm"	"MJ"	"Off"
4100	"PRI Line B Blue Alarm"	"MN"	"Off"
4101	"PRI Line B Red Alarm"	"MJ"	"Off"
4196	"Internal Switch Fabric Test - PRI Interface Failure"	"MN"	"Off"
4197	"Analysis of Internal Switch Fabric Test - PRI Interface indicted"	"MJ"	"Off"

Code	Condition	Level	On Board?
21504	"NameAgent interface library and NameAgent possibly out of sync."	"None"	"Off"
21505	"Unable to get NameAgent VTA from the cw.ini file"	"MN"	"Off"
21506	"Unable to get NameAgent VTA attributes from the cw.ini file"	"MN"	"Off"
21508	"NameAgent interface library and NameAgent out of sync."	"None"	"Off"
21509	"Problem with connection between NameAgent to NameServer."	"None"	"Off"
21511	"Problem with connection between NameAgent to NameServer."	"None"	"Off"
21512	"Problem with connection between NameAgent to NameServer."	"None"	"Off"
21513	"Problem with connection between NameAgent to NameServer."	"None"	"Off"
21514	"Problem with connection between NameAgent to NameServer."	"None"	"Off"
21544	"Unable to get NameAgent VTA from the cw.ini file"	"MN"	"Off"
21545	"Unable to create ROM NameAgent Responder connector."	"None"	"Off"

Code	Condition	Level	On Board?
21564	"Unable to get NameAgent VTA from the cw.ini file"	"MN"	"Off"
22528	"Internal Raima DB error unable to open Namer database files."	"MN"	"Off"
22529	"Internal Raima DB error on a begin write transaction."	"MN"	"Off"
22530	"Internal Raima DB error on a find first record of DOMAIN_REC type."	"MN"	"Off"
22531	"Internal Raima DB error on a find first record of VTA_REC type."	"MN"	"Off"
22533	"Internal Raima DB error on an add of a DOMAIN_VTA_REC type."	"MN"	"Off"
22534	"Internal Raima DB error on end transaction request."	"MN"	"Off"
22535	"Internal Raima DB error on begin transaction request."	"MN"	"Off"
22536	"Internal Raima DB error."	"MN"	"Off"
22537	"Internal Raima DB error."	"MN"	"Off"
22538	"Internal Raima DB error."	"MN"	"Off"
22539	"Internal Raima DB error."	"MN"	"Off"
22540	"Internal Raima DB error."	"MN"	"Off"

Code	Condition	Level	On Board?
22541	"Internal Raima DB error."	"MN"	"Off"
22542	"Internal Raima DB error."	"MN"	"Off"
22543	"Internal Raima DB error."	"MN"	"Off"
22544	"Internal Raima DB error."	"MN"	"Off"
22545	"Internal Raima DB error."	"MN"	"Off"
22546	"Internal Raima DB error."	"MN"	"Off"
22547	"Internal Raima DB error."	"MN"	"Off"
22548	"Internal Raima DB error."	"MN"	"Off"
22549	"Internal Raima DB error."	"MN"	"Off"
22550	"Internal Raima DB error."	"MN"	"Off"
22551	"Internal Raima DB error."	"MN"	"Off"
22552	"Internal Raima DB error."	"MN"	"Off"
22553	"Internal Raima DB error."	"MN"	"Off"
22554	"Internal Raima DB error."	"MN"	"Off"
22555	"Internal Raima DB error."	"MN"	"Off"

Code	Condition	Level	On Board?
22556	"Internal Raima DB error."	"MN"	"Off"
22557	"Internal Raima DB error."	"MN"	"Off"
22558	"Internal Raima DB error."	"MN"	"Off"
22559	"Internal Raima DB error."	"MN"	"Off"
22560	"Internal Raima DB error."	"MN"	"Off"
22561	"Internal Raima DB error."	"MN"	"Off"
22562	"Internal Raima DB error."	"MN"	"Off"
22563	"Internal Raima DB error."	"MN"	"Off"
22564	"Internal Raima DB error."	"MN"	"Off"
22565	"Internal Raima DB error."	"MN"	"Off"
22566	"Internal Raima DB error."	"MN"	"Off"
22567	"Internal Raima DB error."	"MN"	"Off"
22568	"Internal Raima DB error."	"MN"	"Off"
22569	"Internal Raima DB error."	"MN"	"Off"
22570	"Internal Raima DB error."	"MN"	"Off"

Code	Condition	Level	On Board?
22571	"Internal Raima DB error."	"MN"	"Off"
22572	"Internal Raima DB error."	"MN"	"Off"
22573	"Internal Raima DB error."	"MN"	"Off"
22574	"Internal Raima DB error."	"MN"	"Off"
22575	"Internal Raima DB error."	"MN"	"Off"
22576	"Internal Raima DB error."	"MN"	"Off"
22577	"Internal Raima DB error."	"MN"	"Off"
22578	"Internal Raima DB error."	"MN"	"Off"
22579	"Internal Raima DB error."	"MN"	"Off"
22580	"Internal Raima DB error."	"MN"	"Off"
22581	"Internal Raima DB error."	"MN"	"Off"
22582	"Internal Raima DB error."	"MN"	"Off"
22583	"Internal Raima DB error."	"MN"	"Off"
22584	"Internal Raima DB error."	"MN"	"Off"
22585	"Internal Raima DB error."	"MN"	"Off"

Code	Condition	Level	On Board?
22586	"Internal Raima DB error."	"MN"	"Off"
22587	"Internal Raima DB error."	"MN"	"Off"
22588	"Internal Raima DB error."	"MN"	"Off"
22589	"Internal Raima DB error."	"MN"	"Off"
22590	"Internal Raima DB error."	"MN"	"Off"
22591	"Internal Raima DB error."	"MN"	"Off"
22592	"Internal Raima DB error."	"MN"	"Off"
22593	"Internal Raima DB error."	"MN"	"Off"
22594	"Internal Raima DB error."	"MN"	"Off"
22595	"Internal Raima DB error."	"MN"	"Off"
22596	"Internal Raima DB error."	"MN"	"Off"
22597	"Internal Raima DB error."	"MN"	"Off"
22598	"Internal Raima DB error."	"MN"	"Off"
22599	"Internal Raima DB error."	"MN"	"Off"
22600	"Internal Raima DB error."	"MN"	"Off"

Code	Condition	Level	On Board?
22601	"Internal Raima DB error."	"MN"	"Off"
22602	"Internal Raima DB error."	"MN"	"Off"
22603	"Internal Raima DB error."	"MN"	"Off"
22604	"Internal Raima DB error."	"MN"	"Off"
22605	"Internal Raima DB error."	"MN"	"Off"
22606	"Internal Raima DB error."	"MN"	"Off"
22607	"Internal Raima DB error."	"MN"	"Off"
22608	"Internal Raima DB error."	"MN"	"Off"
22609	"Internal Raima DB error."	"MN"	"Off"
22610	"Internal Raima DB error."	"MN"	"Off"
22611	"Internal Raima DB error."	"MN"	"Off"
22612	"Internal Raima DB error."	"MN"	"Off"
22613	"Internal Raima DB error."	"MN"	"Off"
22614	"Internal Raima DB error."	"MN"	"Off"
22615	"Internal Raima DB error."	"MN"	"Off"

Code	Condition	Level	On Board?
22616	"Internal Raima DB error."	"MN"	"Off"
22617	"Internal Raima DB error."	"MN"	"Off"
22618	"Internal Raima DB error."	"MN"	"Off"
22619	"Internal Raima DB error."	"MN"	"Off"
22620	"Internal Raima DB error."	"MN"	"Off"
22621	"Internal Raima DB error."	"MN"	"Off"
22622	"Internal Raima DB error."	"MN"	"Off"
22623	"Internal Raima DB error."	"MN"	"Off"
22624	"Internal Raima DB error."	"MN"	"Off"
22625	"Internal Raima DB error."	"MN"	"Off"
22626	"Internal Raima DB error."	"MN"	"Off"
22627	"Internal Raima DB error."	"MN"	"Off"
22628	"Internal Raima DB error."	"MN"	"Off"
22629	"Internal Raima DB error."	"MN"	"Off"
22630	"Internal Raima DB error."	"MN"	"Off"

Code	Condition	Level	On Board?
22631	"Internal Raima DB error."	"MN"	"Off"
22632	"Internal Raima DB error."	"MN"	"Off"
22633	"Internal Raima DB error."	"MN"	"Off"
22634	"Internal Raima DB error."	"MN"	"Off"
22635	"Internal Raima DB error."	"MN"	"Off"
22636	"Internal Raima DB error."	"MN"	"Off"
22637	"Internal Raima DB error."	"MN"	"Off"
22638	"Internal Raima DB error."	"MN"	"Off"
22639	"Internal Raima DB error."	"MN"	"Off"
22640	"Internal Raima DB error."	"MN"	"Off"
22641	"Internal Raima DB error."	"MN"	"Off"
22642	"Internal Raima DB error."	"MN"	"Off"
22643	"Internal Raima DB error."	"MN"	"Off"
22644	"Internal Raima DB error."	"MN"	"Off"
22645	"Internal Raima DB error."	"MN"	"Off"

Code	Condition	Level	On Board?
22646	"Internal Raima DB error."	"MN"	"Off"
22647	"Internal Raima DB error."	"MN"	"Off"
22648	"Internal Raima DB error."	"MN"	"Off"
22649	"Internal Raima DB error."	"MN"	"Off"
22650	"Internal Raima DB error."	"MN"	"Off"
22651	"Internal Raima DB error."	"MN"	"Off"
22652	"Internal Raima DB error."	"MN"	"Off"
22653	"Internal Raima DB error."	"MN"	"Off"
22654	"Internal Raima DB error."	"MN"	"Off"
22655	"Internal Raima DB error."	"MN"	"Off"
22656	"Internal Raima DB error."	"MN"	"Off"
22657	"Internal Raima DB error."	"MN"	"Off"
22658	"Internal Raima DB error."	"MN"	"Off"
22659	"Internal Raima DB error."	"MN"	"Off"
22660	"Internal Raima DB error."	"MN"	"Off"

Code	Condition	Level	On Board?
22661	"Internal Raima DB error."	"MN"	"Off"
22662	"Internal Raima DB error."	"MN"	"Off"
22663	"Internal Raima DB error."	"MN"	"Off"
22664	"Internal Raima DB error."	"MN"	"Off"
22665	"Internal Raima DB error."	"MN"	"Off"
22666	"Internal Raima DB error."	"MN"	"Off"
22667	"Internal Raima DB error."	"MN"	"Off"
22668	"Internal Raima DB error."	"MN"	"Off"
22669	"Internal Raima DB error."	"MN"	"Off"
22670	"Internal Raima DB error."	"MN"	"Off"
22671	"Internal Raima DB error."	"MN"	"Off"
22672	"Internal Raima DB error."	"MN"	"Off"
22673	"Internal Raima DB error."	"MN"	"Off"
22674	"System vulnerable to loss of administration"	"MN"	"Off"
22675	"Internal Raima DB error."	"MN"	"Off"

Code	Condition	Level	On Board?
22738	"NameServer will exit with this error."	"MN"	"Off"
22742	"NO_MATCH returned by Route method for getting list of NS peers"	"WN"	"Off"
22743	"If ROM Error (data1) there is a problem with the connection to a peer NS."	"WN"	"Off"
22744	"No successful attempts to pass the request to a peer NS."	"None"	"Off"
22745	"Unable to get list of NS peers to satisfy a request."	"WN"	"Off"
22788	"Unable to get NameServer VTA from the cw.ini file"	"MN"	"Off"
22823	"Unable to get NameServer VTA from the cw.ini file"	"MN"	"Off"
22850	"NSPeerTimeOut not set in cw.ini will use default of 5 minutes"	"MN"	"Off"
23647	"Name Server initialization file has no entry for Router.p"	"MN"	"Off"
23649	"The router database needs to be initialized"	"MN"	"Off"
24591	"Internal Raima DB error for Trader file."	"MN"	"Off"
24592	"Internal Raima DB error for Trader file."	"MN"	"Off"
24595	"Internal Raima DB error for Trader file."	"MN"	"Off"
24597	"Internal Raima DB error for Trader file."	"MN"	"Off"

Code	Condition	Level	On Board?
24598	"Internal Raima DB error for Trader file."	"MN"	"Off"
24599	"Internal Raima DB error for Trader file."	"MN"	"Off"
24621	" Trader library interface and Trader out of sync"	"None"	"Off"
24641	" Trader library interface and Trader out of sync"	"None"	"Off"
24661	"Internal Raima DB error for Trader file."	"MN"	"Off"
24662	"Trader library interface and Trader out of sync"	"None"	"Off"
24721	"Unable to get Trader VTA from cw.ini file"	"MN"	"Off"
24741	"Unable to get Trader VTA from cw.ini file"	"MN"	"Off"
26122	"The configuration file was not found in directory indicated by $CWINI in "	"MN"	"Off"
26123	"Configuration file contained a very long line which was ignored"	"MN"	"Off"
26124	"Configuration file had a line which started with [but had no closing]."	"MN"	"Off"
26125	"Configuration file had a line with []"	"MN"	"Off"
26126	"Configuration file's first non-commentary non-empty line was not a [section]."	"MN"	"Off"

Code	Condition	Level	On Board?
26127	"Configuration file line ignored line with no '='."	"MN"	"Off"
26128	"Configuration file line starting with '=' ignored"	"MN"	"Off"
26129	"Configuration file line with no value after the '=' was ignored."	"MN"	"Off"
26130	"Configuration file line with no value after the '=' was ignored."	"MN"	"Off"
26131	"No sections found in configuration file."	"MN"	"Off"
26132	"Could not read configuration information from the configuration file."	"MN"	"Off"
26133	"Could not read configuration information from the configuration file."	"MN"	"Off"
26144	"Failed to establish connection: investigate possible networking problems."	"None"	"Off"
26145	"Object request failed: investigate possible networking problems."	"None"	"Off"
26146	"Object request failed: investigate possible networking problems."	"None"	"Off"
26147	"Object request failed: investigate possible networking problems."	"None"	"Off"

Code	Condition	Level	On Board?
26162	"Failed to read information from network: check network connections."	"None"	"Off"
26163	"Corrupted message. Possible networking problems or internal error."	"None"	"Off"
26168	"Number of threads + rom_queuelen insufficient to handle demand on this process."	"None"	"Off"
26170	"Transport failed to accept incoming connection request."	"None"	"Off"
26171	"Transport connection hung up."	"None"	"Off"
26181	"Attempt to send message failed."	"None"	"Off"
26183	"Number of threads + rom_queuelen insufficient to handle demand on this process."	"None"	"Off"
26192	"ROM handle table full: increase num_romhandles for this process in cw.ini file."	"None"	"Off"
26248	"Failed to send message. Investigate possible networking problems"	"None"	"Off"
26254	"Response message with bad tag usually indicates response arrived after this"	"None"	"Off"
26262	"rom_queuelen specified for this process exceeds system limit."	"None"	"Off"

Code	Condition	Level	On Board?
26268	"Number of threads + rom_queuelen insufficient to handle demand on this process."	"None"	"Off"
26378	"INTERNAL ERROR: No VTA found for minit in the cw.ini file."	"MN"	"Off"
26380	"INTERNAL ERROR: Cannot new a ROMConnector during _ Init"	"None"	"Off"
26381	"INTERNAL ERROR: ROMHandleMapper::MakeROMHandle failed during _Init"	"None"	"Off"
26384	"INTERNAL ERROR: ROMHandleMapper::DeleteROMHandle failed in _cleanup"	"None"	"Off"
26624	"OS error - could be networking problems."	"None"	"Off"
26645	"Failed to send message. Investigate possible networking problems."	"None"	"Off"
26647	"Failed to receive message. Connection may have died or network problems."	"None"	"Off"
26649	"Failed to restart connection. Far end may have died or network problems."	"None"	"Off"
26650	"Failed to send message. Far end may have died or network problems."	"None"	"Off"

Code	Condition	Level	On Board?
26651	"Failed to receive message. Far end may have died or network problems."	"None"	"Off"
26652	"Failed to restart connection. Far end may have died or network problems."	"None"	"Off"
26654	"Failed to post message. Possible networking problems."	"None"	"Off"
26657	"Failed to post message. Possible networking problems."	"None"	"Off"
26659	"Couldn't allocate resources to RANC request. Check system memory."	"None"	"Off"
26660	"OS error - couldn't accept or set socket. Possible networking problems."	"None"	"Off"
26661	"Failed to receive message. Far end may have dropped or network problems."	"None"	"Off"
26663	"Failed to send message. Possible networking problems."	"None"	"Off"
26664	"Failed to send message. Possible networking problems."	"None"	"Off"
26665	"OS error - Could not accept or shutdown socket. Possible networking problem."	"None"	"Off"
26703	"Investigate possible networking problems."	"None"	"Off"

Code	Condition	Level	On Board?
26705	"Failed to send message. Possible networking problems."	"None"	"Off"
26707	"Failed to receive message. Far end may have died or network problems."	"None"	"Off"
26711	"Investigate possible networking problems."	"None"	"Off"
26725	"Internal software error or network problems."	"None"	"Off"
26784	"OS error - possible networking problem."	"None"	"Off"
26787	"OS error - possible networking problem."	"None"	"Off"
26788	"OS error - possible networking problem."	"None"	"Off"
26804	"OS error. Could be networking problems."	"None"	"Off"
26805	"OS error. Could be networking problems."	"None"	"Off"
26806	"OS error. Could be networking problems."	"None"	"Off"
32868	"Can’t get VTA for MTCE Thresholder"	"WN"	"Off"
32885	"BAD HW ECS message length or type in MTCE Thresholder"	"MN"	"Off"
32886	"BAD SW ECS message length or type in MTCE Thresholder"	"MN"	"Off"
32887	"Threshold/Action Table entry not found in MTCE Thresholder"	"MN"	"Off"

Code	Condition	Level	On Board?
32896	"Can't start db transaction in MTCE Thresholder DeleteHWLogEntry"	"MN"	"Off"
32897	"Error deleting db entry in MTCE Thresholder DeleteHWLogEntry"	"MN"	"Off"
32898	"Error aborting db entry in MTCE Thresholder DeleteHWLogEntry"	"MN"	"Off"
32899	"Error ending db transaction in MTCE Thresholder DeleteHWLogEntry"	"MN"	"Off"
32900	"Can't start db transaction in MTCE Thresholder DeleteSWLogEntry"	"MN"	"Off"
32901	"Error deleting db entry in MTCE Thresholder DeleteSWLogEntry"	"MN"	"Off"
32902	"Error aborting db entry in MTCE Thresholder DeleteSWLogEntry"	"MN"	"Off"
32903	"Error ending db transaction in MTCE Thresholder DeleteSWLogEntry"	"MN"	"Off"
32905	"Can't start hw db transaction in MTCE Thresholder UpdateDB"	"MN"	"Off"
32906	"Error deleting hw db entry in MTCE Thresholder UpdateDB"	"MN"	"Off"

Code	Condition	Level	On Board?
32907	"Error aborting hw db transaction in MTCE Thresholder UpdateDB"	"MN"	"Off"
32908	"Error writing hw db entry in MTCE Thresholder UpdateDB"	"MN"	"Off"
32909	"Error ending the hw db transaction in MTCE Thresholder UpdateDB"	"MN"	"Off"
32910	"Can’t start sw db transaction in MTCE Thresholder UpdateDB"	"MN"	"Off"
32911	"Error deleting sw db entry in MTCE Thresholder UpdateDB"	"MN"	"Off"
32912	"Error aborting sw db transaction in MTCE Thresholder UpdateDB"	"MN"	"Off"
32913	"Error writing sw db entry in MTCE Thresholder UpdateDB"	"MN"	"Off"
32914	"Error ending sw db transaction in MTCE Thresholder UpdateDB"	"MN"	"Off"
32915	"Can’t start hw db transaction in MTCE Thresholder UpdateDB_ All"	"MN"	"Off"
32916	"Error deleting hw db entry in MTCE Thresholder UpdateDB_ All"	"MN"	"Off"
32917	"Error aborting hw db transaction in MTCE Thresholder UpdateDB_All"	"MN"	"Off"

Code	Condition	Level	On Board?
32918	"Error writing hw db entry in MTCE Thresholder UpdateDB_All"	"MN"	"Off"
32919	"Error deleting sw db entry in MTCE Thresholder UpdateDB_ All"	"MN"	"Off"
32920	"Error aborting sw db transaction in MTCE Thresholder UpdateDB_All"	"MN"	"Off"
32921	"Error writing sw db entry in MTCE Thresholder UpdateDB_All"	"MN"	"Off"
32922	"Error ending sw db transaction in MTCE Thresholder UpdateDB_All"	"MN"	"Off"
32925	"Mtce::KeyCreate: bad key type in database"	"MN"	"Off"
32926	"Mtce::KeyCreate: bad key type in database"	"MN"	"Off"
32927	"Mtce::KeyCreate: bad key type in database"	"MN"	"Off"
32928	"Mtce::KeyCreate: bad record type in database"	"MN"	"Off"
32929	"Mtce::KeyCreate: bad key type in database"	"MN"	"Off"
32930	"Mtce::KeyCreate: bad key type in database"	"MN"	"Off"
32931	"Mtce::KeyCreate: bad key type in database"	"MN"	"Off"
32932	"Mtce::KeyCreate: bad record type in database"	"MN"	"Off"

Code	Condition	Level	On Board?
32936	"Can’t get ROMConnector for MTCE Thresholder"	"WN"	"Off"
33803	"OOS_FLT_STATE: Must have at least 1 WILD; PRI interface; and NIC working"	"MJ"	"Off"
33842	"BAD_CONSOLE_OPT: Bad option for console for mtce in inittab file"	"MN"	"Off"
33843	"BAD_CONSOLE_OPT: Bad option for console for mtce in inittab file"	"MN"	"Off"
33844	"can’t get VTA for MTCE"	"WN"	"Off"
37889	"SecDBMgr initialization failed."	"MN"	"Off"
37890	"MUMAdmin interface initialization failed."	"MN"	"Off"
37891	"Login VTA initialization failed"	"MN"	"Off"
37892	"Admin VTA initialization failed"	"MN"	"Off"
38048	"Invalid LoginRequest version number."	"MN"	"Off"
38049	"Invalid ChallengeResp version number."	"MN"	"Off"
38050	"Invalid ChangePasswd version number."	"MN"	"Off"
38112	"SecDB add user record failed."	"MN"	"Off"

Code	Condition	Level	On Board?
38113	"SecDB retrieve user record failed."	"MN"	"Off"
38114	"SecDB delete user record failed."	"MN"	"Off"
38115	"SecDB retrieve user record failed."	"MN"	"Off"
38116	"SecDB update user record failed."	"MN"	"Off"
38117	"SecDB retrieve user record failed."	"MN"	"Off"
38118	"SecDB update user record failed."	"MN"	"Off"
38119	"SecDB retrieve user record failed."	"MN"	"Off"
38120	"SecDB retrieve user record failed."	"MN"	"Off"
38121	"SecDB retrieve user record failed."	"MN"	"Off"
38122	"Unable to open binary license file."	"WN"	"Off"
38123	"Unable to read binary license file."	"WN"	"Off"
38124	"Unable to open ascii license file."	"WN"	"Off"
38125	"Unable to read ascii license file."	"WN"	"Off"
38126	"Invalid number for licensed users."	"MJ"	"Off"
38127	"Invalid length for license key."	"MJ"	"Off"

Code	Condition	Level	On Board?
38128	"Invalid binary license key."	"MJ"	"Off"
38129	"Invalid ascii license key."	"MJ"	"Off"
38208	"Invalid database key identifier."	"MN"	"Off"
38209	"Invalid database record identifier."	"MN"	"Off"
38210	"Invalid database key identifier."	"MN"	"Off"
38211	"Invalid database record identifier."	"MN"	"Off"
38212	"RaimaDBMgr StartTransaction failed."	"MN"	"Off"
38213	"RaimaDBMgr AbortTransaction failed."	"MN"	"Off"
38214	"RaimaDBMgr EndTransaction failed."	"MN"	"Off"
39032	"NameAgent or NameServer may be down"	"MJ"	"Off"
39033	"MUM or Trader process is not running."	"MJ"	"Off"
39034	"VT/ROM problem. Contact development."	"MJ"	"Off"
40558	"MEDIA_INTERNAL Fail find foreign server instance corresponding to rmt server."	"WN"	"Off"
40559	"MEDIA_INTERNAL Fail find foreign server instance corresponding to rmt server."	"WN"	"Off"

Code	Condition	Level	On Board?
40560	"MEDIA_INTERNAL Fail find foreign server instance corresponding to rmt server."	"WN"	"Off"
40561	"MEDIA_INTERNAL Fail find foreign server instance corresponding to rmt server."	"WN"	"Off"
40563	"MEDIA_INTERNAL Fail find foreign server instance for remote offering server."	"WN"	"Off"
40564	"MEDIA_INTERNAL Fail find foreign server instance for remote accepting server."	"WN"	"Off"
40566	"MEDIA_INTERNAL Fail find foreign server instance for remote offering server."	"WN"	"Off"
40576	"MEDIA_INTERNAL Fail find foreign server instance for remote offering server."	"WN"	"Off"
40577	"MEDIA_INTERNAL Fail find foreign server instance for remote accepting server."	"WN"	"Off"
40578	"MEDIA_INTERNAL Fail find foreign server instance for remote offering server."	"WN"	"Off"
40579	"MEDIA_INTERNAL Fail find foreign server instance for remote accepting server."	"WN"	"Off"

Code	Condition	Level	On Board?
40580	"MEDIA_INTERNAL Fail find foreign server instance for remote accepting server."	"WN"	"Off"
40581	"MEDIA_INTERNAL Fail find foreign server instance for remote accepting server."	"WN"	"Off"
45064	"NameAgent or NameServer may be down"	"MJ"	"Off"
45065	"dpm process may be down"	"MJ"	"Off"
45066	"dpm process may be down"	"MJ"	"Off"
45067	"dpm process may be down"	"MJ"	"Off"
45068	"dpm process may be down"	"MJ"	"Off"
45069	"dpm process may be down"	"MJ"	"Off"
45070	"dpm process may be down"	"MJ"	"Off"
45071	"dpm process may be down"	"MJ"	"Off"
45072	"dpm process may be down"	"MJ"	"Off"
45096	"NameAgent or NameServer may be down"	"MJ"	"Off"
45097	"dpm process may be down"	"MJ"	"Off"
49201	"Errors have caused loss of database synchronization."	"MN"	"Off"

Code	Condition	Level	On Board?
49202	"Errors have caused loss of database synchronization."	"MN"	"Off"
49203	"Errors have caused loss of database synchronization."	"MN"	"Off"
49204	"Errors have caused loss of database synchronization."	"MN"	"Off"
49205	"Errors have caused loss of database synchronization."	"MN"	"Off"
49206	"Errors have caused loss of database synchronization."	"MN"	"Off"
49207	"Errors have caused loss of database synchronization."	"MN"	"Off"
49208	"Errors have caused loss of database synchronization."	"MN"	"Off"
49209	"Errors have caused loss of database synchronization."	"MN"	"Off"
49212	"Database has been left in an inconsistent state."	"MN"	"Off"
49265	"Errors have caused loss of database synchronization."	"MN"	"Off"
49266	"Errors have caused loss of database synchronization."	"MN"	"Off"
49267	"Errors have caused loss of database synchronization."	"MN"	"Off"
49268	"Errors have caused loss of database synchronization."	"MN"	"Off"
49269	"Errors have caused loss of database synchronization."	"MN"	"Off"
49270	"Errors have caused loss of database synchronization."	"MN"	"Off"

Code	Condition	Level	On Board?
49271	"Errors have caused loss of database synchronization."	"MN"	"Off"
49272	"Errors have caused loss of database synchronization."	"MN"	"Off"
49274	"Errors have caused loss of database synchronization."	"MN"	"Off"
49275	"Errors have caused loss of database synchronization."	"MN"	"Off"
49276	"Errors have caused loss of database synchronization."	"MN"	"Off"
49280	"Errors have caused loss of database synchronization."	"MN"	"Off"
49281	"Errors have caused loss of database synchronization."	"MN"	"Off"
49282	"Errors have caused loss of database synchronization."	"MN"	"Off"
49283	"Errors have caused loss of database synchronization."	"MN"	"Off"
49284	"Errors have caused loss of database synchronization."	"MN"	"Off"
49285	"Errors have caused loss of database synchronization."	"MN"	"Off"
50320	"A kernel call has failed within the subagent"	"MN"	"Off"
50321	"A kernel call has failed within the subagent"	"MN"	"Off"
50322	"A kernel call has failed within the subagent"	"MN"	"Off"
50323	"A kernel call has failed within the subagent"	"MN"	"Off"

Code	Condition	Level	On Board?
50324	"A kernel call has failed within the subagent"	"MN"	"Off"
50325	"A kernel call has failed within the subagent"	"MN"	"Off"
50326	"A kernel call has failed within the subagent"	"MN"	"Off"
50327	"A kernel call has failed within the subagent"	"MN"	"Off"
50328	"A kernel call has failed within the subagent"	"MN"	"Off"
50329	"A kernel call has failed within the subagent"	"MN"	"Off"
50330	"A kernel call has failed within the subagent"	"MN"	"Off"
50331	"A kernel call has failed within the subagent"	"MN"	"Off"
50332	"A kernel call has failed within the subagent"	"MN"	"Off"
50333	"A kernel call has failed within the subagent"	"MN"	"Off"
50334	"A kernel call has failed within the subagent"	"MN"	"Off"
50335	"A kernel call has failed within the subagent"	"MN"	"Off"
50336	"A kernel call has failed within the subagent"	"MN"	"Off"
50337	"A kernel call has failed within the subagent"	"MN"	"Off"
50338	"A kernel call has failed within the subagent"	"MN"	"Off"

Code	Condition	Level	On Board?
50339	"A kernel call has failed within the subagent"	"MN"	"Off"
50340	"A kernel call has failed within the subagent"	"MN"	"Off"
50341	"A kernel call has failed within the subagent"	"MN"	"Off"
50342	"A kernel call has failed within the subagent"	"MN"	"Off"
50343	"A kernel call has failed within the subagent"	"MN"	"Off"
53258	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53259	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53260	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53261	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53262	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53263	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53264	"Try to do ifconfig on a interface failed"	"MJ"	"Off"
53265	"Try to do ifconfig on a interface failed"	"MJ"	"Off"
53266	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53267	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"

Code	Condition	Level	On Board?
53268	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53269	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53270	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53271	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53272	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53273	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53274	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53275	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53276	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53277	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53278	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53279	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53280	"Try to do ifconfig on a interface failed"	"MJ"	"Off"
53308	"Try to do ifconfig on a interface failed"	"MJ"	"Off"
53309	"Try to do ifconfig on a interface failed"	"MJ"	"Off"

Code	Condition	Level	On Board?
53310	"No calling number provided for the incomming call"	"WN"	"Off"
53348	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53349	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53350	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53351	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53352	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53353	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53354	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53355	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53356	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53357	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53358	"Try to do ifconfig on a interface failed"	"MJ"	"Off"
53359	"Try to do ifconfig on a interface failed"	"MJ"	"Off"
53360	"Try to do ifconfig on a interface failed"	"MJ"	"Off"
53361	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"

Code	Condition	Level	On Board?
53362	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53363	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53364	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53365	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53366	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53367	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53368	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53369	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53370	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53371	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53372	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53373	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53374	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53375	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53376	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"

Code	Condition	Level	On Board?
53377	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53378	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53379	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53380	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53381	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53382	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53383	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53384	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53385	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53398	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53399	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53400	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53401	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53402	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53403	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"

Code	Condition	Level	On Board?
53404	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53405	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53406	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53407	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53408	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53409	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53410	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53411	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53412	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53413	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53414	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53415	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53448	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53449	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53450	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"

Code	Condition	Level	On Board?
53451	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53452	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53454	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53455	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53456	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53457	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53458	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53459	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53460	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53461	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53462	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53463	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53464	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53465	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53466	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"

Code	Condition	Level	On Board?
53467	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53468	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53469	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53470	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53471	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53472	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53473	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53498	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53499	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53500	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53501	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53502	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53503	"Try to do ifconfig on a interface failed"	"MJ"	"Off"
53504	"Try to do ifconfig on a interface failed"	"MJ"	"Off"
53505	"Try to do ifconfig on a interface failed"	"MJ"	"Off"

Code	Condition	Level	On Board?
53506	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53507	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53509	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53510	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53511	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53512	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53513	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53514	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53515	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53516	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53517	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53518	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53519	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53586	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"
53587	"Try to save transaction to RAIMA DB failed"	"MN"	"Off"

Code	Condition	Level	On Board?
53760	"out of kernel mbuf buffers"	"MJ"	"Off"
53761	"out of kernel cluster buffers"	"MJ"	"Off"
53762	"IP stack dequeue failure"	"None"	"Off"
53763	"Lynx timeout system call failure"	"None"	"Off"
53764	"transmition attempt timeout - failed link"	"None"	"Off"
53765	"transmit output queue full - failed link"	"None"	"Off"
54017	"LEC MSAP is down"	"MJ"	"On"
54018	"LEC cfg failed because of lack of resources"	"None"	"Off"
54019	"LEC TSAP or AALSAP is down"	"None"	"Off"
54020	"LEC MSAP TSAP or AALSAP has been deleted"	"None"	"Off"
54021	"VCC is down & max number of restarts sent "	"None"	"Off"
54022	"Q.93B DLSAP is down"	"None"	"Off"
54023	"Q.93B cfg has failed 'cause of lack of resources"	"None"	"Off"
54024	"Q.93B DLSAP is in the process of disconnecting"	"None"	"Off"
54025	"Q.93B link has been reset - trying to restart"	"None"	"Off"

Code	Condition	Level	On Board?
54026	"VCC is down"	"None"	"Off"
54027	"Q.SAAL cfg has failed 'cause of lack of resources"	"None"	"Off"
54028	"Q.SAAL data link is down"	"None"	"Off"
54029	"VCC is down"	"None"	"Off"
54030	"UME cfg has failed 'cause of lack of resources"	"None"	"Off"
54031	"UME data link is down"	"None"	"Off"
54116	"No rx buf descr"	"None"	"Off"
54117	"No rx DMA queued"	"None"	"Off"
54118	"Rx on bad VCI"	"None"	"Off"
54119	"Rx bad length"	"None"	"Off"
54120	"Rx dropped"	"None"	"Off"
54121	"Rx exception"	"None"	"Off"
54122	"AAL5 config"	"None"	"Off"
54123	"AAL5 GEN cfg"	"None"	"Off"
54124	"AAL5 SAP cfg"	"None"	"Off"

Code	Condition	Level	On Board?
54125	"AAL5 SAP bind"	"None"	"Off"
54126	"AAL5 SAP unbind"	"None"	"Off"
54127	"AAL5 SAP conn req"	"None"	"Off"
54128	"AAL5 SAP conn cfg"	"None"	"Off"
54129	"AAL5 SAP data req"	"None"	"Off"
54131	"AAL5 SAP disc req"	"None"	"Off"
54132	"AAL5 mpt req"	"None"	"Off"
54133	"AAL5 SAP disc ind"	"None"	"Off"
54134	"AAL5 SAP disc cfm"	"None"	"Off"
54135	"AAL5 SAP data ind"	"None"	"Off"
54136	"AAL5 SAP data cfm"	"None"	"Off"
54137	"No memory"	"None"	"Off"
54138	"No mbufs"	"MJ"	"Off"
54139	"Error count test"	"None"	"Off"
55314	"WILD_BAD_STATE: WILD Card not in NORMAL_OP state"	"None"	"Off"

Code	Condition	Level	On Board?
55333	"WILD_BAD_STATE: WILD Card not in NORMAL_OP state"	"None"	"Off"
55355	"BAD_CONSOLE_OPT: Bad option for console for cm in inittab file"	"MN"	"Off"
55356	"BAD_CONSOLE_OPT: Bad option for console for cm in inittab file"	"MN"	"Off"
55417	"NO_WILD_RESOURCES: No WILD Cards available"	"WN"	"Off"
55418	"NO_WILD_RESOURCES: No PPP Channels available on WILD Card"	"WN"	"Off"
55419	"NO_WILD_RESOURCES: No WILD Cards available to support request"	"WN"	"Off"
55420	"NO_WILD_RESOURCES: No WILD Card resources available to support request"	"WN"	"Off"
55431	"VIDEO_DRIVER_ERROR: Failed to open video driver"	"MJ"	"Off"
55433	"INTERNAL_ERROR: Video MULTICAST_RECV failed"	"None"	"Off"
55434	"INTERNAL_ERROR: Video MULTICAST_SEND failed"	"None"	"Off"
55435	"INTERNAL_ERROR: Video DISC_MULTICAST_RECV failed"	"None"	"Off"
55436	"INTERNAL_ERROR: Video DISC_MULTICAST_SEND failed"	"None"	"Off"

Code	Condition	Level	On Board?
55440	"VIDEO_DRIVER_ERROR: Failed to init Multi-Cast Driver"	"None"	"Off"
55442	"GLOBAL_DB_ERROR: Failed to get MAXCONF from cw.ini"	"MN"	"Off"
55443	"GLOBAL_DB_ERROR: Failed to get LOSSTABLESIZE from cw.ini"	"MN"	"Off"
55444	"GLOBAL_DB_ERROR: Failed to get LOSSTABLE from cw.ini"	"MN"	"Off"
55445	"GLOBAL_DB_ERROR: Failed to get WILDCODEFILES from cw.ini"	"MN"	"Off"
55446	"GLOBAL_DB_ERROR: Failed to get WILDDATAFILES from cw.ini"	"MN"	"Off"
55461	"PRIM_INTF_ERROR: cm could not create connector to PRIM"	"MN"	"Off"
55468	"WILD_DRIVER_ERROR: WILD_CONFIG ioctl failed"	"None"	"Off"
55469	"WILD_DRIVER_ERROR: WILD_RESET ioctl failed"	"None"	"Off"
55470	"WILD_DRIVER_ERROR: WILD_STATUS ioctl failed"	"None"	"Off"
55471	"WILD_DRIVER_ERROR: AUDIO_INIT ioctl failed"	"None"	"Off"
55472	"WILD_DRIVER_ERROR: wildIORecv read failed"	"None"	"Off"
55473	"WILD_DRIVER_ERROR: wildIORecv read incomplete"	"None"	"Off"

Code	Condition	Level	On Board?
55475	"INTERNAL_ERROR: Bad fd or threadID at download"	"None"	"Off"
55478	"WILDCARD_FAILURE: Failed to receive from WILD at download"	"MJ"	"Off"
55479	"INTERNAL_ERROR: Bad response from WILD during download protocol"	"None"	"Off"
55480	"INTERNAL_ERROR: Failed to send code to WILD Card"	"None"	"Off"
55481	"INTERNAL_ERROR: Failed to send data to WILD Card"	"None"	"Off"
55482	"WILD_DRIVER_ERROR: failed write to WILD at download"	"None"	"Off"
55483	"WILDCARD_FAILURE: Did not get ALL-OK (POWER_UP_IND) from WILD at download"	"MJ"	"On"
55484	"DOWNLOAD_FILE_ERROR: Failed to open download file for WILD"	"MJ"	"Off"
55485	"DOWNLOAD_FILE_ERROR: Failed to stat download file for WILD"	"MJ"	"Off"
55486	"DOWNLOAD_FILE_ERROR: Download file size error for WILD"	"MJ"	"Off"
55487	"DOWNLOAD_FILE_ERROR: Failed to read download file"	"MJ"	"Off"

Code	Condition	Level	On Board?
55488	"WILD_DRIVER_ERROR: failed write of download file to WILD"	"None"	"Off"
55489	"INTERNAL_ERROR: Failed download protocol to WILD; no ack"	"None"	"Off"
55490	"INTERNAL_ERROR: Failed download protocol to WILD; no next DNLD request"	"None"	"Off"
55491	"WILD_DRIVER_ERROR: Select failed during download"	"None"	"Off"
55492	"WILD_DRIVER_ERROR: Read failed during download"	"None"	"Off"
55493	"WILD_DRIVER_ERROR: Read failed during download"	"None"	"Off"
55494	"WILDCARD_FAILURE: Failed to reset WILD Card"	"MJ"	"On"
55497	"GLOBAL_DB_ERROR: Bad number of loss types for init"	"MN"	"Off"
55498	"GLOBAL_DB_ERROR: Bad max confs. for init"	"MN"	"Off"
55499	"GLOBAL_DB_ERROR: Bad loss type for init"	"MN"	"Off"
55500	"GLOBAL_DB_ERROR: Bad code file name (length)"	"MN"	"Off"
55501	"GLOBAL_DB_ERROR: Bad data file name (length)"	"MN"	"Off"
56320	"Read Configuration HWIDS Failed"	"MN"	"Off"
56321	"Read Configuration SYSPARMS Failed"	"MN"	"Off"

Code	Condition	Level	On Board?
56322	"Read Configuration DLFWPATH Failed"	"MN"	"Off"
56323	"Read Configuration PRIMDBUG Failed"	"MN"	"Off"
56324	"GetBootLevel Failed"	"MN"	"Off"
56325	"GetBootLevel Value Invalid"	"MN"	"Off"
56326	"Open DLFWPATH File Failed"	"MN"	"Off"
56327	"Read DLFWPATH File Failed"	"MN"	"Off"
56328	"PRI D-channel Down"	"WN"	"Off"
56329	"PRI Board Internal Error"	"MN"	"On"
56420	"PRI Device Open Failed"	"MN"	"Off"
56421	"PRI Open Select Board Failed"	"None"	"Off"
56422	"PRI Management Channel Enable Failed"	"MN"	"Off"
56425	"PRI Download Firmware Start Failed"	"MN"	"Off"
56426	"PRI Downlad Firmware Load Step Failed"	"MN"	"Off"
56427	"PRI Download Firmware Completion Failed"	"MN"	"Off"
56430	"PRI Connect D-channel Failed for HDLC Control"	"MN"	"Off"

Code	Condition	Level	On Board?
56431	"PRI Connect D-channel Failed for MVIP In"	"MN"	"Off"
56432	"PRI Connect D-channel Failed for PRI Line"	"MN"	"Off"
56433	"PRI Connect D-channel Failed for MVIP Out"	"MN"	"Off"
56435	"PRI Set Hardware Failed"	"MN"	"Off"
56436	"PRI Set Idle Code Failed"	"MN"	"Off"
56438	"PRI Enable Protocol Failed"	"MN"	"Off"
56441	"PRI Enable D-channel Failed"	"MN"	"Off"
56443	"PRI Disable D-channel Failed"	"MN"	"Off"
56472	"PRI Clear All MVIP Connections Failed"	"None"	"Off"
57344	"WILD_EXT_MSG_ERR_EV - Communication Error between the Host and the WILD Card"	"MJ"	"Off"
57345	"WILD_OS_SHUTDOWN - WILD Card Operating System Shut Down"	"MJ"	"Off"
57444	"WILD_FROM_HOST_ERR_EV - Problems receiving messages and data from host"	"MJ"	"Off"
57524	"WILD_TO_HOST_ERR_EV - Problems sending messages and data to host"	"MJ"	"Off"

Code	Condition	Level	On Board?
57624	"WILD_SWT0_EV - WILD Card processor occupancy is very high"	"MN"	"On"
61440	"Non-respawnable process abnormally terminated; COLD1 reset required"	"MJ"	"Off"
61441	"Non-respawnable process abnormally terminated; COLD2 reset required"	"MJ"	"Off"
61442	"Respawnable process abnormally terminated"	"MJ"	"Off"
65536	"McapiClient acquire_socket failed"	"None"	"Off"
65537	"McapiClient TheLoop receive failed"	"None"	"Off"
65538	"McapiClient Notify transmit failed"	"None"	"Off"

C BIOS POST codes

Test Number	Test Name
01	80286 register test in-progress
03	BIOS ROM checksum in-progress or failure
02	CMOS write/read test in-progress or failure
04	Programmable Interval Timer test in-progress or failure
05	DMA initialization in-progress or failure
06	DMA page register write/read test in-progress or fail
08	RAM refresh verification in-progress or failure
09	1st 64K RAM test in-progress
0D	1st 64K RAM parity test in_progress or failure
3F	Shadow CPU BIOS
20	slave DMA register test in-progress or failure
21	master DMA register test in-progress or failure
22	master interrupt mask register test in-progress or fail

Test Number	Test Name
23	slave interrupt mask register test in-progress or fail
25	interrupt vector loading in-progress
27	keyboard controller test in-progress or failure
28	CMOS power-fail and checksum checks in-progress
3F	Shadow CPU BIOS
76	PT80_PCI_INIT
77	PT80_PCI_CONFIG_VGA
29	CMOS config info validation in-progress
2B	3-3-4 screen memory test in-progress or failure
2E	search for video ROM in-progress
34	4-2-1 timer tick interrupt test in_progress or failure
35	4-2-2 shutdown test in_progress or failure
00	SYSTEM NORMAL
3A	Interval timer channel 2 test in_progress or failure
38	RAM test in_progress or failure above address 0FFFFh
00	SYSTEM NORMAL

Test Number	Test Name
3B	Time-Of-Day clock test in_progress or failure
78	PT80_PCI_CONFIG_NON_VGA
7A	PT80_PCI_INIT_OPROM
79	PT80_PCI_PCIDSR_DISPATCH
79	PT80_PCI_PCIDSR_DISPATCH
79	PT80_PCI_PCIDSR_DISPATCH
79	PT80_PCI_PCIDSR_DISPATCH
79	PT80_PCI_PCIDSR_DISPATCH
40	CACHE INITIALIZATION

Test Number	Error Message
1-3-3	1st 64K RAM chip or data line failure - multi-bit
1-3-4	1st 64K RAM odd/even logic failure
1-4-1	1st 64K RAM address line failure
2-1-1	1st 64K RAM chip or data line failure - bit 0 thru F
3-1-2	master DMA register test in-progress or failure
3-1-3	master interrupt mask register test in-progress or fail
3-1-4	slave interrupt mask register test in-progress or fail
	interrupt vector loading in-progress
	CMOS config info validation in-progress
3-3-4	screen memory test in-progress or failure
3-4-1	screen initialization in-progress or failure
3-4-2	screen retrace tests in-progress or failure
	screen believed operable
	screen believed running w/ video ROM

Test Number	Error Message
	monochromatic screen believed operable
	40-column color screen believed operable
	80-column color screen believed operable
4-2-3	gate A20 failure"
4-2-4	unexpected interrupt in protected modem
4-4-1	Serial port test test in_progress or failure
4-4-2	Parallel port test test in_progress or failure
4-4-3	Math Coprocessor test in_progress or failure
	Shadow CPU BIOS
	NO MEMORY FOUND ON CPU BOARD
	Chipset Initialization
	Cache Sizing Algorithm
	PT80_PCI_ALIGN_ERROR
	PT80_PCI_BAD_CFG_TYPE
	PT80_PCI_INVALID_PFA
	PT80_PCI_OUT_OF_BARDS

Test Number	Error Message
	PT80_PCI_OUT_OF_FMDS
	PT80_PCI_PRECFG_BARD_ERROR
	PT80_PCI_BEFORE_MEMSIZE

D Alarm and threshold field definitions

This appendix defines the fields displayed when you use the **showalarm** and **showthresh** commands. See the following

The showalarm command

The **showalarm** command displays the following alarm log fields.

STATE

Shows the alarm state.

If no state is specified then all alarms and errors are shown.

The alarm state can be any one of the following:

- **active** - State when error(s) reported exceed an up-threshold and an alarm has been raised.
- **inactive** - State when errors reported do not exceed a threshold. The inactive state will typically be seen by errors with no alarm thresholds.
- **resMaint** - (resolved by maintenance) The state entered when the error count associated with an alarmed entry is decremented by time (leaky bucket) or by software (input indicating the condition went away) to the associated down threshold.
- **resClear** - (resolved by the clearalarm command) The state entered when the error count associated with an alarmed entry is set to zero (cleared) by use of the **clearalarm** command.
- **resBoot** - (resolved by reboot) The state entered when the error count associated with an alarmed entry is set to zero when the system is rebooted.

SVRTY

Shows the severity (**SVRTY**) of the alarm.

Severity can be any one of the following:

- **none** - The alarm is inactive.
- **warning** (WN) - The alarm level for errors that are expected to have little effect on customers.

- **minor** (MN) - The alarm level is for errors that are expected to have significant customer visible effects but not render the total system inoperative.
- **major** (MJ) - The alarm level is for errors that are expected to have significant customer visible effects that possibly render the total system inoperative.

SOURCE

Where the alarm came from.

For hardware alarms, it is the name of the circuit card where the alarm originated.

For example:

- ETHER_PT (Ethernet card)
- ATM/OC3-PT (ATM card)
- WILD (WILD card)
- PRI_INTF (PRI card)
- CPU (CPU card)

ST

The slot (ST) number consists of the prefix for the type of bus (p for PCI, and i for ISA) along with the slot number (1 to 6).

For example, slot 3 on the PCI bus is represented as p3, slot 5 on the ISA bus is represented as i5.

PT

The port (PT) number is the number of the port within a particular slot.

ALARM_TIME

The time at which this event first triggered an alarm.

RESOLVE_TIME

The time at which the alarm was resolved

SEQ#

Sequence numbers (SEQ#) are allocated as alarms are created. So you may find that an alarm you are tracking has been resolved and a new entry of the same type created and given a different sequence number.

COUNT

The number of times this event has occured.

FIRST_OCCUR

The time at which this event first occured.

LAST_OCCUR

The time at which this event last occured.

BRD

This field indicates whether this alarmable event occurred in a specific field-replacable board (BRD) (circuit card).

- **On** indicates that there is a 90% chance that the alarmable event occured in a specific field-replacable board.
- **Off** indicates the alarmable event occured outside of a specific field-replacable board.

SRV

The service (SRV) state of the hardware that caused the event.

- in-service
- out-of-service.

Code

A unique number used by the server to identify the software location of the code logging the error.

RPR

The repair number for this alarm.

AUX

Auxillary (AUX) data used to pass more information about an error. This data is somwetimes referred to in the repair actions.

The showthresh command

The **showthresh** command displays the following alarm log fields.

THRESH_INDEX

A unique number used to identfy an entry in the threshold action table.

RMB_ALARM

The number identifying the RMB USER ALARM passed to INADS when an alarm origination callout is made.

REPAIR_NUM

The repair number for this alarm.

INC_AMOUNT

Increment amount The number the counter is incremented when an error is processed.

DEC_AMOUNT

Decrement amount The number the counter is decremented when software decrements the counter.

DEC_CONDITION

Decrement condition The condition for decrementing a counter.

There are three values for this condition:

1. **TIME** - The condition specified when the error counter is to be decremented periodically (every 5 minutes). This decrementing is used in cases where the error rate is the best indicator of the problem. TIME is the condition that identifies the leaky bucket approach.
2. **DEC** - The condition specified when the error counter is to be decremented by software. This decrementing is used in cases where faults are either present or not (for example: loss of signal conditions on facilities).
3. **NONE** - The condition specified when the error counter is not decremented. This decrementing is used in cases where the number of occurances of the error is the best indicator of the problem.

UP_THRESH1

Upward threshold 1 The first of two error-counter thresholds. It causes **Up_Action1**, **2**, and **3** to be executed.

UP_THRESH2

Upward threshold 2 The second of two error-counter thresholds. It causes **Up_Action4**, **5**, and **6** to be executed.

UP_THRESH_MAX

Upward threshold maximum The maximum value the error counter is allowed to increment.

This value is used to adjust the time to raise and resolve alarms under the leaky bucket scheme.

DOWN_THRESH

Downward threshold The threshold that, when reached by an error counter decrementing after exceeding an upward threshold, causes associated actions to be executed.

UP_ACTION (1-6)

One of up to six actions that can be associated with an upward threshold.

These action include things like raising an alarm and reporting an alarm to INADS.

DOWN_ACTION (1-3)

One of up to three actions that can be associated with an downward threshold.

These action include things like resolving an alarm and reporting an alarm resolution to INADS.

INFO (1-2)

A decription of the error condition.

Glossary

1s density

See *ones density*.

A

administration

Setting system parameters (1) from the system management interface; also called *configuration management*; (2) from the graphical user interface, such as password administration or administering a coverage path.

administration menu

The MMCX server software interface that lets you perform administrative tasks.

ATM

Asynchronous Transfer Mode: a very high-speed, high bandwidth transmission technology that combines features of packet- and circuit-switched networks. ATM transmits data in fixed-length, 58-byte cells containing 5-byte *headers* (routing and signalling information) and a 48-byte *payload*. Cells are sent in a continuous stream over a pre-negotiated path through the network (a

so-called *virtual connection*). ATM can transmit at speeds of up to 622.08 Mbps (622,080,000 bits per second) using fiber-optic lines. ATM is once of two network protocols supported by MMCX (see also *Ethernet*).

Automatic Route Selection (ARS)

A system for automatically routing telephone calls by the least costly route. A feature of the Lucent DEFINITY Enterprise Communications Server. See *Multimedia Applications Server Interface (MASI)*.

B

B8ZS

Binary 8 Zero Substitution: a way of controlling *ones density* that represents every seventh consecutive 0 by violating of the bipolar *line coding* scheme used on T-carrier systems. Bipolar line coding inverts the polarity of every other 1 in a set of binary data. Two consecutive 1s never have the same polarity. B8ZS can thus use two consecutive ones of the same polarity (a *coding violation*) to uniquely represent a 0.

bandwidth

The amount of data that a given *channel* can transmit in a given period of time, measured in bits per second (*not* bytes per senond) on digital networks or in Hertz (cycles per second) on analog networks.

Binary 8 Zero Substitution

See *B8ZS*.

bridge

A device that connects two or more *packet-switched networks* and directs packets sent from one to the other. See *router*.

C

call

See *MMCX call* and *voice interworking call*.

call redirection

See *redirect*.

CALLed Party Number IE

The ISDN information element containing the digits sent to the called party.

CD ROM

Compact Disk Read-Only memory, an optical computer disk widely used for distributing and installing software and electronic documentation.

Centrex

An alternative to an in-house PBX offered by local telephone company central offices. Centrex provides businesses with the equivalent of individual, home service at the individual desktop.

channel

A transmission path linking two endpoints.

circuit-switched network

A network that sets up and maintains a connection for the exclusive use of two or more communicating parties for the duration of their call. The familiar, voice telephone network is circuit-switched. See *packet-switched network*.

clear-channel facility

A digital circuit that requires no in-channel framing or control bits. the whole bandwidth is thus available for data transmission.

client

MMCX client: a workstation capable of making MMCX calls. Such a workstation is a client of one or more MMCX *servers*.

configuration

See *administration*.

configuration management

See *administration*.

console terminal

A computer or dumb terminal attached to the MMCX server. You use the console to control the server directly.

coverage

See *cover calls*.

coverage, immediate

To send incoming calls directly to a *coverage point* without ringing the dialed extension.

coverage point

The phone number in an MMCX call coverage path. See *cover calls*.

cover calls

To *redirect* incoming calls to a pre-defined telephone number. See also *coverage, immediate*.

Covered Call Tone

An MMCX user preference that allows you to receive audible tones when incoming calls are covered or forwarded.

CSN

See *circuit-switched network*.

CWID

The unique identifier for each MMCX user. It consists of the user's Direct Inward Dial telephone number plus the country code. In the

U.S., this means the CWID is **1 - *area_code*** - ***office_code*** - ***location_code***. For example, 1-303-538-1526.

D

distributed application

A computer application that runs simultaneously on a *server* and one or more *clients*. Distributed design lets multiple users run programs using common, centrally located application resources, such as databases.

domain

An addressable location on a network, such as a group of computers, single computer, or subdirectory. See *Domain Name Server (DNS)*.

Domain Name Server (DNS)

An Internet computer that maintains a database of *domain* names.

DNS

See *Domain Name Server (DNS)*.

drop a call

Hang up or otherwise disconnect yourself or another party on a call. You can use the **Drop** button in the MMCX main window to drop one, several, or all parties on a call. Use **Hang Up** to drop yourself.

E

E-1

A digital transmission link with a capacity of 2.048 Mbps (2,048,000 bits per second). The European equivalent of the *T-1*. It can support 30 multiplexed 64-Kbps voice and data channels plus separate 64-Kbps channels for signalling and framing (synchronization). Also spelled **E1**.

Ethernet

A *local area network* (LAN) that works over short distances on twisted-pairs or coaxial cables at speeds up to 10 Mbps (10,000,000 bits per second). One of the two LAN protocols MMCX supports (see also *ATM*).

F

forward a call

Redirect an incoming call to a specified destination entered in the MMCX **Dial** field.

Freeze Video

An option on the **Video** menu in the video viewer window that you can use to freeze the currently displayed picture in that window.

H

H.323

A specification that sets standards for multimedia communications between LANs and telephony networks, such as ISDN.

Help Browser

An option on the MMCX **Help** menu that displays MMCX-specific help topics.

high water mark

The highest value that a current status counter has reached since the last time the counter was initialized.

host

A *server*.

host name

See *server name*.

hypertext

Words, phrases, or sentences you can click to jump to another place in an MMCX document. Hypertext is blue, italicized, and underlined.

immediate coverage

To send incoming calls directly to a *coverage point* without ringing the dialed extension.

Information Element (IE)

The data fields in ISDN messages.

in-service state

The condition or state of an MMCX server that is ready to handle calls.

intercept tone

internal call

A call between endpoints on an MMCX network, where both parties are equipped for MMCX multimedia communications. Internal calls are the only calls that can be multimedia.

International Number

The National Number prepended with the country code. For example, in the U.S., 1-303-538-1234 is an International Number (1 is the U.S. country code).

inter-server routing number

The listed directory number, in ISDN National Number format, of the MMCX server that is used for inter-server communications.

Each server has a unique inter-server routing telephone number. This number is assigned in the *inter-server routing table*.

inter-server routing table

A database that keeps track of the *inter-server routing numbers* on a multiserver MMCX network.

IP user

An *H.323* endpoint on an MMCX network. Such users do not have log ins, so the MMCX server identifies them using an extension number and an IP address.

ISDN National Number

The full dialed number minus the country code. The National Number is composed of office code plus subscriber code. In North America, this means area code plus seven digits. For example, 303-538-1234 is a National Number.

L

LAN

See *local area network*.

local area network

A short-range data communication network linking computers and peripherals, such as printers. Ethernet and Token-Ring are common LAN architectures. See *wide area network*.

line coding

The formatting applied to data sent across a specified telecommunications medium for *signalling* purposes. The familiar T-carrier system uses *bipolar line coding,* a coding scheme that inverts the polarity of every other 1 in a set of binary data. Line coding is also used to control *ones density* (see *B8ZS*).

M

MASI

See *Multimedia Applications Server Interface (MASI)*.

Meeting Room

That area in the MMCX main window where the user accesses conference room features and applications, multimedia controls, and telephone calling features.

messages

(1) Output providing feedback on a user's interactions with MMCX. Messages in the graphical user interface appear in the call display bar, status bar of interactive windows, and in dialogue boxes that pop up. (2) Feedback from the system during installation or administration on the progress of the process. These appear on the *console terminal*.

MMCX call

A telephone call handled by the MMCX network, especially one that integrates audio with video, data, and/or shared applications, such as the MMCX whiteboard feature.

MMCX client

See *client*.

MMCX network

The set of MMCX clients and servers configured through system management to communicate with each other via multimedia calls.

Multimedia Applications Server Interface (MASI)

An optional extension to MMCX that lets an MMCX network take advantage of the advanced call handling features of the Lucent DEFINITY Enterprise Communications Server.

multimedia call

A call that integrates audio with video, data, and/or shared applications, such as the MMCX whiteboard feature.

N

Nameplate

The area above a chair in the meeting room that identifies a calling party.

National Television Standards Committee (NTSC) Standard

The standard format and transmission method for television signals in North America, Central America, and Japan. The NTSC is a division of the Electronic Industries Association (EIA). MMCX video transmissions confrom with NTSC requirements.

National Number

See *ISDN National Number*.

Network Interface Card (NIC)

A circuit board that can be fitted to a personal computer (PC) to allow the PC to communicate with other machines on a network.

MMCX works with Ethernet cards and with asynchronous transfer mode (ATM) cards running Ethernet emulation.

NIC

See *Network Interface Card (NIC)*.

NTSC

See *National Television Standards Committee (NTSC) Standard*.

O

ones density

The minimum number of 1s that the public switched network requires in any 8-digit portion of a binary data stream. The public network sends a binary 0 as a zero voltage, so 0s do not supply signalling pulses that the network can count. If a message contains more than 7 consecutive 0s, the network gets out of synch. To avoid this, the network has to substitute a code for every eighth 0. How this is done depends on the *line coding* method chosen.

online help

Instructions and advice for using an application that you view on your screen or console. You can get online help by (1) selecting **Help | Help Browser** from the MMCX main window menu bar, (2) clicking **Help** buttons in application dialog windows, or (3) pressing **F1** while your cursor is in the MMCX main window.

out-of-service state (OOS)

The condition or state of an MMCX server that is operating but not ready to accept or place calls.

P

packet-switched network

A network that divides messages into smaller packets, each with its own identifying and routing information attached. The packets can then travel to their destinations by varying routes. For data transmissions, a packet switched network can make more efficient use of available bandwidth than a *circuit-switched network*, because it does not dedicate a channel for the duration of a call. Instead, packets are queued and sent on a standby basis, as channel capacity becomes available. The Internet is a good example of a packet-switching network.

PBX

Private Branch Exchange: a customer-owned telephone switch that connects a company's internal telephone network with the loal telephone service provider's central office. Lucent's Definity PBX is a good example.

PEG Counts

Software registers or variables that increment each time a specified event occurs.

Point-to-Point Protocol

A *TCP/IP* implementation tailored for use over telephone lines. It supports router-to-router and host-to-network connections over both synchronous and asynchronous circuits. PPP replaces SLIP (Serial Line Interface Protocol).

PPP

See point-to-point interface protocol.

PSN

See *packet-switched network*.

Public Switched Telephone Network (PSTN)

The worldwide voice telephone system.

R

redirect

To route incoming calls to another destination. MMCX offers 2 ways users can redirect their calls. You can *forward a call* or *cover calls*.

restricted facility

A network that reserves some of the available bandwidth for signalling, the opposite of a *clear-channel facility*.

router

An interface between different networks. Routers support network management, including load balancing, route optimization, prioritizing of calls, and troubleshooting. They are thus more capable than *bridges*.

S

server

MMCX server: the computer that sets up, maintains, and administers MMCX network communications for MMCX *clients*.

server name

The name of the MMCX server as it appears in the host's database. You enter the server name in the boot-time administration menu.

Share

Open an application within MMCX so that the parties to a call can use it. You can use the **Share** tool or the **WhiteBoard** application for simultaneous editing.

signalling

The control information that a network uses to set up and maintain connections. On-hook and off-hook are, for instance, the familiar voice-telephone signals that tell the central office that you have picked up the telephone handset or hung up at the end of a call.

In-channel signalling reserves part of the available data -communication bandwidth for control information (see *restricted*

facility). Out-of-channel signalling schemes use a separate channel for signals, so that data transmissions can use all of the bandwidth available to them (see *clear-channel facility*).

T

T-1

A 4-wire (2 twisted pair), digital communications link with a capacity of 1.544 Mbps (1,544,000 bits per second). A T-1 can handle 24 concurrent 64 Kbps voice and data channels plus separate channels for signalling and framing (synchronization). It is the standard for data communications in North America and Japan. Also spelled **T1**. See *E-1*.

T-carrier

A hierarchy of digital voice- and data-transmission systems used in North America and based on multiples of the capacity of the *T-1* line.

TCP/IP

Transmission Control Protocol/Internet Protocol: a standard that lets different computer hardware and different operating systems (such as PCs, Apple computers, UNIX workstations, and

mainframes) communicate with each other over a network. TCP/IP is the most complete, most widely accepted network protocol currently available.

TDM

See *Time Division Multiplexing*.

Time Division Multiplexing

A way of interleaving digitized voice, video, and/or data so that several calls can be sent concurrently over the same transmission medium. TDM systems divide the available transmission capacity into a series of *time slots*. The system assigns a piece from each message to a time slot until all time slots are full or all messages have been sent. At the far end, the messages are *demultiplexed*. That is, the receiver disassembles the interleaved transmission and uses the sequence of time slots to assign each piece of information to the correct position in the correct message. Time Division Multiplexing is typically used on *circuit-switched networks*.

U

unrestricted facility

See *clear-channel facility*.

V

video capture device

Software and/or hardware that supports the display of transmitted images on a specified computer and video screen.

voice interworking call

A voice interworking call is a call between an MMCX user and a voice terminal (telephone, speakerphone, etc.) *not* on the MMCX network. For example, you can call virtually any public phone number in the world from an MMCX workstation.

W

WAN

See *wide area network*.

wide area network

A data network that connects *local area networks* (LANs) using common-carrier telephone lines, *bridges*, and *routers*.

Index

Numerics

A

B

C

D

E

F

H

I

L

M

N

O

P

R

S

T

U

V

W

Y

Z