

MAX 4000 Series Administration Guide

Ascend Communications, Inc.

Part Number: 7820-0626-001

For software version 7.0.0

MAX is a trademark of Ascend Communications, Inc. Other trademarks and trade names mentioned in this publication belong to their respective owners.

Copyright © November 1998, Ascend Communications, Inc. All Rights Reserved.

This document contains information that is the property of Ascend Communications, Inc. This document may not be copied, reproduced, reduced to any electronic medium or machine readable form, or otherwise duplicated, and the information herein may not be used, disseminated or otherwise disclosed, except with the prior written consent of Ascend Communications, Inc.

Ascend Customer Service

Ascend Customer Service provides a variety of options for obtaining technical assistance, information about Ascend products and services, and software upgrades.

Obtaining technical assistance

You can obtain technical assistance by telephone, email, fax, or modem, or over the Internet.

Enabling Ascend to assist you

If you need to contact Ascend for help with a problem, make sure that you have the following information when you call or that you include it in your correspondence:

- Product name and model.
- Software and hardware options.
- Software version.
- If supplied by your carrier, Service Profile Identifiers (SPIDs) associated with your product.
- Your local telephone company's switch type and operating mode, such as AT&T 5ESS Custom or Northern Telecom National ISDN-1.
- Whether you are routing or bridging with your Ascend product.
- Type of computer you are using.
- Description of the problem.

Calling Ascend from within the United States

In the U.S., you can take advantage of Priority Technical Assistance or an Ascend Advantage Pak service contract, or you can call to request assistance.

Priority Technical Assistance

If you need to talk to an engineer right away, call (900) 555-ASND (2763) to reach Ascend's Priority Call queue. The charge of \$2.95 per minute does not begin to accrue until you are connected to an engineer. Average wait times are less than three minutes.

Ascend Advantage Pak

Ascend Advantage Pak is a one-year service contract that includes overnight advance replacement of failed products, technical support, software maintenance releases, and software update releases. For more information, call (800) ASCEND-4 (272-3634), or access Ascend's Web site at www.ascend.com and select Services and Support, then Advantage Service Family.

Other telephone numbers

For a menu of Ascend's services, call (800) ASCEND-4 (272-3634). Or call (510) 769-6001 for an operator.

Calling Ascend from outside the United States

You can contact Ascend by telephone from outside the United States at one of the following numbers:

Telephone outside the United States	(510) 769-8027
Austria/Germany/Switzerland	(+33) 492 96 5672
Benelux	(+33) 492 96 5674
France	(+33) 492 96 5673
Italy	(+33) 492 96 5676
Japan	(+81) 3 5325 7397
Middle East/Africa	(+33) 492 96 5679
Scandinavia	(+33) 492 96 5677
Spain/Portugal	(+33) 492 96 5675
UK	(+33) 492 96 5671

For a list of support options in the Asia Pacific Region, you can find additional support resources at <http://apac.ascend.com>

Obtaining assistance through correspondence

Ascend maintains two email addresses for technical support questions. One is for customers in the United States, and the other is for customers in Europe, the Middle East, and Asia. If you prefer to correspond by fax, BBS, or regular mail, please direct your inquiry to Ascend's U.S. offices. Following are the ways in which you can reach Ascend Customer Service:

- Email from within the U.S.—support@ascend.com
- Email from Europe, the Middle East, or Asia—EMEAsupport@ascend.com
- Fax—(510) 814-2312
- Customer Support BBS (by modem)—(510) 814-2302
- Write to Ascend at the following address:

Attn: Customer Service
Ascend Communications, Inc.
One Ascend Plaza
1701 Harbor Bay Parkway
Alameda, CA 94502-3002

Finding information and software on the Internet

Visit Ascend's Web site at <http://www.ascend.com> for technical information, product information, and descriptions of available services.

Visit Ascend's FTP site at <ftp.ascend.com> for software upgrades, release notes, and addenda to this manual.

Contents

Ascend Customer Service	iii
-------------------------------	-----

About This Guide..... xvii

How to use this guide.....	xvii
What you should know	xvii
Documentation conventions.....	xviii
Related RFCs	xix
Information about PPP connections.....	xix
Information about IPX routing	xix
Information about IP routers.....	xix
Information about OSPF routing	xx
Information about multicast.....	xx
Information about packet filtering	xx
Information about general network security	xx
ITU-T recommendations.....	xx
Documentation set.....	xxi
Related publications	xxi

Chapter 1 **MAX System Administration..... 1-1**

Introduction	1-1
Activating administrative permissions.....	1-2
System administration parameters	1-2
Understanding the administrative parameters.....	1-3
Name.....	1-3
Location and Contact.....	1-3
Date and Time	1-3
Term rate and Console.....	1-3
Remote Mgmt	1-4
Dial-in and dial-out parameters	1-4
Log out parameters	1-4
DS0 minimum and maximum resets	1-4
High-bit-error parameters	1-4
No Trunks Alarm.....	1-4
Edit and Status	1-5
Finger requests (RFC 1288)	1-5
Configuring the basic parameters	1-5
Terminal-server command-line interface.....	1-6
Accessing the interface	1-6
Displaying terminal-server commands	1-6
Returning to the VT100 menus.....	1-7
Commands for monitoring networks	1-7
Commands for use by terminal-server users.....	1-8

SLIP, CSLIP, and PPP	1-8
Menu	1-8
Specifying raw TCP hosts	1-9
Telnet	1-10
Rlogin command.....	1-11
TCP	1-12
Open, Resume, and Close.....	1-13
Administrative commands	1-13
Test	1-13
Remote	1-15
Set	1-16
Show	1-17
Kill	1-23
Show DNIS session command	1-24
Show DNIS statistics command	1-24
Clear DNIS statistics	1-25

Chapter 2 VT100 Interface DO Commands 2-1

Using DO commands	2-1
List of supported commands.....	2-1
Example of using DO commands to place and clear a call	2-2
DO command reference in alphabetic order	2-3
Answer (DO 3).....	2-3
Beg/End BERT (DO 7).....	2-3
Beg/End Rem LB (DO 6)	2-4
Beg/End Rem Mgm (DO 8).....	2-5
Close Telnet (DO C)	2-6
Contract BW (DO 5).....	2-6
Diagnostics (DO D)	2-6
Dial (DO 1)	2-7
Esc (DO 0)	2-7
Extend BW (DO 4)	2-7
Hang Up (DO 2)	2-8
Load (DO L)	2-8
Menu Save (DO M)	2-8
Password (DO P)	2-9
Resynchronize (DO R).....	2-10
Save (DO S).....	2-10
Termserve (DO E)	2-10

Chapter 3 Diagnostic Commands and Parameters 3-1

Sys Diag commands	3-1
Restore Cfg	3-1
Save Cfg.....	3-2
Use MIF	3-2
Sys Reset.....	3-3
Term Serv	3-3
Upd Rem Cfg	3-3
T1 Line Diag commands.....	3-4
Line LB1	3-4
Line LB2	3-5

Switch D Chan	3-5
Clr Err1	3-5
Clr Perf1	3-5
Clr Err2	3-6
Clr Perf2.....	3-6
E1 Line Diag commands.....	3-6
Line LB1	3-6
Line LB2.....	3-7
BRI/LT Line Diag commands.....	3-7
Line LoopBack	3-8
Corrupt CRC	3-8
Uncorrupt CRC	3-9
Rq Corrupt CRC	3-9
Rq Uncorrupt CRC	3-9
Clr NEBE.....	3-9
Clr FEBE.....	3-9
Host/Dual (Host/6) Port Diag command.....	3-9
Modem Diag parameters.....	3-10
ModemSlot.....	3-10
Modem #N (where N=1–8, 1–12, 1-16).....	3-11

Chapter 4 VT100 Interface Status Windows..... 4-1

Using the MAX status windows	4-1
Navigating the status windows	4-2
Default status window displays	4-2
Line status windows	4-3
Session and system status windows.....	4-3
WAN and Ethernet status windows.....	4-4
Sys Option and Main Status Menu windows.....	4-4
Specifying which status windows appear	4-5
Status-window reference in alphabetic order.....	4-6
BRI/LT window	4-6
Call Status window	4-7
Call Detail Reporting (CDR) window	4-9
Dyn Stat window (dynamic status).....	4-10
Ether Opt window (Ethernet options).....	4-11
Ether Stat window (Ethernet status)	4-11
Ethernet window	4-12
FDL N Stats windows	4-12
Error-register statistics.....	4-13
Performance-register statistics.....	4-13
FR Stat window	4-14
Host/6 (Host/Dual) window.....	4-15
Line Errors window	4-15
Line Stat windows	4-16
Line Status (BRI) window	4-17
Message Log windows.....	4-19
AIM port message logs.....	4-19
System message logs	4-19
Log messages.....	4-20
Modem window	4-23
Net T1, Net E1 and Net BRI windows	4-25

Net Options window	4-25
Port Info window	4-26
Port Leads window	4-27
Port Opts window	4-28
PortN Stat window	4-29
Routes window	4-29
Serial WAN window.....	4-30
Session Err window	4-30
Sessions window.....	4-31
Statistics window	4-31
Syslog window.....	4-32
Level 4 and Level 6 syslog messages	4-33
Level 5 Syslog messages	4-33
Example	4-33
Disconnect codes and Progress codes	4-33
The backoff queue error message in the Syslog file.....	4-38
Syslog messages initiated by a SecureConnect Manger firewall	4-38
Sys Options window	4-40
System Status window	4-42
WAN Stat window	4-43

Chapter 5 **Network Administration 5-1**

Administering WAN lines and calls	5-1
T1 line diagnostics	5-1
E1 line diagnostics	5-2
BRI/LT diagnostics.....	5-2
Example of performing loopback diagnostics for IDSL	5-4
Performing port diagnostics.....	5-4
Disabling digital modems and modem slots	5-5
E1 ISDN call information	5-6
Incoming call routing state diagram	5-7
Managing IP routes and sessions	5-10
Working with the IP routing table	5-10
Displaying the routing table	5-10
Adding an IP route.....	5-12
Deleting an IP route	5-13
Displaying route statistics	5-13
Pinging other IP hosts	5-15
Configuring Finger support	5-16
Configuring the DNS Fallback Table	5-16
Displaying IP routing and related information	5-17
Displaying the ARP cache	5-17
Displaying ICMP packet statistics.....	5-18
Displaying interface statistics	5-18
Displaying IP statistics and addresses	5-20
Displaying UDP statistics and listen table.....	5-21
Displaying TCP statistics and connections.....	5-22
Displaying address pool status	5-22
Monitoring IPX routes and sessions	5-23
Verifying the transmission path to NetWare stations	5-23
Displaying IPX packet statistics	5-24
Displaying the IPX service table	5-24

Displaying the IPX routing table	5-25
Managing OSPF routes and sessions	5-25
Working with the routing table	5-25
Multipath routing	5-26
Third-party routing	5-27
How OSPF adds RIP routes.....	5-28
Route preferences	5-28
Displaying OSPF information	5-29
Displaying the size of the OSPF routing table	5-30
Displaying OSPF areas	5-31
Displaying general information about OSPF.....	5-31
Displaying information about OSPF interfaces.....	5-33
Displaying OSPF Link-State Advertisements (LSAs)	5-35
Displaying OSPF neighbor information	5-37
Displaying OSPF routers	5-37
Displaying OSPF External AS advertisements	5-38
Displaying the OSPF routing table	5-38
Displaying summarized OSPF database information	5-39
Managing multicast routing	5-40
Displaying the multicast forwarding table	5-40
Listing multicast clients	5-41
Displaying multicast activity	5-41
Monitoring Frame Relay connections	5-42
Displaying Frame Relay statistics.....	5-42
Displaying link management information	5-43
Displaying Data Link Connection Indicator (DLCI)status	5-43
Displaying circuit information.....	5-44
Turning off a circuit without disabling its endpoints.....	5-44
Monitoring X.25 and PAD connections.....	5-45
Displaying information about PAD sessions	5-45
Displaying information about X.25	5-45
Setting up ISDN D-channel X.25 support	5-47
PAD service signals.....	5-47
X.25 clear cause codes.....	5-47
X.25 diagnostic field values.....	5-48

Chapter 6 SNMP and Syslog Configuration..... 6-1

Configuring SNMP	6-1
Configuring SNMP access security	6-1
enabling SNMP Set commands	6-2
Setting community strings	6-2
Setting up and enforcing address security	6-2
Resetting the MAX and verifying reset	6-2
Example of SNMP security configuration.....	6-2
Setting SNMP traps	6-3
Understanding the SNMP trap parameters	6-3
Example SNMP trap configuration	6-4
Ascend enterprise traps	6-4
Alarm events	6-4
Port state change events.....	6-5
Security events.....	6-6
Supported MIBs	6-7

Configuring Syslog	6-7
Configuring the MAX to send Syslog messages	6-7
Syslog message format	6-8
Syslog messages and their meanings	6-8
Establishment of a call	6-8
Graceful disconnect of a call	6-9
Unexpected disconnect of a call	6-9
Additional messages	6-10
Disconnect codes and progress codes	6-12
Disconnect codes and their meanings	6-12
Progress codes and their meanings	6-15

Appendix A Troubleshooting..... A-1

Indicator lights	A-1
MAX front panel.....	A-1
MAX back panel.....	A-3
ISDN cause codes	A-4
Common problems and their solutions	A-14
General problems	A-14
Calls fail between AIM ports.....	A-14
DO menus do not allow most operations.....	A-14
POST takes more than 30 seconds to complete.....	A-14
Configuration problems	A-15
The MAX cannot dial out on a T1 or E1 line	A-15
Some channels do not connect.....	A-15
Data is corrupted on some international calls.....	A-15
Only the base channel connects.....	A-15
No Channel Avail error message.....	A-16
Restored configuration has incorrect RADIUS parameters.....	A-16
Hardware configuration problems	A-16
Cannot access the VT100 interface	A-16
Fault LED is off but no menus are displayed	A-16
Random characters appear in the VT100 interface.....	A-17
A Power-On Self Test fails.....	A-17
AIM-port interface problems	A-17
The MAX reports data errors on all calls	A-18
Calls cannot be made, answered, or cleared using control leads.....	A-18
The codec indicates that there is no connection	A-18
The codec does not receive data	A-18
The codec cannot establish a call when Data Transmit Ready (DTR) is active... ..	A-19
Calls initiated by control-lead toggling are cleared too soon	A-19
The codec cannot clear a call.....	A-19
ISDN PRI and BRI interface problems.....	A-20
Calls are not dialed or answered reliably.....	A-20
The Net/BRI lines do not dial or answer calls.....	A-20
No Logical Link status	A-21
WAN calling errors occur in outbound Net/BRI calls	A-21
ISDN PRI and BRI circuit-quality problems.....	A-21
Excessive data errors on calls to AIM ports	A-22
Excessive handshaking on calls to AIM ports.....	A-22
Inbound data is scrambled during an AIM Static call	A-22
Problems indicated by the LEDs	A-22

	LEDs are not lit for the secondary E1 or T1 line.....	A-22
	The E1 or T1 line is in a Red Alarm state	A-22
	A PRI line is in use and the Alarm LED blinks.....	A-23
	Problems in accessing the WAN	A-23
	Only some channels are dialed for AIM or BONDING calls.....	A-23
	The MAX never uses some channels	A-24
	An outgoing call using inband signaling fails to connect to the remote end.....	A-24
	Incoming call routing problems	A-24
	Call status drops back to IDLE.....	A-24
	Dual-port call status drops back to IDLE	A-25
	AIM or BONDING call status drops back to IDLE	A-25
	Bridge/router problems	A-25
	The link is of uncertain quality	A-25
	The MAX hangs up after answering an IP call	A-25
Appendix B	MAX Diagnostic Command Reference.....	B-1
	Using MAX diagnostic commands	B-1
	Command reference	B-2
	PPP decoding primer.....	B-38
	Breaking down the raw data	B-38
	Annotated Traces	B-39
	Example of a PPP connection attempt.....	B-39
	Example of MP+ call negotiation	B-41
	Relevant RFCs	B-43
Appendix C	Upgrading System Software	C-1
	Definitions and terms	C-2
	Guidelines for upgrading system software.....	C-3
	Guidelines for downgrading system software.....	C-4
	Before you begin.....	C-5
	Upgrading system software with a standard load	C-6
	Using TFTP to upgrade to a standard load	C-6
	Upgrading system software with a fat or thin load	C-7
	Recovering from a failed fat load upgrade	C-9
	Upgrading system software with an extended load	C-9
	Upgrading system software from versions earlier than 4.6C to version 5.0A or above	C-11
	Using the serial port to upgrade to a standard or a thin load	C-12
	Changing to system software that does not support V.90.....	C-15
	System messages.....	C-15
Appendix D	Machine Interface Format (MIF).....	D-1
	What is MIF?	D-1
	How to access MIF	D-2
	Use MIF command	D-2
	MIF escape sequence	D-2
	Transfer command	D-2
	MIF addresses	D-3
	MIF commands	D-5
	MIF responses.....	D-5
	Loading and saving entities	D-5

	Getting an entity's current value.....	D-6
	Getting the address and value of the next entity	D-6
	Modifying parameter values	D-7
	MIF traps and asynchronous reports.....	D-7
	Lexical sequence of MIF types	D-8
	Command line basics	D-31
	Editor basics	D-31
Appendix E	Example environments.....	E-1
	IP-routing environment	E-2
	MAX configuration.....	E-2
	Pipeline configuration	E-4
	IP-routing and AppleTalk-routing environment	E-6
	MAX configuration.....	E-7
	Pipeline configuration	E-9
	Index.....	Index-1

Figures

Figure Status windows	4-2
Figure IDSL connection with repeaters	5-4
Figure Example of a local DNS table	5-17

Tables

Table 2-1	DO commands	2-1
Table 4-1	Call-status characters and messages	4-7
Table 4-2	FDL performance registers	4-13
Table 4-3	T1/E1 link-status indicators	4-16
Table 4-4	T1 channel status indicators	4-17
Table 4-5	BRI line-status indicators	4-18
Table 4-6	B1 and B2 channel-status indicators	4-18
Table 4-7	Informational log messages	4-20
Table 4-8	Warning log messages	4-21
Table 4-9	Message indicators	4-23
Table 4-10	Modem-status characters	4-24
Table 4-11	Call-status characters for AIM ports	4-26
Table 4-12	RS-366 abbreviations	4-27
Table 4-13	Serial host port abbreviations	4-28
Table 4-14	Serial WAN port abbreviations	4-28
Table 4-15	Port Opts information	4-29
Table 4-16	Routes-window values	4-30
Table 4-17	Session status characters	4-31
Table 4-18	Ascend Disconnect codes	4-34
Table 4-19	Ascend Progress codes	4-37
Table 4-20	Syslog message fields for SecureConnect firewalls	4-39
Table 4-21	Sys Options information	4-41
Table 5-1	PAD service signals	5-47
Table 5-2	Clear cause codes	5-47
Table 5-3	X.25 diagnostic field values	5-48

About This Guide

How to use this guide

This guide explains how to configure and use the MAX as an Internet Service Provider (ISP) or telecommuting hub. Following is a chapter-by-chapter description of the topics:

- Chapter 1, “MAX System Administration,” explains how to administer and manage the MAX.
- Chapter 2, “VT100 Interface DO Commands,” describes each of the VT100 interface DO commands in alphabetic order.
- Chapter 3, “Diagnostic Commands and Parameters,” lists and explains the diagnostic commands provided for WAN lines and ports.
- Chapter 4, “VT100 Interface Status Windows,” describes status windows in alphabetic order.
- Chapter 5, “Network Administration,” discusses how to perform line diagnostic commands on T1, E1, and BRI lines, how to remove digital modems from service, and how to display call information. The chapter also discusses administering and managing TCP/IP, OSPF, multicast, IPX, Frame Relay, and X.25 networks.
- Chapter 6, “SNMP and Syslog Configuration,” explains how to configure SNMP and Syslog support.
- Appendix A, “Troubleshooting,” discusses common problems and offers possible solutions.
- Appendix B, “MAX Diagnostic Command Reference,” lists and explains the most helpful commands available from diagnostic mode on the MAX. The chapter includes a discussion of decoding Point-to-Point (PPP) packet traces.
- Appendix C, “Upgrading System Software,” explains how to upgrade the MAX system software.
- Appendix D, “Machine Interface Format (MIF),” discusses MIF concepts and lists all MIF commands.

This guide also includes an index.



What you should know

This guide is for the person who configures and maintains the MAX. To configure the MAX, you need to understand the following:

- Wide area network (WAN) concepts
- Local area network (LAN) concepts, if applicable

Documentation conventions

Following are all the special characters and typographical conventions used in this manual:

Convention	Meaning
Monospace text	Represents text that appears on your computer's screen, or that could appear on your computer's screen.
Boldface mono-space text	Represents characters that you enter exactly as shown (unless the characters are also in <i>italics</i> —see <i>Italics</i> , below). If you could enter the characters but are not specifically instructed to, they do not appear in boldface.
<i>Italics</i>	Represent variable information. Do not enter the words themselves in the command. Enter the information they represent. In ordinary text, italics are used for titles of publications, for some terms that would otherwise be in quotation marks, and to show emphasis.
[]	Square brackets indicate an optional argument you might add to a command. To include such an argument, type only the information inside the brackets. Do not type the brackets unless they appear in bold type.
	Separates command choices that are mutually exclusive.
>	Points to the next level in the path to a parameter or menu item. The item that follows the angle bracket is one of the options that appears when you select the item that precedes the angle bracket.
Key1-Key2	Represents a combination keystroke. To enter a combination keystroke, press the first key and hold it down while you press one or more other keys. Release all the keys at the same time. (For example, Ctrl-H means hold down the Control key and press the H key.)
Press Enter	Means press the Enter, or Return, key or its equivalent on your computer.
Note:	Introduces important additional information.
 Caution:	Warns that a failure to follow the recommended procedure could result in loss of data or damage to equipment.
 Warning:	Warns that a failure to take appropriate safety precautions could result in physical injury.

Note: In a menu-item path, include a space before and after each “>” character.

Related RFCs

RFCs are available on the Web at <http://ds.internic.net>

Information about PPP connections

For information about PPP connections and authentication, you might want to download one or more of the following:

- RFC 2153: *PPP Vendor Extensions*
- RFC 2125: *The PPP Bandwidth Allocation Control Protocol (BACP)*
- RFC 1994: *PPP Challenge Handshake Authentication Protocol (CHAP)*
- RFC 1990: *The PPP Multilink Protocol (MP)*
- RFC 1969: *The PPP DES Encryption Protocol (DESE)*
- RFC 1989: *PPP Link Quality Monitoring*
- RFC 1974: *PPP Stac LZS Compression Protocol*
- RFC 1962: *The PPP Compression Control Protocol (CCP)*
- RFC 1877: *PPP Internet Protocol Control Protocol Extensions for Name Server Addresses*
- RFC 1662: *PPP in HDLC-like Framing*
- RFC 1661: *The Point-to-Point Protocol (PPP)*
- RFC 1638: *PPP Bridging Control Protocol (BCP)*
- RFC 1332: *The PPP Internet Protocol Control Protocol (IPCP)*
- RFC 1552: *The PPP Internetwork Packet Exchange Control Protocol (IPXCP)*
- RFC 1378: *The PPP AppleTalk Control Protocol (ATCP)*

Information about IPX routing

- RFC 1634: *Novell IPX Over Various WAN Media (IPXWAN)*

Information about IP routers

RFCs that describe the operation of IP routers include:

- RFC 2030: *Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI*
- RFC 2002: *IP Mobility Support*
- RFC 1812: *Requirements for IP Version 4 Routers*
- RFC 1787: *Routing in a Multi-provider Internet*
- RFC 1519: *Classless Inter-Domain Routing (CIDR): An Address Assignment and Aggregation Strategy*
- RFC 1433: *Directed ARP*
- RFC 1393: *Traceroute Using an IP Option*
- RFC 1256: *ICMP Router Discovery Messages*

Information about OSPF routing

For information about OSPF routing, see:

- RFC 1850: *OSPF Version 2 Management Information Base*
- RFC 1587: *The OSPF NSSA Option*
- RFC 1586: *Guidelines for Running OSPF Over Frame Relay Networks*
- RFC 1583: *OSPF Version 2*
- RFC 1246: *Experience with the OSPF Protocol*
- RFC 1245: *OSPF protocol analysis*

Information about multicast

For information about multicast, see:

- RFC 1949: *Scalable Multicast Key Distribution*
- RFC 1584: *Multicast Extensions to OSPF*
- RFC 1458: *Requirements for Multicast Protocols*

Information about packet filtering

RFCs that describe firewalls and packet filters include:

- RFC 1858: *Security Considerations for IP Fragment Filtering*
- RFC 1579: *Firewall-Friendly FTP*

Information about general network security

RFCs pertinent to network security include:

- RFC 1704: *On Internet Authentication*
- RFC 1636: *Report of IAB Workshop on Security in the Internet Architecture*
- RFC 1281: *Guidelines for the Secure Operation of the Internet*
- RFC 1244: *Site Security Handbook*

ITU-T recommendations

ITU-T recommendations (formerly CCITT) are available commercially. You can order them at <http://www.itu.ch/publications/>

Documentation set

The MAX 4000 Series documentation set consists of the following manuals:

- *MAX 4000 Series Administration Guide*
- *MAX 4000 Series Hardware Installation Guide*
- *MAX 4000 Series Network Configuration Guide*
- *MAX Reference Guide*
- *MAX Security Supplement*
- *MAX RADIUS Configuration Guide*
- *MAX Glossary*

Related publications

This guide and documentation set do not provide a detailed explanation of products, architectures, or standards developed by other companies or organizations.

Following are some publications that you might find useful:

- *The Guide to T1 Networking*, William A. Flanagan.
- *Data Link Protocols*, Uyless Black
- *The Basics Book of ISDN*, Motorola University Press.
- *ISDN*, Gary C. Kessler
- *TCP/IP Illustrated*, W. Richard Stevens
- *Firewalls and Internet Security*, William R. Cheswick and Steven M. Bellovin

MAX System Administration

1

This chapter covers the following topics:

Introduction	1-1
Activating administrative permissions	1-2
System administration parameters	1-2
Terminal-server command-line interface	1-6

Introduction

The MAX unit's VT100 interface provides a wide variety of features for monitoring and administering the unit's activities.

The initial display of the VT100 interface shows the Main Edit Menu and a group of status windows. You configure several system administration parameters from the Main Edit Menu. The status windows display a variety of information about the operation of your MAX. You also have access to DO commands, which enable you to perform additional tasks. (To perform any of the administrative tasks, you must activate administrative permissions.)

Also, the VT100 interface provides access to the terminal-server command-line interface, which features a large assortment of powerful commands. For example, you can view the MAX unit's routing tables and statistical information. You can access detailed information about the unit's IP routing table, OSPF routing table, and Frame Relay connections. You can also use the administrative commands Ping, Traceroute, Telnet, and IPXping to establish and test connectivity. You can manually add, delete or change routes in your IP routing table. Descriptions of the commands available through the terminal-server command-line interface form the major part of this chapter.

Note: You can manage the MAX from your workstation by establishing a Telnet session and logging in with sufficient administrative privileges. You can also use Telnet to manage remote Ascend units, such as Pipeline or MAX units.

Activating administrative permissions

Before you can use the administrative commands and profiles, you must log in a superuser by activating a Security profile that has sufficient permissions (for example, the Full Access profile.) Proceed as follows:

- 1 Press Ctrl-D. The DO menu appears:

```
00-300 Security
DO...
>0=ESC
P=Password
```

- 2 Press P (or select P=Password).
- 3 In the list of Security profiles that opens, select Full Access.
The MAX prompts you for the Full Access password:

```
00-300 Security
Enter Password:
[ ]
```

Press > to accept

- 4 Type the password assigned to the profile, and press Enter. The default password for the Full Access login is Ascend .
When you enter the correct password, the MAX displays a message informing you that the password was accepted and that the MAX is using the new security level:

```
Message #119
Password accepted.
Using new security level.
```

If the password you enter is incorrect, the MAX prompts you again for the password.

Note: The first task you should perform after logging in as the superuser is to assign a new password to the Full Access profile.

System administration parameters

Following are the VT100 system administration parameters (shown with sample settings):

```
System
Sys Config
Name=gateway-1
Location=east-bay
Contact=thf
Date=2/20/97
Time=10:00:29
Term Rate=9600
Console=Standard
Remote Mgmt=Yes
Parallel Dial=5
Single Answer=Yes
Auto Logout=No
Idle Logout=0
DS0 Min Rst=Off
```



```
Max DS0 Mins=N/A
High BER=10 ** -3
High BER Alarm=No
No Trunk Alarm=No
Edit=00-000
Status 1=10-100
Status 2=10-200
Status 3=90-100
Status 4=00-200
Status 5=90-300
Status 6=90-400
Status 7=20-100
Status 8=20-200

Ethernet
  Mod Config
    Log...
      Syslog=Yes
      Log Host=10.65.212.12
      Log Port=514
      Log Facility=Local0
```

Understanding the administrative parameters

This section provides some background information about the administrative options. For more details about the parameters, see the *MAX Reference Guide*. For background information about additional parameters that appear in the System profile, see the *Network Configuration Guide* for your MAX.

Name

The Name parameter specifies the system name, which can consist of up to 16 characters. Keeping the name simple (no special characters) is a good idea because it is used in negotiating bridged PPP, AIM, and BONDING connections.

Location and Contact

The Location and Contact settings are SNMP readable and settable. The Location parameter should specify the unit's location, and the Contact parameter should specify the name of the person to contact concerning any problems with the unit. You can enter up to 80 characters.

Date and Time

The Date and Time parameters set the system date and time. If you are using Simple Network Time Protocol (SNTP), the MAX can maintain its date and time by accessing the SNTP server. (For details, see the *Network Configuration Guide* for your MAX.)

Term rate and Console

The Term Rate parameter specifies the transmission rate for communications with your terminal-emulation program. Any rate higher than 9600 can cause transmission errors.

The Console parameter lets you change the configuration interface, for example, (from Standard to MIF, for example, if you set it to MIF, the Machine Interface Format interface comes up when you power up the MAX. Limited brings up simplified menus for operation with the serial host ports (but not for bridging and routing). For details, see *Appendix D, "Machine Interface Format (MIF)."*

Also verify that the data rate of your terminal-emulation program is set to 9600 bps or lower.

Remote Mgmt

You can set Remote Mgmt to Yes to enable management of the MAX from a WAN link.

Dial-in and dial-out parameters

The Parallel Dial parameter specifies the number of channels that the MAX can dial simultaneously over the T1/PRI line, or that the MAX can disconnect simultaneously. Although you can specify any number of channels, the initial number of channels in a connection never exceeds the value of the Base Ch Count parameter (in the Connection profile).

The Single Answer parameter specifies whether the MAX completes the answering and routing of one call before answering and routing the next call.

Log out parameters

The Auto Logout parameter specifies whether to log out and go back to default privileges upon loss of DTR from the serial port. Idle Logout specifies the number of minutes an administrative login can remain inactive before the MAX logs out and hangs up.

DS0 minimum and maximum resets

A DS0 minute is the online usage of a single 56-Kbps or 64-Kbps switched channel for one minute. For example, a 5-minute, 6-channel call uses 30 DS0 minutes.

The DS0 Min Rst parameter specifies when the MAX should reset accumulated DS0 minutes to 0 (zero). You can also use this parameter to specify that the MAX should disable the timer altogether.

The Max DS0 Mins parameter specifies the maximum number of DS0 minutes a call can be online. When the usage exceeds the maximum specified by the Max DS0 Mins parameter, the MAX cannot place any more calls, and it takes any existing calls offline.

High-bit-error parameters

The High BER parameter specifies the maximum bit-error rate for any PRI line. The bit-error rate consists of the number of bit errors that occur per second. The number that comes after the double asterisks specifies the power of 10 for the current ratio of error bits to total bits.

The High BER Alarm parameter specifies whether the back-panel alarm relay closes when the bit-error rate exceeds the value specified by the High BER parameter.

No Trunks Alarm

The No Trunk Alarm parameter specifies whether the back-panel alarm relay closes when all T1/PRI lines (or trunks) go out of service.

Edit and Status

The Edit and Status parameters customize the status windows in the VT100 interface so that particular screens appear at startup. For details, see the *Reference Guide* for your MAX.

Finger requests (RFC 1288)

The MAX supports Finger remote user information protocol (RFC 1288). You can use Finger to get information about users currently logged into the MAX. The information includes the host address, name, port, and channel. For security reasons, the MAX does not forward Finger requests. For complete details of the Finger protocol, see RFC 1288.

Configuring the basic parameters

To configure the system name and other basic parameters in the System profile:

- 1 Open the System profile.
- 2 Specify a system name up to 16 characters long, enter the physical location of the MAX unit, and indicate a person to contact in case of problems. For example:

```
System
  Sys Config
    Name=gateway-1
    Location=east-bay
    Contact=thf
```

- 3 If necessary, set the system date and time.

```
Date=2/20/97
Time=10:00:29
```
- 4 Specify the data transfer rate of the MAX control port.

```
Term Rate=9600
```
- 5 Close the System profile.

Terminal-server command-line interface

The terminal-server command-line interface can provide commands for monitoring networks, initiating sessions, and administering the system.

Accessing the interface

You can start a terminal-server command-line session if you have administrative privileges. (For more information, see “Activating administrative permissions” on page 1-2). You can start a session using one of the following methods:

- From the main VT100 menu, select System > Sys Diag > Term Serv, and press Enter.
- In the Main Edit Menu, press Ctrl-D to open the DO menu, and select E=Termsrv.
- Enter the following keystroke sequence (Escape key, left bracket, Escape key, zero) in rapid succession:

```
Esc [ Esc 0
```

If you have sufficient privileges to invoke the command line, the MAX displays a command-line prompt. For example:

```
** Ascend Terminal Server **
ascend%
```

Note: If you have a MAX running Multiband simulation, the following terminal server commands are disabled: Close, Ipxping, Open, Resume, Rlogin, Telnet.

Displaying terminal-server commands

To display the list of terminal-server commands, enter a question mark:

```
ascend% ?
```

or the Help command:

```
ascend% help
```

The system responds by listing the terminal-server commands, with brief explanations:

?	Displays help information
help	Displays help information
quit	Closes terminal server session
hangup	Closes terminal server session
test	test <number> frame-count.] [<optional fields>]
local	Go to local mode
remote	remote <station>
set	Set various items. Type ‘set ?’ for help
show	Show various tables. Type ‘show ?’ for help

<code>clear dnis statistics</code>	Clears DNIS session statistics
<code>iproute</code>	Manage IP routes. Type 'iproute ?' for help
<code>dnstab</code>	Displays help information about the DNS table. Type 'dnstab ?' for help
<code>slip</code>	SLIP command
<code>cslip</code>	Compressed SLIP command
<code>ppp</code>	PPP command
<code>menu</code>	Host menu interface
<code>telnet</code>	telnet [-a -b -t] <host-name> [<port-number>]
<code>tcp</code>	tcp <host-name> <port-number>
<code>ping</code>	ping <host-name>
<code>ipxping</code>	ipxping <host-name>
<code>tracert</code>	Trace route to host. Type 'tracert -?' for help
<code>rlogin</code>	rlogin [-l user -ec] <host-name> [-l user]
<code>open</code>	open < modem-number slot:modem-on-slot >
<code>resume</code>	resume virtual connect session
<code>close</code>	close virtual connect session
<code>kill</code>	terminate session

Returning to the VT100 menus

The following commands close the terminal-server command-line interface and return the cursor to the VT100 menus:

<code>quit</code>	Closes terminal server session
<code>hangup</code>	Closes terminal server session
<code>local</code>	Go to local mode

For example:

```
ascend% quit
```

When a dial-in user enters the Local command, a Telnet session begins.

Commands for monitoring networks

The following commands are specific to IP or IPX routing connections:

<code>iproute</code>	Manage IP routes. Type 'iproute ?' for help
<code>ping</code>	ping <host-name>
<code>ipxping</code>	ipxping <host-name>
<code>tracert</code>	Trace route to host. Type 'tracert -?' for help

For details about each of the commands, see Chapter 5, “Network Administration.”

Commands for use by terminal-server users

The following commands must be enabled for use in Ethernet > Mod Config > TServ Options. If they are enabled, login users can initiate a session by invoking the commands in the terminal- server interface.

slip	SLIP command
cslip	Compressed SLIP command
ppp	PPP command
menu	Host menu interface
telnet	telnet [-a -b -t] <host-name> [<port-number>]
rlogin	rlogin [-l user -ec] <host-name> [-l user]
tcp	tcp <hostname> <port-number>
open	open < modem-number slot:modem-on-slot >
resume	resume virtual connect session
close	close virtual connect session

These commands initiate a session with a host or modem, or toggle to a different interface that displays a menu selection of Telnet hosts.

SLIP, CSLIP, and PPP

The SLIP, CSLIP, and PPP commands initiate Serial Line IP, Compressed SLIP, and PPP sessions, respectively, from the terminal-server command line.

Menu

The Menu command invokes the terminal server’s menu mode, which lists up to four hosts. The four hosts can be either Telnet hosts, raw TCP hosts or a mixture of the two types.

Specifying Telnet hosts

The Menu command invokes the terminal server’s menu mode, which lists up to four Telnet hosts as configured in the Ethernet > Mod Config > TServ Options subprofile. For example:

```
Up to 16 lines of up to 80 characters each
will be accepted. Long lines will be truncated.
Additional lines will be ignored

1. host1.abc.com
2. host2.abc.com
3. host3.abc.com
4. host4.abc.com
Enter Selection (1-4, q)
```

This menu was configured in the Tserv Options menu by setting the Host #N Addr and Host #N Text parameters to specify the IP addresses and menu names, respectively, of the four hosts. For example, Host # 1 Addr specifies the IP address of Host1, and Host #1 Text is set to host.abc.com.

To return to the command-line, press 0. Terminal server security must be set up to allow the operator to toggle between the command line and menu mode, or the Menu command has no effect. Enable this function by setting the Toggle Scrn parameter (Ethernet > Mod Config > Tserv Options) to Yes. (For more information on this parameter, see the *MAX Reference Guide*.)

Specifying raw TCP hosts

To specify IP addresses or DNS names of hosts to which you establish a raw TCP connection, proceed as follows:

- 1 Open the Ethernet > Mod Config > TServ options menu.
- 2 Select one of the Host # Addr fields and enter the following:

rawTcp host portnumber

rawTcp is the required string that causes the MAX to establish a raw TCP connection when the user chooses this host number. This entry is case-sensitive and must be entered exactly as shown.

host can be the DNS name of the host or the IP address of the host. The total number of characters, including all three strings and the delimiting spaces, must not exceed 31.

portnumber is the number of the port on which the connection for this host is to be established.

- 3 Enter a description of the host in the Host # Text field.

Note: You cannot configure raw TCP hosts if you are using a RADIUS server to provide the list of hosts.

Example of configuration combining Telnet hosts and raw TCP hosts

Suppose you specify the following values in the TServ Options menu:

```
Remote Conf=No
Host #1 Addr=10.10.10.1
Host #1 Text=Cleveland
Host #2 Addr=
Host #2 Text=
Host #3 Addr=
Host #3 Text=
Host #4 Addr=rawTcp corp-host 7
Host #4 Text=The Office - port 7
Immed Service=None
Immed Host=N/A
Immed Port=N/A
Telnet Host Auth=No
```

If you then execute the Menu command, the following menu appears:

```
** Ascend Pipeline Terminal Server **

1. Cleveland
2. The Office - port 7

Enter Selection (1-2,q)
```

If you select 2, the MAX establishes raw a CP connection on port 7 to the host named `corp-host`.

If a you select 1, the MAX establishes a Telnet connection on port 23, the default Telnet port, to the host address 10.10.10.1.

Telnet

The Telnet command initiates a login session to a remote host. It uses the following format:

where **telnet** [-a|-b|-t] **hostname** [**port-number**]

- **-a** | **-b** | **-t** are optional arguments specifying ASCII, Binary, or Transparent mode, respectively. If one of the arguments is entered, it overrides the setting of the Telnet Mode parameter.

In ASCII mode, the MAX uses standard 7-bit mode. In Binary mode, the MAX tries to negotiate 8-bit mode with the server at the remote end of the connection, so that the user can send and receive binary files by means of 8-bit file transfer protocols. In transparent mode, either of the other modes can be used without specifying the mode.

- **hostname** can be the remote system's DNS name if you have configured DNS. If you have not, you must specify the IP address of the remote system.
- **port-number** is an optional argument specifying the port to use for the session. The default is 23, which is the port number of the well-known port for Telnet.

For example, if your DNS table has an entry for `myhost`, you can open a telnet session with that host as follows:

```
ascend% telnet myhost
```

If you do not configure DNS, you must specify the host's IP address instead. There are also several options in the Ethernet > Mod Config > TServ Options subprofile that affect Telnet; for example, if you set Def Telnet to Yes, you can just type a hostname to open a Telnet session with that host:

```
ascend% myhost
```

Another way to open a session is to invoke Telnet first, then enter the Open command at the Telnet prompt. For example:

```
ascend% telnet
telnet> open myhost
```

When your screen displays the `telnet>` prompt, you can enter any of the Telnet commands described in "Telnet session commands" on page 1-11. You can quit the Telnet session at any time by entering the Quit command at the Telnet prompt:

```
telnet> quit
```

Note: During an open Telnet connection, press Ctrl-] to display the `telnet>` prompt and the Telnet command-line interface. Any valid Telnet command returns you to the open session. Note that Ctrl-] does not function in binary mode Telnet. If you log into the MAX by Telnet, you might want to change the escape sequence from Ctrl-] to a different setting.

Telnet session commands

The commands in this section can be entered at the Telnet prompt during an open session. To display the Telnet prompt while logged in to a host, press Ctrl-] (hold down the Control key and type a right bracket). To display information about Telnet session commands, use the Help or ? command. For example:

```
telnet> ?
```

To open a Telnet connection after invoking Telnet, use the Open command. For example:

```
telnet> open myhost
```

To send standard Telnet commands such as Are You There or Suspend Process, use the Send command. For example:

```
telnet> send susp
```

For a list of Send commands and their syntax, enter the Send command with a question mark:

```
telnet> send ?
```

To specify special characters for use during the Telnet session, use the Set command. For example:

```
telnet> set eof ^D
```

To display current settings, enter the Set All command:

```
telnet> set all
```

To display a list of Set commands, enter the Set command with a question mark:

```
telnet> set ?
```

To quit the Telnet session and close the connection, enter the Close or Quit command. For example:

```
telnet> close
```

Telnet error messages

The MAX generates an error message for any condition that causes the Telnet session to fail or terminate abnormally. The following error messages can appear:

- no connection: host reset—The destination host reset the connection.
- no connection: host unreachable—The destination host is unreachable.
- no connection: net unreachable—The destination network is unreachable.
- Unit busy. Try again later.—The host already has open the maximum number of concurrent Telnet sessions.

Rlogin command

The Rlogin command initiates a login session to a remote host. The command has the following format:

```
rlogin [-echar] hostname [-lusername]
```

where:

- **-echar** sets the escape character to *char*. For example:

```
rlogin -e$ 10.2.3.4
```

The default escape character is a tilde (~).
- **hostname** can be the remote system's DNS name if you have configured DNS. If you have not, you must specify the IP address of the remote system.
- **-lusername** specifies that you log into the remote host as **username**, rather than as the name with which you logged into the terminal server. (If you logged in through RADIUS or TACACS, you must be prompted for this option.) If you can specify this option on the command line, you can enter it either before or after the hostname argument. For example, the following two lines perform identical functions:

```
rlogin -l jim 10.2.3.4  
rlogin 10.2.3.4 -l jim
```

To terminate the remote login, choose the Exit command at the remote system's prompt. Or, you can press the Enter key, then type the escape character followed by a period.

<CR><ESC-CHAR><PERIOD>

For example, to terminate a remote login that was initiated with the default escape character (a tilde), press the Enter key, then the ~ key, then the . key.

~.

TCP

The TCP command initiates a login session to a remote host. The command has the following format:

tcp hostname [port-number]

where:

- **hostname** can be the remote system's DNS name if you have configured DNS. If you have not, you must specify the IP address of the remote system.
- **port-number** specifies the port to use for the session. The port number typically indicates a custom application that runs on top of the TCP session. For example, port number 23 starts a Telnet session. However, terminating the Telnet session does not terminate the raw TCP session.

When the raw TCP session starts running, the MAX displays the word *connected*. You can then use the TCP session to transport data by running an application on top of TCP. You can hang up the device at either end to terminate the raw TCP session. If you are using a remote terminal-server session, ending the connection also terminates raw TCP.

If a raw TCP connection fails, the MAX returns one of the following error messages:

- `Cannot open session: hostname port-number`—You entered an invalid or unknown value for *hostname*, you entered an invalid value for *port-number*, or a port number was required and you failed to enter it.
- `no connection: host reset`—The destination host reset the connection.
- `no connection: host unreachable`—The destination host is unreachable.
- `no connection: net unreachable`—The destination network is unreachable.

Open, Resume, and Close

If the MAX has digital modems installed and Modem Dialout is enabled in the TServ Options submenu, a local user can issue AT commands to the modem as if connected locally to the modem's asynchronous port. To set up a virtual connection to a modem, enter the Open command. Use the following format:

```
open [modem number | slot:modemOnSlot]
```

For example:

```
ascend% open 7:1
```

If you are unsure which slot or item number to specify, the Show Modems command displays the possible choices. If you enter the Open command without specifying any of the optional arguments, the MAX opens a virtual connection to the first available modem.

Once you have connected to the modem, you can issue AT commands to the modem and receive responses from it.

You can temporarily suspend a virtual connection by pressing Ctrl-C three times. This control sequence causes the MAX to display the terminal-server interface again. To resume a virtual connection suspended with Ctrl-C, can enter the Resume command at the terminal-server prompt:

```
ascend% resume
```

To terminate a virtual connection, enter the Close command at the terminal-server prompt:

```
ascend% close
```

Administrative commands

The following commands (shown as they appear in the Help display) are useful for system administration:

```
test      test <number> frame-count> ] [ <optional fields> ]
remote    remote <station>
set        Set various items. Type 'set ?' for help
show      Show various tables. Type 'show ?' for help
kill       terminate session
```

Test

The MAX can use two open channels to run a self-test in which it calls itself, by placing the call on one channel and receiving it on the other channel. To run the test, execute the TEST command which has the following format:

test phonenumber [frame-count] [optional fields]

where **phonenumber** is the phone number of the channel receiving the test call. This can include the numbers 0 through 9 and the characters ()[]-, but cannot include spaces.

[frame-count] The optional frame-count argument is a number from 1 to 65535 specifying the number of frames to send during the test. The default is 100. The

optional fields are the following:

- **[data-svc=data-svc]**
where data-svc, is a data service identical to any of the values available for the Data Svc parameter of the Connection profile. (For a list of valid values, see the *Reference Guide* for your MAX.) If you do not specify a value, the default value is the one specified for the Data Svc parameter.
- **[call-by-call=T1-PRI-service]**
where T1-PRI-service, is any value available to the Call-by-Call parameter of the Connection profile. The Call-by-Call parameter specifies the PRI service that the MAX uses when placing a PPP call. (For a list of valid values, see the *Reference Guide* for your MAX.) If you do not specify a value, the default is as specified for the Call-by-Call parameter.
- **[primary-number-type=AT&T-switch]**
where AT&T-switch, is any value available to the PRI # Type parameter of the Connection profile. The PRI # Type parameter specifies an AT&T switch. (For a list of valid values, see the *Reference Guide* for your MAX.) If you do not specify a value, the default value is the one specified for the PRI # Type parameter.
- **[transit-number=IEC]**
where IEC, is any value available to the Transit # parameter of the Connection profile. The Transit # parameter specifies the U.S. Interexchange Carrier (IEC) you use for long distance calls over a PRI line. (For a list of valid values, see the *Reference Guide* for your MAX.) If you do not specify a value, the default is as specified for the Transit # parameter.

Here is a simple example of entering the Test command:

```
ascend% test 555-1212
```

You can press Ctrl-C at any time to terminate the test. While the test is running, the MAX displays the status. For example:

```
calling...answering...testing...end
200 packets sent, 200 packets received
```

If you enable trunk groups on the MAX, you can specify the outgoing lines to be used in the self-test. If you do not, the MAX uses the first available T1 (or E1) line. For example, if you assign trunk group 7 to line 1 on a Net/BRI module, and your PBX requires a preceding 9 is for an outgoing call, the following command places the outgoing call on line 1 of the Net/BRI module:

```
ascend% test 7-9-555-1212
```

The MAX generates an error message for any condition that causes the test to terminate before sending the full number of packets. The following error messages can appear:

Message	Explanation
bad digits in phone number	The phone number you specified contained a character other than the numbers 0 through 9 and the characters () [] -
call failed	The MAX did not answer the outgoing call. Can indicate a wrong phone number or a busy phone number. Use the Show ISDN command to determine the nature of the failure
call terminated <i>N1</i> packets sent <i>N2</i> packets received	This message indicates the number of packets sent (<i>N1</i>) and received (<i>N2</i>).
cannot handshake	The MAX answered the outgoing call, but the two sides did not properly identify themselves. Can indicate that the call was routed to the wrong MAX module, or that the phone number was incorrect.
frame-count must be in the range 1-65535	The number of frames requested exceeded 65535.
no phone number	You did not specify a phone number on the command line.
test aborted	The test was terminated (Ctrl-C).
unit busy	You attempted to start another self-test when one was already in progress. You can run only one self-test at a time.
unknown items on command-line	The command line contained unknown items. Inserting one or more spaces in the telephone number can generate this error.
unknown option <i>option</i>	The command-line contained the option specified by <i>option</i> , which is invalid.
unknown value <i>value</i>	The command-line contained the value specified by <i>value</i> , which is invalid
wrong phone number	A device other than the MAX answered the call. Therefore, the phone number you specified was incorrect

Remote

After an MP+ connection has been established with a remote station (for example, by using the DO Dial command), you can start a remote management session with that station by entering the Remote command in the following format:

remote *station*

For example:

```
ascend% remote lab17gw
```

During the remote management session, the user interface of the remote device replaces your local user interface, as if you had opened a Telnet connection to the device. You can enter Ctrl-\

at any time to terminate the Remote session. Note that either end of an MP+ link can terminate the session by hanging up all channels of the connection.

The argument to the Remote command is the name of the remote station. It must match the value of a Station parameter in a Connection profile that allows outgoing MP+ calls, or the user-id at the start of a RADIUS profile set up for outgoing calls.

Note: A remote management session can time out because the traffic it generates does not reset the idle timer. Therefore, the Idle parameter in the Connection profile at both the calling and answering ends of the connection should be disabled during a remote management session, and restored just before exiting. Remote management works best at higher terminal speeds.

At the beginning of a remote management session, you have privileges set by the default Security profile at the remote end of the connection. To activate administrative privileges on the remote station, activate the appropriate remote Security profile by using the DO Password command (as described in “Activating administrative permissions” on page 1-2).

The MAX generates an error message for any condition that causes the test to terminate before sending the full number of packets. The following error messages can appear:

Message	Explanation
not authorized	Your current security privileges are insufficient for beginning a remote management session. To assign yourself the required privileges, log in with the DO PASSWORD command to a Security profile whose Edit System parameter is set to Yes.
cannot find profile for <station>	The MAX could not locate a local Connection profile containing a Station parameter whose value matched <station>.
profile for <station> does not specify MPP	The local Connection profile containing a Station value equal to <station> did not contain Encaps=MPP.
cannot establish connection for <station>	The MAX located a local Connection profile containing the proper Station and Encaps settings, but it could not complete the connection to the remote station.
<station> did not negotiate MPP	The remote station did not negotiate an MP+ connection. This error occurs most often when the remote station does not support MP+, but does support PPP.
far end does not support remote management	The remote station is running a version of MP+ that does not support remote management.
management session failed	A temporary condition, such as premature termination of the connection, caused the management session to fail.
far end rejected session	The remote station was configured to reject remote management; its Remote Mgmt parameter was set to No in the System profile.

Set

The Set command takes several arguments. To display them, enter the Set command with a question mark:

```
ascend% set ?
set ?          Display help information
set all        Display current settings
set term       Sets the telnet/rlogin terminal type
set password   Enable dynamic password serving
set fr         Frame Relay datalink control
set circuit    Frame Relay Circuit control
```

The Set All command displays current settings. For example:

```
ascend% set all
term = vt100
dynamic password serving = disabled
```

To specify a terminal type other than VT100, use the Set Term command.

The Set Password command puts the terminal server in password mode, in which a third-party ACE or SAFWORD server at a secure site can display password challenges dynamically in the terminal-server interface. When the terminal server is in password mode, it passively waits for password challenges from a remote ACE or SAFWORD server. The Set Password command applies only when using security card authentication. Enter the command as follows:

```
ascend% set password
Entering Password Mode...

[^C to exit] Password Mode>
```

To return to normal terminal-server operations and thereby disable password mode, press Ctrl-C.

Note that each channel of a connection to a secure site requires a separate password challenge, so for multichannel connections to a secure site, you must leave the terminal server in password mode until all channels have been established. The APP Server utility provides an alternative way to allow users to respond to dynamic password challenges obtained from hand-held security cards. For details about dynamic password serving, see the *MAX Security Supplement*.

The Set FR commands enable you to bring down the nailed connection specified in the named Frame Relay profile. The connection reestablished within a few seconds. The Set Circuit commands let you activate or deactivate a Frame Relay circuit. For details, see the *Network Configuration Guide* for your MAX.

Show

The Show command takes several arguments. To display them, enter the Show command with a question mark:

ascend% **show ?**

show ?	Display help information
show arp	Display the arp cache
show icmp	Display ICMP information
show if	Display Interface info. Type 'show if ?' for help
show ip	Display IP information. Type 'show ip ?' for help
show udp	Display UDP information. Type 'show udp ?' for help
show igmp	Display IGMP information. Type 'show igmp ?' for help
show mrouting	Display MROUTING information. Type 'show mrouting ? f ?'
show ospf	Display OSPF information. Type 'show ospf ?' for help.
show tcp	Display TCP information. Type 'show tcp ?' for help
show dnstab	Display local DNS table. Type 'show dnstab ?' for help
show netware	Display IPX information. Type 'show netware ? ' for help
show isdn	Display ISDN events. Type 'show isdn <line number>' for help
show fr	Display Frame relay info. Type 'show fr ?' for help
show pools	Display the assign address pools
show modems	Display status of all modems
show calls	Display status of calls
show pad	Display X25/PAD information
show uptime	Display system uptime
show revision	Display system revision
show v.110s	Display status of all v.110 cards
show users	Display concise list of active users
show x25	Display status of X.25 stack
show dnis session	Display active DNIS sessions
show dnis statistics	Display DNIS statistics

Note: Many of the Show commands are specific to a particular type of usage, such as, IP routing or OSPF. The chapters of this guide that relate to these types of connection and routing describe the relevant Show commands.

Show commands related to network information

The following Show commands are related to monitoring protocols and other network-specific information and are discussed in Chapter 5, “Network Administration”:


```
show arp
show icmp
show if
show ip
show udp
show igmp
show mrouting
show ospf
show tcp
show dnstab
show netware
show fr
show pools
show pad
show x25
```

Show ISDN

The Show ISDN command enables the MAX to display the last 20 events that have occurred on the specified ISDN line. Enter the command in the following format:

```
show isdn line-number
```

where **line-number** is the number of the ISDN line. (For details about how lines are numbered, see the *Network Configuration Guide* for your MAX.) For example, to display information about the leftmost built-in WAN port, you would enter the following command:

```
ascend% show isdn 0
```

The MAX responds with one or more of the following messages:

```
PH: ACTIVATED
PH: DEACTIVATED
DL: TEI ASSIGNED (BRI interfaces only)
DL: TEI REMOVED (BRI interfaces only)
NL: CALL REQUEST
NL: CLEAR REQUEST
NL: ANSWER REQUEST
NL: CALL CONNECTED
NL: CALL FAILED/T303 EXPIRY
NL: CALL CLEARED/L1 CHANGE
NL: CALL REJECTED/OTHER DEST
NL: CALL REJECTED/BAD CALL REF
NL: CALL REJECTED/NO VOICE CALLS
NL: CALL REJECTED/INVALID CONTENTS
NL: CALL REJECTED/BAD CHANNEL ID
NL: CALL FAILED/BAD PROGRESS IE
NL: CALL CLEARED WITH CAUSE
```

In some cases, the message can include a phone number (prefixed by #), a data service (suffixed by K for Kbps), a channel number, TEI assignment, and cause code. For example, the following information might appear:

```
PH: ACTIVATED
NL: CALL REQUEST: 64K, #442
NL: CALL CONNECTED: B2, #442
```

```
NL: CLEAR REQUEST: B1
NL: CALL CLEARED WITH CAUSE 16 B1 #442
```

For information about each of the messages that can appear, see the CCITT Blue Book Q.931 or other ISDN specifications.

Show Modems

To display the status of the MAX unit's digital modems, enter the Show Modems command. For example, the following output is from a MAX with a V.34 modem slot card in slot 8:

```
ascend% show modems

slot:item    modem    status
8:1          1        online
8:2          2        online
8:3          3        online
8:4          4        idle
8:5          5        idle
8:6          6        idle
8:7          7        idle
8:8          8        idle
```

For 8-MOD and 12-MOD K56Flex modem slot cards, the numbering is not sequential, but the numbering does not affect functionality. For example, if you have an 8-MOD modem card in slot 8 in a MAX, the Show Modems command in the terminal-server displays the following output:

```
ascend% show modems

slot:item    modem    status
8:0          1        idle
8:1          2        idle
8:2          3        idle
8:3          4        idle
8:6          5        idle
8:7          6        idle
8:10         7        idle
8:11         8        idle
```

As another example, if you have a 12-MOD modem card in slot 8 in a MAX, the Show Modems command in the terminal-server displays the following output:

```
ascend% show modems

slot:item    modem    status
8:0          1        idle
8:1          2        idle
8:2          3        idle
8:3          4        idle
8:4          5        idle
8:5          6        idle
8:6          7        idle
8:7          8        idle
8:8          9        idle
8:9          10       idle
8:12         11       idle
8:13         12       idle
```

Following are descriptions of the output contains these fields:

Field	Description
slot item	The slot and port number of the modem. For example, 8:1 indicates the first port on the digital modem card installed in slot 8.
modem	The SNMP interface number of each modem.
status	Modem status, which can be one of the following strings: <ul style="list-style-type: none">– <code>idle</code>—The modem is not in use.– <code>awaiting DCD</code>—The call is up and waiting for DCD.– <code>awaiting codes</code>—DCD is up, and the call is waiting for modem result codes.– <code>online</code>—The call is up. The modem can now send and receive data.– <code>initializing</code>—The modem is being reset.

Show Calls

The Show Calls command displays information about active calls on a German ITR6 or Japanese NTT switch type. For example:

```
ascend% show calls

Call ID   Called Party ID   Calling Party ID   InOctets   OutOctets
3         5104563434        4191234567         0          0
4         4197654321        5108888888         888888    99999
```

The output includes the following fields:

Field	Description
CallID	An identifier for the call
CalledPartyID	The telephone number of the answering device (that is, this unit). This ID is obtained from layer 3 protocol messages during call setup.
CallingPartyID	The telephone number of the caller. This ID is obtained from layer 3 protocol messages during call setup.
InOctets	The total number of octets received by the user from the moment the call begins until it is cleared.
OutOctets	The total number of octets sent by the user from the moment the call begins until it is cleared.

Show Uptime

To see how long the MAX has been running, enter the Show Uptime command. For example:

```
ascend% show uptime

system uptime: up 2 days, 4 hours, 38 minutes, 43 seconds
```

If the MAX stays up for 1000 consecutive days with no power cycles, the number of days displayed resets to 0 and begins to increment again.

Show Revision

The Show Revision command displays the software load and version number currently running on the MAX. For example:

```
ascend% show revision
techpubs-lab-17 system revision: ebiom.m40 5.0A
```

Show V.110s

To display the status of the MAX unit's V.110 cards, enter the Show V.110s command:

```
ascend% show v.110s

slot:item    v.110s    status
4:1          1      in use
4:2          2      in use
4:3          3      in use
4:4          4      open issued
4:5          5      carrier detected
4:6          6      session closed
4:7          7      idle
4:8          8      in use
```

The output includes the following fields:

Field	Description
slot item	The slot and port number of the V.110 port. For example, 8:1 indicates the first port on the V.110 card installed in slot 8.
v.110s	The SNMP interface number of each V.110 card.
status	V.110 port status, which can be one of the following strings: <ul style="list-style-type: none">idle—The V.110 port is not in use.open issued—An open was issued, but the MAX has not synced up with the far end.carrier detected—A carrier was detected from the remote end.in use—A V.110 session is up.

Show Users

To display the number of active sessions, enter the Show Users command. For example:

```
ascend% show users

I Session      Line: Slot: Tx   Rx   Service      Host      User
O ID           Chan  Port  Data  Rate  Type[mpID]  Address   Name
O 231849873    1:1   9:1   56K   56K   MPP[1]      10.10.68.2  jdoe
I 231849874    1:3   3:1   28800 33600 Termsrv      N/A        Modem 3:1
O 214933581    1:2   9:2   56K   56K   MPP[1]      10.10.4.9  arwp50
```

```
O 214933582 1:6 9:3 56K 56K MPP[1] MPP Bundle arwp50
```

The output includes the following fields:

Field	Content
IO	I for an incoming call or O for an outgoing call
Session ID	Unique session-ID. This is the same as Acct-Session-ID in RADIUS.
Line:Chan	Line and channel on which the session is established.
Slot: Port	Slot and port of the service being used by the session. Can indicate the number of a slot containing a modem card, and the modem on that card. Or can indicate the virtual slot of the MAX unit's bridge/router, with the port indicator showing the virtual interfaces to bridge/router starting with 1 for the first session of a multichannel session.
Tx Data	Transmit data rate in bits per second.
Rx Rate	Receive data rate in bits per second.
Service Type	Type of session, which can be Termsrv or a protocol name. For MP and MPP (MPT), shows the bundle ID shared by the calls in a multichannel session. The special values <i>Initial</i> and <i>Login</i> document the progress of a session. <i>Initial</i> identifies sessions that do not yet have a protocol assigned. <i>Login</i> identifies Termsrv sessions during the login process.
Host Address	Network address of the host originating the session. For some sessions this field is N/A. For outgoing MPP sessions only, the first connection has a valid network address associated with it. All other connections in the bundle have the network address listed as <i>MPP Bundle</i> .
User Name	The station name associated with the session. Initially, the value is <i>Answer</i> , which is usually replaced with the name of the remote host. For terminal-server sessions User Name is the login name. Before completion of login, the field contains the string <i>modem x:y</i> where <i>x</i> and <i>y</i> are the slot and port, respectively, of the modem servicing the session.

Kill

The Kill command enables you to disconnect a user who establishes a Telnet connection to the MAX. You can disconnect the user by specifying the session ID. The resulting disconnect code is identical to the RADIUS disconnect code, allowing you to track all administrative disconnects. To terminate a Telnet session, enter the command as follows:

```
kill session ID
```

where *session ID* is the session ID as displayed by the Show Users command described in the preceding section. The reported disconnect cause is *DIS_LOCAL_ADMIN*. The active Security profile must have Edit All Calls set to Yes. If Edit All Calls=No, the following message appears when you enter the Kill command:

```
Insufficient security level for that operation.
```

When the session is properly terminated, a message similar to the following appears:

```
Session 216747095 killed.
```

When the session is not terminated, a caution similar to the following appears:

```
Unable to kill session 216747095.
```

Show DNIS session command

To display active DNIS sessions, enter the Show DNIS Session command:

```
ascend% show dnis session
```

	GLOBAL	MODEM	HDLC	V110
DNIS#	Used/Max	Used/Max	Used/Max	Used/Max
0. Unspecified	0/999	0/1	0/0	0/0
1. 68149	0/123	0/456	0/1	0/0
2. 8867764	0/1	0/1	0/1	0/1
3. 45566778800	0/0	0/0	0/0	0/0
4.	0/0	0/0	0/0	0/0
5.	0/0	0/0	0/0	0/0
6.	0/0	0/0	0/0	0/0
7.	0/0	0/0	0/0	0/0
8.	0/0	0/0	0/0	0/0
9.	0/0	0/0	0/0	0/0
10.	0/0	0/0	0/0	0/0
11.	0/0	0/0	0/0	0/0
12.	0/0	0/0	0/0	0/0
13.	0/0	0/0	0/0	0/0
14.	0/0	0/0	0/0	0/0
15.	0/0	0/0	0/0	0/0
16.	0/0	0/0	0/0	0/0

In the output:

- **DNIS#**—Displays the last eleven digits of the DNIS number.
- **Used**—Specifies the number of active sessions to the specified DNIS number.
- **Max**—Specifies the value specified in the Ethernet > Mod Config > DNIS options submenu.

If Ethernet > Mod Config > DNIS options > DNIS Limitation = No, and you enter the Show DNIS Sessions command, the MAX displays the following message:

```
DNIS Inactive
```

Show DNIS statistics command

To display DNIS session statistics, enter the Show DNIS Statistics command:

```
ascend% show dnis statistics
```

	GLOBAL	MODEM	HDLC	V110
DNIS#	Tot/Accept	Tot/Accept	Tot/Accept	Tot/Accept
0. Unspecified	10/9	0/0	0/0	0/0

1.	68149	0/0	8/8	4/4	0/0
2.	8867764	0/0	0/0	0/0	0/0
3.	45566778800	0/0	0/0	0/0	0/0
4.		0/0	0/0	0/0	0/0
5.		0/0	0/0	0/0	0/0
6.		0/0	0/0	0/0	0/0
7.		0/0	0/0	0/0	0/0
8.		0/0	0/0	0/0	0/0
9.		0/0	0/0	0/0	0/0
10.		0/0	0/0	0/0	0/0
11.		0/0	0/0	0/0	0/0
12.		0/0	0/0	0/0	0/0
13.		0/0	0/0	0/0	0/0
14.		0/0	0/0	0/0	0/0
15.		0/0	0/0	0/0	0/0
16.		0/0	0/0	0/0	0/0

In the output:

- DNIS#—Displays the last eleven digits of the DNIS number.
- Tot—Specifies the total number of calls *received* to the specified DNIS number.
- Accept—Specifies the total number of calls *accepted* to the specified DNSI number.

Note: A counter resets when it reaches 10,000, or when you enter the Clear DNIS Statistics command.

If Ethernet > Mod Config > DNIS options > DNIS Limitation = No, and you enter the Show DNIS Statistics command, the MAX displays the following message:

DNIS Inactive

Clear DNIS statistics

To clear DNIS session statistics, enter the Clear DNIS Statistics command. The MAX displays the following message:

Clearing all DNIS Statistics...

VT100 Interface DO Commands

This chapter describes the context-sensitive DO commands. This chapter covers the following topics:

Using DO commands	2-1
DO command reference in alphabetic order	2-3

Using DO commands

The DO menu is a context-sensitive list of commands that appears when you press Ctrl-D. The commands in the DO menu vary, depending on the context in which you invoke it. For example, if you press Ctrl-D in a Connection profile, the DO menu looks similar to the following:

```
DO...
>0=ESC
1=Dial
P=Password
S=Save
E=Termserve
D=Diagnostics
```

To execute a DO command, press and release the DO key on the palmtop or the Ctrl-D on a VT-100 system, and then press and release the next key in the sequence (such as 1 to invoke the Dial command.) On a VT100 terminal, The PF1 function key is equivalent to Ctrl-D.

List of supported commands

Table 2-1 lists all the DO commands. The availability of a particular command depends on your location in the interface and your permission level.

Table 2-1. DO commands

Command	Description
Answer (DO 3)	Answer an incoming call.
Beg/End BERT (DO 7)	Begin/End a byte-error test.
Beg/End Rem LB (DO 6)	Begin/End a remote loopback.
Beg/End Rem Mgm (DO 8)	Begin/End remote management.

Table 2-1. DO commands (continued)

Command	Description
Close TELNET (DO C)	Close the current Telnet session.
Contract BW (DO 5)	Decrease bandwidth.
Diagnostics (DO D)	Access the diagnostic interface.
Dial (DO 1)	Dial the selected or current profile.
ESC (DO 0)	Abort and exit the DO menu.
Extend BW (DO 4)	Increase bandwidth.
Hang Up (DO 2)	Hang up from a call in progress.
Load (DO L)	Load parameter values into the current profile.
Menu Save (DO M) 8	Save the VT100 interface menu layout.
Resynchronize (DO R)	Resynchronize a call in progress.
Save (DO S)	Save parameter values in the specified profile.
Password (DO P) 9	Log into or out of the MAX.
Termmserv (DO E)	Access the terminal- server interface.
Toggle (DO T)	Toggle the palmtop controller.

Example of using DO commands to place and clear a call

To manually place a call, the Connection profile for that call must be open or selected in the list of profiles. To clear a call, you can either open the Connection profile for the active connection or tab over to the status window in which that connection is listed. (as described in Chapter 4, “VT100 Interface Status Windows.”)

To manually place a call:

- 1 Open the Connection profile for the destination you want to call.
- 2 Press Ctrl-D.

The DO menu appears:

```
DO...
>0=ESC
1=Dial
P=Password
S=Save
E=Termserv
D=Diagnostics
```

- 3 Press 1 (or select 1=Dial) to invoke the Dial command.

- 4 Watch the information in the Sessions status window. You should see the number being called, followed by a message that the network session is up.

To manually clear a call:

- 1 Open the Connection profile or tab over to the status window that displays information about the active session you want to clear.
- 2 Press Ctrl-D.

The DO menu for the active session appears. For example:

```
10-200 1234567890
DO...
>0=ESC
2=Hang Up
P=Password
S=Save
E=Termserve
D=Diagnostics
```

- 3 Press 2 (or select 2=Hang Up) to invoke the Hang Up command.

The status-window displays changes when the call has been terminated.

DO command reference in alphabetic order

This section describes the DO commands in detail. The commands are listed in alphabetic order.

Answer (DO 3)

The Answer (DO3) command answers an incoming call. You can apply the command only from a menu specific to a serial host port. You cannot answer a call if another call is currently using the port. The command applies when Answer=Terminal at the serial host port and an incoming call is ringing at that port. It is not available from the secondary serial host port of a dual-port pair.

Beg/End BERT (DO 7)

The DO Beg/End BERT command starts and stops a channel-by-channel Byte Error test (BERT). The test runs over the currently called circuits from end-to-end. It reports the total number of incorrect bytes errors found, and breaks the errors down according to DS0 channel. The results are displayed in the Session Err window.

When you select DO Beg/End BERT, the following events occur:

- 1 The local device sends a known data pattern over the network.
- 2 The responding end goes into a DS0-by-DS0 loopback mode of operation.
The signal at the remote end of the test is looped back at the application-MAX interface, rather than at the network-MAX interface.
- 3 By monitoring the data being received against the transmitted pattern, the local device counts the errors it receives on each individual DS0 channel.

If a single byte has two or more errors, it is recorded as a single error.

The call status letter T, for Test, appears in the upper right-hand corner of the display of both the local and the remote MAX unit to indicate that a BERT is in progress. To resume normal operation, end the BERT by selecting DO 7 or entering Ctrl-D 7.

Keep in mind the following additional information:

- A BERT suspends any transfer of user data in either directions.
- All commands that affect the call are disabled, except the command that ends the BERT.
- You must be in a port-specific edit menu or status window to execute the DO Beg/End BERT command.
- You can run the BERT in only one direction at a time. That is, only one side can be the requester.
- To allow the MAX time to complete handshaking, you must wait at least 20 seconds between toggling the BERT on and off.
- The DO Beg/End BERT command does not appear if you are not logged in with operational privileges.

For related information, see the Operations parameter in the *MAX Reference Guide*, and the Line Errors, Session Err, Port Info, Call Status, and Statistics sections in Chapter 4, “VT100 Interface Status Windows.”

Beg/End Rem LB (DO 6)

The DO Begin/End Rem LB command begins and ends a loopback at the serial host port at the remote end of the call.

To begin a remote loopback, select DO Beg/End Rem LB. The call status character L appears in the upper right-hand corner of the screen at both the local and the remote device. A remote loopback tests the entire connection from host interface to host interface. The following events occur:

- 1 The serial host interface of the local MAX begins the remote loopback test.
- 2 The data loops at the serial host interface of the remote MAX and comes back to the local MAX.

This loopback is also known as a remote data loopback, because the loopback occurs at the DTE/DCE interface. To end a remote loopback, select DO 6 or Ctrl-D 6. Unplugging the palmtop controller also terminates a remote loopback.

Keep in mind the following additional information:

- A remote loopback disables data flow from the remote host, but the call remains online.
- A remote loopback disables Dynamic Bandwidth Allocation (DBA).
- Only switched and nailed-up channels active during the current call are looped back.
- Drop-and-Insert channels are not looped back.
- You must be in a port-specific edit menu or status window to use the DO Beg/End LB command.
- To allow the MAX time to complete handshaking, you must wait at least 20 seconds between toggling the remote loopback on or off.

- When the remote device is a not an Ascend inverse multiplexer, you cannot set up a remote loopback if the network connection occurs over an ISDN line and the Call profile includes any of the following settings:
 - Call Type is set to 1 Chnl or 2 Chnl
 - Call Type is set to AIM or BONDING and Call Mgm is set to Static or Mode 1.
- If the remote device is an ISDN TA (Terminal Adapter), the MAX cannot usually perform a remote loopback. ISDN TAs cannot recognize the loopback signal. However, most switching Channel Service Units/Data Service Units (CSU/DSUs) recognize the remote loopback signal that the MAX sends, and remote loopbacks are usually possible with such equipment.
- The MAX uses a proprietary loopback message when the AIM management subchannel is present (Call Mgm is set to Manual, Dynamic, or Delta in a Call profile).
- The MAX uses the CCITT V.54 loopback pattern when no management subchannel is present (Call Type is set to 1 Chnl or 2 Chnl and Call Mgm=Static in a Call profile).
- If the MAX fails to set up a remote loopback, it establishes a loopback at the local host interface that tried to establish the call.
- The DO Beg/End LB command does not appear if you are not logged in with operational privileges.

For related information, see the Call Mgm, Call Type, and Operations parameters in the *MAX Reference Guide*.

Beg/End Rem Mgm (DO 8)

The DO Beg/End Rem Mgm command begins and ends remote management of the device at the remote end of an Ascend Inverse Multiplexing (AIM) call. When you enter the command, the VT100 interface displays the following message at the top of its screen:

```
REMOTE MANAGEMENT VIA port
```

where, *port* specifies the serial host port through which you are conducting remote management. To end an AIM remote management session, enter DO 8 or Ctrl-D 8. You cannot exit remote management from a port other than the port from which you began remote management. When the message at the top of the VT100 screen disappears, the screens associated with the local MAX appear.

Note: Ascend strongly recommends that you use only the VT100 interface to perform remote management. The palmtop controller provides no indication as to whether you are in remote management or local management.

Keep in mind the following additional information:

- During an AIM call, remote management adds 20 Kbps to the 0.2% overhead of the call, and to that small extent reduces the bandwidth provided to serial host devices using the connection.
- The DO Beg/End Rem Mgm command is available for connections with the Call profile's Call Type parameter set to FT1-AIM, FT1-B&O, or AIM (but not with Call Mgm set to Static).

- An error message of `Remote Mgmt Denied` indicates that you have tried to control a MAX that is not configured to allow remote management. You cannot remotely manage a device for which `Remote Mgmt=No` in the System profile.
- You cannot begin remote management if you do not have a call on line to the remote device. Furthermore, you must select the `DO Beg/End Rem Mgm` command from a menu specific to that call.
- The `DO Beg/End Rem Mgm` command does not appear if you are not logged in with operational privileges.

For related information, see the `Call Mgm`, `Call Type`, `Operations`, and `Remote Mgm` parameters in the *MAX Reference Guide*.

Close Telnet (DO C)

The `DO Close Telnet` command closes the current Telnet session. You must be running a Telnet session from the MAX unit's terminal-server interface.

Contract BW (DO 5)

The `DO Contract BW` command decreases the bandwidth by the amount specified in the `Dec Ch Count` parameter of the current Call profile. If the specified amount is not available, the MAX removes the maximum number of channels possible without clearing the call.

Keep in mind the following additional information:

- The `DO Contract BW` command is available only from a menu specific to an online call with at least two channels.
- The command is available for inverse-multiplexed calls using switched circuits.
- The command does not appear if you are not logged in with operational privileges.

For related information, see the `Dec Ch Count` and `Operations` parameters in the *MAX Reference Guide*.

Diagnostics (DO D)

The `DO D` command invokes diagnostics mode. The user must have sufficient privileges in the active Security profile. In diagnostics mode, the VT100 interface displays a command-line prompt:

```
>
```

Use the `Help Ascend` command to display a list of diagnostic commands:

```
> help ascend
```

To exit diagnostics mode and return to the VT100 interface, enter the `Quit` command:

```
> quit
```

Dial (DO 1)

The DO Dial command dials a selected Call or Connection profile. Before you dial a Call profile, the selector (>) must be in one of the following positions:

- In front of a Call profile in the Directory menu
- At any parameter within a Call profile
- In front of or within any port-specific menu, but not at any specific Call profile. (Because the current Call profile contains the parameters of the last call made from a port, this option redials that call.)

Dial automatically executes a DO Load to load the selected profile. It overwrites the current Call profile, including any Call profile parameters you might have edited. However, edited parameters are not overwritten if the current Call profile is protected by Security profiles.

Before you bring a specific session online, the cursor must be in front of the associated Connection profile in the Connections menu.

Keep in mind the following additional information:

- Dial is not available when the link is busy.
- You cannot place a call from the secondary port of a dual-port pair.
- The DO Dial command does not appear if you are not logged in with operational privileges.
- You cannot dial if you have not selected the correct profile, if Dial # does not appear in the profile, or if no IP address is set for the profile when IP routing is enabled.

For related information, see the Operations parameter in the *MAX Reference Guide*.

Esc (DO 0)

The DO ESC command exits the DO menu.

Extend BW (DO 4)

The DO Extend BW command increases the bandwidth by the amount specified in the Inc Ch Count parameter of the current Call profile. If the specified amount is not available, the MAX adds the maximum number of channels available to the call.

You must apply this command from a menu specific to an online serial host port. This command is available only from connections whose bandwidth can be incremented.

Keep in mind the following additional information:

- The DO Extend BW command is available for AIM and BONDING calls using switched circuits, but is not available for MP+ or MP calls.
- The DO Extend BW command does not appear if you are not logged in with operational privileges.

For related information, see the Inc Ch Count and Operations parameters in the *MAX Reference Guide*.

Hang Up (DO 2)

The DO Hang up command ends an online call. Either the caller or the receiver can terminate at any time.

Keep in mind the following additional information:

- The DO Hangup command works only from the caller end of an Nailed/MPP connection (when Call Type=Nailed/MPP in a Call profile).
- You must be in a menu specific to an online serial host port or session to use this command.
- The DO Hangup command does not appear if you are not logged in with operational privileges.

For related information, see the Call Type and Operations parameters in the *MAX Reference Guide*.

Load (DO L)

The DO Load command loads a saved or edited profile and overwrites the values of the current profile. For example, suppose you have saved a profile named Memphis in the Directory location 21-102 and your screen currently displays the following lines:

```
21-100 Directory
21-1 Factory
21-101 Tucson
>21-102 Memphis
```

If you execute DO Load, the following display:

```
Load profile...?
0=Esc (Don't load)
1=Load profile 102
```

If you choose the first option by pressing 0 (zero), the MAX aborts the load operation. If you choose the second option by pressing 1, the following status window appears:

```
Status #116
profile loaded
as current profile
```

The Directory menu shows the results of the load operation:

```
21-100 Directory
21-1** Memphis
21-101 Tucson
>21-102 Memphis
```

The DO Load command is not available if you are not logged in with operational privileges. For more information, see the Operations parameter in the *MAX Reference Guide*.

Menu Save (DO M)

The DO Menu Save command saves the entire current VT100 interface layout. The current layout replaces the default layout.

Keep in mind the following additional information:

- The DO Menu Save command appears only if the cursor is in front of the Sys Config menu.
- The command always places Sys Config in the default Edit display. (To change the default Edit display, you must configure the Edit parameter in the System profile after using the DO Menu Save command.)
- Menu Save does not apply to palmtop controllers, nor does it apply when your VT100 is plugged into an RPM or palmtop port.

For related information, see the Edit parameter in the *MAX Reference Guide*.

Password (DO P)

The DO Password command enables you to log into the MAX.

During login, you select and activate a Security profile. The Security profile remains active until you log out or replace it by activating a different Security profile, or until the MAX automatically logs you out. The MAX can have several simultaneous user sessions and, therefore, several simultaneous Security profiles.

To log into the MAX, use the DO P command. You can log in or log out from any menu. Whenever you select the DO P command, a list of Security profiles appears. Select the desired profile with the Enter or Right Arrow key, and enter its corresponding password when prompted. If you enter the correct password for the profile, the security of the MAX is reset to the Security profile you have selected.

If you select the first Security profile, Default, simply press Enter or Return when prompted for a password. The password for this profile is always null.

If you are operating the MAX locally and you want to secure the MAX against the next user, use the DO P command and select the first profile, Default. Typically, the Default profile has been edited to disable all operations you wish to secure.

The MAX logs you out to the Default profile if any one of the following situations occurs:

- You end a console session.
- You exceed the time set by the Idle Logout parameter in the System profile.
- You are connected to a palmtop control port and you disconnect your terminal.
- Auto Logout=Yes in the System profile and you are connected to the VT100 control port.

A single Security profile can be used simultaneously by any number of users. If both you and another user enter the same password, you both get the same Security profile and can perform the same operations. If each of you uses a different password to log in, each of you gets a separate Security profile with separate lists of privileges.

If you edit a Security profile, the changes do not affect anyone who is logged in and using that profile. However, the next time someone logs in and uses that profile, security for the user will be limited according to the changes you have made.

For related information, see the Auto Logout and Idle Logout parameters in the *MAX Reference Guide*.

Resynchronize (DO R)

The DO Resynchronize command causes the MAX to resynchronize a call in progress between serial hosts by performing a handshake with the remote end. A handshake is an exchange of data over the management subchannel. It verifies that the transmission is reliable on both ends of the call.

Keep in mind the following additional information:

- You must be in a serial host port edit menu or status window to use this command.
- Resynchronize is not available for all call management types specified by the Call Mgm parameter in the Call profile.
- Resynchronize is not available when the host port is idle or when the host port is the secondary port of a dual-port pair.
- Resynchronize does not appear if you are not logged in with operational privileges.

For related information, see the Call Mgm and Operations parameters in the *MAX Reference Guide*.

Save (DO S)

The DO Save command saves the current parameter values in a specified profile.

Keep in mind the following additional information:

- If a profile is protected by a Security profile, you might not be able to overwrite it.
- Save does not appear if you are not logged in with operational privileges.

For more information, see the Operations parameter in the *MAX Reference Guide*.

Termserve (DO E)

The DO Termserve command invokes the terminal-server command-line interface. The user must have sufficient privileges in the active Security profile. In terminal-server mode, the VT100 interface displays a command-line prompt. By default the prompt is:

```
ascend%
```

Enter the Help command to display a list of terminal-server commands:

```
ascend% help
```

For examples that use terminal-server commands, see the *MAX Reference Guide*. To exit terminal-server mode and return to the VT100 interface, enter the Quit command:

```
ascend% quit
```

Diagnostic Commands and Parameters

3

This chapter covers the following topics:

Sys Diag commands	3-1
T1 Line Diag commands	3-4
E1 Line Diag commands	3-6
BRI/LT Line Diag commands	3-7
Host/Dual (Host/6) Port Diag command	3-9
Modem Diag parameters	3-10

This chapter lists the VT100 interface diagnostic commands provided for WAN lines and ports. To use these commands, you must have sufficient permissions in the active Security profile.

Sys Diag commands

The MAX provides the following system diagnostic commands which appear in the System > Sys Diag menu:

```
System
  Sys Diag
    Restore Cfg
    Save Cfg
    Use MIF
    Sys Reset
    Term Serv
    Upd Rem Cfg
```

To enter a command, highlight the command in the Sys Diag menu and press Enter.

Note: To use these commands, the operator must have sufficient permissions in the active Security profile.

Restore Cfg

The Restore Cfg command restores a MAX configuration that was saved with the Save Cfg parameter, or transfers the profiles to another MAX. Because the Save Cfg command does not save passwords, the Restore Cfg command does not restore them. Follow these instructions to restore your configuration from backup, proceed as follows:

- 1 Verify that the Upload and Edit Security permissions are enabled in the active Security profile.
- 2 Verify that the Term Rate parameter in the System profile is set to 9600.
- 3 Verify that your terminal-emulation program has a disk-capture feature and an autotype feature, and that its data rate is set to 9600 bps.
- 4 Connect the backup device to the MAX unit's control port.
- 5 Highlight Restore Cfg and press Enter.
- 6 When the Waiting for upload data prompt appears, turn on the autotype function on your emulator and supply the filename of the saved MAX data.
- 7 Verify that the configuration data is going to your terminal-emulation screen and is being restored to the target MAX.
The restore process is complete when the message `Upload complete--type any key to return to menu` appears on your emulator's display.

Save Cfg

The Save Cfg command enables you to save the MAX configuration to a file. It does not save Security profiles or passwords.

Note: Using the Save Cfg command to save the configuration and then restoring it from the saved file clears all passwords.

To save your configuration, proceed as follows:

- 1 Verify that the Download permission is enabled in the active Security profile.
- 2 Verify that the Term Rate parameter in the System profile is set to 9600.
- 3 Verify that your terminal-emulation program has a disk-capture feature and an autotype feature, and that its data rate is set to 9600 bps or lower.
- 4 Connect the backup device to the MAX unit's control port.
- 5 Turn on the autotype function on your emulator, and start the save process by pressing any key on the emulator.
- 6 Highlight Save Cfg and press Enter.
- 7 Verify that configuration data is being echoed to the terminal-emulation screen and that the captured data is being written to a file on your disk.
The save process is complete when the message `Download complete--type any key to return to menu` appears on your emulator's display. The backup file is an ASCII file.
- 8 Turn off the autotype feature.

Use MIF

The Use MIF command opens the Machine Interface Format (MIF) interface. You can also access MIF by setting Console to MIF in the System profile. You can enter **Use MIF** to switch to the MIF interface either on a local workstation or during a Telnet session.

To return to the standard VT100 interface, press Ctrl-C.

Note: The Use MIF command runs MIF only at the control port that makes the request (not system-wide). Similarly, Ctrl-C restores the standard VT100 interface only at the control port that makes the request.

Sys Reset

The Sys Reset command restarts the MAX and clears all calls without disconnecting the device from its power source. The MAX logs out all users and returns user security to its default state. In addition, the MAX performs Power-On Self Tests (POSTs) when it restarts. The POSTs are diagnostic tests. A system reset of a MAX causes momentary loss of T1 framing (that is, the data-encapsulation format), and the T1 line might shut down. In any event, the feedback from the MAX to the switch is incorrect until T1 framing is reestablished.

To perform a system reset, proceed as follows:

- 1 Highlight System Reset and press Enter.

The MAX prompts you to confirm that you want to perform the reset.

- 2 Confirm the reset.

In addition to clearing calls, the MAX performs a series of POSTs. The POST display appears. If you do not see the POST display, press Ctrl-L. These messages may be displayed:

```
OPERATOR RESET:  Index: 99   Revision: 5.0a
                  Date: 03/04/1997.   Time: 22:32:23
                  MENU Reset from unknown in security profile 1.
SYSTEM IS UP:    Index: 100  Revision: 5.0a
                  Date: 03/04/1997.   Time: 22:33:00
```

While the yellow Fault LED on the front panel remains solidly lit, the MAX checks system memory, configuration, installed modules, and T1 connections. If the MAX fails any of these tests, the Fault LED remains lit or blinks. The alarm relay remains closed while the POST is running and opens upon successful completion of the test, at which time the following message appears:

```
Power-On Self Test PASSED
Press any key...
```

- 3 Press any key to display the Main Edit Menu.

Term Serv

The Term Serv command starts a terminal-server session. The system displays the terminal-server command-line prompt (by default, `ascend%`). For information about the terminal-server commands, enter a question mark at the prompt. For more details about the terminal-server interface, see the *Network Configuration Guide* for your MAX.

Upd Rem Cfg

The Upd Rem Cfg (Upload Remote Configuration) command opens a connection to a RADIUS server to upload the MAX terminal-server banner, list of Telnet hosts, IP static

routes, IP address pool, and other configuration information from the RADIUS user file. The MAX retrieves configuration from RADIUS at system startup or by use of this command.

When you highlight Upd Rem Cfg and press Enter, the MAX opens a connection to the RADIUS server and uploads the configuration information.

When you upload this remote configuration information, keep in mind the following information:

- The MAX reads Dialout-Framed-User entries with the password `ascend`.
- The Upd Rem Cfg command does not update the terminal-server banner or list of Telnet hosts if the Remote Conf parameter is set to No.
- If the Ascend-Authen-Alias attribute is defined in RADIUS, the Upd Rem Cfg command also updates the MAX system name used when establishing PPP calls.

T1 Line Diag commands

The MAX provides the following T1 line diagnostic commands, which appear in the Net/T1 > Line Diag menu:

```
Net/T1
  Line Diag
    Line LB1
    Line LB2
    Switch D Chan
    Clr Err1
    Clr Perf1
    Clr Err2
    Clr Perf2
```

To execute one of the commands, select the command and press Enter.

Line LB1

Line LB1 is a Line LoopBack command for Line 1 in a T1 slot. When you start the line loopback test for a T1 line, a remote device can test the T1 line and the MAX unit's interface to the T1 line. All signals received by the MAX are looped back (behind the MAX unit's CSU repeater or DSX signal-conditioning module) toward the remote device. The remote device can determine the quality of the T1 line by comparing the sent signal to the received signal.

Line LoopBack (LLB) occurs behind the MAX unit's CSU repeater or DSX signal-conditioning module. Drop-and-Insert channels are also looped back. Do not activate LLB when a call is active on the line; doing so disrupts the data flow between the codecs connected to either end of the network line. The MAX responds to both the inband LLB signal and the Facility Data Link (FDL) LLB message. Therefore, a management device can put the MAX into LLB. A management device is a unit, on a T1 line, that measures the line's performance and can send management signals to other devices on the line.

To initiate a loopback test on the first T1 line, highlight Line LB1 and press Enter. After prompting for confirmation, the MAX starts the loopback test and the Alarm LED lights up. When you exit the menu option, the MAX automatically deactivates the loopback.

For related information, see the FDL parameter in the *MAX Reference Guide* and the FDL Status window in the *Administration Guide* for your MAX.

Line LB2

Line LB2 is a Line LoopBack command for Line 2 in a T1 slot. When you start the line loopback test for a T1 line, a remote device can test the T1 line and the MAX unit's interface to the T1 line. All signals received by the MAX are looped back (behind the MAX unit's CSU repeater or DSX signal-conditioning module) toward the remote device. The remote device can determine the quality of the T1 line by comparing the sent signal to the received signal.

Line LoopBack (LLB) occurs behind the MAX unit's CSU repeater or DSX signal-conditioning module. Drop-and-Insert channels are also looped back. Do not activate LLB when a call is active on the line. Doing so disrupts the data flow between the codecs connected to either end of the network line. The MAX responds to both the inband LLB signal and the Facility Data Link (FDL) LLB message. Therefore, a management device can put the MAX into LLB. A management device is a unit, on a T1 line, that measures the line's performance and can send management signals to other devices on the line.

To initiate a loopback test on the second T1 line, highlight Line LB2 and press Enter. After prompting for confirmation, the MAX starts the loopback test and the Alarm LED lights up. When you exit the menu option, the MAX automatically deactivates the loopback.

For related information, see the FDL parameter in the *MAX Reference Guide* and the FDL Status window in the *Administration Guide* for your MAX.

Switch D Chan

The Switched D Chan command swaps the status of the primary and secondary NFAS D channels. It applies only to T1 lines using NFAS signaling.

Clr Err1

The Clr Err1 command clears the user error event register of Line 1, but does not clear the performance registers for the line. To clear all performance registers for Line 1, use Clr Perf1. To clear all performance registers for Line 2, use Clr Perf2.

Note: Error events have no meaning for D4-framed lines. A D4 line uses the Superframe format to frame data at the physical layer. This format consists of 12 consecutive frames separated from one another by framing bits.

Clr Perf1

The Clr Perf1 command clears all performance registers for Line 1, restarts the current time period, and begins accumulating new performance data.

For related information, see the FDL parameter in the *MAX Reference Guide* and the FDL Status window in the *Administration Guide* for your MAX.

Clr Err2

The Clr Err2 command clears the user error event register of Line 2, but does not clear the performance registers for the line. To clear all performance registers for Line 1, use Clr Perf1. To clear all performance registers for Line 2, use Clr Perf2.

Note: Error events have no meaning for D4 lines. A D4 line uses the Superframe format to frame data on the physical layer. This format consists of 12 consecutive frames, separated by framing bits.

For related information, see the FDL parameter in the *MAX Reference Guide* and the FDL Status window in the *Administration Guide* for your MAX.

Clr Perf2

The Clr Perf2 command clears all performance registers for Line 2, restarts the current time period, and begins accumulating new performance data.

For related information, see the FDL parameter in the *MAX Reference Guide* and the FDL Status window in the *Administration Guide* for your MAX.

E1 Line Diag commands

Diagnostic commands for E1 lines appear in the Net/E1 > Line Diag menu:

```
Net/E1
  Line Diag
    Line LB1
    Line LB2
```

To execute one of the commands, select the command and press Enter.

Line LB1

Line LB1 is a Line LoopBack command for Line 1 in an E1 slot. When you start the line loopback test for a E1 line, a remote device can test the E1 line and the MAX unit's interface to the E1 line. All signals received by the MAX are looped back (behind the MAX unit's CSU repeater or DSX signal-conditioning module) toward the remote device. The remote device can determine the quality of the E1 line by comparing the sent signal to the received signal.

Line LoopBack (LLB) occurs behind the MAX unit's CSU repeater or DSX signal-conditioning module. Drop-and-Insert channels are also looped back. Do not activate LLB when a call is active on the line. Doing so disrupts the data flow between the codecs connected to either end of the network line. The MAX responds to both the inband LLB signal and the Facility Data Link (FDL) LLB message. Therefore, a management device can put the MAX into LLB. A management device is a unit, on an E1 line, that measures the line's performance and can send management signals to other devices on the line.

To initiate a loopback test on the first E1 line, highlight Line LB1 and press Enter. After prompting for confirmation, the MAX starts the loopback test and the Alarm LED lights up. When you exit the menu option, the MAX automatically deactivates the loopback.

Line LB2

Line LB2 is a Line LoopBack command for Line 2 in an E1 slot. When you start the line loopback test for an E1 line, a remote device can test the E1 line and the MAX unit's interface to the E1 line. All signals received by the MAX are looped back (behind the MAX unit's CSU repeater or DSX signal-conditioning module) toward the remote device. The remote device can determine the quality of the E1 line by comparing the sent signal to the received signal.

LLB occurs behind the MAX unit's CSU repeater or DSX signal-conditioning module. Drop-and-Insert channels are also looped back. Do not activate LLB when a call is active on the line. Doing so disrupts the data flow between the codecs connected to either end of the network line. The MAX responds to both the inband LLB signal and the Facility Data Link (FDL) LLB message. Therefore, a management device can put the MAX into LLB. A management device is a unit, on an E1 line, that measures the line's performance and can send management signals to other devices on the line.

To initiate a loopback test on the second E1 line, highlight Line LB2 and press Enter. After prompting for confirmation, the MAX starts the loopback test and the Alarm LED lights up. When you exit the menu option, the MAX automatically deactivates the loopback.

BRI/LT Line Diag commands

Diagnostic commands for BR/LT lines appear in the BRI/LT > Line Diag > Line *N* menu:

```
BRI/LT
  Line Diag
    Line N...
      Line LoopBack
      Corrupt CRC
      UnCorrupt CRC
      Rq Corrupt CRC
      UnRq Corrupt CRC
      Clr NEBE
      Clr FEBE
```

To execute one of the commands, select the command and press Enter.

Note: Maintenance functions supported by the BRI/LT driver use the BRI-U interface's Embedded Operations Channel (EOC). The EOC transfers data from the exchange to the terminal side and vice versa without occupying either the B or the D channel. The EOC is used to transmit diagnostic function and signaling information, (obtaining the block errors in close to real time or performing line diagnostics such as loopback or corrupt CRC, for example.)

The EOC monitor commands are sent in the M1, M2, and M3 bits of the U superframe. (For more information about usage of the M1, M2, and M3 bits of the superframe, see ANSI T1-601, from ANSI 1991.

The remote U-interface/echo canceller provides internal counters for far-end and near-end block errors. A Near-End Block Error (NEBE) indicates that the error has been detected in the receive direction. A Far-End Block Error (FEBE) identifies errors in the transmission direction.

You can use the block error counters to monitor transmission quality at the U interface. A block error is detected each time when the calculated checksum of the received data does not correspond to the control checksum transmitted in the successive superframe. One block error indicates that one U-superframe has not been transmitted correctly. The block error count does not provide information regarding the number of bit errors in the U superframe, but states only that the CRC failed in that superframe. About every 4 seconds, a daemon running in the MAX obtains the remote block error counter values and displays their cumulative value in the block-error status screens.

The block-error totals are obtained from the remote TA. These cumulative totals are reset when you clear the block-error buffer(s) from the Line diagnostics submenu, or when you restart the MAX. The totals reset to zero when they reach 65535.

Note: See the Block Error status display in the BRI/LT status window of the block-error information displayed.

Line LoopBack

The Line LoopBack command puts the line into loopback mode. When you select the Line LoopBack command and press Enter, the following screen appears:

```
Line LoopBack
0=ESC
1=Line X LB
```

Select 1 to execute the loopback command. Test frames are sent continuously in the D channel until the command is cancelled. The transmitted frames are each 24 bytes long. The frames differ in content and should cover every possible bit pattern.

Note: Only one loopback test can be performed at a time on the same line. If another user attempts to invoke the loopback command for a line that is already in loopback mode, the following error message appears:

```
Line LB already.
Cmd ignored.
```

Because UnRq Corrupt CRC acts similarly when requesting the same command to request that the remote end cancel the loopback, UnRq Corrupt CRC is unavailable when the MAX exits loopback mode.

Select the LB Counters status screen to display the number of transmitted frames as opposed to the number of correctly received frames. The MAX continuously sends frames to the remote end. When the MAX receives a frame that matches the transmitted frame in size (and the bytes of the received frame exactly match the bytes in the transmitted frame), it sends out a new frame and increments the receive counter for that frame. When the MAX receives a frame that does not match the transmitted frame, it still sends out a new frame, but does not increment the receive counter for that frame. Also, when the MAX does not receive a frame back, the timeout between two consecutive transmitted frames is about 4 seconds.

Press ESC to cancel the loopback function. The following message appears:

```
Line loopback terminated.
```

Corrupt CRC

The Corrupt CRC command causes the BRI-U interface to transmit inverted CRCs, until you

cancel the command. When the command is issued, the Far-End Block Error counter should be viewed from the remote TA. The command is used to test the NEBE and FEBE counters, by simulating transmission errors with artificially corrupted CRCs.

Uncorrupt CRC

The Uncorrupt CRC command cancels a previous Corrupt CRC command.

Rq Corrupt CRC

The Rq Corrupt CRC command requests NT1 to corrupt the CRC to artificially simulate transmission errors. The command is used to verify that the block error counters are working, or providing the right information. When you enter the command, check the Near-End Block Error counter.

Rq Uncorrupt CRC

The Rq Uncorrupt CRC command requests NT1 to return to normal.

Clr NEBE

The Clr NEBE command clears the Near-End Block Error (NEBE) counter.

Clr FEBE

The Clr FEBE command clears the Far-End Block Error (FEBE) counter.

Host/Dual (Host/6) Port Diag command

The Local LB command in the Host/Dual (Host/6) > Port *N* Menu > Port Diag menu tests the Ascend Multiplexing (AIM) port. To execute the command, select it and press Enter.

Note: To use the Local LB command, you must have sufficient permissions in the active Security profile.

The Local LB command activates a local loopback test. In a local loopback test, data originating at the local site is looped back to its originating port without going out over the WAN. It is as though a *data mirror* were held up to the data at the WAN interface, and the data were reflected back to the originator. The WAN interface is the MAX port that is connected to a WAN line.

The AIM port on the MAX must be idle when you run the local loopback test. It can have no calls online.

Highlight Local LB and press Enter. When the local loopback test is in progress, control moves to the Local LB menu, which presents a set of parameters you can modify. Press Enter to cycle through the parameters in the Local LB menu, and press the selector (>) or Right Arrow key to toggle between the settings for each parameter:

- DSR toggles the host port Data Set Ready (DSR) V.25 signal between active and inactive.

- RI toggles the host port Ring Indicate (RI) V.25 output signal between active and inactive.
- CD toggles the host port Carrier Detect (CD) output signal between active and inactive.
- DLO toggles the host port Data Line Occupied (DLO) RS-366 output signal between active and inactive.
- PND toggles the host port Present Next Digit (PND) RS-366 output signal between active and inactive.
- ACR toggles the host port Abandon Call and Retry (ACR) output signal between active and inactive.
- Inc Ch Count simulates an increase in the number of channels in a call by increasing the clock rate to the host.
- Dec Ch Count simulates a decrease in the number of channels in a call by decreasing the clock rate to the host.
- Rate toggles the data rate of the simulated channels between 56 Kbps and 64 Kbps.

When the loopback screen shows 56K or 64K channels looped back, think of the channels as simulated. The Call Status window displays the loopback serial data rate. You can calculate the data speed by multiplying the number of simulated channels by the data rate. Changes you make take effect immediately, and remain in effect until you end the local loopback test. Terminate the test by pressing the Left Arrow key.

When you end the test, all control signals revert to the state they were in when the test began.

Modem Diag parameters

The MAX provides the following modem diagnostic parameters, which appear in the V.34 (K56) Modem > Modem Config menu:

```
V.34 Modem (or K56 Modem)
  Modem Config
    ModemSlot=enable slot
    Modem #1=enable modem
    Modem #2=enable modem
    Modem #3=enable modem
    Modem #4=enable modem
    Modem #5=enable modem
    Modem #6=enable modem
    Modem #7=enable modem
    Modem #8=enable modem
```

To set one of the parameters, select the parameter and press Enter.

ModemSlot

You can set the ModemSlot parameter to quiesce a digital-modem slot card. That is, you can disable a digital-modem slot card in the MAX without disrupting existing connections. Active calls are not torn down. When an active call is dropped, that modem is added to the disabled modem list and is not available for use. If all modems are on the disabled list, incoming callers receive a busy signal until the modems have been restored for service. When you re-enable the quiesced modem slot card, a delay of up to 20 seconds can occur before the modems become available for service.

You can specify one of the following values:

- **Enable Slot**—The default value. Enables any modems on the selected slot card that were on the disabled list, making them available for service.
- **Dis Slot**—All modems that are not active appear in a disabled modem list, indicating that they are not available for use.
- **Dis Slot+Chan**—All modems on the selected slot card are disabled, along with an equal number of B channels. The B channels appear on a disabled-channel map. The MAX polls all channels on the map with Out-Of-Service messages until the modems on the associated slot card return to service.

To quiesce all the available modems on a slot card:

- 1 Open the Mod Config submenu from the Modem profile and select ModemSlot.
- 2 Press Enter to disable (quiesce) the slot card, the value is dis slot or to disable the slot card and the channel, press Enter again, the value will be dis slot+chan).

For example,

```
V.34 Modem
  Modem Config
    ModemSlot=dis slot
    Modem #1=NA
    Modem #2=NA
    ..
    ..
    ..
```

- 3 Close the Modem profile.

Note: Booting the MAX restores the quiesced slot to service.

Modem #N (where N=1–8, 1–12, 1–16)

You can set the Modem #N parameter to quiesce a digital-modem. That is, you can disable a digital modem without disrupting existing connections. Active calls are not torn down. If you specify a modem that is currently inactive, the modem is added to the disabled list. If the modem has a call active, it is not added to the disabled list until it drops the call. If all modems are on the disabled list, incoming callers receive a busy signal until the modems have been restored for service. When you re-enable the quiesced modem, a delay of up to 20 seconds can occur before the modem becomes available for service.

You can specify one of the following values:

- **Enable Modem**—The default value. Enables any modems that were on the disabled list, entering them on the enabled modem list and making them available for service.
- **Dis Modem**—Places the modem on the disabled modem list, indicating that it is not available for use. When the last active connection is dropped, the card becomes available for maintenance.
- **Dis Modem+Chan**—An arbitrary B channel is taken out of service along with the disabled modem. The B channel appears on a disabled-channel map, and the MAX polls all channels on the map with Out-Of-Service messages until the associated modem is re-enabled.

To quiesce a digital modem:

Diagnostic Commands and Parameters

Modem Diag parameters

- 1 Open the Mod Config submenu from the Modem profile and select the Modem #N you want to disable. (The modem ports on a slot card are numbered starting with #1 for the leftmost port on the card.)
- 2 Press Enter to disable (quiesce) the modem, the value is dis modem or to disable the modem and the channel, press Enter again (the value will be dis modem+chan).

For example,

```
V.34 Modem
  Modem Config
    ModemSlot=enable slot
    Modem #1=dis modem
```

- 3 Close the Modem profile.

Note: Booting the MAX restores all quiesced lines, slots, and ports to service.

VT100 Interface Status Windows

This chapter describes the MAX unit's status windows. This chapter covers the following topics:

Using the MAX status windows	4-1
Status-window reference in alphabetic order.	4-6

Using the MAX status windows

The right side of the screen in the MAX configuration interface displays eight status windows (Figure 4-1). The status windows provide a great deal of read-only information about what is currently happening in the MAX.

This section provides an overview of the information contained in the eight windows that are displayed by default, and shows you how to replace a default window with a status window of your choice. Following are the parameters for customizing the display:

```
System
  Sys Config
    Status 1=10-100
    Status 2=10-200
    Status 3=50-100
    Status 4=00-200
    Status 5=50-300
    Status 6=50-400
    Status 7=00-100
    Status 8=00-000
```

The Status numbers 1 through 8 refer to the status-window positions, which start with 1 in the upper left and continue with 2 in the upper right, and so forth. For details about each parameter, see the *MAX Reference Guide*.

Figure 4-1. Status windows

----- 10-100 1234567890 L1/LA nnnnnnnnnn 12345678901234 nnnnnnnnnnnnnn -----	----- 10-200 1234567890 L2/RA 12345678901234 -----
----- 90-100 Sessions > 1 Active O slc-lab-236 -----	1----- 00-200 15:10:34 >M31 Line Ch LAN session up slc-lab-236 -----
----- 90-300 WAN Stat >Rx Pkt: 184318^ Tx Pkt: 159232 CRC: 0v -----	----- 90-400 Ether Stat >Rx Pkt: 3486092 Tx Pkt: 10056 Col: 3530 -----
----- 00-100 Sys Option >Security Prof: 1 ^ Software +5.0A0+ S/N: 5210003 v -----	----- Main Status Menu >00-000 System ^ 10-000 Net/T1 20-000 Net/T1 v -----

Navigating the status windows

To make a status window active, press the Tab key until that window is highlighted by a thick border. The Tab key moves the active window in sequence from left to right, top to bottom, and then returns to the Main Edit window (the menu).

To scroll the selections in the Main Status Menu in a status window, Tab to the window, then use the Up Arrow or the Down Arrow key to scroll the window. To access a sub-menu, use the Right Arrow key, and to return to the original menu use the Left Arrow key.

Some of the status windows contain more information than can be displayed in the small window. A lowercase v in the lower-right corner of a window, indicates that more information is available. You can scroll through additional information if you make the window active.

Default status window displays

You can set the Status parameters in the System profile to specify which status windows are displayed when the MAX powers up. For descriptions of all of the codes and information that can be displayed in each window, see “Status-window reference in alphabetic order” on page 4-6.

Note: Depending on your MAX configuration, some of these status windows will appear as defaults and some may not. If a status window does not appear as a default, each of the descriptions below instruct you how to display the menu from any status window. Obviously if the status window described is already displayed on your VT100 interface, all you may want to do is scroll through the submenus to view its contents.

Line status windows

Slots 1 and 2 contain the built-in T1 (or E1) lines, with Slot 1 containing the two leftmost lines (when you look at the unit's back panel.) To display the Line Status window, tab to status window, then use the arrow keys to access the Net/T1 > Line *N* Stat window.

By default, the status of the lines in Slot 1 are shown in the top two status windows. For example:

10-100 1234567890	10-200 1234567890
L1/LA nnnnnnnnnn	L2/RA
12345678901234	12345678901234
nnnnnnnnnnnnnn

Each window displays four lines:

- The first line shows the menu number and column numbers for channels 1–10.
- The second line identifies the line (L1 or L2) , displays a 2-character link-status indicator, and displays a 1-character channel-status indicator for each channel. For example:
 - LA indicates Link Active (the line is physically connected).
 - n means the channel is nailed.
 - * indicates a current connection.
 - – means the channels is idle but in service.
 - s means the channel is an active D channel (ISDN only).
- The third line has column headers for channels 11–24.
- The fourth line shows a 1-character channel-status indicator for channels 11–24.

Session and system status windows

The system itself is assigned slot number 0, and the slot number 9 is assigned to the built-in Ethernet port. By default, the next two status windows show active routing sessions on Ethernet and up to 32 log messages related to the system itself:

90-100 Sessions	100-200 15:10:34
> 1 Active	>M31 Line Ch
O slc-lab-236	LAN session up
	slc-lab-236

The Sessions window shows the number of active bridging/routing and modem (terminal server) sessions. When this window is active, you can scroll down to see the name, address, or CLID of each connected device. Each line starts with a 1-character session-status indicator. For example, O means online. For terminal-server sessions, the modem number is identified.

To display the Sessions window, tab to a status window, then use the arrow keys to access the Ethernet > Sessions window.

The system message log provides a log of up to 32 of the most recent system events. To display the System Message Log window, tab to a status window, then use the arrow keys to access the System > Message Log window.

Use an arrow key to scroll up (previous messages) or down (later messages). The Delete key clears all the messages in the log. The message log window is organized as follows:

- The first line shows the menu number and the time the most recently logged event occurred.
- The second line identifies the log entry number (M00-M31) and, if applicable, the line and channel on which the event occurred.
- The third line contains the text of the message. For example:
 - Call Terminated (An active call disconnected normally.)
 - LAN session up (An incoming connection has been established.)
 - No Connection (The remote device did not answer the call.)
- The fourth line contains a message qualifier, such as a name or phone number that qualifies the message displayed.

WAN and Ethernet status windows

By default, the fifth and sixth status windows show statistics about each active WAN link and the Ethernet interface. For example:

-----	-----
90-300 WAN Stat	90-400 Ether Stat
>Rx Pkt: 184318^	>Rx Pkt: 3486092
Tx Pkt: 159232	Tx Pkt: 10056
CRC: 0v	Col: 3530
-----	-----

The WAN Stat window shows the current count of received frames, transmitted frames, and frames with errors for each active WAN link and for the entire WAN. When this window is active, you can scroll down to see the statistics for each link. The first line of each per-link count shows the name, IP address, or MAC address of the remote device. To display the WAN Stat window, tab to a status window, then use the arrow keys to access the Ethernet > WAN Stat window.

The Ether Stat window shows the current count of received frames, transmitted frames, and frames with errors at the Ethernet interface. To display the Ether Stat window, tab to a status window, then use the arrow keys to access the Ethernet > Ether Stat window.

Sys Option and Main Status Menu windows

The bottom two status windows are usually the Sys Option window, which contains management information about the MAX, and the Main Status Menu window. For example:

-----	-----
00-100 Sys Option	Main Status Menu
>Security Prof: 1 ^	>00-000 System ^
Software +5.0A0+	10-000 Net/T1
S/N: 5210003 v	20-000 Net/T1 v
-----	-----

The Sys Options window shows which Security profile is active, which Ascend software version is running, the unit's serial number (S/N). Additionally, it can list a variety of hardware or software options. It also displays a system uptime value, which is updated every few seconds to show the number of days, hours, minutes, and seconds the MAX has been operating. For example:

Up: 12:17:18:26

When the Sys Options window is active, you can use the arrow keys to scroll down and display the list of system options. Appearing, for example, are the software load name, various installed-software options (such as Frame Relay, AIM, and BONDING), and the AuthServer and AcctServer options, which specify the IP addresses of the RADIUS (or TACACS) authentication server and the RADIUS accounting server.

To display the System Options window, tab to a status window, then use the arrow keys to access the System > Sys Option window.

The last status window contains the Main Status Menu, a hierarchical menu that contains an entry for each line or installed card in the MAX. The structure of the Main Status Menu exactly follows the Main Edit Menu (the top-level configuration menu).

When the window that displays the Main Status Menu is active, the menu works like the Main Edit Menu. Use the arrow keys to scroll to a particular status menu. Then press the Enter key to open that menu and the Escape key to close it.

Specifying which status windows appear

You can specify which status windows the VT100 interface displays. The total number of status windows is always limited to eight, but you can set these parameters to focus on a selected area of functionality. (For details about the windows you can choose to display and the information in each one, see "Status-window reference in alphabetic order" on page 4-6.)

To specify which status window appears on the VT100 interface, proceed as follows:

- 1 From the Main Edit Menu, select System > Sys Config.
- 2 Arrow-Down to the Status # parameter(s) of the status window(s) you would like to customize. For example, the MAX displays line-status windows for the T1 (or E1) lines in Slot 1 as windows 1 and 2 by default. Continue with the steps below to redefine the MAX to use status windows 3 and 4 to display line-status windows for the T1 (or E1) lines in Slot 2.
- 3 For the Status 3 parameter, specify the number identifying the status window menu it will be changed to.

Note: Every menu and submenu has an identifying number, for example, 20-100, or 20-200. You can scroll through the Main Status Menu to get the identifying status numbers.

Status 3=20-100

- 4 For the Status 4 parameter, specify the number identifying the status window menu it will be changed to.

Status 4=20-200

- 5 Save and close the System profile.

When the MAX resets, the status windows will appear with the new selections.

For more details about slot, line, and port numbers, see the *Network Configuration Guide* for your MAX.

Status-window reference in alphabetic order

This section describes in detail the contents of each status window. It lists the windows in alphabetic order.

BRI/LT window

BRI/LT is a branch of the Main Status Menu that lists windows indicating the status of the ISDN BRI interfaces. The BRI/LT window appears only if a BRI/LT module is installed. The BRI/LT window displays the following list:

```
X0-000 BRI/LT
X0-100 Line Status
X0-200 Line Errors
X0-300 Block Errors
X0-400 LB Counters
X0-500 Net Options
```

The Line Status window shows the condition of the electrical link to the carrier and the status of the B1 and B2 channels. (For details, see “Line Status (BRI) window” on page 4-17.)

The Line Errors status window displays the errors recorded on all current channels, in a channel-by-channel, line-by-line list. (For details, see “Line Errors window” on page 4-15.)

The Block Errors status window shows the errors for Near-End Block Errors (NEBE) and Far-End Block Errors (FEBE). The numbers displayed are totals accumulated since the last time the block error buffers were cleared. The FEBE and NEBE error buffers can be cleared per line and per counter. (You can clear the FEBE buffer for a line without clearing the NEBE buffer). The totals for each buffer reset to zero after they reach 65535. Restarting the MAX clears the buffers. For example, when a MAX with eight BRI lines is restarted, the Block Errors status window has the following contents:

X0-X00	FEBE	NEBE
1:	0	0
2:	0	0
3:	0	0
4:	0	0
5:	0	0
6:	0	0
7:	0	0
8:	0	0

The LB Counters window shows the number of test frames sent and received since the loopback command was issued. The numbers displayed are totals accumulated since the Line Loopback Command was issued. When the loopback command is started or restarted, the LB counters are reset to 0. For example, when a MAX with eight BRI lines is restarted, the LB Counter status window has the following contents:

X0-XXX	XMIT	RECV
1:	0	0

```
2:      0      0
3:      0      0
4:      0      0
5:      0      0
6:      0      0
7:      0      0
8:      0      0
```

The Net Options window lists the interface features with which your MAX has been equipped. (For details, see “Net Options window” on page 4-25.)

Call Status window

The Call Status window is a read-only window that indicates whether a call is active at a specific AIM port. If there is an active call, the Call Status window displays its current state.

A Call Status window exists for each host port. It is the first option listed in the Port*N* Stat window, and its window number is *XN*-100, where *X* is the module number and *N* is the AIM port number. For example:

```
71-000 Port1 Stat
>71-100 Call Status
71-200 Message Log
71-300 Statistics
71-400 Port Opts
71-500 Session Err
71-600 Port Leads
```

Following is an example, of a Call Status window for the first AIM port on the base system:

```
71-100 Albuquerque+ C
CALLING/ONLINE
336K      6 channels
Albq. NM
```

The first line of the Call Status window shows the status window number, the name of the current Call profile, and a call-status character (described in Table 4-1).

The second line shows the call-status message corresponding to the current state. The message can change dynamically as you dial, modify, or receive calls. Table 4-1 lists the call status characters and messages that can appear:

Table 4-1. Call-status characters and messages

Status indicator	Status message	Description
Blank	IDLE	No calls exist and no other MAX operations are being performed.
A	ANSWERING	An incoming call is being answered.
R	RINGING	An incoming call is on the line, ready to be answered.
C	CALLING	An outgoing call is being dialed.

Table 4-1. Call-status characters and messages (continued)

Status indicator	Status message	Description
O	ONLINE	A call is up on the line.
Blank	/Online	Appended to another message to indicate that the MAX is currently adding or removing channels.
H	CLEARING	The current call is being cleared.
D	LOCAL LOOP	Local loopback diagnostic tests are in progress.
!	HANDSHAK	The MAX is exchanging information with the inverse multiplexer at the remote end and verifying the reliability of the transmission.
!	SETUP ADD	The MAX is preparing to add channels while a call is online and transmitting data.
!	SETUP REM	The MAX is preparing to remove channels while a call is online and transmitting data.
!	SETUP HND	The MAX is preparing to handshake for resynchronization while a call is online and transmitting data.
L	LOOP MAST	You have selected DO 6 or Control-D 6 to begin a remote loopback test. While the loopback test is in progress, the remote end displays the status message LOOP SLAV.
T	BERT MAST	The MAX has connected with the remote-end AIM-compatible product and is performing an automatic Byte Error Rate Test (BERT). Or, you are performing a manual BERT from the local MAX.
T	BERT SLAVE	Your MAX has received a call and the calling AIM-compatible product is performing an automatic BERT. Or, someone using the remote MAX is performing a manual BERT.

For calls other than FT1-B&O, the third line of the Call Status window shows both the current data rate in Kbps, and how many channels this data rate represents. If the current call type is FT1-B&O, the third line of the Call Status window shows how many channels the online data represents, followed by the number of nailed-up channels the MAX has placed offline because their quality was poor. For example, the following display shows the call status of an FT1-B&O call with six channels online and two channels offline:

```
21-100 Albuquerque+ C
CALLING
```

```
336K  6/2  channels
Albq.  NM
```

In some types of calls, you might notice that the data rate to your host is actually somewhat less than reported on line 3. Line 3 shows the bandwidth the PRI interface provides, but does not show how much of this bandwidth an AIM or BONDING management subchannel consumes. (For further information, see the Call profile parameters Call Type and Call Mgm in the *MAX Reference Guide*. In addition, see FT1-B&O under the Call Type parameter for information about how FT1-B&O calls handle channels.)

The last line of the Call Status window contains the name of the AIM port of the remote-end AIM-compatible product. If the remote-end Port profile is not named, the MAX uses the remote-end module name taken from the Host-Module profile. If neither the module nor the port is named, the MAX uses the remote-end system name.

Call Detail Reporting (CDR) window

Call Detail Reporting (CDR) provides a database of information about each call, including date, time, duration, called number, calling number, call direction, service type, associated inverse-multiplexing session, and port. Because the network carrier bills for bandwidth on an as-used basis, and bills each connection in an inverse multiplexed call separately, you might want to use CDR to understand and manage bandwidth usage and the cost of each inverse-multiplexed session.

You can arrange the information to create a wide variety of reports, which can be based on factors such as individual call costs, inverse-multiplexed WAN-session costs, costs on an application-by-application basis and bandwidth usage patterns over specified time periods. With the resulting better understanding of your bandwidth usage patterns, you can make any necessary adjustments to the ratio of switched to nailed bandwidth between network sites.

Like the MAX message logs, CDR shows the most recent session event. The MAX generates new CDR messages as events occur. However, unlike a log, the MAX does not store past CDR events. CDR is primarily a source of data captured by external devices.

To display the Call Detail Reporting (CDR) window, tab to a status window, then use the arrow keys to access the System > CDR window.

Following is a sample four-line CDR display:

```
00-400 CDR
93:05:28:10:33:52
OR 025 384KR 02-01
15105551212
```

The first line displays the status-window number and title.

The second line displays the time at which the event occurred, in the following format:

year:month:day:hour:minute:second

The third line displays the following items of information about the CDR event in the order shown:

Item	Description
CDR event description	Consists of one of the following abbreviations: <ul style="list-style-type: none">• OR—Originated (outgoing call)• AN—Answered (incoming call)• AP—Assigned to Port or module (incoming call)• CL—Cleared• OF—Overflowed All events except OF are associated with calls. OF indicates that the CDR buffer overflowed because events occurred faster than the MAX could report them.
CDR event ID	The MAX creates a new event ID for every DS0 channel originating a connection. The event ID ranges from 0 to 255. Events after 255 start the count again at 0. In addition, CDR creates a new event ID for every change in a channel's status. Because a MAX call can consist of several channels, the MAX can generate multiple CDRs for every change in call status.
Data service in use	Indicates the data service, using values nearly identical to those available to the Data Svc parameter in the Call profile. The only difference is that the Data Svc values 384K/H0 and 1536K correspond to the CDR data service values 384K and 1536KR, respectively.
Slot-port address	The address at which event occurred. For example, if the event occurred on the first port of a Host/6 card installed in slot 3, the slot-port address is 03-01.

The fourth line displays either the dialed or called-party phone number. If the event description on line 3 is OR (outgoing call), the number dialed appears. If the event description on line 3 is AN (incoming call), the called-party number appears. To get the called-party number on incoming calls, you must have DNIS service from your WAN provider. In some cases, the called-party number is not delivered, (for example, when the MAX is behind some types of PBX).

For related information, see the Data Svc parameter in the *MAX Reference Guide*.

Dyn Stat window (dynamic status)

The Dyn Stat window shows the name, quality, bandwidth, and bandwidth utilization of each online multichannel PPP connection with dynamic bandwidth management. To display the Dyn Stat window, tab to a status window, then use the arrow keys to access the Ethernet > Dyn Stat window.

Following is the Dyn Stat display for an Ethernet module in slot 9:

```
90-500 Dyn Stat
Qual Good 00:02:03
```



```
56K      1 channels
CLU  12%  ALU  23%
```

Note: Press the Down Arrow key to see additional online multichannel PPP connections.

The first line of the Dyn Stat window shows the window number and the name of the current Connection profile. If no connection is currently active, the window name appears instead.

The second line lists the quality of the link and the amount of time the link has been active. When a link is online more than 96 hours, the MAX reports the duration in number of days. The link quality can have one of the following values:

- Good—The current rate of CRC errors is less than 1%.
- Fair—The current rate of CRC errors is between 1% and 5%.
- Marg—The current rate of CRC errors is between 5% and 10%.
- Poor—The current rate of CRC errors is more than 10%.
- N/A—The link is not online.

The third line of the Dyn Stat window shows the current data rate in Kbps, and how many channels this data rate represents.

The fourth line displays the following values:

- CLU—Current Line Utilization. The percentage of bandwidth currently being used by the call for transmitted data, divided by the total amount of bandwidth available.
- ALU—Average Line Utilization. ALU is the average amount of available bandwidth used by the call for transmitted data during the current history period as specified by the Sec History and Dyn Alg parameters.

Note: The MAX currently does not calculate CLU or ALU for nailed connections through the serial WAN interface.

Ether Opt window (Ethernet options)

The Ether Opt window lists the type of Ethernet interface specified in the Ethernet I/F parameter, and its MAC address. To display the Ether Opt window, tab to a status window, then use the arrow keys to access the Ethernet > Ether Opt window.

Following is an example of an Ether Opt display for an Ethernet module in slot 9:

```
90-600 Ether Opt
>I/F: COAX
Adrs: 00c07b322bd8
```

The interface type may be AUI, UTP, or COAX. The MAC address is a 6-byte hexadecimal address assigned to the Ethernet controller by the manufacturer. For related information, see the entry for the Ethernet I/F parameter in the *MAX Reference Guide*.

Ether Stat window (Ethernet status)

The Ether Stat window shows the number of Ethernet frames received and transmitted and the number of collisions at the Ethernet interface. To display the Ether Stat window, tab to a status window, then use the arrow keys to access the Ethernet > Ether Stat window.

VT100 Interface Status Windows

Status-window reference in alphabetic order

For example, the following screen shows the Ether Stat display for an Ethernet module in slot 9:

```
90-400 Ether Stat
>Rx Pkt:      106
    Col:       0
Tx Pkt:      118
```

The screen shows the following fields:

- Rx Pkt—the number of Ethernet frames received on the Ethernet interface
- Col—the number of collisions detected at the Ethernet interface
- Tx Pkt—the number of Ethernet frames transmitted over the Ethernet interface

The counts return to 0 (zero) when the MAX is switched off or reset. Otherwise, the counts continuously increase, up to the maximum allowed by the display.

Ethernet window

The Ethernet window is a branch of the Main Status Menu window. The Ethernet window itself has branches, which display the status of the Ethernet interface. When you choose Ethernet from the Main Status Menu window, the following menu appears:

```
50-000 Ethernet
50-100 Sessions
50-200 Routes
50-300 WAN Stat
```

FDL N Stats windows

To display the FDL *N* Stats (Facilities Data Link Status) window, tab to a status window, then use the arrow keys to access the Net/T1 > FDL *N* Stats window.

The MAX has two windows that list the performance registers of the PRI interface: FDL1 Stats for line 1 and FDL2 Stats for line 2.

Note: The name of this window does not imply that you must have a Facility Data Link for the MAX to accumulate data. The registers accumulate data whether you have D4 or ESF lines, and whether or not you have a Facility Data Link.

The FDL Stats windows are the fourth and fifth options listed in the Net/T1 window:

```
10-000 Net/T1
10-300 Line Errors ^
10-400 FDL1 Stats
>10-500 FDL2 Stats
10-600 Net Options
```

The following display shows the contents of the FDL2 Stats window:

```
10-500 FDL2 Stats
>Error Events...
Current Period...
```

```
Last 24 Hours...
00:00...      v
```

Note: Pressing the Down Arrow key displays additional statistics.

Error-register statistics

If you select Error Events, the MAX displays the accumulated error events in the user and carrier error events registers.

Performance-register statistics

You can display the statistics accumulated during the current 15-minute period (Current Period), the summed performance data accumulated during the past 24 hours, or the statistics for any 15-minute period in the previous 24 hours. If you select Last 24 Hours, you can get any past period's registers, select an hour from the window, (03:00, for example), and then select any 15-minute period within that hour. You can select any hour within the last 24.

If you have a D4 (SF) interface, no carrier performance data is recorded.

The performance registers contain both user and carrier Extended Superframe Format (ESF) statistics. The user performance-registers appear in the middle column after the register names, and the carrier performance-registers appear in the last column:

```
10-500 FDL2 Stats
03:45
ES:000005 000005
US:000000 000000
SS:000000 000000
BS 000000 000000
LF:000000 000000
CS:000000 000000
```

Use the Clr Perf1 and Clr Perf2 parameters in the Line Diag menu to reset the user performance registers but only the carrier can reset the carrier registers. All performance registers are reset upon power-up or software reset.

Table 4-2 describes the FDL performance registers.

Table 4-2. FDL performance registers

Register name	Description
EE	Displays the number of error events accumulated since the last time this register was reset. An ESF error event is counted when the CRC-6 calculations at the receiving end of the T1 span do not match the CRC-6 calculations at the sending end. This mismatch indicates that the frame had at least one data error. Error events have no meaning for D4 lines. Only ESF lines carry the CRC-6 signature used to check the quality of the PRI line as a whole.

Table 4-2. FDL performance registers (continued)

Register name	Description
ES	Specifies errored seconds. For ESF lines, this register displays the number of seconds in the 15-minute period in which there was at least one error event, or in which two or more framing errors were detected within a 3 ms interval. For D4 lines, this register displays the number of seconds in which one or more framing bit errors (FE) were detected or in which a controlled slip (CS) occurred.
US	Indicates unavailable seconds—the number of seconds in the 15-minute period preceded by at least 10 consecutive severely errored seconds (SS).
SS	Displays severely errored seconds—the number of seconds, during the 15-minute period, in which there were at least 320 CRC-6 errors as detected by the MAX, or in which the T1 line was out of frame. For D4 lines, this register displays the number of one-second intervals containing eight or more framing bit errors (FEs) or one or more SEFs.
BS	Specifies bursty errored seconds—the number of seconds, during the 15-minute period, in which there were at least 2, but not more than 319, CRC-6 errors as detected by the MAX.
LF	Indicates loss of frame seconds—the number of seconds in the 15-minute period in which the T1 line was out of frame.
CS	Displays controlled slip seconds—the number of seconds in the 15-minute period in which a frame was either replicated or deleted.

For related information, see Clr Err1, Clr Err 2, Clr Perf1, and Clr Perf2 in the *MAX Reference Guide*.

FR Stat window

The FR Stat (Frame Relay status) window shows the status of each online link defined in a Frame Relay profile. To display the FR Stat window, tab to a status window, then use the arrow keys to access the Ethernet > FR Stat > *any active Frame Relay connection* window.

For example, the following screen shows an FR profile display for a link using a serial WAN module is installed in slot B:

```
B0-500 FR profile
Rx Pxt:      2560
Tx Pxt:      3000
CRC:         003
CprofX       16
Rx Pxt:      2560
Tx Pxt:      3000
```

The window shows the number of packets received and transmitted on the Frame Relay connection. It also shows the number of frames received with CRC errors.

Host/6 (Host/Dual) window

The Host/6 (or Host/Dual) status window is a branch of the Main Status Menu window. It holds a list of windows that show the status of the MAX unit's AIM host interface and the status of calls to and from the AIM ports of that interface. To display the Host/Dual status window, tab to a status window, then use the arrow keys to access the Host/Dual window. To display the statistics for a port, choose a port from the Port/*N* Stat Menu submenus.

For example, the following screen shows a Host/Dual status window for a module installed in slot 6:

```
60-000 Host/Dual
60-100 Host Config
60-200 Port1 Menu
60-300 Port2 Menu
```

Line Errors window

The Line Errors status window shows errors recorded on all current channels, in a channel-by-channel, line-by-line list. The display even if the interface is disabled in the Line *N* profile.

To display the Line Errors window, tab to a status window, then use the arrow keys to select a menu item representing a slot configuration (this section assumes a slot configured for T1 lines). After selecting that item, select the Line errors window:

```
10-000 Net/T1
10-100 Line 1 Stat
10-200 Line 2 Stat
10-300 Line Errors
```

Then, when you press Enter or the Right Arrow key, the T1 Line Errors window displays the channel-by-channel errors accumulated during all current calls. The window is divided into three columns. For example:

```
10-300 Ln1  Ln2
1:      0    -
3:     33    -
4:      0    -
```

The first column displays the T1 channel number followed by a colon (:). For a BRI line, it lists the line numbers (1 through 8).

The second column indicates the number of byte errors the MAX has detected on the channel in Line 1 during the current call. The third column displays the number of byte errors the MAX has detected on the channel in Line 2 during the current call.

If a channel is not associated with a current call, a hyphen (-) appears instead of a number. Any channel that would not have a number in either is omitted from the display.

Line Stat windows

The Line Stat windows (Line 1 Stat and Line 2 Stat) show the dynamic status of each WAN line, the condition of its electrical link to the carrier, and the status of its individual channels. To display the Line Status window, tab to a status window, then use the arrow keys to access the Net/T1 > Line *N* Stat (or Net/E1 >Line *N* Stat) window.

For example:

```
10-100 1234567890
L1/LA  -----
      12345678901234
      -----S
```

The first line of a Line Stat window shows the window number followed by columns for channels 1 through 10.

The second line begins with the line number, followed by the link status, which is indicated by one of the two-character abbreviations listed in Table 4-3. Following the link status is followed by a single-character that indicates channel status. Table 4-4 lists the channel-status indicators.) The third line has column headers for the remaining channels. The fourth line continues where the second line left off, showing the status of the remaining channels.

Table 4-3. T1/E1 link-status indicators

Link status	Mnemonic	Description
LA	Link active	The line is active and physically connected.
RA	Red Alarm/Loss of Sync	The line is not connected, improperly configured, experiencing a very high error rate, or is not supplying adequate synchronization. The Alarm LED lights when the line is in this state.
YA	Yellow Alarm	The MAX is receiving a Yellow Alarm pattern. The Yellow Alarm pattern is sent to the MAX to indicate that the other end of the line cannot recognize the signals the MAX is transmitting. The Alarm LED lights when the line is in this state.
DF	D-channel failure	The D channel for a PRI line is not currently communicating.
1S	Keep alive (all ones). Also known as Blue Alarm.	A signal is being sent from the T1 PRI network to the MAX to indicate that the T1 PRI line is currently inoperative. The Alarm LED lights when the line is in this state.
DS	Disabled link	The line is physically connected, but you have disabled the line in the Line <i>N</i> profile.

A single character represents the status of each channel in the line, as described in Table 4-4:

Table 4-4. T1 channel status indicators

Channel status	Mnemonic	Description
.	Not available	The channel is not available because the line is disabled, has no physical link, or does not exist, or because the channel is set to Unused in the Ch <i>N</i> parameter of the Line <i>N</i> profile.
*	Current	The channel is connected in a current call.
-	Idle	The channel is currently idle (but in service).
d	Dialing	The MAX is dialing from this channel for an outgoing call.
r	Ringing	The channel is ringing for an incoming call.
m	Maintenance	The channel is in maintenance/backup (ISDN only).
n	Nailed	The channel is marked Nailed in the Line <i>N</i> profile.
x	Drop-and-Insert	The channel is configured for Drop-and-Insert for a DASS 2 E1 line or DPNSS E1 line.
o	Out of Service	The channel is out of service (ISDN only).
s	ISDN D channel	The channel is an active D channel (ISDN only).
b	Backup ISDN D channel	The channel is the backup D channel (ISDN only).

Note: If the MAX is configured for Drop-and-Insert functionality, and a Red Alarm (RA) or Loss of Synch condition is detected, the failure is conveyed to the device by sending an all ones (A1S) over line 2. During the time this failure is active, devices connected to line 2 cannot place calls.

Line Status (BRI) window

The Line Status window shows the dynamic status of each BRI line, the condition of its electrical link to the carrier, and the status of each line's individual channels. To display the Line Status window, tab to a status window, then use the arrow keys to access the Host/BRI (or Net/BRI) > Line Status window.

For example, the following screen shows a Line Status window for a Net/BRI module installed in slot 4:

```
40-100 12345678    O
Link    PPP-----
```

VT100 Interface Status Windows

Status-window reference in alphabetic order

```
B1      ***.....
B2      ***.....
```

The first line of the Line Status window shows the window number and the column headers for each of the 8 BRI lines in an expansion module. The second line of the window uses the one-character abbreviations listed in Table 4-5 to characterize the overall state of the line. The third and fourth lines show a single-character abbreviations, listed in Table 4-6, that indicate B1 and B2 channels, respectively.

Table 4-5. BRI line-status indicators

Line status	Mnemonic	Description
.	Not available	The line is not active at this time, but it is physically connected.
-	Idle	The line is disabled. The Ch <i>N</i> parameter in the Line <i>N</i> profile is set to Unused.
P	Point-to-point	The line is in a point-to-point active state and is physically connected.
D	Dual-terminal	The line is in a multipoint active state, initialized in dual-terminal mode, and is physically connected.
M	Multipoint	The line is in a multipoint active state, initialized in single-terminal mode, and is physically connected.
X	Not connected	The line is not physically connected and cannot pass data. In some countries outside the U.S., the character X might appear even though the line is physically connected.

The third and fourth lines indicate the state of the B1 and B2 channels, respectively, with the indicators shown in Table 4-6.

Table 4-6. B1 and B2 channel-status indicators

Channel status	Mnemonic	Description
.	Not available	The channel is not available because the line is disabled, has no physical link, or does not exist, or because the channel is set to Unused in the channel usage parameter of the Line <i>N</i> profile.
*	Current	The channel is connected in a current call.
-	Idle	The channel is currently idle (but in service).
d	Dialing	The MAX is dialing from this channel for an outgoing call.
r	Ringing	The channel is ringing for an incoming call.

Message Log windows

You can display the Message Log window for an AIM module (such as Host/6 or Host/Dual) or for the system itself. The contents of the port-specific message log and the contents of the system message log do not overlap. That is, an event described in the system message log is not displayed in the message log specific to an AIM port.

Each message log displays up to 32 of the most recent system events the MAX has recorded. When you select the Message Log option, the most recent message appears. The message logs update dynamically. Press the Up-Arrow key to display the previous entry. Press the Down Arrow key to display the next entry.

To display the Message Log window, tab to a status window, then use the arrow keys to access the Host/Dual > PortN Stat > Messages window.

AIM port message logs

The Message Log window for an AIM port provides a log of events that occurred at each AIM port during call dialing and transmission. You access the window by selecting it from the Port N Stat menu. The following example shows a Message Log entry generated by an incoming call on an AIM port installed in slot 7:

```
71-200 12:23:47    O
>M31 Line 1 Ch 13
Moved to primary
  1 secondary chans
```

The first line of the window shows the status window number and the time the event occurred. The second line identifies the log entry number (M00-M31) and, if applicable, the line and channel on which the event occurred. The third line contains the text of the message (as described in “Log messages” on page 4-20). The fourth line of the log changes when an online FT1-B&O call restores or removes nailed-up channels. The following display shows that one channel has been restored to an FT1-B&O call:

```
00-200 12:23:47    O
>M31 Line 1 Ch 13
Moved to primary
  1 secondary chans
```

System message logs

The Message Log window for the system provides a log of system events. You access the window by selecting it in the System status window. The following example shows a Message Log entry generated by an incoming call not yet assigned to an AIM port:

```
00-200 11:23:55
>M31 Line 1 Ch 07
Incoming Call
MBID 022
```

The first line of the window shows the status window number and the time the event occurred. The second line identifies the log entry number (M00-M31) and, if applicable, the line and channel on which the event occurred. The third line contains the text of the message (as described in “Log messages”). The fourth line contains connection-specific messages (as described in Table 4-9 on page 4-23).

Log messages

Table 4-7 shows the informational messages that can appear in the Message Log window:

Table 4-7. Informational log messages

Message	Description
Added Bandwidth	The MAX has added bandwidth to an active call.
Assigned to port	The MAX has assigned an incoming call to an AIM port, a digital modem, the packet-handling module, or the terminal server.
Call Terminated	An active call was disconnected normally, although not necessarily by operator command.
Callback Pending	The MAX is waiting for callback from the remote end.
Ethernet up	The Ethernet interface has been initialized and is running.
Handshake Complete	The handshake was completed, but no channels were added. Either an operator entered the DO R command to resynchronize channels, or an attempt to add channels to an inverse-multiplexing call failed.
Incoming Call	The MAX has answered an incoming call at the T1 PRI network interface, but has not yet assigned the call to an AIM port or to the IP router.
Incomplete Add	An attempt to add channels to an inverse-multiplexing call failed. The MAX added some channels, but fewer than the number requested. This situation can occur when placing a call. The first channel connects, but the requested base channel count fails.
LAN session down	Appears before Call Terminated if a PPP, MP+, or Combinet session is terminated.
LAN session up	Appears after Incoming Call if a PPP, MP+, or Combinet session is established.
Moved to primary	Some nailed-up channels that the MAX removed from an FT1-B&O call have been restored because their quality was no longer poor. The fourth line of the Message Log window indicates the number of channels restored.
Moved to secondary	The MAX has detected some poor quality nailed-up channels in an FT1-B&O call, and has backed up the call on switched channels. The fourth line of the Message Log window indicates the number of channels removed.
Outgoing Call	The MAX has dialed a call.
Port use exceeded	Call usage for an AIM port has exceeded the maximum specified by either the MAX DS0 Mins or MAX Call Mins parameter in the Port profile.

Table 4-7. Informational log messages (continued)

Message	Description
Removed Bandwidth	The MAX has removed bandwidth from an active call.
Sys use exceeded	Call usage for the entire system has exceeded the maximum specified by the MAX DS0 Mins parameter in the System profile.
RADIUS config error	The MAX has detected an error in the configuration of a RADIUS user entry.
Requested Service Not Authorized	Appears in the terminal-server interface if the user requests a service not authorized by the RADIUS server.

Table 4-8 shows the warning messages that can appear in the Message Log windows.

Table 4-8. Warning log messages

Message	Description
Busy	The phone number was busy when the call was dialed.
Call Disconnected	The call has ended unexpectedly.
Call Refused	An incoming call could not be connected to the specified AIM port, digital modem, packet-handling module, or terminal server because the resource was busy or otherwise unavailable.
Dual Port req'd	The call could not be placed because one or both ports of the dual-port pair were not available.
Far End Hung Up	The remote end terminated the call normally.
Incoming Glare	The MAX could not place a call because it saw an incoming <i>glare</i> signal from the switch. Glare occurs when you attempt to place an outgoing call and answer an incoming call simultaneously. If you receive this error message, you have probably selected incorrect settings in the Line <i>N</i> profile.
Internal Error	Call setup failed because of a lack of system resources. If this type of error occurs, notify Ascend Customer Service.
LAN security error	Appears after Incoming Call but before Call Terminated if a PPP, MP+, terminal-server, or Combinet session has failed authentication, another session by the same name already exists, or the timeout period for RADIUS/TACACS authentication has been exceeded. For details, see the entry for the Auth Timeout parameter in the <i>MAX Reference Guide</i> .

Table 4-8. Warning log messages (continued)

Message	Description
Network Problem	The call setup was faulty because of problems within the WAN or in the Line <i>N</i> profile configuration. The D channel might be getting an error message from the switch, or the telco might be experiencing a problem.
No Chan Other End	No channel was available on the remote end to establish the call.
No Channel Avail	No channel was available to dial the initial call.
No Connection	The remote end did not answer when the call was dialed.
No Phone Number	No phone number exists in the Call profile being dialed.
No port DSO Mins	No maximum has been specified for the MAX DSO Mins or MAX Call Mins parameter in the Port profile.
No System DSO Mins	No maximum has been specified for the MAX DSO Mins parameter in the System profile.
Not Enough Chans	A request to dial multiple channels or to increase bandwidth could not be completed because there were not enough channels available.
Not FT1-B&O	The local MAX attempted to connect an FT1-B&O call to the remote end, but the call failed because the call type at the remote end was not FT1-B&O.
Remote Mgmt Denied	The MAX rejected a request to run the remote MAX by AIM remote management because the Remote Mgmt parameter in the System profile at the remote end is set to No.
Request Ignored	The MAX denied a request to manually change bandwidth during a call because the Call Mgm parameter in the Call profile is set to Dynamic. With this setting, the MAX allows only automatic bandwidth changes.
Wrong Sys Version	The remote-end product version was incompatible with the version of the local MAX. The software version appears on the Sys Options status window.

Table 4-9 shows connection messages that can appear on the fourth line of the Message Log windows.

Table 4-9. Message indicators

Indicator	Description
MBID value	Appears with either the Incoming Call or Assigned to Port (line 3) messages. The first message means an incoming call has been received and the second message means it has been routed to a MAX port. If you cannot match the MBID value of an incoming call log to the MBID value in an assigned-to-port log, the call disconnected, often because the intended port was busy. MBID also appears in the System log.
Channels	Number of channels added to or removed from a call. Appears with the Added Bandwidth, Removed Bandwidth, Moved to Primary, and Moved to Secondary messages. When line 3 is an Outgoing Call, line 4 displays the phone number dialed. In multichannel calls, line 4 displays the phone number for the first connection. Only the phone number appears. The parameter name, Phone Number, does not.
Cause Code	Indicates a signaling error or event. The code number was sent by the ISDN network equipment and received by the MAX.
Name	When the message in line 3 is either LAN session up or LAN session down, line 4 displays the remote end's name. If the session is a Combind bridging link, the MAC address is displayed. If the session is a PPP link, either the remote end's system name (as specified by the Name parameter in the System profile) or IP address (as specified by the IP Adrs parameter in the Ethernet profile) is displayed. The IP address is displayed only if the system's name is not known.
CLID	When an incoming call is answered and the calling party number is known, line 4 specifies the calling line ID (CLID). When the CLID appears, the MBID does not.

Modem window

The Main Status Menu window contains an entry for each modem card. When you select the modem entry for a card, the Modem Stat (modem status) menu appears in the window. In this menu, each modem corresponds to a display character. To display the Modem Stat window for a modem module, tab to a status window, then use the arrow keys to access the V.34 Modem > Modem Stat window.

Following is an example of a Modem Stat window for an 8 modem card:

```
80-000 Modem Stat
12345678
_**_*_**
```

The first line shows the window name. The second line lists the modems by number, and the third line contains a status indicator. Table 4-10 describes the status indicators.

Table 4-10. Modem-status characters

Indicator	Mnemonic	Description
.	Nothing	Modem is nonexistent.
f	Failed	Modem failed the Power-On Self Test (POST). The modem is unavailable for use.
-	Not used	The modem is not in use.
a	Waiting to go active	Modem has been instructed to dial or answer a call, and the unit is waiting for Received Line Signal Detector (RLSD) to go active.
A	Active	RLSD is already active and the unit is waiting for result codes to be decoded. This state is entered only if RLSD precedes the codes.
*	Connected	A call is connected, and the unit is monitoring RLSD.
i	Initializing	Modem is reinitializing after being reset.
q	Open request	Modem is reinitializing after being reset and an open request is waiting to be processed when reinitialization is completed.
Q	Open request for virtual connection	Modem is reinitializing after being reset and an open request for virtual connection is waiting to be processed when reinitialization is completed.
d	Dialing	The first part of the dial string has been sent. This unit is pausing for the modem to read and process the first part before sending the second part.
v	Virtual connection	Virtual connection session is active on modem. No call is yet active.
o	out of service in interface	User has disabled the modem from the MAX configuration interface. The modem is unavailable for calls.
O	Out of service	User has disabled the modem from the MAX configuration interface. The modem is unavailable for calls and a Bchannel is set to OutOfService.

Net T1, Net E1 and Net BRI windows

Net/T1, Net/E1 and Net/BRI windows are branches of the Main Status Menu window. The Net/BRI window is available only if a Net/BRI module is installed. To display the Net/BRI window, tab to a status window, then use the arrow keys to access the Net/BRI window.

Following are the contents of the Net/T1 window for the base system's T1 PRI interface:

```
10-000 Net/T1
  10-100 Line 1 Stat
>10-200 Line 2 Stat
  10-300 Line Errors
```

Following are the contents of the Net/E1 window for the base system's E1 PRI interface:

```
10-000 Net/E1
  10-100 Line 1 Stat
>10-200 Line 2 Stat
  10-300 Line Errors
```

Following are the contents of the Net/BRI window:

```
40-000 Net/BRI
>40-100 Line Status
  40-200 Line Errors
```

Net Options window

The Net Options window lists the WAN interface features installed on your MAX. To display the Net Options window, tab to a status window, then use the arrow keys to access the Net/T1 > Net Options window.

The following screen shows the Net Options window:

```
Net Options
>T1/PRI Network I/F
  2 Network I/F(s)
Type: CSU/CSU
```

The first line shows the type of physical interface to the WAN or, in the case of Host BRI modules, to the local BRI lines. The line can specify either T1/PRI Network I/F or BRI Network I/F.

The second line shows the number of network interfaces associated with the module.

The third line shows whether internal CSUs are installed for the T1 lines. Following are the values that can appear:

- Type: DSX/DSX
- Type: CSU/DSX
- Type: DSX/CSU
- Type: CSU/CSU

Port Info window

The Port Info window displays the status of active calls and indicates the bandwidth that current calls are not using. To display the Port Info window, tab to a status window, then use the arrow keys to access the Host/Dual > Port/V Stat > Statistics window.

Following is an example of a Port Info window:

```
00-300 Port Info
  Avail BW= 128K
  DS0 Mins=12
>71 O G 384K      v
```

The first line specifies the window number and name. The second line indicates the available bandwidth. The third line displays the current accumulated DS0 minutes for all calls placed from the MAX.

The fourth line and subsequent lines that follows it display the AIM host-interface status. Each line includes the following fields, in the order shown:

- Module and port number.
- Call-status indicator (described in Table 4-11).
- Call-quality indicator (the quality of the link for an active call). Possible values are G (good), F (fair), M (marginal), N (not applicable), or P (poor). The *N* value appears before the call is connected end-to-end.
- Bandwidth (the approximate bandwidth given to the codec). For an FT1-B&O call, both specify the offline bandwidth and the online bandwidth of the call are shown. For example, the following screen shows statistics for an FT1-B&O call on the base system's AIM port 2:

```
00-300 Port Info
  Avail BW= 128K
  21 O G 384K
>22 O G 128K/ 64K
```

In the preceding example, the fourth line shows that AIM port 2 has an FT1-B&O call online. The call is running at 128 Kbps, and an additional 64 Kbps is available but has been removed from the call. Whenever nailed-up channels in an FT1-B&O call are bad, the MAX removes them from the call and monitors them for possible restoration. In this example, the MAX has removed one 64K channel and is monitoring it.

Table 4-11 shows call-status indicators for AIM port calls.

Table 4-11. Call-status characters for AIM ports

Indicator	Mnemonic	Description
Blank	Nothing	No calls exist and no other MAX operations are being performed.
R	Ringing	An incoming call is ringing on the line, ready to be answered.
A	Answering	The MAX is answering an incoming call.

Table 4-11. Call-status characters for AIM ports (continued)

Indicator	Mnemonic	Description
C	Calling	The MAX is dialing an outgoing call.
O	Online	A call is up on the line.
H	Hanging up	The MAX is clearing the call.
D	Diagnostics	The MAX is performing a local loopback.
!	Handshaking	Handshaking is in progress.
L	Loopback	A remote loopback is in progress.
S	Setting up	The MAX is setting up handshaking.
T	BERT	A BERT is in progress.
??	Alarm	A WAN network alarm is in effect.

Port Leads window

The MAX provides a Port Leads status window for checking the state of the input and output control leads of the associated AIM port. A Port Leads status window exists for each AIM port. A Port Leads status window also exists for the serial WAN port. By checking the status of an AIM port's control leads, you can monitor an automatic dialing or answering process, such as X.21, V.25 bis, RS-366, or control-lead dialing.

To display the Port Leads window for an AIM module, tab to a status window, then use the arrow keys to access the Host/Dual > PortN Stat > Port Leads window.

Following is an example of a Port Leads window for the serial WAN port:

```
B0-100 Port Leads
DSR+ DCD+ RI + DTR+
```

Note: DCD stands for Data Carrier Detect and is sometimes abbreviated simply as CD.

The first line of the window shows the slot-port address of the AIM port. The remaining lines show the state of the control leads going into and out of the serial port. A plus symbol (+) indicates an active control lead. A minus symbol (-) indicates that the lead is inactive. For RS-366 dialing output and input signals, the MAX uses the abbreviations in Table 4-12.

Table 4-12. RS-366 abbreviations

Output	Input
acr (Abandon Call and Retry)	dp (Digit Present)

VT100 Interface Status Windows

Status-window reference in alphabetic order

Table 4-12. RS-366 abbreviations (continued)

Output	Input
pnd (Present Next Digit)	crq (Call Request)
dlo (Data Line Occupied)	

If the port is an RS-366 dialing interface, the lower right-hand corner of the Post Leads window has a Digit field that displays the last digit dialed.

Table 4-13 lists the abbreviations for dialing output and input signals at the AIM port. The Clear to Send (CTS) output signal is not monitored in this window. The standard cables supplied with the MAX tie CD and CTS together.

Table 4-13. Serial host port abbreviations

Output	Input
DSR (Data Set Ready)	DTR (Data Terminal Ready)
CD (Carrier Detect)	RTS (Request to Send)
RI (Ring Indicate)	

Table 4-14 lists the abbreviations used for dialing output and input signals at the serial WAN port.

Table 4-14. Serial WAN port abbreviations

Output	Input
DSR (Data Set Ready)	DTR (Data Terminal Ready)
CD (Carrier Detect)	
RI (Ring Indicate)	

Port Opts window

The Port Opts window is a read-only window that displays information about the configuration options for the MAX unit's AIM ports. A Port Opts status window exists for each AIM port. To display the Port Opts window for an AIM module, tab to a status window, then use the arrow keys to access the Host/Dual > Port*n* Stat > Port Opts window.

Following is an example of the Port Opts window for the fourth AIM port on a Host/6 card in slot 7:

```
71-400 Port Opts
>V.35 Host I/F
```

The first line of the window shows the slot-port address of the AIM port. The second line indicates the electrical interface of the port. The MAX senses the type of cable you plugged into the AIM port and changes its electrical characteristics accordingly. Table 4-15 describes the values that can appear.

Table 4-15. Port Opts information

Value	Description
V.35 Host I/F	The port is electrically compatible with CCITT V.35.
RS-449 Host I/F	The port is electrically compatible with RS-449/422 and X.21.
Universal Host I/F	The MAX displays this value for every host port of the Host/6 module, regardless of whether a cable is installed at the port. The port is compatible with V.35, RS-449/422, and X.21.

PortN Stat window

The PortN Stat window appears in the Host/6 or Host/Dual branch of the Main Edit Menu. It displays a list of windows, each of which shows the status of an AIM port. For example, if you select the listing for the first port of an AIM card installed in slot 7, the following window appears:

```
71-000 Port1 Stat
71-100 Call Status
71-200 Message Log
71-300 Statistics
>71-400 Port Opts
71-500 Session Err
71-600 Port Leads
```

Routes window

The Routes window displays the current routing table. To display the Routes window, tab to a status window, then use the arrow keys to access the Ethernet > Routes window.

A Routes window initially displays the first route in the table. For example:

```
50-200 Routes
>D: 223.0.100.129
G: 223.0.100.129
LOOP Active
```

Note: Press the Down Arrow key to display the next route, or the Up Arrow key to display the previous one.

The second line in a Routes window contains the destination address. The destination can be a network address or the address of a single station. If the route is the default route, the word Default replaces the address.

The third line shows the address of the router.

The fourth line can have one of the values listed in Table 4-16.

Table 4-16. Routes-window values

Value	Description
LAN Active	Active route. Has a destination on the local subnet.
WAN Active	Active route. Has a destination off the local subnet.
LOOP Active	Active route. Has this MAX as a router and destination. No data packets are propagated.
LAN Inactive	Inactive route. Has a destination on the local subnet.
WAN Inactive	Inactive route. Has a destination off the local subnet.

A route becomes inactive if taken out of service. Whether a dialed-up link in a route has or has not been connected does not affect the active or inactive status of the route

Serial WAN window

The Serial WAN status window is a branch of the Main Status Menu. It displays the status of the serial WAN interface. From this window, you can show the Port Leads status display, which indicates the status of the serial WAN port's control signals. To display the Serial WAN window, tab to a status window, then use the arrow keys to access the Serial WAN > Port Leads window.

Session Err window

The Session Err status window displays the errors encountered during the current call, on a channel-by-channel, line-by-line basis. A Session Err window exists for each host port. The second and subsequent rows of this window each reports the accumulated errors on one of the channels active in the call. Each row has four fields, separated by colons. For example:

```
21-500 Errors      O
1: 1: 1:          0  -
1: 1: 3:         33  -
1: 1: 4:          0  -
```

The first column in this display shows the T1 line's slot number. The second column shows the line number (1 or 2), and the third column 3 shows the channel number on which the error occurred.

Column 4 shows the number of byte errors detected during the current call. In an online FT1-B&O call, any channels that the MAX has removed have an asterisk (*) after the error column.

If a channel is not associated with the current call, its session errors are displayed as a hyphen (-). Any line in the display that would show dashes in both columns is omitted.

(For related information, see "Line Errors window" on page 4-15.)

Sessions window

The Sessions status window indicates the number of active bridging/routing links or remote terminal-server sessions. An online link, as configured in the Connection profile, constitutes a single active session. A session can be PPP or Combinet-encapsulated. The MAX treats each multichannel MP+ or MP link as a single session. The following screen shows the display when the Ethernet module is installed in slot 5:

```
50-100 Sessions
>5 Active
O Headquarters
```

The first line specifies the number and name of the window. The second line shows the number of active sessions. The third and all remaining lines use the following format:

```
status remote device
```

where *status* is a status indicator and *remote device* is the name, address, or CLID of the remote device. Table 4-17 lists the session-status characters that can appear.

Table 4-17. Session status characters

Indicator	Mnemonic	Description
Blank	Nothing	No calls exist and no other MAX operations are being performed.
R	Ringing	An incoming call is ringing on the line, ready to be answered.
A	Answering	The MAX is answering an incoming call.
C	Calling	The MAX is dialing an outgoing call.
O	Online	A call is up on the line.
H	Hanging up	The MAX is clearing the call.

Note: For remote terminal-server sessions, the third and following lines of the Sessions window appear in the format Modem *slot:position*, where *slot* specifies the slot of the active digital modem, and *position* is a number indicating the position of the modem in that slot.

Statistics window

The Statistics window is an AIM-port-specific window that provides information about line utilization and synchronization delay while a call is up. A Statistics window exists for each AIM port. For example, a Statistics window with the following contents would apply to the first port of an AIM card installed in slot 7:

```
71-300 Albuquerque+ O
Qual Good 01:23:44
MAX Rel Delay 10
CLU 80% ALU 77%
```

The first line of the Statistics window shows the status window number. This number includes the host port's number, the name of the current Call profile, and the call-status character.

The second line lists the quality of the call and the call duration. When a call lasts more than 96 hours, the window displays the call duration in number of days. The call quality, or Qual, can be Good, Fair, Marg (marginal), or Poor. The meaning of each value is as follows:

- Good—No errors have been detected during the transmission of the call.
- Fair—Some errors have been detected in transmission.
- Marg—A significant number of errors have been detected. In this case, reliable transmission is not guaranteed and resynchronization is recommended.
- Poor—The MAX might drop individual channels from the call, or clear the call automatically.

For FT1-B&O calls, the second line of the Statistics window might not show the call duration. When an FT1-B&O call has no bad channels, the call duration appears as usual. But if it does, the number of offline nailed-up channels appears after the call quality. The following screen shows the Statistics window of an FT1-B&O call with two channels offline:

```
21-300 Albuquerque+ O
Qual Good 00:04:01
MAX Rel Delay 10
CLU 80% ALU 77%
```

The third line displays the MAX Rel Delay value. During a MAX call, different channels can take different paths through the WAN and can arrive at the destination at different times. This difference is known as a relative delay. The MAX Rel Delay value indicates the largest amount of delay between any two channels in the call. The delay is calculated and reported in multiples of 125 microseconds, and cannot exceed 3000.

The last line displays the following values:

- CLU—Current line utilization. The percentage of bandwidth currently being used by the call for transmitted data, divided by the total amount of bandwidth that is available.
- ALU—Average line utilization. The average amount of available bandwidth used by the call for transmitted data during the current history period as specified by the Sec History and Dyn Alg parameters.

CLU and ALU apply only to calls for which Call Mgm=Dynamic and Call Type=FT1-AIM or FT1-B&O in the Call profile.

(For related information, see the Call Mgm, Call Type, Dyn Alg, and Sec History parameters in the *MAX Reference Guide*.)

Syslog window

Syslog is not a MAX status display, but an IP protocol that sends system-status messages to a host computer, known as the Syslog host. The Log Host parameter in the Ethernet profile specifies the Syslog host, which saves the system-status messages in a log file. The messages are derived from two sources—the Message Log display and the CDR display.

Note: See the UNIX man pages about `logger(1)`, `syslog(3)`, `syslog.conf(5)`, and `syslogd(8)` for details of the `syslog` daemon. The Syslog function requires UDP port 514.

Level 4 and Level 6 syslog messages

The data for Level 4 (warning) and Level 6 Syslog messages is derived from the Message Log displays. Level 4 and Level 6 messages are presented in the following format:

```
ASCEND: slot-n port-n | line-n, channel-n, text-1
ASCEND: slot-n port-n | line-n, channel-n, text-2
```

The device address (slot, port or line, and channel) is followed by two lines of text, which are displayed on lines 3 and 4 of the Message Log window. The device address is suppressed when it is not applicable or unknown.

The line represented by `text-2` specifies the system name and IP address or MAC address of the remote end of a session for the LAN Session Up and LAN Session Down messages in the line represented by `text-1`.

Level 5 Syslog messages

The data for Level 5 (notice) Syslog messages is derived from the CDR display, lines 3 and 4. Level 5 messages are presented in the following format:

```
ASCEND: call-event-ID event-description slot-N port-N
data-svcK phone-N
```

- `call-event-ID` specifies the event ID in the CDR display.
- `event description` is a description of the CDR event.
- `slot N port N` address indicates the AIM port, which is suppressed when it is not applicable or is unknown.
- `data-svcK` indicates the data service in use.
- `phone-N` is the phone number.

Example

Because the date, type, and name of a Syslog message are added by the Syslog host, the MAX does not include that data in the message format. Following are sample Syslog entries from a Syslog host:

```
Oct 21 11:18:07 marcsMAX ASCEND: slot 0 port 0, line 1, channel
1, \
No Connection
```

```
Oct 21 11:18:07 marcsMAX ASCEND: slot 4 port 1, Call Terminated
```

```
Oct 21 11:19:07 marcsMAX ASCEND: slot 4 port 1, Outgoing Call,
123
```

In this example, three messages are displayed for the system `marcsMAX`. Notice that the back-slash (\) indicates the continuation of a log entry onto the next line.

Disconnect codes and Progress codes

If the Syslog option is set, a Call-Close (CL) message is sent to the Syslog daemon whenever a connection is closed. Additional information about the user name, Disconnect code, Progress

VT100 Interface Status Windows

Status-window reference in alphabetic order

code, and login host is appended to each CL message. The CL message uses the following format:

```
[name, ]c=xxxx,p=yyyy,[ip-addr]
```

where:

- name is the name of a profile. It can contain up to 64 characters. A name containing more than 64 characters is truncated, and a plus sign is added to the truncated name. The name appears for incoming calls only.
- xxxx is the Disconnect code.
- yyyy is the connection Progress code.
- ip-addr is the login host's IP address for Telnet and raw TCP connections (if applicable).

Table 4-18 lists the Ascend Disconnect codes.

Table 4-18. Ascend Disconnect codes

Disconnect code	Description
1	Not applied to any call.
2	Unknown disconnect.
3	Call disconnected.
4	CLID authentication failed.
5	RADIUS timeout during authentication.
6	Successful authentication. MAX is configured to call the user back.
7	Pre-T310 Send Disc timer triggered.
9	No modem is available to accept call.
10	Modem never detected Data Carrier Detect (DCD).
11	Modem detected DCD, but modem carrier was lost.
12	MAX failed to successfully detect modem result codes.
13	MAX failed to open a modem for outgoing call.
14	MAX failed to open a modem for outgoing call while ModemDiag diagnostic command is enabled.
20	User exited normally from the terminal server.
21	Terminal server timed out waiting for user input.
22	Forced disconnect when exiting Telnet session.
23	No IP address available when invoking PPP or SLIP command.

Table 4-18. Ascend Disconnect codes (continued)

Disconnect code	Description
24	Forced disconnect when exiting raw TCP session.
25	Exceeded maximum login attempts.
26	Attempted to start a raw TCP session, but raw TCP is disabled on MAX.
27	Control-C characters received during login.
28	Terminal-server session cleared ungracefully.
29	User closed a terminal-server virtual connection normally.
30	Terminal-server virtual connect cleared ungracefully.
31	Exit from Rlogin session.
32	Establishment of rlogin session failed because of bad options.
33	MAX lacks resources to process terminal-server request.
35	MP+ session cleared because no null MP packets received. A MAX sends (and should receive) null MP packets throughout an MP+ session.
40	LCP timed out waiting for a response.
41	LCP negotiations failed, usually because user is configured to send passwords via PAP, and MAX is configured to only accept passwords via CHAP (or vice versa).
42	PAP authentication failed.
43	CHAP authentication failed.
44	Authentication failed from remote server.
45	MAX received Terminate Request packet while LCP was in open state.
46	MAX received Close Request from upper layer, indicating graceful LCP closure.
47	MAX cleared call because no PPP Network Core Protocols (NCPs) were successfully negotiated. Typically, there is no agreement on the type of routing or bridging that is supported for the session.
48	Disconnected MP session. The MAX accepted an added channel, but cannot determine the call to which to add the new channel.
49	Disconnected MP call because no more channels can be added.

Table 4-18. Ascend Disconnect codes (continued)

Disconnect code	Description
50	Telnet or raw TCP session tables full.
51	MAX has exhausted Telnet or raw TCP resources.
52	For Telnet or raw TCP session, IP address is invalid.
53	For Telnet or raw TCP session, MAX cannot resolve hostname.
54	For Telnet or raw TCP session, MAX received bad or missing port number.
60	For Telnet or raw TCP session, host reset.
61	For Telnet or raw TCP session, connection was refused.
62	For Telnet or raw TCP session, connection timed out.
63	For Telnet or raw TCP session, connection closed by foreign host.
64	For Telnet or raw TCP session, network unreachable.
65	For Telnet or raw TCP session, host unreachable.
66	For Telnet or raw TCP session, network admin unreachable.
67	For Telnet or raw TCP session, host admin unreachable.
68	For Telnet or raw TCP session, port unreachable.
100	Session timed out.
101	Invalid user.
102	Callback enabled.
105	Session timeout on the basis of encapsulation negotiations.
106	MP session timeout.
115	Instigating call no longer active.
120	Requested protocol is disabled or unsupported.
150	Disconnect requested by RADIUS server.
151	Call disconnected by local administrator.
152	Call disconnected via SNMP.
160	Exceeded maximum number of V.110 retries.

Table 4-19 lists the Ascend Progress codes.

Table 4-19. Ascend Progress codes

Progress code	Description
1	Not applied to any call.
2	Unknown progress.
10	MAX has detected and accepted call.
30	MAX has assigned modem to call.
31	Modem is awaiting DCD from far-end modem.
32	Modem is awaiting result codes from far-end modem.
40	Terminal-server session started.
41	Raw TCP session started.
42	Immediate Telnet session started.
43	Connection made to raw TCP host.
44	Connection made to Telnet host.
45	Rlogin session started.
46	Connection made with Rlogin session.
47	Terminal-server authentication started.
50	Modem outdial session started.
60	LAN session is up.
61	Opening LCP.
62	Opening CCP.
63	Opening IPNCP.
64	Opening BNCP.
65	LCP opened.
66	CCP opened.
67	IPNCP opened.
68	BNCP opened.
69	LCP in Initial state.
70	LCP in Starting state.

Table 4-19. Ascend Progress codes (continued)

Progress code	Description
71	LCP in Closed state.
72	LCP in Stopped state.
73	LCP in Closing state.
74	LCP in Stopping state.
75	LCP in Req-Sent state.
76	LCP in Ack-Rcvd state.
77	LCP in Ack-Sent state.
80	IPX NCP in Open state.
81	AT NCP in Open state.
82	BACP being opened.
83	BACP is now open.
84	CBCP being opened.

The backoff queue error message in the Syslog file

The MAX keeps accounting records until the accounting server acknowledges them. The backoff queue stores up to 100 unacknowledged records. If the unit never receives an acknowledgment to an accounting request, it eventually runs out of memory. To prevent this situation, the MAX might delete an accounting record and send the following error message to the Syslog file:

```
Backoff Q full, discarding user username
```

This error generally occurs for one of the following reasons:

- You enabled RADIUS accounting on the MAX but not on the RADIUS server.
- The Accounting Port or Accounting Key value is incorrect. The Accounting Key value must match the value assigned in the RADIUS clients file or in the TACACS+ configuration file.
- You are using the Livingston server instead of the Ascend server.

Syslog messages initiated by a SecureConnect Manager firewall

Depending on the settings specified in SecureConnect Manager (SCM), the MAX might generate Syslog messages about packets detected by a firewall. By default, SCM specifies generation of a Syslog message about every packet blocked by the firewall. All messages initiated by a firewall are in the following format:

```
date time router name ASCEND: interface message
```

- *date* is the date the message was logged by Syslog.
- *time* is the time the message was logged by Syslog.
- *router name* is the router this message was sent from.
- *interface* is the name of the interface (ie0, wan0, and so on) unless a call filter logs the packet as it brings up the link, in which case the word *call* appears.
- *message* format has a number of fields, one or more of which may be present.

The message fields appear in the following order:

protocol local direction remote length frag log tag

Table 4-21 describes the fields.

Table 4-20. Syslog message fields for SecureConnect firewalls

Field	Description
<i>protocol</i>	The four-character (hexadecimal) Ether Type or one of the following network protocol names: ARP, RARP, IPX, Appletalk. For IP protocols, the field contains either the IP protocol number (up to three decimal digits) or one of the following names: IP-IN-IP, TCP, ICMP, UDP, ESP, AH. In the special case of ICMP, the field also includes the ICMP Code and Type ([<i>Code</i>]/[<i>Type</i>]/icmp).
<i>local</i>	For non-IP packets, <i>local</i> is the source Ethernet MAC address of transmitted packets and the destination Ethernet MAC address of received packets. For a nonbridged WAN connection, the two MAC addresses are all zeros. For IP protocols, <i>local</i> is the IP source address of transmitted packets and the IP destination address of received packets. In the case of TCP or UDP, it also includes the TCP or UDP port number ([<i>IP-address</i>];[<i>port</i>]).
<i>direction</i>	An arrow (<- or ->) indicating the direction in which the packet was traveling (receive and send, respectively).
<i>remote</i>	For non-IP protocols, <i>remote</i> has the same format that <i>local</i> has for non-IP packets, but shows the destination Ethernet MAC address of transmitted packets and the source Ethernet MAC address of received packets. For IP protocols, <i>remote</i> has the same format as <i>local</i> but shows the IP destination address of transmitted packets and the IP source address of received packets.
<i>length</i>	The length of the packet in octets (8-bit bytes).
<i>frag</i>	Indicates that the packet has a nonzero IP offset or that the IP More-Fragments bit is set in the IP header.

Table 4-20. Syslog message fields for SecureConnect firewalls

Field	Description
<i>log</i>	Reports one or more messages based on the packet status or packet header flags. The packet status messages include: <ul style="list-style-type: none">• <i>corrupt</i>—the packet is internally inconsistent• <i>unreach</i>—the packet was generated by an “unreach=” rule in the firewall• <i>!pass</i>—the packet was blocked by the data firewall• <i>bringup</i>—the packet matches the call firewall• <i>!bringup</i>—the packet did not match the call firewall• <i>syn, fin, rst</i>—TCP flag bits. The <i>syn</i> bit is only displayed for the initial packet, which has the <i>syn</i> flag set instead of the <i>ack</i> flag set.
<i>tag</i>	Any user-defined tags specified in the filter template used by SCM

Sys Options window

The Sys Options window provides a read-only list that identifies your MAX and names each feature that has been installed. The following screen shows the Sys Options window:

```
00-100 Sys Options
>Security Prof:1  ^
  Software +1.0+
  S/N:42901
```

Table 4-21 describes the information that the Sys Options window can contain:

Table 4-21. Sys Options information

Option	Description
Security Prof: 1, Security Prof: 2...	Shows which of the nine Security profiles is active.
Software	Defines the version and revision of the system ROM code.
S/N	Displays the serial number of the MAX. The serial number of your MAX can also be found on the model number/serial number label on the MAX unit's bottom panel.
Up: <i>uptime</i>	<p>Displays the system uptime in the following format: Up: <i>days:hours:minutes:seconds</i></p> <p>For example: Up: 13:12:18:26</p> <p>The Days value <i>turns over</i> every 999 days. If the unit stays up continuously for 1000 days, the initial field resets to a 0 and begins incrementing again.</p>
MAX 6000	<p>Identifies the Ascend unit.</p> <p>Note: If you have a MAX running Multiband Simulation, the name that appears here is Multiband MAX 6000.</p>
Load	Indicates the software load name. Ascend software releases are distributed in software loads, which vary according to the functionality and target platform for the binary.
Switched Installed or Switched Not Inst	Indicates whether the MAX can place calls over switched circuits.
Frm Rel Installed or Frm Rel Not Inst	Indicates whether the Frame Relay option is installed.
Sec Acc Installed or Sec Acc Not Installed	Indicates whether the Secure Connect Firewall option is installed.
MAX Link Installed or MAX Link Not Inst	Indicates whether the MAX Link option is installed.
PRI <-> T1 Installed or PRI <-> T1 Not Inst	Indicates whether the PRI to T1 signaling option is installed. The option is used for PBX support.
MRate Installed or MRate Not Installed	Indicates whether the unit supports MultiRate and GloBand ISDN data services. Currently, T1 PRI providers in the U.S. do not support GloBand.
RS-366 Installed or RS-366 Not Inst	Indicates whether the EIA RS-366 dialing protocol has been installed.

Table 4-21. Sys Options information (continued)

Option	Description
Dyn Bnd Installed or Dyn Bnd Not Inst	Indicates whether Dynamic Bandwidth Allocation functionality is available.
ISDN Sig Installed or ISDN Sig Not Inst	Indicates whether or not ISDN signaling is installed.
AIM Nx56 Installed or AIM Nx56 Not Inst	Indicates whether Ascend Inverse Multiplexing (AIM) functionality is available. This functionality includes AIM remote management and BONDING, a prerequisite for Dynamic Bandwidth Allocation.
BONDING Installed or BONDING Not Inst	Indicates whether BONDING functionality is available.
V.25bis Installed or V.25bis Not Inst	Indicates whether the CCITT V.25 bis dialing and answering protocol is installed.
X.21 Installed or X.21 Not Inst	Indicates whether the X.21 dialing and answering protocol is installed.
MAX Dial Installed or MAX Dial Not Inst	Indicates whether the MAX Dial client software option is installed.
AuthServer: <i>a.b.c.d</i>	Shows the IP address of the current RADIUS authentication server for this unit.
AcctServer: <i>a.b.c.d</i>	Shows the IP address of the current RADIUS accounting server for this unit.
Dual Slot T1	Does not apply to this version of the MAX.
Data Call	Indicates whether the Hybrid Access option is installed.
SerialPortT1-CSU	Indicates whether the nailed T1 (or E1) line is installed. Does not apply to E1 units.

Note: Although GloBanD (Q.931W) does not appear in the Sys Options window, its presence can be verified by checking the value of the Switch Type parameter. For more information, see the *MAX Reference Guide*.

System Status window

The System Status window is a branch of the Main Status Menu. It displays the windows that show the status of the MAX system as a whole.

The System Status window contains the following selections:

```
00-000 System
  00-100 Sys Options
>00-200 Message Log
```



```
00-300 Port Info
00-400 CDR
```

These selections provide information, about the MAX, that pertains to the system as a whole, and that would not fall under the classification of its T1 PRI or ISDN BRI line interfaces, its Ethernet interface, or its AIM host interface.

WAN Stat window

The WAN Stat window displays the current count of received frames, transmitted frames, and frames with errors for each active WAN link. It also indicates the overall count for all data packets received or transmitted across the WAN.

The following screen shows WAN statistics:

```
50-300 WAN Stat
>Rx Pkt:  387112
Tx Pkt:   22092
CRC:    0
```

The first line displays the window number and name of the window. You can press the Down-Arrow key to get per-link statistics. The first line of a per-link display shows the name, IP address, or MAC address of the remote device. The per-link count is updated every 30 seconds. The overall count is updated at the end of every active link.

The second and third lines show the number of frames received and transmitted, respectively. The fourth line indicates the number of CRC errors. A CRC error indicates a frame containing at least one data error.

Network Administration

5

Administering WAN lines and calls	5-1
Managing IP routes and sessions	5-10
Monitoring IPX routes and sessions	5-23
Managing OSPF routes and sessions	5-25
Managing multicast routing	5-40
Monitoring Frame Relay connections	5-42
Monitoring X.25 and PAD connections	5-45
Setting up ISDN D-channel X.25 support	5-47

Administering WAN lines and calls

The MAX allows you to manage WAN lines, ports, and modems. This section describes how to:

- Perform diagnostics on T1, E1, and BRI lines, and ports
- Display call information
- Disable digital modems and modem slots
- Understand how the MAX routes an incoming call

For reference information about each of the commands described in this section, see the *MAX Reference Guide*.

T1 line diagnostics

The MAX provides T1 diagnostic commands you can use to test the configuration of your T1 lines. Access the commands from Net/T1 > Line Diag.

The Line Diag menu for T1 includes the following commands, which you execute by selecting the command in the menu and pressing Enter:

Command	Purpose
Line LB1	Respectively, to test Line 1 or Line 2 in a T1 slot, places a call from the MAX to itself over the WAN to determine the MAX unit's ability to initiate and receive calls and to diagnose the soundness of the digital access line and WAN.
Line LB2	
	Do not activate these commands when a call is active on the line because they disrupt data flow between the codecs connected to either end of the network line.
Switch D Chan	Swaps status of the primary and secondary Non-Facility Associated Signaling (NFAS) D channels on T1 lines that use NFAS signaling.
Clr Err1	Respectively, clears the user error event register of line 1 or line 2.
Clr Err2	
Clr Perf1	Respectively, clears all performance registers for line 1 or line 2, restarts the current time period, and begins accumulating new performance data.
Clr Perf2	

E1 line diagnostics

The MAX provides E1 diagnostic commands you can use to test the configuration of your E1 lines. Access the commands from Net/E1 > Line Diag.

The Line Diag menu for E1 includes the following commands, which you execute by selecting the command in the menu and pressing Enter:

Command	Purpose
Line LB1	Respectively, to test Line 1 or Line 2 in an E1 slot, places a call from the MAX to itself over the WAN to determine the MAX unit's ability to initiate and receive calls and to diagnose the soundness of the digital access line and WAN.
Line LB2	
	Do not activate these commands when a call is active on the line because they disrupt data flow between the codecs connected to either end of the network line.

BRI/LT diagnostics

The MAX provides BRI/LT diagnostic commands you can use to test the configuration of your BRI/LT lines. Access the commands from BRI/LT> Line Diag > Line *N* where *N* is the number of the line you want to check.

BRI/LT diagnostic commands use the BRI-U interface's embedded operations channel (EOC). The EOC transfers diagnostic and signaling data from the exchange to the terminal side and vice versa without transmitting on either the B or D channels.

To monitor transmission quality at the U-interface, the MAX uses internal block-error counters. Block errors encountered in the receive direction are called Near-End Block Errors

(NEBE). Block errors encountered in the transmission direction are called Far-End Block Errors (FEBE).

A block error is detected each time the calculated checksum of the received data does not correspond with the control checksum transmitted in the successive superframe. Block error totals are received from the remote TA. Totals are reset when you restart the MAX or use a Line Diag command for clearing counters. You can view Block Error status in the BRI/LT status window while conducting the diagnostic tests.

Before executing diagnostic test commands, you must specify the EOC address to which you want to apply the command. Set the EOC Address Parameter in the Line Diag menu. The values permitted include:

- 0 (the default)—Remote ISDN TA device.
- 1 through 6—Number of an ISDN repeater between the MAX and the remote TA. The number 1 specifies the repeater closest to the MAX.
- 7—Broadcast the command to all nodes on the IDSL connection.

The EOC address reverts to its default value of 0 when you exit from the Line Diag submenu.

The Line Diag menu includes the following commands for running diagnostic tests, which you access by selecting the command and pressing Enter:

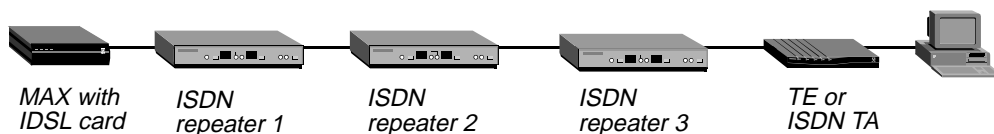
Command	Purpose
Line LoopBack	Sends 24-byte-long test frames continuously on the D channel until you cancel the command. When you execute the command, by selecting Line LoopBack and pressing Enter, a submenu appears with 0=Esc and 1=Line N LB. Selecting 1 begins the loopback command. You can examine the LB Counters status screen to see the number of transmitted frames. Selecting 0 cancels the command.
Corrupt CRC	BRI-U interface permanently transmits inverted CRCs until the command is canceled. While the test is conducted, view the far-end block error status from the remote TA. This tests NEBE and FEBE signal counters.
Uncorrupt CRC	Cancels the Corrupt CRC command.
RQ Corrupt CRC	Requests that NT1 corrupt the CRC to simulate transmission errors. After issuing the command, you can check the near-end block counter to verify that it is working.
Rq Uncorrupt CRC	Requests that the NT1 cancel the RQ Corrupt CRC transmission.
Clr NEBE	Clears the Near-End Block Error counter.
Clr FEBE	Clears the Far-End Block Error counter.

The Line Diag menu also includes a parameter Sealing Current. This parameter enables sealing, which is the ability of an ISDL card to send 40V current on the line to prevent corrosion caused by inactivity. To enable sealing, specify Yes. The default value is No sealing.

Example of performing loopback diagnostics for ISDL

The MAX supports loopback tests from itself to any device on the ISDL connection. For example, you can loop back the signal from the ISDL card to the remote TA or TE, or from the ISDL card to any intermediate repeater.

Figure 5-1. ISDL connection with repeaters



In Figure 5-1, for example, you could set up a loopback test from the MAX to any of the ISDN repeaters, or from the MAX all the way to the remote ISDN at the end of the connection. This ability enables you to isolate trouble anywhere in the connection.

To configure a loopback test on the BRI lines provided by the ISDL slot card:

- 1** Select BRI/LT > Line Diag > Line *N*, where *N* is the number of the line you want to loop back.
- 2** Specify the EOC Address parameter to specify the device that is the terminating point for the loopback test. Use one of the following values:
 - 0—specifies the remote TA or MAX.
 - 1-6—specifies a repeater between the MAX and the remote TA, with 1 representing that closest to the MAX.
 - 7—specifies all devices.
- 3** Select Line LoopBack and press Enter.
- 4** In the confirmation dialog box that appears, select 1=Line *N* LB.
While the line loops back, normal data transfer is disrupted.
- 5** Press Escape to cancel the loopback.

In a local loopback test, data originating at the local site loops back to its originating port without going out over the WAN. It is as though a data mirror were held up to the data at the WAN interface, and the data reflected back to the originator. The WAN interface is the MAX port that connects to a WAN line.

Performing port diagnostics

After configuring a port, you can perform a loopback test to verify port configuration. You access the loopback command from the Port Diag menu (Host/Dual (or Host/6) > Port *N* Menu > Port Diag menu).

The loopback test sends data originating at the host (the local application) back to the originating port.

To run a loopback test:

- 1** Select Local LB and press Enter. The Local LB menu appears:
31-201 Local LB

```
> DSR = Active
   RI=Inactive
   CD=Inactive
   DLO=Inactive
   PND=Inactive
   ACR=Inactive
   Inc Ch Count
   Dec Ch Count
   Rate=64K
```

- 2 Use the standard VT100 interface commands to select settings to change. The settings available include the following:

Parameter	Description
DSR	Toggles the host port's Data Set Ready V.25 signal between active and inactive.
RI	Toggles the host port's Ring Indicate V.25 output signal between active and inactive.
CD	Toggles the host port's Carrier Detect output signal between active and inactive.
DLO	Toggles the host port's Data Line Occupied RS-366 output signal between active and inactive.
PND	Toggles the host port's Present Next Digit RS-366 output signal between active and inactive.
ACR	Toggles the host port's Abandon Call and Retry output signal between active and inactive.
Inc Ch Count	Simulates an increase in the number of channels in a call by increasing the clock rate to the host.
Dec Ch Count	Simulates a decrease in the number of channels in a call by decreasing the clock rate to the host.
Rate	Toggles the data rate of the simulated channels between 56 Kbps and 64 Kbps.

- 3 When you have completed your tests, exit by pressing the Left Arrow key. When you exit, all control signals revert to the state they were in when the test began.

Disabling digital modems and modem slots

You can temporarily disable digital modems or modem slots without disrupting existing connections. This action is called quiescing, and it prepares a modem for maintenance.

Quiescing a modem or modem slot does not result in active calls being torn down. Instead, when active call drops, that modem or modem slot is added to a disabled list and is unavailable for use. If all modems are disabled, incoming callers receive a busy signal until the modems have been restored for service. A quiesced modem is available for use approximately 20 seconds after it has been re-enabled.

To quiesce a modem or modem slot, access the V.34 (V.42) Modem > Modem Diag menu.

To quiesce a modem, use the `Modem #N` command, where *N* is the modem number from 1 to 12. You can set one of the following values:

Value	Result
<code>enable modem</code>	Enables disabled modems. This is the default value.
<code>disable modem</code>	Places the modem on the disabled list. When an active connection drops, the card becomes available for maintenance.
<code>enable modem+chan</code>	Enables the modem and a disabled B channel.
<code>disable modem+chan</code>	Places the modem and an arbitrary B channel on disabled lists.

To quiesce a modem slot, use the `ModemSlot` command. You can set one of the following values:

Value	Result
<code>enable slot</code>	Enables disabled modems on the slot. This is the default value.
<code>disable slot</code>	Places all modems that are not active on the disabled list. When the active connections drop, the card becomes available for maintenance.
<code>enable slot+chan</code>	Restores the slot card and channels to use. Modems on the selected slot that appear on the disabled list are enabled. For each modem enabled, an out-of-service B channel returns to service.
<code>disable slot+chan</code>	Disables all modems on the slot, along with an equal number of B channels.

E1 ISDN call information

If the E1/PRI line or BRI line switch-type is German ITR6 or Japanese NTT, you can display information about ISDN calls by invoking the terminal-server command line and entering the `Show Calls` command. For example:

```
ascend% show calls
```

The command displays statistics about current calls. For example:

Call ID	Called Party ID	Calling Party ID	InOctets	OutOctets
3	5104563434	4191234567	0	0
4	4197654321	5108888888	888888	99999

The Call ID column contains an index number specific to the call.

Called Party ID and Calling Party ID show the telephone number of the answering device and calling device, respectively.

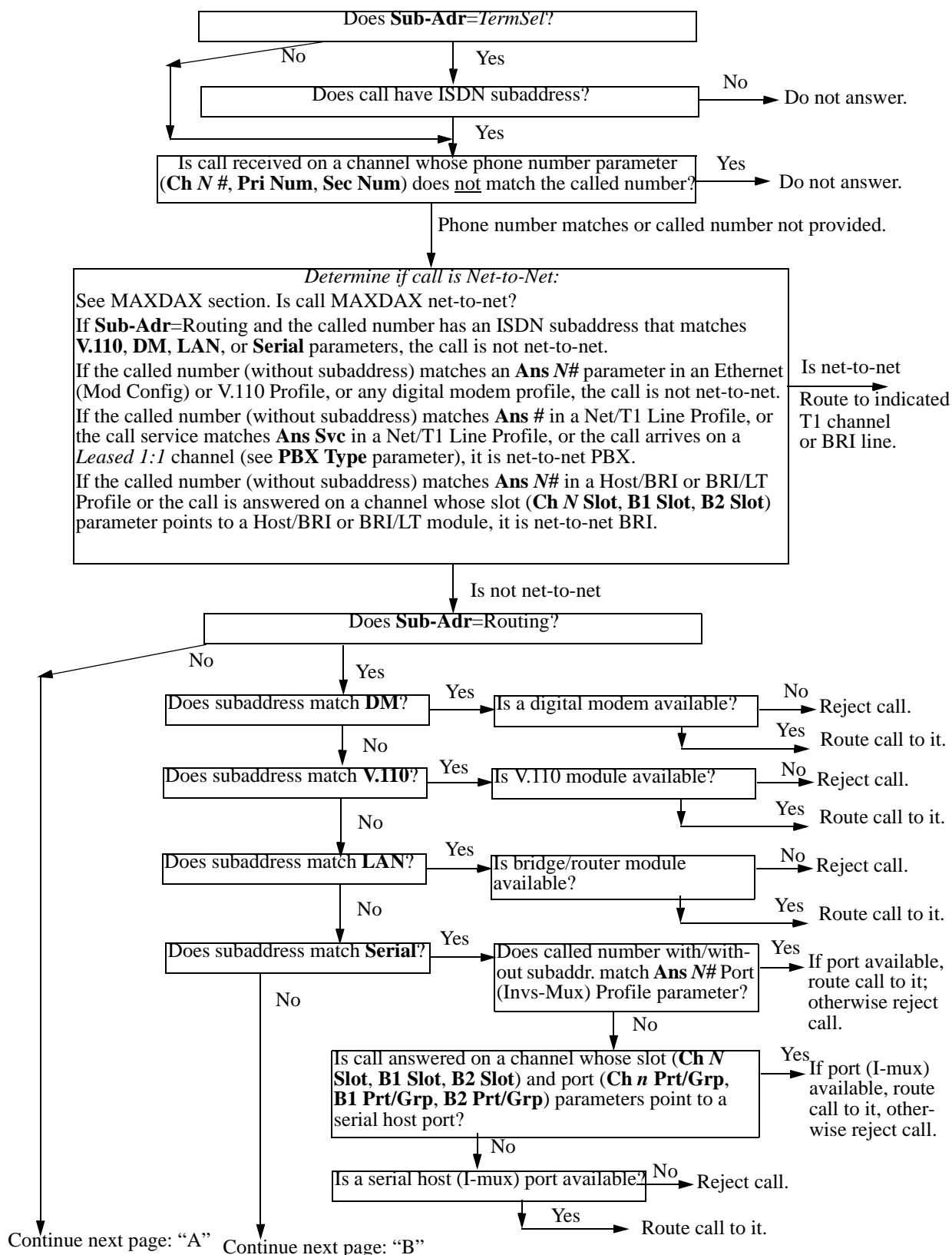
InOctets and OutOctets show the number of bytes received by the answering device and transmitted by the calling device, respectively.

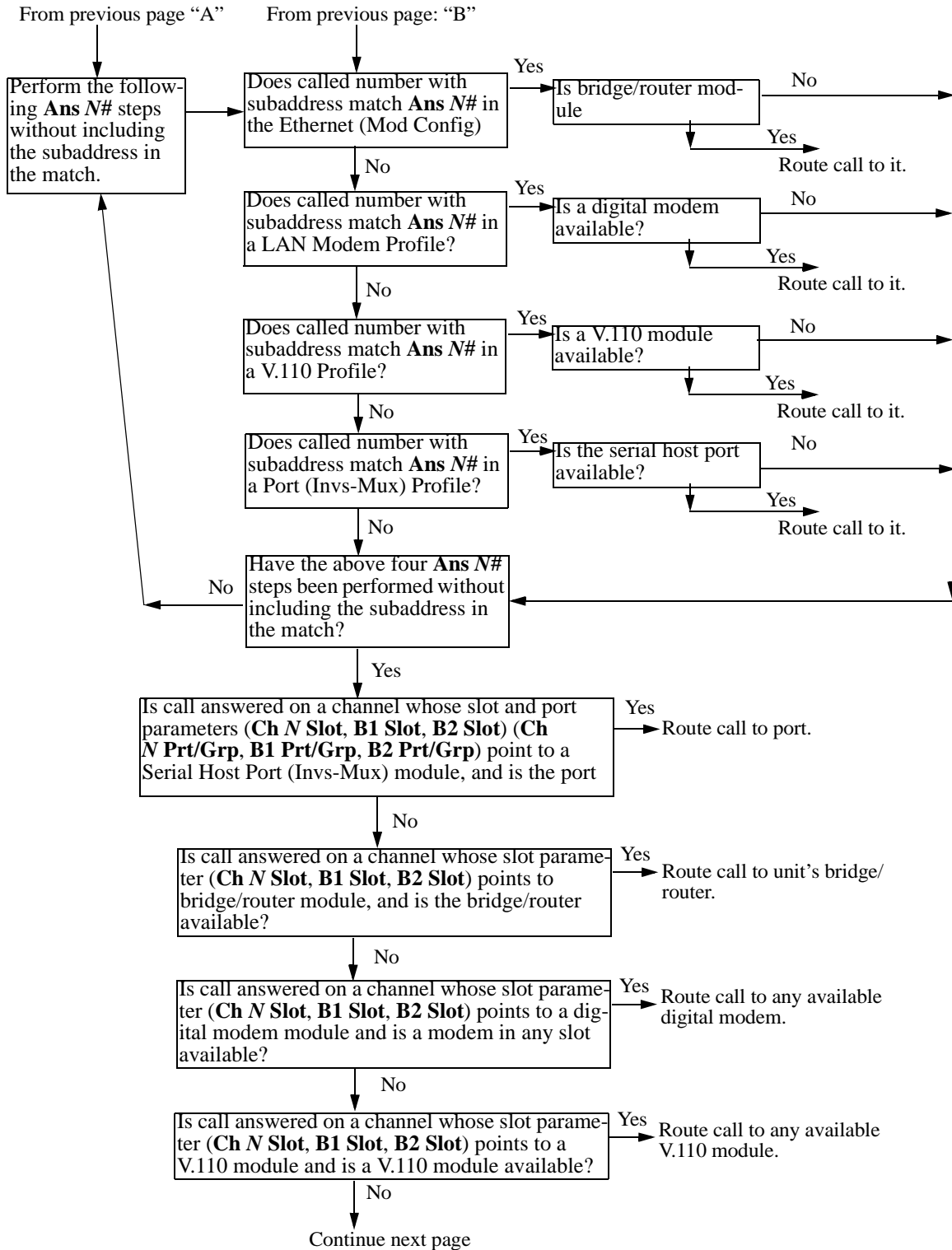
Note: When an ISDN call disconnects from either a German ITR6 switch or a Japanese NTT switch, the switch sends call billing information to the call originator as part of the call tear-down process. This information is written to the `eventCallCharge` (eventEntry 17) SNMP

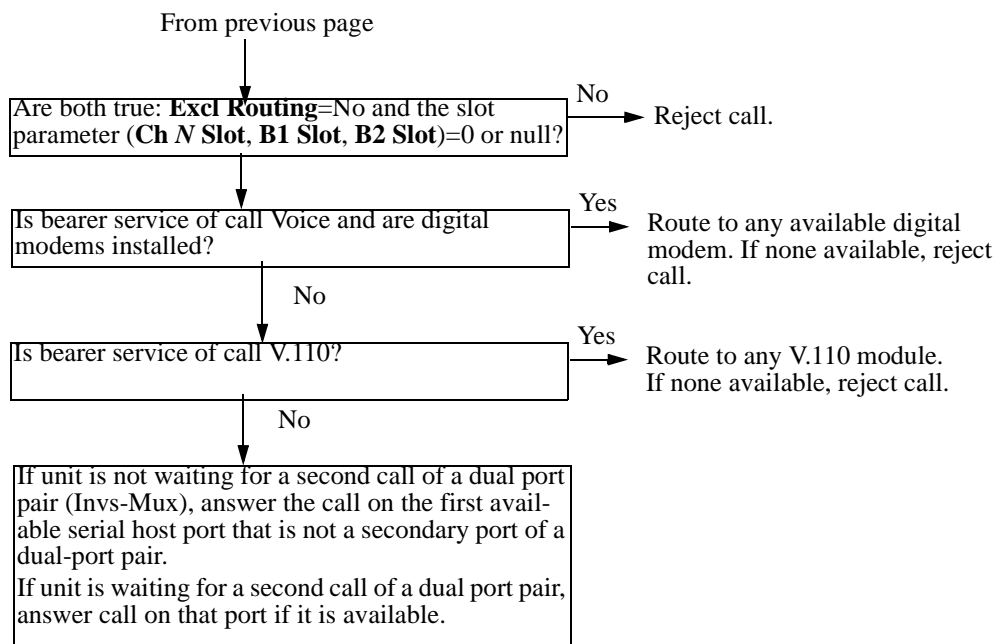
object in the Ascend Enterprise MIB events group (10). An SNMP manager can then read this object to determine the cost of the call. The eventCallCharge object is a read-only integer and is applicable only if eventType is callCleared (3). Otherwise, 0 is returned.

Incoming call routing state diagram

The following pages show detailed state information about inbound call routing in the MAX. For more information about any of the parameters, see the *MAX Reference Guide*.







Managing IP routes and sessions

This section describes how to monitor TCP/IP/UDP and related information in the terminal-server command-line interface. To invoke the terminal-server interface, select System > Sys Diag > Term Serv and press Enter. The terminal-server command-line prompt appears: ascend%.

Working with the IP routing table

The terminal-server IProute commands display the routing table and enable you to add or delete routes. The changes you make to the routing table by using the IProute command last only until the MAX unit is reset. To display the IProute commands, enter the IP route command with a question mark:

```
ascend% iproute ?

iproute ?      Display help information
iproute add    iproute add <destination/size> <gateway> [ pref ] [ m
iproute delete iproute delete <destination/size> <gateway> [ proto ]
iproute show   displays IP routes (same as "show ip routes" command)
```

Displaying the routing table

You can use either the IProute Show command or the Show IP Routes command to display the IP routing table: For example:

```
ascend% iproute show
```

Destination	Gateway	IF	Flg	Pref	Met	Use	Age
0.0.0.0/0	10.0.0.100	wan0	SG	1	1	0	20887
10.207.76.0/24	10.207.76.1	wanidle0	SG	100	7	0	20887
10.207.77.0/24	10.207.76.1	wanidle0	SG	100	8	0	20887
127.0.0.1/32	–	lo0	CP	0	0	0	20887
10.0.0.0/24	10.0.0.100	wan0	SG	100	1	21387	20887
10.1.2.0/24	–	ie0	C	0	0	19775	20887
10.1.2.1/32	–	lo0	CP	0	0	389	20887
255.255.255.255/32	–	ie0	CP	0	0	0	20887

The output includes the following information:

Field	Destination
Destination	Target address of a route. To send a packet to this address, the MAX uses this route. Note that the router uses the most specific route (having the longest mask) that matches a given destination.
Gateway	Address of the next hop router that can forward packets to the given destination. Direct routes (without a gateway) do not show a gateway address in the gateway column.
IF	Name of the interface through which a packet addressed to this destination is sent. <ul style="list-style-type: none"> • ie0—Ethernet interface • lo0— Loopback interface • wanN—Each of the active WAN interfaces • wanidle0— Inactive interface (the special interface for any route whose WAN connection is down).
Flg	Flag values, including the following: <ul style="list-style-type: none"> • C— A directly connected route, such as Ethernet • I—ICMP Redirect dynamic route • N—Placed in the table via SNMP MIB II • O—Route learned from OSPF (Open Shortest Path First) • R—Route learned from RIP • r—RADIUS route • S—Static route • ?—Route of unknown origin, which indicates an error • G—Indirect route via a gateway • P—Private route • T—Temporary route • *—Hidden route that will not be used unless another better route to the same destination goes down
Pref	Preference value of the route. Note that all routes that come from RIP have a preference value of 100, while the preference value of each individual static route can be set independently.

Field	Destination
Metric	RIP-style metric for the route, with a valid range of 0-16. Routes learned from OSPF show a RIP metric of 10. OSPF Cost infinity routes show a RIP metric of 16.
Use	Count of the number of times the route was referenced since it was created. (Many of these references are internal, so this is not a count of the number of packets sent over this route.)
Age	Age of the route in seconds, used for troubleshooting to determine when routes are changing rapidly or flapping.

Continuing the example, the first route shown is the default route with destination 0.0.0.0/0, defined through the active Connection profile.

```
0.0.0.0/0      10.0.0.100    wan0      SG    1      1      0      20887
```

The IP Route profile for the default route specifies a preference of 1, so this route is preferred over dynamically learned routes. The next route is specified in a Connection profile that is inactive:

```
10.207.76.0/24  10.207.76.1    wanidle0 SG    100    7      0      20887
```

The next route in the table is a static route through an inactive gateway:

```
10.207.77.0/24  10.207.76.1    wanidle0 SG    100    8      0      20887
```

The static route is followed by the loopback route:

```
127.0.0.1/32    -                lo0       CP    0      0      0      20887
```

The loopback route specifies a special address. Packets sent to this special address will be handled internally. The C flag indicates a connected route, while the P flag indicates that the router will not advertise this route.

The next route is specified in a Connection profile that is currently active:

```
10.0.0.0/24      10.0.0.100    wan0      SG    100    1      21387 20887
```

These are routes followed by a connection to the Ethernet interface. It is directly connected, with a preference and metric of zero.

```
10.1.2.0/24      -                ie0       C     0      0      19775 20887
```

The last two routes are a private loopback route and a private route to the broadcast address:

```
10.1.2.1/32      -                lo0       CP    0      0      389   20887
255.255.255.255/32 -                ie0       CP    0      0      0     20887
```

The private loopback route shown is a host route with the Ethernet address. It is private, so it will not be advertised. The private route to the broadcast address is used in cases in which the router must to broadcast a packet but the route is otherwise unconfigured. It is typically used when the MAX is trying to locate a server on a client machine to handle challenges for a token security card.

Adding an IP route

To add to the MAX unit's routing table a static route that will be lost when the MAX resets, enter the IProute Add command in the following format:

```
iproute add destination gateway [metric]
```

where **destination** is the destination network address, **gateway** is the IP address of the router that can forward packets to that network, and **metric** is the virtual hop count to the destination network (default 8). For example, to add a route to the 10.1.2.0 network and all of its subnets through the IP router located at 10.0.0.3/24 with a metric of 1 (the router is one hop away), enter the following command:

```
ascend% iproute add 10.1.2.0 10.0.0.3/24 1
```

If you try to add a route to a destination that already exists in the routing table, the MAX replaces the existing route, but only if it has a higher metric than the new route. If you get the message **Warning: a better route appears to exist**, the MAX has rejected your attempt to add a route because the routing table already contained a route, to the same destination, with a lower metric. Note that RIP updates can change the metric for the route.

Deleting an IP route

To remove a route from the MAX unit's routing table, enter the IProute Delete command in the following format:

```
iproute delete destination gateway
```

For example:

```
ascend% iproute delete 10.1.2.0 10.0.0.3/24
```

Note: RIP updates can add back any route you remove with IProute Delete. Also, after a system reset, the MAX restores all routes listed in the Static Route profile.

Displaying route statistics

The Traceroute command is useful for locating slow routers or diagnosing IP routing problems. It traces the route an IP packet follows by launching UDP probe packets with a low Time-To-Live (TTL) value and then listening for an ICMP time exceeded reply from a router. The Traceroute command uses the following syntax:

```
traceroute [-n] [-v] [-m max_ttl] [-p port] [-q nqueries]  
[-w waittime] host [datasize]
```

All flags are optional. The only required parameter is the destination hostname or IP address. The elements of the syntax are as follows:

Syntax element	Description
-n	Print hop addresses numerically rather than symbolically and numerically (this eliminates a name server address-to-name lookup for each gateway found on the path).
-v	Verbose output. Lists all received ICMP packets other than Time Exceeded and ICMP Port Unreachable are listed.
-m max_ttl	Sets the maximum time-to-live (maximum number of hops) for outgoing probe packets. The default is 30 hops.

-p port	Set the base UDP port number used in probes. Traceroute depends on having nothing listening on any of the UDP ports from the source to the destination host (so that an ICMP Port Unreachable message will be returned to terminate the route tracing). If something is listening on a port in the default range, you can set the -p option to specify an unused port range. The default is 33434.
-q nqueries	Set the maximum number of queries for each hop. The default is 3.
-w waittime	Set the time to wait for a response to a query. The default is 3 seconds.
host	The destination host by name or IP address.
datasize	Sets the size of the data field of the UDP probe datagram sent by Traceroute. The default is 0. This results in a datagram size of 38 bytes (a UDP packet carrying no data).

For example, to trace the route to the host `server1`:

```
ascend% traceroute server1
traceroute to server1 (10.65.212.19), 30 hops MAX, 0 byte packets
 1  server1.corp.com (10.65.212.19)  0 ms  0 ms  0 ms
```

Probes start with a TTL of one and increase by one until one of the following conditions occurs:

- The MAX receives an ICMP Port Unreachable message.
The UDP port in the probe packets is set to an unlikely value, such as 33434, because the target host is not intended to process the packets. A “port unreachable” message indicates that the packets reached the target host and were rejected.
- The TTL value reaches the maximum value.
By default, the maximum TTL is set to 30. You can specify a different TTL by using the **-m** option. For example:

```
ascend% traceroute -m 60 techpubs
traceroute to server1 (10.65.212.19), 60 hops MAX, 0 byte packets
 1  server1.corp.com (10.65.212.19)  0 ms  0 ms  0 ms
```

Three probes are sent at each TTL setting. The second line of command output shows the address of the router and round trip time of each probe. If the probe answers come from different gateways, the address of each responding system is shown. If there is no response within a three second timeout interval, the command output is an asterisk. The following annotations can appear after the time field in a response:

- **!H**—Host reached.
- **!N**—Network unreachable.
- **!P**—Protocol unreachable.
- **!S**—Source route failed. Might indicate a problem with the associated device.
- **!F**—Fragmentation needed. Might indicate a problem with the associated device.
- **!h**—Communication with the host is prohibited by filtering.
- **!n**—Communication with the network is prohibited by filtering.
- **!c**—Communication is otherwise prohibited by filtering.
- **!?**—ICMP subcode detected. This event should not occur.

- `!??`—Reply received with inappropriate type. This event should not occur.

Pinging other IP hosts

The terminal-server Ping command is useful for verifying that the transmission path is open between the MAX and another station. It sends an ICMP echo-request packet to the specified station. If the station receives the packet, it returns an ICMP echo-response packet. The Ping command has the following syntax:

```
ping [-q] [-v] [-c count] [-i sec | -I msec] [-s packetsize]
[-x src_address] host
```

All flags are optional. The only required parameter is the destination hostname or IP address. The elements of the syntax are as follows:

Syntax element	Description
-q	Quiet mode. The MAX displays only the summary of all Ping responses it has received.
-v	Verbose output. The MAX displays information from each ping response that it receives as well as the summary of all Ping responses. This is the default.
-c count	Specifies the number of Ping requests that the MAX sends to the host. By default, the MAX sends continual ping requests until you press Ctrl-C.
-i sec	Specifies the length of time, in seconds, between Ping requests. You can specify seconds, using the <code>-i</code> option, or milliseconds, using the <code>-I</code> option, but not both. The default is one second.
-I msec	Specifies the length of time, in milliseconds, between Ping requests. You can specify milliseconds, using the <code>-I</code> option, or seconds, using the <code>-i</code> option, but not both.
-s packetsize	Specifies the size of each Ping request packet that the MAX sends to the host. The default is 64 bytes.
-x srcaddress	Specifies a source IP address that overwrites the default source address.
host	The destination host by name or IP address.

For example, to Ping the host `techpubs`:

```
ascend% ping techpubs
PING techpubs (10.65.212.19): 56 data bytes
64 bytes from 10.65.212.19: icmp_seq=0 ttl=255 time=0 ms
64 bytes from 10.65.212.19: icmp_seq=3 ttl=255 time=0 ms
^C
--- techpubs ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/MAX = 0/0/0 ms
```

You can terminate the Ping exchange at any time by pressing Ctrl-C. When you press Ctrl-C, the command reports the number of packets sent and received, the percentage of packet loss,

any duplicate or damaged echo-response packets, and round-trip statistics. In some cases, round-trip times cannot be calculated.

During the Ping exchange, the MAX displays information about the packet exchange, including the Time-To-Live (TTL) of each ICMP echo-response packet.

Note: The maximum TTL for ICMP Ping is 255, and the maximum TTL for TCP is often 60 or lower, so you might be able to Ping a host but not be able to run a TCP application (such as Telnet or FTP) to that station. If you Ping a host running a version of Berkeley UNIX earlier than 4.3BSD-Tahoe, the TTL report is 255 minus the number of routers in the round-trip path. If you Ping a host running the current version of Berkeley UNIX, the TTL report is 255 minus the number of routers in the path from the remote system to the station performing the Ping.

The Ping command sends an ICMP Mandatory echo-request datagram, which asks the remote station “Are you there?” If the echo-request reaches the remote station, the station sends back an ICMP echo-response datagram, which tells the sender “Yes, I am alive.” This exchange verifies that the transmission path is open between the MAX and a remote station.

Configuring Finger support

You can configure the MAX to respond to Finger requests, as specified in RFC 1288, *The Finger User Information Protocol*.

To enable the MAX to respond to Finger requests:

- 1 Open the Ethernet > Mod Config.
- 2 Set Finger to Yes.
- 3 Exit and save the changes.

Configuring the DNS Fallback Table

The local DNS table provides a list of IP addresses for a specific host name when the remote DNS server fails to resolve the host name. If the local DNS table contains the host name for the attempted connection, it provides the list of IP addresses.

You create the DNS table from the Ethernet > Mod Config > DNS menu by entering up to eight host names. Enter the IP addresses for each host through the terminal-server interface. You can configure a maximum of 35 IP addresses for each host. If you specify automatic updating, you only have to enter the first IP address of each host. Additional IP addresses are added automatically.

Automatic updating replaces the existing address list for a host each time the remote DNS server succeeds in resolving a connection to a host that is in the table. You specify how many of the addresses returned by the remote server can be included in the new list.

On the MAX, the table, which you display from the terminal-server interface, provides additional information for each table entry. The information is in the following two fields, which are updated when the system matches the table entry with a host name that was not found by the remote server:

- # Reads (the number of reads since entry was created). This field is updated each time a local name query match is found in the local DNS table.
- Time of Last Read

You can use the terminal-server command Show Dnstab to check the list of host names and IP addresses in the table. Figure 5-2 shows an example of a DNS table on a MAX.

Figure 5-2. Example of a local DNS table

Local DNS Table

Name	IP Address	# Reads	Time of last read
1: " "	-----	-----	
2: "server.corp.com."	200.0.0.0	2	Feb 10 10:40:44
3: "boomerang"	221.0.0.0	2	Feb 10 9:13:33
4: " "	-----	-----	
5: " "	-----	-----	
6: " "	-----	-----	
7: " "	-----	-----	

Displaying IP routing and related information

The following Show commands for monitoring IP routing and related protocols are described in this section:

show arp	Display the Arp Cache
show icmp	Display ICMP information
show if	Display Interface info. Type 'show if ?' for help.
show ip	Display IP information. Type 'show ip ?' for help.
show udp	Display UDP information. Type 'show udp ?' for help.
show tcp	Display TCP information. Type 'show tcp ?' for help.
show pools	Display the assign address pools.

Displaying the ARP cache

To display the ARP cache, enter the Show ARP command. For example:

ascend% **show arp**

entry	typ	ip address	ether addr	if	rtr	pkt	insert
0	DYN	10.65.212.199	00C07B605C07	0	0	0	857783
1	DYN	10.65.212.91	0080C7C4CB80	0	0	0	857866
2	DYN	10.65.212.22	080020792B4C	0	0	0	857937
3	DYN	10.65.212.3	0000813DF048	0	0	0	857566
4	DYN	10.65.212.250	0020AFF80F1D	0	0	0	857883
5	DYN	10.65.212.16	0020AFEC0AFB	0	0	0	857861
6	DYN	10.65.212.227	00C07B5F14B6	0	0	0	857479
7	DYN	10.65.212.36	00C07B5E9AA5	0	0	0	857602
8	DYN	10.65.212.71	0080C730041F	0	0	0	857721
9	DYN	10.65.212.5	0003C6010512	0	0	0	857602
10	DYN	10.65.212.241	0080C72ED212	0	0	0	857781
11	DYN	10.65.212.120	0080C7152582	0	0	0	857604
12	DYN	10.65.212.156	0080A30ECE6D	0	0	0	857901
13	DYN	10.65.212.100	00C07B60E28D	0	0	0	857934
14	DYN	10.65.212.1	00000C065D27	0	0	0	857854
15	DYN	10.65.212.102	08000716C449	0	0	0	857724

16	DYN	10.65.212.33	00A024AA0283	0	0	0	857699
17	DYN	10.65.212.96	0080C7301792	0	0	0	857757
18	DYN	10.65.212.121	0080C79BF681	0	0	0	857848
19	DYN	10.65.212.89	00A024A9FB99	0	0	0	857790
20	DYN	10.65.212.26	00A024A8122C	0	0	0	857861
21	DYN	10.65.212.6	0800207956A2	0	0	0	857918
22	DYN	10.65.212.191	0080C75BE778	0	0	0	857918
23	DYN	10.65.212.116	0080C72F66CC	0	0	0	857416
24	DYN	10.65.212.87	0000813606A0	0	0	0	857666
25	DYN	10.65.212.235	00C07B76D119	0	0	0	857708
26	DYN	10.65.212.19	08002075806B	0	0	0	857929

The ARP table displays the following information:

- **entry**—A unique identifier for each ARP table entry.
- **typ**—How the address was learned, dynamically (DYN) or statically (STAT).
- **ip address**—The address contained in ARP requests.
- **ether addr**—The MAC address of the host with that IP address.
- **if**—The interface on which the MAX received the ARP request.
- **rtr**—The next-hop router on the specified interface.

Displaying ICMP packet statistics

To display the number of ICMP packets received intact, received with errors, and transmitted, enter the `Show icmp` command. For example:

```
ascend% show icmp
3857661 packet received.
20 packets received with errors.
   Input histogram: 15070
2758129 packets transmitted.
0 packets transmitted due to lack of resources.
   Output histogram: 15218
```

The Input and Output histograms show the number of ICMP packets received and transmitted, respectively.

Displaying interface statistics

To display the supported interface-statistics commands, enter the `Show IF` command with a question mark. For example:

```
ascend% show if ?
show if ?                Display help information
show if stats             Display Interface Statistics
show if totals            Display Interface Total counts
```

To display the status and packet count of each active WAN link and of local and loopback interfaces, enter the `Show IF Stats` command. For example:

```
ascend% show if stats
```

Interface	Name	Status	Type	Speed	MTU	InPackets	Out- packet
ie0	ethernet	Up	6	10000000	1500	107385	85384
wan0		Down	1	0	1500	0	0
wan1		Down	1	0	1500	0	0
wan2		Down	1	0	1500	0	0
wanidle0		Up	6	10000000	1500	0	0
lo0	loopback	Up	24	10000000	1500	0	0

The output contains the following fields:

Field	Description
Interface	Interface name. For more information, see the <i>Network Configuration Guide</i> for your MAX.
Name	Name of the profile or a text name for the interface.
Status	Up (the interface is functional) or Down (the interface is not functional).
Type	Type of application being used on the interface, as specified in RFC 1213 (MIB-2). For example, 23 indicates PPP and 28 indicates SLIP.
Speed	Data rate in bits per second.
MTU	The maximum packet size allowed on the interface. MTU stands for Maximum Transmission Unit.
InPackets	The number of packets the interface has received.
OutPackets	The number of packets the interface has transmitted.

To display the packet count at each interface, broken down by type of packet, enter the Show If Totals command. For example:

```
ascend% show if totals
```

Name	--Octets--	Ucast--	-NonUcast-	Discard	-Error-	Unknown	-Same IF-
ie0 i:	7813606	85121	22383	0	0	0	0
o:	101529978	85306	149	0	0	0	0
wan0 i:	0	0	0	0	0	0	0
o:	0	0	0	0	0	0	0
wan1 i:	0	0	0	0	0	0	0
o:	0	0	0	0	0	0	0
wan2 i:	0	0	0	0	0	0	0
o:	0	0	0	0	0	0	0
wanidle0 i:	0	0	0	0	0	0	0
o:	0	0	0	0	0	0	0
lo0 i:	0	0	0	0	0	0	0
o:	0	0	0	0	0	0	0

The output contains the following fields:

Field	Description
Name	Interface name. For more information, see the <i>Network Configuration Guide</i> for your MAX.

Field	Description
Octets	Total number of bytes processed by the interface.
Ucast	Packets with a unicast destination address.
NonUcast	Packets with a multicast address or a broadcast address.
Discard	Number of packets that the interface could not process.
Error	Number of packets with CRC errors, header errors, or collisions.
Unknown	Number of packets the MAX forwarded across all bridged interfaces because of unknown or unlearned destinations.
Same IF	Number of bridged packets whose destination is the same as the source.

Displaying IP statistics and addresses

To display the IP statistics and addresses supported commands, enter the Show IP command with a question mark:

```
ascend% show ip ?
show ip ?          Display help information
show ip stats      Display IP Statistics
show ip address    Display IP Address Assignments
show ip routes     Display IP Routes
```

Note: For information about the Show IP Routes command, see “Working with the IP routing table” on page 5-10.

To display statistics on IP activity, including the number of IP packets the MAX has received and transmitted, enter the Show IP Stats command. For example:

```
ascend% show ip stats
107408 packets received.
    0 packets received with header errors.
    0 packets received with address errors.
    0 packets forwarded.
    0 packets received with unknown protocols.
    0 inbound packets discarded.
107408 packets delivered to upper layers.
85421 transmit requests.
    0 discarded transmit packets.
    1 outbound packets with no route.
    0 reassembly timeouts.
    0 reassemblies required.
    0 reassemblies that went OK.
    0 reassemblies that Failed.
    0 packets fragmented OK.
    0 fragmentations that failed.
    0 fragment packets created.
    0 route discards due to lack of memory.
64 default ttl.
```

To display IP interface address information, enter the Show IP Address command. For example:

```
ascend% show ip address
```

Interface	IP Address	Dest Address	Netmask	MTU	Status
ie0	10.2.3.4	N/A	255.255.255.224	1500	Up
wan0	0.0.0.0	N/A	0.0.0.0	1500	Down
wan1	13.1.2.0	13.1.2.128	255.255.255.248	1500	Down
wan2	0.0.0.0	N/A	0.0.0.0	1500	Down
wan3	0.0.0.0	N/A	0.0.0.0	1500	Down
lo0	127.0.0.1	N/A	255.255.255.255	1500	Up
rj0	127.0.0.2	N/A	255.255.255.255	1500	Up
bh0	127.0.0.3	N/A	255.255.255.255	1500	Up

Displaying UDP statistics and listen table

To display the supported UDP-statistics commands, enter the Show UDP command with a question mark:

```
ascend% show udp ?
```

```
show udp ?          Display help information
show udp stats      Display UDP Statistics
show udp listen     Display UDP Listen Table
```

To display the number of UDP packets received and transmitted, enter the Show UDP Stats command. For example:

```
ascend% show udp stats
```

```
22386 packets received.
  0 packets received with no ports.
  0 packets received with errors.
  0 packets dropped
  9 packets transmitted.
```

The Show Udp Listen command displays the socket number, UDP port number and the number of packets queued for each UDP port on which the MAX is currently listening. The command's output also includes the following fields:

Field	Description
InQMax	Maximum number of queued UDP packets on the socket. (See Queue Depth and Rip Queue Depth parameters.)
InQLen	Current number of queued packets on the socket.
InQDrops	Number of packets discarded because it would cause InQLen to exceed InQMax.
Total Rx	Total number of packets received on the socket, including InQDrops.

For example:

```
ascend% show udp listen
```

```
udp:
```

Socket	Local Port	InQLen	InQMax	InQDrops	Total Rx
0	1023	0	1	0	0
1	520	0	50	0	532
2	7	0	32	0	0
3	123	0	32	0	0
4	1022	0	128	0	0
5	161	0	64	0	0

Displaying TCP statistics and connections

To display the supported TCP-statistics commands, enter the Show TCP command with a question mark:

```
ascend% show tcp ?
```

```
show tcp ?          Display help information
show tcp stats      Display TCP Statistics
show tcp connection Display TCP Connection Table
```

To display the number of TCP packets received and transmitted, enter the Show TCP Stats command. For example:

```
ascend% show tcp stats
```

```
0 active opens.
11 passive opens.
1 connect attempts failed.
1 connections were reset.
3 connections currently established.
85262 segments received.
85598 segments transmitted.
559 segments re-transmitted.
```

An active open is a TCP session that the MAX initiated, and a passive open is a TCP session that the MAX did not initiate.

To display current TCP sessions:

```
ascend% show tcp connection
```

Socket	Local	Remote	State
0	*.23	*.*	LISTEN
1	10.2.3.23	15.5.248.121.15003	ESTABLISHED

Displaying address pool status

To view the status of the MAX unit's IP address pool:

```
ascend% show pools
```

Pool #	Base	Count	InUse
1	10.98.1.2	55	27
2	10.5.6.1	128	0

Number of remaining allocated addresses: 0

If you change an address pool while users are still logged in using the addresses from the previous pool, Number of remaining allocated addresses reflects how many users are currently using addresses from the previous pool. Typically, the value is 0 (zero).

Monitoring IPX routes and sessions

Show commands for monitoring IPX connections in the MAX are available at the terminal-server command-line interface. To open the terminal-server interface select System > Sys Diag > Term Serv and press Enter.

Verifying the transmission path to NetWare stations

The IPXping command provides network layer verification of the transmission path to NetWare stations. The command works on the same LAN as the MAX or across a WAN connection that has IPX Routing enabled. Following is the command's syntax:

```
ipxping [-c count] [-i delay] [-s packet-size] hostname
```

where:

Option	Description
hostname	The IPX address of the host, or if the host is a NetWare server, its advertised name.
-c count	Stop the test after sending and receiving the number of packets specified by count .
-i delay	Wait the number of seconds specified by delay before sending the next packet. The default is for one second.
-s packet-size	Send the number of data bytes specified by packet-size .

You can specify **hostname** as is either the IPX address of the NetWare workstation or the advertised name of a server. The IPX address consists of the IPX network and node numbers for a station. For example:

```
ascend% ipxping CFFF1234:0000000000001
```

If you are using the IPXping command to verify connectivity with an advertised NetWare server, you can simply enter the symbolic name of the server. For example:

```
ascend% ipxping server-1
```

You can terminate the IPXping command at any time by pressing Ctrl-C.

During the IPXping exchange, the MAX calculates and reports the following statistics:

```
PING server-1 (EE000001:0000000000001): 12 data bytes
52 bytes from (EE000001:0000000000001): ping_id=0 time=0ms
52 bytes from (EE000001:0000000000001): ping_id=1 time=0ms
52 bytes from (EE000001:0000000000001): ping_id=2 time=0ms
?
--- novll Ping statistics ---
```

```
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/MAX = 0/0/0 ms
```

These statistics include the following information:

- The IPX address of the source and destination nodes.
- The byte counts of the request and response packets.
- The ping ID of the command. (The ping Request # replied to by target host.)
- The number of milliseconds required to send the IPXping and receive a response.
- The number of packets transmitted and received.
- Duplicate or damaged packets, if applicable.
- Average round-trip times for the ping request and reply. In some cases, round-trip times cannot be calculated.

To display statistics related to the IPXping command, enter the Show Network Pings command. For example:

```
ascend% show network pings

InPing Requests/OutPing Replies OutPing Requests/InPing Replies
      10              10              18              18
```

The output shows how many NetWare stations have pinged the MAX (InPing requests and replies) and how many times the IPXping command has been executed in the MAX (OutPing requests and replies).

Displaying IPX packet statistics

To display IPX packet statistics, enter the Show Network Stats command. For example:

```
ascend% show network stats

27162 packets received.
25392 packets forwarded.
0 packets dropped exceeding maximum hop count.
0 outbound packets with no route.
```

The MAX drops packets that exceed the maximum hop count (that have already passed through too many routers).

Displaying the IPX service table

To display the IPX service table, enter the Show Network Servers command. For example:

```
ascend% show network servers

IPX address          type          server name
ee000001:000000000001:0040  0451         server-1
```

The output includes the following fields:

Field	Description
IPX address	IPX address of the server. The address uses this format: <i>network number:node number:socket number</i>

Field	Description
type	Type of service available (in hexadecimal format). For example, 0451 designates a file server
server name	The first 35 characters of the server name.

Displaying the IPX routing table

To display the IPX routing table, enter the Show Netware Networks command:

```
ascend% show netware networks

network  next router  hops  ticks  origin
CFFF0001  000000000000    0     1    EthernetS
```

The output includes the following fields:

Field	Descriptions
network	IPX network number.
next router	Address of the next router, or 0 (zero) for a direct or WAN connection.
hops	Hop count to the network.
ticks	Tick count to the network.
origin	Name of the profile used to reach the network.

Note: An S or an H flag might appear next to the origin. S indicates a static route. H indicates a hidden, or inactive, static route. Hidden static routes occur when the router learns of a better route.

Managing OSPF routes and sessions

This section describes how to work with Open Shortest Path First (OSPF) information in the routing table and how to monitor OSPF activity in the terminal-server command-line interface.

To invoke the terminal-server interface, select System > Sys Diag > Term Serv and press Enter.

Working with the routing table

The OSPF routing table includes routes built from the router's link-state database as well as those added by external routing protocols such as RIP. You can also add routes statically (for example, to direct traffic destined for a remote site through one of several possible border routers). For details about adding static routes (for example, if you want to force the use of one route over those learned from OSPF, see the *Network Configuration Guide* for your MAX).

To display the IP routing table with added OSPF information, invoke the terminal server (System > Sys Diag > Term Serv) and enter the IProute Show command with the -1 option:

```
ascend% iproute show -1
```

When you include the -1 option, three columns of OSPF-specific fields appear at the routing table:

...	Cost	T	Tag
...	1	0	0xc0000000
...	9	1	0xc8000000
...	10	0	0xc0000000
...	9	1	0xc8000000
...	1	1	0xc0000000
...	3	1	0xc8000000
...	9	1	0xc8000000
...	4	1	0xc8000000
...	5	1	0xc8000000
...	3	1	0xc8000000
...	3	1	0xc8000000
...	3	1	0xc8000000

Field	Description
Cost	Cost of an OSPF route. The interpretation of this cost depends on the type of external metric, which is displayed in the next column. If the MAX is advertising Type-1 metrics, OSPF can use the specified number as the cost of the route. Type-2 external metrics are an order of magnitude larger.
T	Link-state advertisement (LSA)-type of the metric to be advertised for an external route. A 0 (zero) in this column means that the metric is an external-Type-1 or an OSPF internal route. A 1 means that the route is an external-Type-2 route.
Tag	Specifies a 32-bit hexadecimal number attached to each external route to tag it as external to the AS. The number may be used by border routers to filter this record.

Multipath routing

A MAX running OSPF can alternate between two equal-cost gateways. When OSPF detects equally good gateways, in terms of routing costs, it puts each equal-cost gateway on an equal-cost list. The router alternates between the gateways on the list in what is called equal-cost multipath routing.

For example, if router A has two equal-cost routes to `example.com`, one via router B and the other via router C, router A's routing table might include the following entries:

Destination	Gateway	IF	Flg	Pref	Met	Use	Age
10.174.88.0/25	10.174.88.12	wan2	OGM	10	10	52	19
10.174.88.0/25	10.174.88.13	wan3	OGM	10	10	52	19
10.174.88.12/32	10.174.88.12	wan2	OG	10	10	0	28
10.174.88.13/32	10.174.88.13	wan3	OG	10	10	0	28
192.168.253.0/24	-	ie0	C	0	0	1	49
192.168.253.6/32	-	lo0	CP	0	0	53	49
223.1.1.0/24	10.174.88.12	wan2	OG	10	10	0	19
223.5.1.0/24	10.174.88.12	wan2	OG	10	10	0	19
223.12.9.0/24	10.174.88.12	wan2	OG	10	10	0	19
255.255.255.255/32	-	ie0	CP	0	0	0	49

The M in the Flg column indicates an equal-cost multipath. A Traceroute from router A to example.com would produce the following display:

```
ascend% traceroute -q 10 example.com
traceroute to example.com (10.174.88.1), 30 hops max, 0 byte packets
 1  C.example.com (10.174.88.13)  20 ms B .example.com (10.174.88.12)
    20 ms C.example.com (10.174.88.13)  20 ms B .example.com
      (10.174.88.12)  20 ms  20 ms C.example.com (10.174.88.13)  60 ms  20 ms
        B .example.com (10.174.88.12)  20 ms C.example.com (10.174.88.13)  20
          ms B .example.com (10.174.88.12)  20 ms
 2  example.com (10.174.88.1)  20 ms  20 ms  20 ms  20 ms  30 ms  20 ms
    20 ms  30 ms  20 ms  30 ms
```

Notice the alternating replies. The replies are statistically dispatched to router B and router C, with roughly 50% of the packets sent through each gateway. (For background information about the routing table and about the Traceroute command, see the *Network Configuration Guide* for your MAX.)

Third-party routing

A MAX running OSPF can advertise routes to external destinations on behalf of another gateway (a *third-party*). This is commonly known as advertising a forwarding address. Depending on the exact topology of the network, other routers might be able to use this type of link-state advertisement (LSA) and route directly to the forwarding address without involving the advertising MAX, thereby increasing the total network throughput.

Third-party routing requires that all OSPF routers know how to route to the forwarding address. This usually means that the forwarding address must be on an Ethernet that has an OSPF router acting as the forwarding router, or that the designated router is sending LSAs for that Ethernet to any area that sees the static route's forwarding-address LSAs. The following example shows how to configure a static route for OSPF to advertise a third-party gateway:

- 1 Open a static route in Ethernet > Static Rtes.
- 2 Set the Gateway to the forwarding address and set Third-Party to Yes.

```
Ethernet
  Static Rtes
    Name=third-party
    Silent=No
    Active=Yes
    Dest=10.212.65.0/24
    Gateway=101.2.3.4
    Metric=3
    Preference=100
    Private=No
    Ospf-Cost=1
    LSA-Type=Type1
    ASE-tag=c00000000
    Third-Party=Yes
```

- 3 Close the static route.

How OSPF adds RIP routes

When the MAX establishes an IP routing connection with a caller that does not support OSPF, it imports the AS-external route from the Connection profile and adds it to the routing table. The MAX does not have to run RIP to learn these routes. RIP should be turned off when the MAX is running OSPF.

To enable OSPF to add the RIP-v2 routes to its routing table, configure RIP-v2 normally in the Connection profile. OSPF will import all RIP routes as Type-2 Autonomous System Externals (ASEs). The reason that RIP routes are imported with Type-2 metrics by default is that RIP metrics are not directly comparable to OSPF metrics. To prevent OSPF from interpreting RIP metrics, the imported ASE route is assigned a Type-2 metric, which is so large compared to OSPF costs that the metric can be ignored.

Route preferences

Route preferences provide additional control over which types of routes take precedence over others. They are necessary in a router that supports multiple routing protocols, largely because RIP metrics are not comparable with OSPF metrics.

For each IP address and subnet mask pair, the routing table holds one route per protocol. The routes are assigned preferences as follows:

- Connected routes, such as Ethernet, have Preference=0.
- Routes learned from ICMP Redirects have Preference=30.
- Routes placed in the table by SNMP MIB II have Preference=100.
- Routes learned from OSPF have a default of Preference=10. You can modify the default in Ethernet > Mod Config > Route Pref.
- Routes learned from RIP have a default of Preference=100. You can modify the default in Ethernet > Mod Config > Route Pref.
- A statically configured IP Route or Connection profile has a default of Preference=100. You can modify the default in the Connection or IP Route profile.

When choosing which routes should be put in the routing table, the router first compares the Preference values, preferring the lowest number. If the Preference values are equal, the router compares the Metric field and uses the route with the lowest Metric.

If multiple routes exist for a given address and subnet mask pair, the route with the lowest Preference is best. If two routes have the same Preference, then the lower Metric is better. The best route by these criteria is that actually used by the router. The others remain latent, or *hidden*, in case the best route is removed.

To assign a WAN link the same preference as a route learned from OSPF:

- 1 Open Connections > IP Options.
- 2 Specify a Preference value of 10 (the default value for OSPF routes). For example:

```
Ethernet
  Connections
    IP options...
      LAN Adrs=10.9.8.10/22
      WAN Alias=0.0.0.0
      IF Adrs=0.0.0.0
```

```
Metric=5
Preference=10
Private=No
RIP=Off
Pool=0
```

3 Close the Connection profile.

On Ethernet, the route preferences also include ASE-type and ASE-tag information for routes learned from RIP. These values affect all RIP information learned across the Ethernet. To change the route preferences on Ethernet:

- 1** Open Ethernet > Mod Config > Route Pref.
- 2** Modify the parameters to adjust Preference values. For example, the following profile assigns static routes the same Preference value as those learned from OSPF:

```
Ethernet
  Mod Config
    Route prefs...
      Static Preference=10
      Rip Preference=100
      RipAseType=Type2
      Rip Tag=c8000000
      OSPF Preference=10
```

Or, you might change RIP metrics to Type-1:

```
Ethernet
  Mod Config
    Route prefs...
      Static Preference=100
      Rip Preference=100
      RipAseType=Type1
      Rip Tag=c8000000
      OSPF Preference=10
```

3 Close the Ethernet profile.

Displaying OSPF information

The terminal-server command-line interface provides commands for monitoring OSPF in the MAX. To display the supported commands, enter the Show OSPF command with a question mark:

```
scend% show ospf ?

show ospf ?          Display help information
show ospf size       Display OSPF size
show ospf areas      Display OSPF areas
show ospf stats      Display OSPF statistics
show ospf intf...    Display OSPF summary/detail interface information
show ospf internal   Display OSPF internal routes
show ospf lsa ...    Display OSPF detail link-state advertisements
show ospf lsdb ...   Display OSPF link-state DB summary for an area
show ospf nbrs ...   Display OSPF summary/detail neighbor information
show ospf routers    Display OSPF routers
show ospf ext        Display OSPF external AS advertisements
```

```
show ospf rtab          Display OSPF routing table
show ospf database      Display OSPF entire database summary
```

Note: For additional information, see RFC 1583.

Displaying the size of the OSPF routing table

To display the size of the OSPF routing table, enter the Show OSPF Size command. For example:

```
ascend% show ospf size
# Router-LSAs:                2
# Network-LSAs:               0
# Summary-LSAs:               0
# Summary Router-LSAs:        0
# AS External-LSAs (type-5):   1
# AS External-LSAs (type-7):   0

# Intra-area routes:          4
# Inter-area routes:           0
# Type 1 external routes:      0
# Type 2 external routes:      0
```

The output includes the following fields:

Fields	Description
# Router-LSAs	Number of router link advertisements that are also Type-1 Link State Advertisements.
# Network-LSAs	Number of network link advertisements that are also Type-2 LSAs.
# Summary-LSAs	Number of summary link advertisements that are also Type-3 LSAs. Type-3 LSAs describe routes to networks.
# Summary Router-LSAs	Number of summary link advertisements that are also Type-4 LSAs. Type-4 LSAs describe routes to AS boundary routers.
# AS External-LSAs (type-5)	Number of AS external link advertisements which are also Type-5 LSAs.
# AS External-LSAs (type-7)	Number of ASE-7 link advertisements that are also Type-7 LSAs.
Intra-area routes	Number of routes with a destination within the area.
Inter-area routes	Number of routes with a destination outside the area.
Type 1 external routes	Number of external Type-1 routes that are typically in the scope of OSPF-IGP.
Type 2 external routes	Number of external Type-2 routes that are typically outside the scope of OSPF-IGP.

Displaying OSPF areas

To display information about OSPF areas, enter the Show OSPF Areas command. For example:

```
ascend% show ospf area
Area ID   Authentication   Area Type #ifcs  #nets  #rtrs  #brdrs  #intnr
0.0.0.0   Simple-passwd    Normal    1       0       2       0       3
```

The output includes the following fields:

Field	Description
Area ID	Area number in dotted-decimal format
Authentication	Type of authentication, Simple-passwd, MD5, or Null.
Area Type	Type of OSPF area: Normal, Stub, or NSSA
#ifcs	Number of MAX interfaces specified in the area.
#nets	Number of reachable networks in the area.
#rtrs	Number of reachable routers in the area.
#brdrs	Number of reachable area border routers in the area.
#intnr	Number of reachable internal routers in the area.

Displaying general information about OSPF

To display general information about OSPF, enter the Show OSPF Stats command. For example:

```
ascend% show ospf stats
      OSPF version:                2
      OSPF Router ID:              192.192.192.2
      AS boundary capability:      Yes
Attached areas:                    1   Estimated # ext.(5) routes:    300
OSPF packets rcvd:                94565   OSPF packets rcvd w/ errs:    0
Transit nodes allocated:          3058   Transit nodes freed:        3056
LS adv. allocated:                1529   LS adv. freed:              1528
Queue headers alloc:              32   Queue headers avail:        32
# Dijkstra runs:                  4   Incremental summ. updates:   0
Incremental VL updates:           0   Buffer alloc failures:       0
Multicast pkts sent:              94595   Unicast pkts sent:          5
LS adv. aged out:                 0   LS adv. flushed:            0
Incremental ext.(5) updates:      0   Incremental ext.(7) updates: 0
External (type-5) LSA database -
Current state:                    Normal
Number of LSAs:                   1
Number of overflows:              0
```

The output includes the following fields:

Field	Description
OSPF version	Version of the OSPF protocols running.

Field	Description
OSPF Router ID	IP address assigned to the MAX, typically, the address specified for the Ethernet interface.
AS boundary capability	Displays Yes if the MAX functions as an ASBR or No if it does not. f
Attached areas	Number of areas to which this MAX attaches.
Estimated # ext.(5) routes	Maximum number of ASE-5 routes that the MAX can maintain before it goes into an overload state.
OSPF packets rcvd	Total number of OSPF packets received by the MAX.
OSPF packets rcvd w/ errs	Total number of OSPF erroneous packets received by the MAX.
Transit nodes allocated	Allocated transit nodes, which are generated only by Router LSAs (Type 1) and Network LSAs (Type 2).
Transit nodes freed	Freed transit nodes, which are generated only by Router LSAs (Type 1) and Network LSAs (Type 2).
LS adv. allocated	Number of LSAs allocated.
LS adv. freed	Number of LSAs freed.
Queue headers alloc	Number of queue headers allocated. LSAs can reside in multiple queues. Queue headers are the elements of the queues that contain the pointer to the LSA.
Queue headers avail	Available memory for queue headers. To prevent memory fragmentation, the MAX allocates memory in blocks and allocates queue headers from the memory blocks. When the MAX frees all queue headers from a specific memory block, it returns the block to the pool of available memory blocks.
# Dijkstra runs	Number of times that the MAX has run the Dijkstra algorithm (short path computation).
Incremental summ. updates	Number of summary updates that the MAX runs when small changes occur that result in generation of Summary LSAs (Type 3) and Summary Router LSAs (Type 4).
Incremental VL updates	Number of incremental virtual link updates that the MAX performs.
Buffer alloc failures	Number of buffer allocation problems that the MAX has detected and from which it has recovered.
Multicast pkts sent	Number of Multicast packets sent by OSPF.
Unicast pkts sent	Number of unicast packets sent by OSPF.
LS adv. aged out	Number of LSAs that the MAX has aged and removed from its tables.
LS adv. flushed	Number of LSAs that the MAX has flushed.

Field	Description
Incremental ext.(5) updates	Number of incremental ASE-5 updates.
Incremental ext.(7) updates	Number of incremental ASE-7 updates.
Current state	State of the External (Type-5) LSA database, either Normal or Overload.
Number of LSAs	Number of LSAs in the External (Type-5) LSA database.
Number of overflows	Number of ASE-5 that exceeded the limit of the database.

Displaying information about OSPF interfaces

Enter the Show OSPF Intf command to display either summarized information about all OSPF interfaces or specific information about a single interface.

Displaying summarized information

To display summarized information on OSPF interfaces, enter the Show OSPF Intf command. For example:

```
ascend% show ospf intf
```

Ifc Address	Phys	Assoc. Area	Type	State	#nbrs	#adjs	DInt
194.194.194.2	phani	0.0.0.0	P-P	P-P	1	1	120

The output includes the following fields:

Field	Description
Ifc Address	Address assigned to the MAX's Ethernet interface. To identify WAN links, use the Type and Cost fields.
Phys	Name of the interface or the Connection profile for WAN links.
Assoc. Area	Area in which the interface resides.
Type	Point-to-Point (P-P) or Broadcast (Bcast). WAN links are P-P links.
State	State of the link according to RFC 1583. There are many possible states, and not all states apply to all interfaces.
#nbrs	Number of neighbors of the interface.
#adjs	Number of adjacencies on the interface.
DInt	Number of seconds that the MAX waits for a router update before removing the router's entry from its table. The interval is called the Dead Interval.

Displaying specific information on a specific interface

To display detailed information for a specific interface, enter the Show OSPF Intf command in the following format:

```
ascend% show ospf intf (ip address or physical name)
```

For example:

```
ascend% sh ospf intf 194.194.194.2
      Interface address:      194.194.194.2
      Attached area:         0.0.0.0
      Physical interface:    phani (wan1)
      Interface mask:        255.255.255.255
      Interface type:        P-P
      State:                 (0x8) P-P
      Designated Router:     0.0.0.0
      Backup DR:             0.0.0.0
      Remote Address:        194.194.194.3
DR Priority:      5  Hello interval:  30  Rxmt interval:  5
Dead interval:   120 TX delay:        1  Poll interval:  0
Max pkt size:   1500 TOS 0 cost:      10
# Neighbors:    1  # Adjacencies:    1  # Full adjs.:   1
# Mcast floods: 1856 # Mcast acks:   1855
```

The output includes the following fields:

Field	Description
Interface Address	The IP address specified for the MAX's Ethernet interface.
Attached Area	Area in which the interface resides.
Physical interface	Name of the interface or the Connection profile for WAN links.
Interface type	Point-to-Point (P-P) or Broadcast (Bcast). WAN links are P-P links.
State	State of the link according to RFC 1583. There are many possible states, and not all states apply to all interfaces.
Designated Router	IP address of the designated router for the interface.
Backup DR	IP address of the backup designated router for the interface.
Remote Address	IP address of the remote end of a Point to Point (WAN) link.
DR Priority	Priority of the designated router.
Hello interval	Interval in seconds that the MAX sends Hello packets as defined in RFC 1583.
Rxmt interval	Retransmission interval as described in RFC 1583.
Dead interval	Number of seconds that the MAX waits for a router update before removing the router's entry from its table.
TX delay	Interface transmission delay.

Field	Description
Poll interval	Poll interval of non-broadcast multi-access networks.
Max pkt size	Maximum packet size that the MAX can send to the interface.
TOS 0 Count	Type of Service normal (0) cost.
# neighbors	Number of neighbors.
# adjacencies	Number of adjacencies.
# Full adjs.	Number of fully formed adjacencies.
# Mcast floods	Number of multicast floods on the interface.
# Mcast acks	Number of multicast acknowledgments on the interface.

Displaying OSPF Link-State Advertisements (LSAs)

You can enter Show OSPF commands to display a router's link state database and to expand the display of a particular LSA.

Displaying the OSPF link-state database

To display the router's link-state database, enter the Show OSPF LSDB command. For example:

```
ascend% show ospf lsdb
                        Area: 0.0.0.0
Type LS ID              LS originator      Segno      Age      Xsum
RTR  192.192.192.2      192.192.192.2  0x800005f8  696     0x6f0b
RTR  192.192.192.3      192.192.192.3  0x800005f8  163     0x6f09
                        # advertisements:      2
                        Checksum total:      0xde14
```

The output includes the following fields:

Field	Description
Area	Area ID.
Type	Type of link as defined in RFC 1583: <ul style="list-style-type: none">• Type 1 (RTR)—Outer-LSAs that describe the collected states of the router's interfaces.• Type 2 (NET)—Network-LSAs that describe the set of routers attached to the network.• Types 3 and 4 (SUM)—Summary-LSAs that describe point-to-point routes to networks or AS boundary routers.• Type 7 (ASE)—Link advertisements that are flooded only within an NSSA.
LS ID	Target address of the route.
LS originator	Address of the advertising router.

Field	Description
Seqno	Hexadecimal number that begins with 80000000 and increments by one for each LSA received.
Age	Age of the route in seconds.
Xsum	Checksum of the LSA.
# advertise-ments	Total number of entries in the link-state database.
Checksum total	Checksum of the link-state database.

Displaying expanded OSPF link-state advertisements

To specify a link-state advertisement to be expanded, first display the database. To specify an LSA, enter a Show OSPF command in the following format, then specify the LSA to expand:

show ospf lsa area *ls-type* *ls-id* *ls-orig*

The Show OSPF LSA command requires that you include the first four fields of the LSA as listed in the database. You can select the first four fields and paste them into the command line. For example, to display an expanded view of the last entry in the link-state database shown in the preceding section:

```
ascend% show ospf lsa 0.0.0.0 ase 10.5.2.160 10.5.2.162
LSA  type: ASE ls id: 10.5.2.160 adv rtr: 110.5.2.162 age: 568
      seq #: 80000037 cksum: 0xffffa
      Net mask: 255.255.255.255 Tos 0 metric: 10 E type: 1
      Forwarding Address: 0.0.0.0 Tag: c0000000
```

The output includes the following fields:

Field	Description
LSA type	Type of link as defined in RFC 1583 and identified by the type of LSA: <ul style="list-style-type: none">• Type 1 (RTR)—Outer-LSAs that describe the collected states of the router's interfaces.• Type 2 (NET)—Network-LSAs that describe the set of routers attached to the network.• Types 3 and 4 (SUM)—Summary-LSAs that describe point-to-point routes to networks or AS boundary routers.• Type 7 (ASE)—Link advertisements that are flooded only within an NSSA.
ls id	Target address of the router.
adv rtr	Address of the advertising router.
age	Age of the route in seconds.
seq #	Number that begins with 80000000 and increments by one for each LSA received.
cksum	Checksum for the LSA.
Net mask	Subnet mask of the LSA.

Field	Description
Tos	Type Of Service for the LSA.
metric	Cost of the link, not of a route. The cost of a route is the sum of all intervening links, including the cost of the connected route.
E type	External type of the LSA indicating either 1 (Type 1) or 2 (Type 2).
Forwarding Address	Forwarding Address of the LSA, described in RFC 1583.
Tag	Tag of the LSA which is described in the OSPF RFC.

Displaying OSPF neighbor information

To display information about OSPF neighbors to the MAX, enter the Show OSPF NBRs command. For example:

```
ascend% show ospf nbrs
Neighbor ID      Neighbor addr    State           LSrxl DBsum LSreq Prio Ifc
192.192.192.3    194.194.194.3   Full/-          0      0      0      5  phani
```

The output includes the following fields:

Field	Description
Neighbor ID	Address assigned to the interface. In the MAX, the IP address is always the address assigned to the Ethernet interface.
Neighbor addr	IP address of the router used to reach a neighbor. This is often the same address as the neighbor itself.
State	State of the link-state database exchange. Full indicates that the databases are fully aligned between the MAX and its neighbor.
LSrxl	Number of LSAs in the retransmission list.
DBsum	Number of LSAs in the database summary list.
LSreq	Number of LSAs in the request list.
Prio	Designated router election priority assigned to the MAX.
Ifc	Name for the Ethernet or Connection profile name for the WAN.

Displaying OSPF routers

To display OSPF routers, enter the Show OSPF Routers command. For example:

```
ascend% show ospf routers
DType RType Destination Area Cost Next hop(s) #
ASBR OSPF 192.192.192.3 0.0.0.0 10 194.194.194.3 2
```

The output includes the following fields:

Field	Description
DType	Internal route type.
RType	Internal router type.

Field	Description
Destination	Router's IP address.
Area	Area in which the router resides.
Cost	Cost of the router.
Next hop(s)	Next hop in the route to the destination.
#	Number of the interface used to reach the destination.

Displaying OSPF External AS advertisements

To display OSPF External AS advertisements, enter the Show OSPF Ext command. For example:

```
ascend% show ospf ext
Type LS ID          LS originator      Seqno      Age    Xsum
ASE5 192.192.192.0  192.192.192.2     0x800005f6  751    0xc24d
# advertisements:    1
Checksum total:      0xc24d
```

The output includes the following fields:

Field	Description
Type	Displays ASE5.
LS ID	Target address of the route.
LS originator	Address of the advertising router.
Seqno	Hexadecimal number that begins with 80000000 and increments by one for each LSA received.
Age	Age of the route in seconds.
Xsum	Checksum of the LSA.
# advertise-ments	Total number of entries in the ASE5 database.
Checksum total	Checksum of the ASE5 database.

Displaying the OSPF routing table

To display the OSPF routing table, enter the Show OSPF Rtab command. For example:

```
ascend% show ospf rtab
```

DType	RType	Destination	Area	Cost	Flags	Next hop(s)	#
RTE	FIX	192.192.192.0/24	-	1	0x82	0.0.0.170	170
RTE	OSPF	194.194.194.2/32	0.0.0.0	20	0x1	194.194.194.3	2
ASBR	NONE	192.192.192.2/32	-	0	0x0	None	-1
RTE	OSPF	192.192.192.2/32	0.0.0.0	0	0x1	0.0.0.170	170
RTE	OSPF	194.194.194.3/32	0.0.0.0	10	0x101	194.194.194.3	2
RTE	NONE	194.194.194.0/24	-	0	0x2	None	-1
ASBR	OSPF	192.192.192.3/32	0.0.0.0	10	0x100	194.194.194.3	2
RTE	OSPF	192.192.192.3/32	0.0.0.0	10	0x1	194.194.194.3	2

The output includes the following fields:

Field	Description
DType	Internal route type. DType displays one of the following values: RTE (generic route), ASBR (AS border route), or BR (area border route).
RType	Internal router type. RType displays one of the following values: FIX (static route), NONE, DEL (deleted or bogus state), OSPF (OSPF-computed), OSE1 (type 1 external), or OSE2 (type 2 external).
Destination	Destination address and subnet mask of the route.
Area	Area ID of the route.
Cost	Cost of the route.
Flags	Hexadecimal number representing an internal flag.
Next hop(s)	Next hop in the route to the destination.
#	Number of the interface used to reach the destination.

Displaying summarized OSPF database information

To display summarized information about the OSPF database, enter the Show OSPF Database command. For example:

```
ascend% show ospf database
```

```
Router Link States (Area: 0.0.0.0)
Type LS ID          LS originator      Seqno      Age      Xsum
RTR  192.192.192.2   192.192.192.2      0x800005f8 783     0x6f0b
RTR  192.192.192.3   192.192.192.3      0x800005f8 250     0x6f09
      # advertisements:      2
      Checksum total:        0xde14
```

```
External ASE5 Link States
Type LS ID          LS originator      Seqno      Age      Xsum
ASE5 192.192.192.0   192.192.192.2      0x800005f6 783     0xc24d
      # advertisements:      1
      Checksum total:        0xc24d
```

The output includes the following fields:

Type	RTR (Router LSAs), NET (Network LSAs), ASE5 (External ASE5 link advertisements to destinations external to the autonomous system), or ASE7 (ASE-7 link advertisements that are flooded only within an NSSA).
LS ID	Target address of the route.
LS originator	Address of the advertising router.
Seqno	Hexadecimal number that begins with 80000000 and increments by one for each LSA received.
Age	Age of the route in seconds.
Xsum	Checksum of the LSA.

Type	RTR (Router LSAs), NET (Network LSAs), ASE5 (External ASE5 link advertisements to destinations external to the autonomous system), or ASE7 (ASE-7 link advertisements that are flooded only within an NSSA).
# advertisements	Total number of entries in the database.
Checksum total	Checksum of the database.

Managing multicast routing

The terminal-server command-line interface provides commands to support IP multicast functionality. To display the options, invoke the terminal-server interface (System > Sys Diag > Term Serv) and enter the Show IGMP and/or show Mrouting command with a question mark:

```
ascend% show igmp ?
show igmp ?          Display help information
show igmp stats      Display IGMP Statistics
show igmp groups     Display IGMP groups Table
show igmp clients    Display IGMP clients

ascend% show mrouting ?
show mrouting ?      Display help information
show mrouting stats  Display MROUTING Statistics
```

Displaying the multicast forwarding table

To display active multicast group addresses and clients (interfaces) registered for each group:

```
ascend% show igmp groups
IGMP Group address Routing Table Up Time: 0:0:22:17
Hash      Group Address  Members    Expire time  Counts
N/A       Default route    *(Mbone)   .....      2224862
10        224.0.2.250
                2           0:3:24     3211 :: 0 S5
                1           0:3:21     145  :: 0 S5
                0(Mbone)   .....      31901 :: 0 S5
```

The output includes the following fields:

Field	Description
Hash	Index to a hash table that is displayed for debugging purposes only. The Default route is not an entry in the hash table.
Group Address	IP multicast address used. The Default route is the interface on which the multicast router resides.
Note: The IP multicast address being monitored is marked with an asterisk, meaning that this address is joined by local application.	

Field	Description
Members	Interface ID on which the membership resides. The number 0 represents the Ethernet interface. Other numbers represent WAN interfaces, numbered according to when they became active. The interface labeled Mbone is the one on which the multicast router resides.
Expire time	Time at which this membership expires. The MAX sends out IGMP queries every 60 seconds, so the expiration time is usually renewed. If the expiration time is reached, the entry is removed from the table. Periods in this field indicates that the membership never expires.
Counts	Number of packets forwarded to the client, number of packets dropped because of a lack of resources, and state of the membership (the state is displayed for debugging purposes).

Listing multicast clients

To display a list of multicast clients, enter the Show IGMP Clients command. For example:

```
ascend% show igmp clients
```

IGMP Clients

Client	Version	RecvCount	CLU	ALU
0 (Mbone)	1	0	0	0
2	1	39	68	67
1	1	33310	65	65

The output includes the following fields:

Field	Description
Client	Interface ID on which the client resides. The number 0 represents the Ethernet. Other numbers are WAN interfaces, numbered according to when they became active. The interface labeled Mbone is the one on which the multicast router resides.
Version	Version of IGMP being used.
RecvCount	Number of IGMP messages received on that interface.
CLU (Current Line Utilization) and ALU (Average Line Utilization)	Percentage of bandwidth utilized across this interface. If bandwidth utilization is high, some IGMP packet types will not be forwarded.

Displaying multicast activity

To display the number of IGMP packet types sent and received, enter the Show IGMP Stats command. For example:

```
ascend% show igmp stats
```

```
46 packets received.  
0 bad checksum packets received.
```

```
0 bad version packets received.  
0 query packets received.  
46 response packets received.  
0 leave packets received.  
51 packets transmitted.  
47 query packets sent.  
4 response packets sent.  
0 leave packets sent.
```

To display the number of multicast packets received and forwarded, enter the Show Mrouting Stats commands. For example:

```
ascend% show mrouting stats  
  
34988 packets received.  
57040 packets forwarded.  
0 packets in error.  
91 packets dropped.  
0 packets transmitted.
```

In many cases, the number of packets forwarded is greater than the number of packets received, because packets can be duplicated and forwarded across multiple links.

Monitoring Frame Relay connections

The terminal-server command-line interface includes Show FR commands for monitoring Frame Relay in the MAX. To display the options, invoke the terminal-server interface (System > Sys Diag > Term Serv) and enter the Show FR command with a question mark:

```
ascend% show fr ?  
  
show fr ?Display help information  
show fr statsDisplay Frame Relay information  
show fr lmiDisplay Frame Relay LMI information  
show fr dlci [name]Display all DLCI information or just for [name]  
show fr circuitsDisplay the FR Circuit table
```

Displaying Frame Relay statistics

To display Frame Relay statistics, enter the Show FR Stats commands: For example:

```
ascend% show fr stats  
  
Name           Type    Status    Speed    MTU      InFrame    OutFrame  
fr1            DCE     Down      64000    1532     0          1  
fr1-temp       DCE     Up        64000    1532     0          1  
fr1-temp-9     DCE     Up        64000    1532     0          0
```

The output includes the following fields:

Field	Description
Name	Name of the Frame Relay profile associated with the interface.
Type	Type of interface.

Field	Description
Status	Status of the interface. Up means the interface is functional, but is not necessarily handling an active call. Down means the interface is not functional.
Speed	Data rate in bits per second.
MTU	Maximum packet size allowed on the interface.
InFrame	Number of frames the interface has received.
OutFrame	Number of frames transmitted.

Displaying link management information

To display Link Management Information (LMI) for each link activated by a Frame Relay profile, enter the Show FR LMI command. For example:

```
ascend% show fr lmi

Tl_617D LMI for fr1
  Invalid Unnumbered info          0  Invalid Prot Disc          0
  Invalid Dummy Call Ref           0  Invalid Msg Type           0
  Invalid Status Message           0  Invalid Lock Shift        0
  Invalid Information ID            0  Invalid Report Type       0
  Num Status Enqs Sent             0  Num Status Msgs Rcvd      0
  Num Update Status Rcvd           0  Num Status Timeouts      2779

LMI is not on for fr1-temp
LMI is not on for fr1-temp-9
```

ANSI T1.617 Annex D local in-channel signaling protocol is the basis for this information.
(For a full definition of each of the fields reported, see Annex D.)

Displaying Data Link Connection Indicator (DLCI)status

To display the status of each Data Link Connection Indicator (DLCI), enter the Show FR LMI command. For example:

```
ascend% show fr dlci

DLCIs for fr1
DLCIs for fr1-temp
eng-lab-236-CirDLCI = 17Status = ACTIVE
    input pkts0output pkts0
    input octets0output octets0
    input FECN0input DE0
    input BECN0
last time status changed: 03/05/1997 14:44:17
DLCIs for fr1-temp-9
eng-lab-236-Cir-9 DLCI = 16 Status = ACTIVE
    input pkts0output pkts0
    input octets0output octets0
    input FECN0input DE0
```

```
input BECN0
last time status changed: 03/05/1997 14:45:07
DLCIs not assigned
```

The output includes the following fields:

Field	Description
DLCI	DLCI number.
Status	ACTIVE if the connection is up or INACTIVE if not.
input pkts	Number of frames the interface has received.
output pkts	Number of frames the interface has transmitted.
input octets	Number of bytes the interface has received.
output octets	Number of bytes the interface has transmitted.
in FECN pkts	Number of packets received with the Forward Explicit Congestion Notification (FECN) bit set. This field always contains a 0 (zero), because congestion management is not currently supported.
in BECN pkts	Number of packets received with the Backward Explicit Congestion Notification (BECN) bit set. This field always contains a 0 (zero), because congestion management is not currently supported.
in DE pkts	Number of packets received with the Discard Eligibility (DE) indicator bit set.
last time status changed	Time at which the DLCI state changed.

Displaying circuit information

The Show FR Circuits command displays the Frame Relay profile name, the DLCI, and the status of configured circuits. For example:

```
ascend% show fr circuits
cir-9 User Setting Up
fr1-temp-916 Up
fr1-temp17 Up
```

Turning off a circuit without disabling its endpoints

The Set Circuit command enables you to turn off traffic going through a Frame Relay circuit without disabling the circuit endpoints. This command prevents traffic from traveling between endpoints, but does not disrupt the state of the DLCI. To display the support options:

```
ascend% set circuit ?
set circuit ?          Display help information
set circuit active [name] Set the CIRCUIT to active
set circuit inactive [name] Set the CIRCUIT to inactive
```

To allow data to flow through a circuit, enter the Set Circuit Active command and append the name of the circuit. parameter. For example:

```
ascend% set circuit active circuit-1
```

To turn off data flow without disrupting the state of the DLCIs, enter the Set Circuit Inactive command and append the name of the circuit. For example:

```
ascend% set circuit inactive circuit-2
```

Monitoring X.25 and PAD connections

The terminal server supports two commands for obtaining information about X.25 and PAD service. To invoke the terminal server, select System > Sys Diag > Term Serv and press Enter.

Displaying information about PAD sessions

To display information about PAD sessions, enter the Show PAD commands. For example:

```
ascend% show pad
```

Port	State	LCN	BPS	User	Called Addr.
1	connected	0	9600	rchan	419342855555
2	connected	0	9600	dhersh	

The output includes the following fields:

Field	Description
Port	Port for the X.25 connection.
Stat	State of the connection, which can be one of the following: Idle—The PAD is open, but no call has been issued. Calling—A call has been issued and is awaiting acceptance. Connected—The call is connected and in session. Clearing—A Clear command has been issued and the transmitter is awaiting a clear confirmation.
LCN	Logical Channel Number for a PVC. An LCN of 0 means the circuit is not a PVC (but is a switched virtual circuit).
BPS	Data rate of the connection in bits per second.
User	Connection profile name of the caller.
Called Addr	X.121 address of the remote node.

Displaying information about X.25

To display information about X.25 frame and packet layers, enter the Show X25 command. For example:

```
ascend% show x25
```

Frame	State	BytesIn	BytesOut
1	LinkUp	15	45

Packet	State	BytesIn	BytesOut
1	Ready	0	0

The output includes the following fields:

Field	Description
-------	-------------

Frame	Frame layer and packet layer, respectively.
-------	---

Stat	State of the connection at that layer.
------	--

For the frame layer, the following states can occur:

- **SABMSent**—The MAX has sent an Set Asynchronous Balanced Mode (SABM) message to establish the operating mode as Link Access Balanced Protocol (LABP), and the transmitter is waiting for a an Unnumbered Acknowledge response (UA).
- **DISCSent**—The MAX sends a DISC message to disconnect the frame level, and the transmitter is waiting for a UA.
- **FRMRSent**—The MAX sends an FRMR message, indicating that the MAX received a malformed frame, and the sender is waiting for a SABM message.
- **LinkUp**—The link is up and sending I-frames and S-frames.
- **Disconnected**—The MAX requests a disconnect, and the sender is waiting for a SABM message.

For the packet layer, the following states can occur:

- **Ready**—The packet layer is ready to send and receive data.
- **DTERestart**—The DTE issues a Restart Request.
- **DCERestart**—The DCE issues a Restart Request.
- **BothRestart**—The MAX sends Restart Requests to both the DTE and the DCE.
- **InitState**—Indicates the initial state of a call.

BytesIn	Number of bytes the MAX receives from the remote node.
---------	--

BytesOut	Number of bytes the MAX transmits to the remote node.
----------	---

Setting up ISDN D-channel X.25 support

PAD service signals

The PAD transmits PAD service signals to the terminal server to acknowledge PAD commands and to inform the user about the internal state of the PAD. The terminal-server user can suppress the reception of PAD service signals by setting PAD parameter #6 to 0 (zero). Figure 5-1 lists the PAD service signals.

Table 5-1. PAD service signals

Service signal	Description
RESET DTE	The remote DTE has reset the virtual circuit.
RESET ERR	A reset has occurred because of a local procedure error.
RESET NC	A reset has occurred because of network congestion.
COM	A call has been connected.
PAD ID	Precedes a string that identifies the PAD.
ERROR	The terminal-server user used faulty syntax when entering an X.25/PAD command.
CLR	A virtual circuit has been cleared.
ENGAGED	In response to the Stat command, indicates that a virtual call is up.
FREE	In response to the Stat command, indicates that a virtual call is cleared.
PAR with X.3 parameter reference numbers and their current values	A response to the Set? command.

X.25 clear cause codes

Table 5-2 shows hexadecimal X.25 clear cause codes.

Table 5-2. Clear cause codes

Hex value	Cause code
01	Number busy

Table 5-2. Clear cause codes (continued)

Hex value	Cause code
03	Invalid facility request
05	Network congestion
09	Out of order
0B	Access barred
0D	Not obtainable
11	Remote procedure error
13	Local procedure error
15	RPOA out of order
19	Reverse charging acceptance not subscribed
21	Incompatible destination
29	Fast select acceptance not subscribed
39	Ship absent
C1	Gateway-detected procedure error
C3	Gateway congestion

X.25 diagnostic field values

Table 5-3 shows X.25 diagnostics:

Table 5-3. X.25 diagnostic field values

Hex value	Dec value	Diagnostic
0	0	No additional information
1	1	Invalid P(S)
2	2	Invalid P(R)
10	16	Packet type invalid
11	17	State r1
12	18	State r2

Table 5-3. X.25 diagnostic field values (continued)

Hex value	Dec value	Diagnostic
13	19	State r3
14	20	State p1
15	21	State p2
16	22	State p3
17	23	State p4
18	24	State p5
19	25	State p6
1A	26	State p7
1B	27	State d1
1C	28	State d2
1D	29	State d3
20	32	Packet not allowed
21	33	Unidentifiable packet
22	34	Call on one-way LC
23	35	Invalid packet type on a PVC
25	37	Reject not subscribed to
26	38	Packet too short
27	39	Packet too long
29	41	Restart packet with non-zero LC
2B	43	Unauthorized interrupt confirmation
2C	44	Unauthorized interrupt
2D	45	Unauthorized reject
30	48	Timer expired
31	49	Incoming call (or DTE timer expired for call request)
32	50	Clear indication (or DTE timer expired or retransmission count surpassed for clear request)

Table 5-3. X.25 diagnostic field values (continued)

Hex value	Dec value	Diagnostic
33	51	Reset indication (or DTE timer expired or retransmission count surpassed for reset request)
34	52	Rstart indication (or DTE timer expired or retransmission count surpassed for restart request)
40	64	Call setup, call clearing, or registration problem
41	65	Facility/registration code not allowed
42	66	Facility parameter not allowed
43	67	Invalid called address
44	68	Invalid calling address
45	69	Invalid facility/registration length
46	70	Incoming call barred
47	71	No logical channel available
48	72	Call collision
49	73	Duplicate facility requested
4A	74	Nonzero address length
4B	75	Nonzero facility length
4C	76	Facility not provided when expected

SNMP and Syslog Configuration

6

Configuring SNMP	6-1
Configuring Syslog	6-7
Disconnect codes and progress codes	6-12

MAX configurations control which classes of events will generate traps to be sent to an SNMP manager, and which managers have SNMP access to the unit. A configuration includes community strings to prevent unauthorized access. This chapter shows you how to set up the unit to work with SNMP.

Configuring *SNMP*

The MAX supports SNMP on a TCP/IP network. An SNMP management station that uses the Ascend Enterprise MIB can query the MAX, set some parameters, sound alarms when certain conditions appear in the MAX, and so forth. An SNMP manager must be running on a host on the local IP network, and the MAX must be able to find that host, through either a static route or RIP.

The MAX supports the Ascend Enterprise MIB, MIB II, and some ancillary SNMP features. The MAX can send management information to an SNMP manager without being polled. SNMP security uses a community name sent with each request. The MAX supports two community names, one with read-only access, and the other with read/write access to the MIB.

SNMP has its own password security, which you should set up to prevent reconfiguration of the MAX from an SNMP station.

Configuring **SNMP access security**

There are two levels of SNMP security: community strings, which must be known by a community of SNMP managers to access the box, and address security, which excludes SNMP access unless it is initiated from a specified IP address. Following are the relevant parameters (shown with sample settings):

```
Ethernet
  Mod Config
    SNMP options...
      Read Comm=Ascend
      R/W Comm Enable=No
      R/W Comm=Secret
      Security=Yes
```

```
RD Mgr1=10.0.0.1
RD Mgr2=10.0.0.2
RD Mgr3=10.0.0.3
RD Mgr4=10.0.0.4
RD Mgr5=10.0.0.5
WR Mgr1=10.0.0.11
WR Mgr2=10.0.0.12
WR Mgr3=10.0.0.13
WR Mgr4=10.0.0.14
WR Mgr5=10.0.0.15
```

For complete information about each parameter, see the *MAX Reference Guide*.

enabling SNMP Set commands

The R/W Comm Enable parameter disables SNMP set commands by default. Before you can use an SNMP Set command, you must set R/W Comm Enable to Yes.

Note: Even if you enable R/W Comm, you must still know the read-write community string to use a Set command.

Setting community strings

The Read Comm parameter specifies the SNMP community name for read access (up to 32 characters), and the R/W Comm parameter specifies the SNMP community name for read/write access.

Setting up and enforcing address security

If the Security parameter is set to No (its default value), any SNMP manager that presents the right community name will be allowed access. If you set this parameter to Yes, the MAX checks the source IP address of the SNMP manager and allows access only to those IP addresses listed in the RD MgrN and WR MgrN parameters, each of which specifies up to five host addresses.

Resetting the MAX and verifying reset

You can use SNMP (sysReset object) to reset a MAX from an SNMP manager. After the Reset command is issued, a one-minute timeout (not modifiable) permits the MAX to confirm the request before the unit is reset.

Information held in the Ascend Events Group is erased and its values are initialized when the MAX is reset by software or by toggling the power off and on. The SNMP object sysAbsoluteStartupTime is the time in seconds since January 1, 1990, and is not modified. To determine whether the MAX has actually reset, you can retrieve sysAbsoluteStartupTime and compare its value against the previous poll's value for Ascend Events Group variables.

Example of SNMP security configuration

The following procedure sets the community strings, enforces address security, and prevents write access:

- 1 Open Ethernet > Mod Config > SNMP Options.
- 2 Set R/W Comm Enable to Yes.
- 3 Specify the Read Comm and R/W Comm parameter strings.
- 4 Set Security to Yes.
- 5 Specify up to five host addresses in the RD MgrN parameters. Leave the WR MgrN parameters set to zero to prevent write access.
- 6 Close the Ethernet profile.

Following is an example of a profile configured with the preceding procedure.

```
Ethernet
  Mod Config
    SNMP options...
      Read Comm=Secret-1
      R/W Comm Enable=Yes
      R/W Comm=Secret-2
      Security=Yes
      RD Mgr1=10.0.0.1
      RD Mgr2=10.0.0.2
      RD Mgr3=10.0.0.3
      RD Mgr4=10.0.0.4
      RD Mgr5=10.0.0.5
      WR Mgr1=0.0.0.0
      WR Mgr2=0.0.0.0
      WR Mgr3=0.0.0.0
      WR Mgr4=0.0.0.0
      WR Mgr5=0.0.0.0
```

Setting SNMP traps

A trap is a mechanism for reporting system change in real time (for example, reporting an incoming call to a serial host port). When a trap is generated by some condition, a traps-PDU (Protocol Data Unit) is sent across the Ethernet to the SNMP manager.

Following are the parameters related to setting SNMP traps (shown with sample settings):

```
Ethernet
  SNMP Traps
    Name=
    Alarm=Yes
    Port=Yes
    Security=Yes
    Comm=
    Dest=10.2.3.4
```

For complete information about each parameter and the events that generate traps in the various classes, see the *MAX Reference Guide*.

Understanding the SNMP trap parameters

To specify the SNMP trap profile name, set the Name parameter. Use a name of 31 or fewer characters.

To specify the community string for communicating with the SNMP manager, set the Comm parameter to the community name associated with the SNMP PDU.

The Alarm, Port, and Security fields specify whether the MAX traps respectively alarm events, port events, and/or security events, and sends a trap-PDU to the SNMP manager.

The Dest field specifies the destination address for the trap-status report. If DNS or YP/NIS is supported, the Dest field can contain the hostname of a system running an SNMP manager. If the DNS or YP/NIS is not supported, the Dest field must contain the host's address.

Note: To turn off SNMP traps, set Dest to 0.0.0.0 and delete the value for Comm.

Example SNMP trap configuration

The following procedure creates a profile that specifies a community name, all the trap types, and the host's IP address in the Dest parameter.

- 1 Open an SNMP Traps profile and assign it a name.
- 2 Specify the community name (for example, Ascend).
- 3 Set the trap types to Yes.
- 4 Specify the IP address of the host to which the trap-PDUs will be sent.
- 5 Close the SNMP Traps profile.

Following is an example of a profile configured with this procedure:

```
Ethernet
  SNMP Traps
    Name=security-traps
    Alarm=Yes
    Port=Yes
    Security=Yes
    Comm=Ascend
    Dest=10.2.3.4
```

Ascend enterprise traps

This section provides a brief summary of the traps generated by alarm, port, and security events. For more details, see the Ascend Enterprise MIB. To obtain the Ascend MIB, see "Supported MIBs" on page 6-7.

Alarm events

Alarm events (also called *error events*) use trap types defined in RFC 1215 and 1315, as well as an Ascend enterprise trap type. The MAX provides the following trap types:

Alarm event	Signifies that the MAX sending the trap:
coldStart (RFC-1215 trap-type 0)	Is reinitializing itself and that the configuration of the SNMP manager or the unit might be altered.
warmStart (RFC-1215 trap-type 1)	Is reinitializing itself but neither the configuration of the SNMP manager nor that of the unit will be altered.

Alarm event	Signifies that the MAX sending the trap:
linkDown (RFC-1215 trap-type 2)	Recognizes a failure in one of the communication links represented in the SNMP manager's configuration.
linkUp (RFC-1215 trap-type 3)	Recognizes that one of the communication links represented in the SNMP manager's configuration has come up.
frDLCIStatusChange (RFC-1315 trap-type 1)	Recognizes that one of the virtual circuits (to which a DLCI number has been assigned) has changed state. That is, the link has either been created or invalidated, or has toggled between the active and inactive states.
eventTableOverwrite (ascend trap-type 16)	Detected that a new event has overwritten an unread event. This trap is sent only for systems that support Ascend's accounting MIB. Once sent, additional overwrites will not cause another trap to be sent until at least one table's worth of new events has occurred.

Port state change events

Port state change event traps are effective on a port-by-port basis for each port pointed to by `ifIndex`. The `hostPort` objects are used to associate a change with `ifIndex` objects.

The following trap types signify a change in the state of the Ascend Inverse Multiplexer (AIM) port associated with the passed index.

Trap type	Indicates that the indexed AIM port:
portInactive (ascend trap-type 0)	Has become inactive.
portDualDelay (ascend trap-type 1)	Is delaying the dialing of a second to avoid overloading devices that cannot handle two calls in close succession.
portWaitSerial (ascend trap-type 2)	Has detected DTR and is waiting for an HDLC controller to come online. CTS is off (V.25 bis dialing only).
portHaveSerial (ascend trap-type 3)	Is waiting for V.25 bis commands. CTS is on.
portRinging (ascend trap-type 4)	Has been notified of an incoming call.
portCollectDigits (ascend trap-type 5)	Is receiving digits from an RS366 interface (RS-366 dialing only).
portWaiting (ascend trap-type 6)	Is waiting for connect notification from the WAN after dialing or answer notification has been issued.

Trap type	Indicates that the indexed AIM port:
portConnected (ascend trap-type 7)	Has changed state. This change of state can be from connected to unconnected or vice versa. If connected to the far end, end-to-end data can flow but has not yet been enabled. The following trap report sequence shows that a link is up: portWaiting (6) portConnected (7) portCarrier (8) The following trap report sequence shows that a link is down: portConnected (7) portInactive (0)
portCarrier (ascend trap-type 8)	Has end-to-end data flow enabled
portLoopback (ascend trap-type 9)	Has been placed in local loopback mode.
portAcrPending (ascend trap-type 10)	Has set ACR on the RS366 interface, and is waiting for the host device (RS-366 dialing only).
portDTENotReady (ascend trap-type 11)	Is waiting for DTE to signal a ready condition when performing X.21 dialing.

Security events

Security events are used to notify users of security problems and track access to the unit from the console. The MIB-II event *authenticationError* is a security event. The other security events are Ascend-specific. The include:

Security event	Signifies
authenticationFailure (RFC-1215 trap-type 4)	The MAX sending the trap is the addressee of a protocol message that is not properly authenticated.
consoleStateChange (ascend trap-type 12)	The console associated with the passed console index has changed state. To read the console's state, get <code>ConsoleEntry</code> from the Ascend enterprise MIB.
portUseExceeded (ascend trap-type 13)	The serial host port's use exceeds the maximum set by the Max DS0 Mins Port parameter associated with the passed index (namely, the interface number).
systemUseExceeded (ascend trap-type 14)	The serial host port's use exceeds the maximum set by the Max DS0 Mins System parameter associated with the passed index (namely, the interface number).
maxTelnetAttempts (ascend trap-type 15)	A user has failed in three consecutive attempts to log into this MAX via Telnet.

Supported MIBs

You can download the most up-to-date version of the Ascend Enterprise MIB by logging in as anonymous to `ftp.ascend.com`. (No password is required.) In addition to the Ascend MIB, the MAX also supports objects related to Ascend functionality in the following Internet standard MIBs:

- MIB-II implementation (RFC 1213)
- DS1 MIB implementation (RFC 1406)
- RS232 MIB implementation (RFC-1317)
- Frame Relay MIB implementation (RFC-1315)
- Modem MIB implementation (RFC 1696)

You can download the most recent version of these RFCs by logging in as anonymous to `ftp.ds.internic.net`. (No password is required.)

Configuring Syslog

You can configure the MAX to send messages containing call and system events to an IP host running a syslog daemon.

To configure Syslog support, you must set parameters specifying the IP address of the host running the Syslog daemon. In addition, there are optional parameters you can set to customize the way the MAX sends its Syslog messages.

The IP host running the syslog daemon is typically a UNIX host, but can be a Microsoft Windows workstation or server. If the MAX is on a different network than the IP host, you must configure the routers so that the MAX can successfully communicate with the IP host.

Note: Do not configure the MAX to send reports to a IP host that can be reached only by means of a dial-up connection.

Configuring the MAX to send Syslog messages

To configure the MAX to send messages to a syslog daemon:

- 1 Open the Ethernet > Mod Config > Log menu.
- 2 Set the Syslog parameter to Yes.
- 3 Set Log Host to the IP address of the host running the syslog daemon.
- 4 Set Log Port to the port at which the syslog daemon listens for Syslog messages from the MAX. The default is 514.
- 5 Set the Log Facility value to be attached to each Syslog message.
The syslog daemon can receive messages from several devices, and it groups the messages. If the daemon receives messages from devices that specify the same log facility, it stores them in the same file.
- 6 Exit and save the changes.

To configure the syslog daemon on a UNIX host, you need to modify the host's `/etc/syslog.conf` file. This file specifies a specific action the daemon performs when it

receives messages with a particular Log Facility number. For example, if you set Log Facility to Local5 in the MAX, and the `syslog` daemon should store messages from the MAX in the file `/var/log/MAX`, add the following line to the `/etc/syslog.conf` file:

```
local5.info tab /var/log/MAX
```

Note: After making changes to the `/etc/syslog.conf` file, you must direct the UNIX host to reread the file.

Syslog message format

MAX units generate Syslog messages in the following format:

```
date time router_name ASCEND: message
```

where:

- *date* is the date the message was logged by the `syslog` daemon. The MAX does not timestamp the Syslog messages.
- *time* is the time the message was logged by the `syslog` daemon. The MAX does not timestamp the `syslog` messages.
- *router_name* is the name of the MAX sending the message.
- *message* is the specific activity that caused the MAX to send the Syslog packet.

Syslog messages and their meanings

Syslog messages are recorded during establishment of a call, during graceful or unexpected disconnection of a call, and during various other events.

In a Syslog message, `slot x port y` indicates that action occurred in a session with the module (slot card) located in slot `x`. Because slot cards support multiple simultaneous sessions, the MAX assigns the session to a specific port. For modem calls, port indicates a specific modem on a modem slot card. For digital calls, port typically indicates an HDLC channel on an Ethernet card or Ether-Data card, although port can indicate a port on a slot card supporting inverse multiplexing.

Establishment of a call

Following are examples of messages that might be logged during establishment of a call:

slot 0 port 0, line *n*, channel *m*, Incoming Call, *xxxxxxxxxx*—The MAX has received a call on channel *m* of line *n*. The MAX has assigned it an identification number of *xxxxxxxxxxxx*. The MAX has not assigned a slot card to the call.

Note: The internally used identification number might be displayed in the format MBID *xxx*.

slot *x* port *y*, Assigned to port, *xxxxxxxxxx*—The MAX has assigned the incoming call to port *y* on the module in slot *x*. The MAX assigns calls on the basis of the bearer service of the call, the configured call routing, or configured answer number routing.

slot *x* port *y*, Call connected, *xxxxxxxxxx*—The call has connected.

call *n* AN slot *x* port *y* data *service*—Port *y* on the module in slot *x* answers the call. The MAX has assigned another identifier (**call *n***) to the session. For *data service*, 56K indicates that the call is a 56Kbps call, and VOICE indicates an analog call.

slot *x* port *y*, LAN session up, *username*—The session has successfully completed authentication, the MAX displays the username, and the connection is complete.

Graceful disconnect of a call

To gracefully disconnect a call, the dial-in caller uses the connection software rather than simply turning off the computer or unplugging the modem.

The MAX displays the following messages in the order shown:

slot *x* port *y*, LAN session down, *username*—The MAX has cleared the user's session. If the user gracefully closes down the PPP connection, the MAX indicates a valid slot number and port number.

slot *x* port *y*, Call terminated—The call that was connected to port *y* on the module in slot *x* terminated. Typically, the dial-in client has terminated the call. The MAX begins clearing the resources that it had allocated for the call.

call *n* CL OK—The MAX has freed all the remaining internal resources that were used by the call.

Unexpected disconnect of a call

When a dial-in user disconnects a session by turning off the computer or unplugging the modem, the call clears before the MAX clears the PPP session. The MAX displays the following messages, which are similar to those shown in “Graceful disconnect of a call” on page 6-9.

call *n* CL OK u= *username* c=*n* p=*m*—The session for *username*, identified by **call *n***, is disconnecting. The MAX supplies disconnect and progress information about the call. The disconnect code *n* details why the call disconnected. The progress code *m* indicates the last action the MAX logged before the disconnect occurred. For detailed information, see “Disconnect codes and progress codes” on page 6-12.

Note: If the MAX has not successfully authenticated the user before the call disconnects, **u= *username*** does not appear.

slot *x* port *y*, line *n*, channel *m*, Call Disconnected—The switch clears the channel on which the call had been active.

slot *x* port *y*, Call Terminated—The call that was connected to port *y* on the module in slot *x* terminated. The dial-in client has terminated the call. The MAX begins clearing the resources that it had allocated for the call.

slot 0 port 0, LAN session down, *username*—The MAX has cleared the user's session. Because the user ended the session ungracefully, the call disconnected before the resources could be completely cleared. The MAX does not require the call to be active while freeing software resources, and records the slot and port as 0 (zero).

call *n* CL OK—The MAX has cleared up all the internal resources that were used for the call.

Additional messages

Additional Syslog messages can include the following:

LAN security error, Modem *x:y*—The MAX received a call on modem *y* in the module in slot *x*. The call has failed either because authentication failed, or because the IP address of the user did not match the IP address configured in the user's profile.

Busy—The MAX dialed a phone number that was busy.

No connection—There was no response from the far end unit when the MAX dialed.

No Channel Avail—All channels on the MAX are either supporting active calls or are disabled.

Not enough Chans—The outgoing call requested more channels than the MAX has available.

No Chan Other End—The called unit did not have an available channel on which to answer the call.

Network Problem—The telephone network has reported a protocol error.

Far End Hung Up—The telephone network notified the MAX that the calling unit has disconnected the call.

Remote Mgmt Denied—A user attempted to initiate a remote management session, which was denied by the far end unit.

Call Refused—The MAX dialed an outgoing call that was refused by the far end unit, or the MAX answered an incoming call, then immediately disconnected. The latter event might be due to of incorrect line provisioning.

Incoming Net-2-Net—The MAX received an incoming Net-2-Net call.

Sys user exceeded—The MAX dropped the call because the call had exceeded the configured maximum system DS0 minutes.

Port use exceeded—The MAX dropped the call because the call had exceeded the maximum port DS0 minutes specified in the Port profile.

High Bit Errors—During a Bit Error Rate Test (BERT), the MAX detected a high number of bit errors.

Normal Bit Errors—During a Bit Error Rate Test (BERT), the MAX detected a normal number of bit errors.

No Trunk Available—The MAX has no active WAN links.

Trunk Down—A WAN link has gone down.

Trunk Up—A WAN link has become active.

Ethernet Up—The Ethernet interface of the MAX has become active or been reinitialized. This message is logged when the Ethernet interface first comes up, or on the basis of a change to the Ethernet interface.

Callback pending—The MAX received a call configured for callback. The initial call cleared. The MAX is preparing to call back to the user.

IP address 0.0.0.0 not valid for login service—A user attempted to initiate a login service with an invalid IP address.

TACACS+:No more TCP sockets—The MAX could not initiate a TACACS+ session.

TACACS+:Unexpected TCP close event. Server down?—The MAX received a TCP Close packet before the TACACS+ TCP session was established.

TACACS+:Resource shortage—The MAX experienced a low memory condition while processing TACACS+ session.

TACACS+:Shutdown in read—The MAX experienced an unexpected end to a TACACS+ session.

TACACS+:Server timeout—The MAX timed out while waiting to connect to the TACACS+ server.

TACACS+:Table exhausted—The MAX has no available entries in its TACACS+ entry table.

TACACS+:Illegal server response—The MAX received an illegal response from the TACACS+ server.

Backoff Q full, discarding user 10.10.10.1[250725066]—Backoff-queue overflow has resulted in silent discarding of the oldest entry. When a RADIUS accounting event occurs, the MAX (the NAS) sends an Accounting-Request message to the RADIUS Accounting server, which sends back an Accounting-Response message to acknowledge receipt. The NAS is required to buffer the event until it receives an acknowledgment. The NAS employs a simple exponential backoff algorithm between attempts. The backoff algorithm is:

`backoff_time = 3 * backof_time`

`where backoff_time = [1..N]`

Once the NAS sends an accounting request, if no response is received from the Accounting server, the NAS enters backoff mode.

If the backoff queue is not empty when an accounting event occurs (a new user logs in or an existing user logs out), the event goes directly onto the backoff queue.

A maximum of 100 entries is allowed on the backoff queue. If the queue overflows, the oldest entry is silently discarded, and the MAX sends the Syslog message.

The backoff queue can be cleared by setting Acct = None on the MAX or by resetting the MAX.

When you see this Syslog message, your Accounting Server is not functioning properly. If Acct = RADIUS on the MAX, verify that you are using the correct Port number (e.g. 1646) and that the Acct Key matches the password in the clients file on the RADIUS server. Also, be aware that the default location for your accounting records is /usr/adm/radacct. You have to create the radacct directory. RADIUS will automatically create a subdirectory with the name or IP address of the MAX (depending on your entry in the clients file) and will then write to the detail file. You can redirect your accounting output by starting RADIUS with the -a option (for example, radiusd -a /usr/adm/ascendlog).

Disconnect codes and progress codes

When a call disconnects, the MAX typically sends the following message:

```
call n CL OK u= username c=n p=m
```

where:

- *n* specifies a disconnect code indicating why the call disconnected.
- *m* specifies a progress code indicating how far the call had progressed when it disconnected.

Disconnect codes and their meanings

Following is a list of disconnect codes and their meanings:

Disconnect code	Description
1	Not applied to any call.
2	Unknown disconnect.
3	Call disconnected.
4	CLID authentication failed.
5	RADIUS timeout during authentication.
6	Successful authentication. MAX is configured to call the user back.
7	Pre-T310 Send Disc timer triggered.
9	No modem is available to accept call.
10	Modem never detected Data Carrier Detect (DCD).
11	Modem detected DCD, but modem carrier was lost.
12	MAX failed to successfully detect modem result codes.
13	MAX failed to open a modem for outgoing call.
14	MAX failed to open a modem for outgoing call while ModemDiag diagnostic command is enabled.
20	User exited normally from the terminal server.
21	Terminal server timed out waiting for user input.
22	Forced disconnect when exiting Telnet session.

Disconnect code	Description
23	No IP address available when invoking PPP or SLIP command.
24	Forced disconnect when exiting raw TCP session.
25	Exceeded maximum login attempts.
26	Attempted to start a raw TCP session, but raw TCP is disabled on MAX.
27	Control-C characters received during login.
28	Terminal-server session cleared ungracefully.
29	User closed a terminal-server virtual connection normally.
30	Terminal-server virtual connect cleared ungracefully.
31	Exit from Rlogin session.
32	Establishment of rlogin session failed because of bad options.
33	MAX lacks resources to process terminal-server request.
35	MP+ session cleared because no null MP packets received. A MAX sends (and should receive) null MP packets throughout an MP+ session.
40	LCP timed out waiting for a response.
41	LCP negotiations failed, usually because user is configured to send passwords via PAP, and MAX is configured to only accept passwords via CHAP (or vice versa).
42	PAP authentication failed.
43	CHAP authentication failed.
44	Authentication failed from remote server.
45	MAX received Terminate Request packet while LCP was in open state.
46	MAX received Close Request from upper layer, indicating graceful LCP closure.
47	MAX cleared call because no PPP Network Core Protocols (NCPs) were successfully negotiated. Typically, there is no agreement on the type of routing or bridging that is supported for the session.
48	Disconnected MP session. The MAX accepted an added channel, but cannot determine the call to which to add the new channel.
49	Disconnected MP call because no more channels can be added.
50	Telnet or raw TCP session tables full.
51	MAX has exhausted Telnet or raw TCP resources.
52	For Telnet or raw TCP session, IP address is invalid.
53	For Telnet or raw TCP session, MAX cannot resolve hostname.
54	For Telnet or raw TCP session, MAX received bad or missing port number.
60	For Telnet or raw TCP session, host reset.
61	For Telnet or raw TCP session, connection was refused.
62	For Telnet or raw TCP session, connection timed out.
63	For Telnet or raw TCP session, connection closed by foreign host.
64	For Telnet or raw TCP session, network unreachable.

Disconnect code	Description
65	For Telnet or raw TCP session, host unreachable.
66	For Telnet or raw TCP session, network admin unreachable.
67	For Telnet or raw TCP session, host admin unreachable.
68	For Telnet or raw TCP session, port unreachable.
100	Session timed out.
101	Invalid user.
102	Callback enabled.
105	Session timeout on the basis of encapsulation negotiations.
106	MP session timeout.
115	Instigating call no longer active.
120	Requested protocol is disabled or unsupported.
150	Disconnect requested by RADIUS server.
151	Call disconnected by local administrator.
152	Call disconnected via SNMP.
160	Exceeded maximum number of V.110 retries.
170	Timeout waiting to authenticate far end.
180	User disconnected by executing Do Hangup from VT100 interface.
181	Call cleared by MAX.
185	Signal lost from far end, typically because the far end modem was turned off.
190	Resource has been quiesced.
195	Maximum duration time reached for call.
201	MAX has low memory.
210	MAX modem card stops working while it has calls outstanding.
220	MAX requires CBCP, but client does not support it.
230	MAX deleted Vrouter.
240	MAX disconnected call on the basis of LQM measurements.
241	MAX cleared backup call.
250	IP FAX call cleared normally.
251	IP FAX call cleared because of low available memory.
252	MAX detected an error for an incoming IP FAX call.
253	MAX detected an error for an outgoing IP FAX call.
254	MAX detected no available modem to support an IP FAX call.
255	MAX detected problem opening IP FAX session.
256	MAX detected a problem when performing a TCP function during an IP FAX call.
257	IP FAX session cleared abnormally.
258	MAX detected problem when parsing telephone number for IP FAX call.

Disconnect code	Description
260	MAX detected problem when decoding IP FAX variables.
261	MAX detected problem when decoding IP FAX variables.
262	MAX has no configured IP FAX server.
300	MAX detects X.25 error.

Progress codes and their meanings

Following are the progress codes and their meanings:

Progress code	Description
1	Not applied to any call.
2	Unknown progress.
10	MAX has detected and accepted call.
30	MAX has assigned modem to call.
31	Modem is awaiting DCD from far-end modem.
32	Modem is awaiting result codes from far-end modem.
40	Terminal-server session started.
41	Raw TCP session started.
42	Immediate Telnet session started.
43	Connection made to raw TCP host.
44	Connection made to Telnet host.
45	Rlogin session started.
46	Connection made with Rlogin session.
47	Terminal-server authentication started.
50	Modem outdial session started.
60	LAN session is up.
61	Opening LCP.
62	Opening CCP.
63	Opening IPNCP.
64	Opening BNCP.
65	LCP opened.
66	CCP opened.
67	IPNCP opened.
68	BNCP opened.
69	LCP in Initial state.
70	LCP in Starting state.
71	LCP in Closed state.
72	LCP in Stopped state.

Progress code	Description
73	LCP in Closing state.
74	LCP in Stopping state.
75	LCP in Req-Sent state.
76	LCP in Ack-Rcvd state.
77	LCP in Ack-Sent state.
80	IPX NCP in Open state.
81	AT NCP in Open state.
82	BACP being opened.
83	BACP is now open.
84	CBCP being opened.
85	CBCP is now open.
90	MAX has accepted V.110 call.
91	V.110 call in Open state.
92	V.110 call in Carrier state.
93	V.110 call in Reset state.
94	V.110 call in Closed state.
100	MAX determines that call requires callback.
101	Authentication failed.
102	Remote authentication server timed out.
120	Frame Relay link is inactive. Negotiations are in progress.
121	Frame Relay link is active and has end-to-end connectivity.
200	Starting Authentication layer.
201	Authentication layer moving to opening state.
202	Skipping Authentication layer.
203	Authentication layer in opened state.

Troubleshooting

A

Indicator lights	A-1
ISDN cause codes	A-4
Common problems and their solutions	A-13

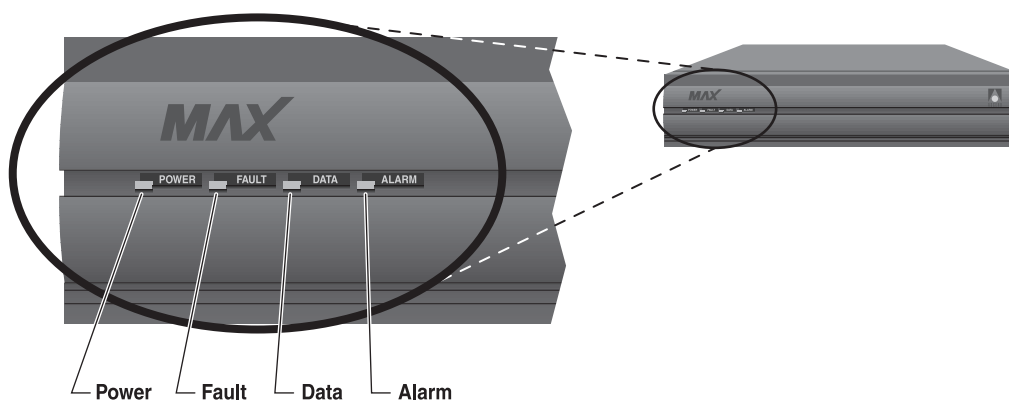
Indicator lights

Lights (LEDs) on the MAX front and back panel indicate the status of the unit.

MAX front panel

Figure A-1 shows the LEDs on the front panel of the MAX:

Figure A-1. MAX front-panel LEDs



The front-panel LEDs indicate the status of the system, the PRI interface, and the data transfer in active sessions.

Table A-1 lists and describes each LED.

Table A-1. MAX front-panel LEDs

LED	Description
Power	On when the MAX power is on.
Fault	On in one of two cases: Hardware self-test in progress or a hardware failure. When a hardware self-test is in progress, the LED stays on. If any type of hardware failure occurs, the LED flashes. If the failure is isolated to an expansion card, the MAX might continue to function without the expansion card.
Data	On when calls are active.
Alarm	On indicates a WAN alarm or a trunk out of service (during line loopback diagnostics, for example). WAN alarms include Loss of Sync, Red Alarm, Yellow Alarm, and All Ones (or AIS).

Figure A-2 shows the location of the LEDs on the front panel of the Redundant MAX.

Figure A-2. Location of LEDs on the Redundant MAX

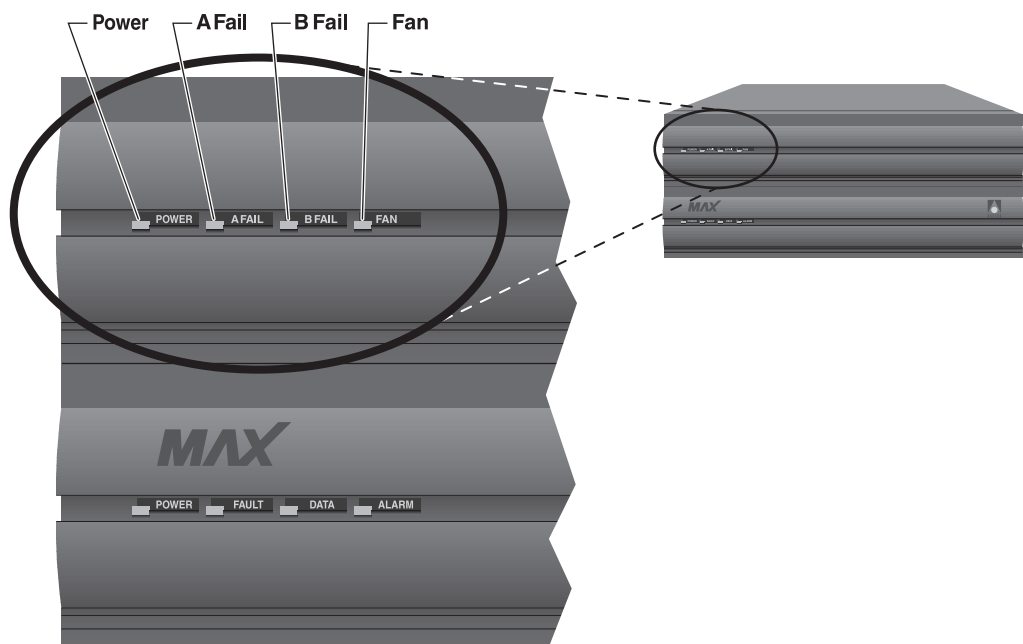


Table A-2 lists and describes each LED on the Redundant MAX.

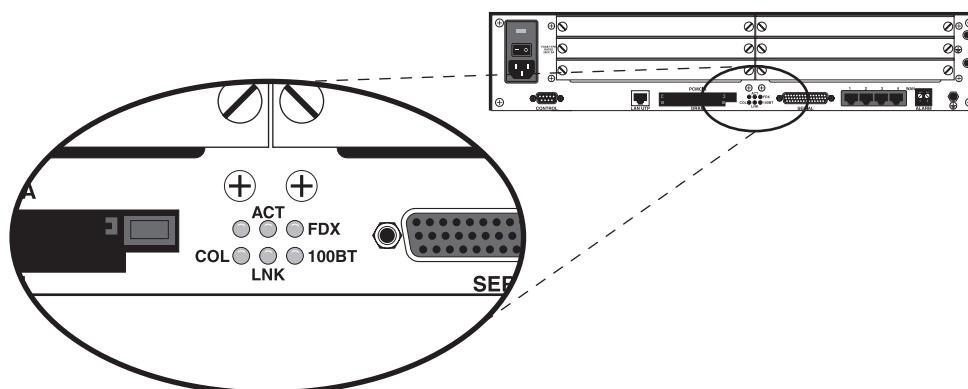
Table A-2. Redundant MAX LEDs

LED	Description
Power	On when the Redundant MAX power supply is on.
A Fail	On only if one or more of the voltages from side A of the power supply has failed (+12, +5, +3.3, -12, -5.)
B Fail	On only if one or more of the voltages from side B of the power supply has failed (+12,+5, +3.3, -12, -5.)
Fan	On when the fans are functioning properly (if +12 Vdc from either A or B is good). This LED goes off is in the event of a fan failure.

MAX back panel

Figure A-3 shows the MAX back-panel LEDs, which display the status of the Ethernet interface:

Figure A-3. Ethernet interface LEDs on MAX back panel



Note: The Classic MAX back panel shows similar LEDs on the Ethernet expansion card if one is installed. The Classic MAX has one LED for each possible Ethernet interface (10Base-T, and COAX (10Base-2), which illuminate when the interface is in use. The ACT and COL LEDs are the same as those on the MAX 6000 (Table A-3).

Table A-3 describes the Ethernet interface LEDs.

Table A-3. Ethernet interface LEDs on back panel

LED	Description
ACT (Activity)	On when the MAX is detecting activity (network traffic) on its Ethernet interface.
COL (Collisions)	On when the MAX detects packet collisions on the Ethernet.

Table A-3. Ethernet interface LEDs on back panel (continued)

LED	Description
FDX	On indicates full duplex on the Ethernet.
100ST	On indicates 100BT. Off indicates 10BT.
LINK (Link integrity)	On when the Ethernet interface is functional.

ISDN cause codes

ISDN cause codes are numerical diagnostic codes sent from an ISDN switch to a DTE. These codes provide an indication of why a call failed to be established or why a call terminated. The cause codes are part of the ISDN D-channel signaling communications supported by the Signaling System 7 supervisory network (WAN). When you dial an ISDN call from the MAX, the MAX reports the cause codes in the Message Log status menu. When the MAX clears the call, a cause code is reported even if inband signaling is in use. If the PRI or BRI switch type is ITR6 (Germany), see Table A-5.

Table A-4 lists the numeric cause codes and provides a description of each.

Table A-4. ISDN cause codes

Code	Cause
0	Valid cause code not yet received
1	Unallocated (Unassigned) Number. Indicates that the destination requested by the calling user cannot be reached because, although the number is in a valid format, it is not currently assigned.
2	No Route To Specified Transit Network. Indicates that the equipment sending this cause has received a request to route the call through a particular transit network which it does not recognize. The equipment sending this cause does not recognize the transit network either because the transit network does not exist or because that particular transit network, while it does exist, does not serve the equipment which is sending this cause.
3	No Route To Destination. Indicates that the called party cannot be reached because the network through which the call has been routed does not serve the destination desired. This cause is supported on a network dependent basis.
4	Send Special Information Tone (Five One Zero NT). Indicates that the called party cannot be reached for reasons that are of a long term nature and that the special information tone should be returned to the calling party.
5	Misdialed Trunk Prefix. Indicates the erroneous inclusion of a trunk prefix in the called party number. This number is supposed to be stripped from the dialed number being sent to the network by the customer premises equipment.

Table A-4. ISDN cause codes (continued)

Code	Cause
6	Channel Unacceptable. Indicates that the channel most recently identified is not acceptable to the sending party for use in this call.
7	Call awarded, being delivered in an established channel. Indicates that the user has been awarded the incoming call, and that the incoming call is being connected to a channel already established to that user for similar calls (e.g. packet-mode x.25 virtual calls).
8	Preemption. Indicates that the call is being preempted.
9	Preemption - Circuit Reserved For Reuse. Indicates that the call is being preempted and the circuit is reserved for reuse by the preempting exchange.
10	Prefix 1 dialed but not required
11	More digits received than allowed, but the call is proceeding
16	Normal Call Clearing. Indicates that the call is being cleared because one of the users involved in the call has requested that the call be cleared.
17	User Busy. Also called Cause Code 16/4. Is used when the called user has indicated the inability to accept another call. This cause may code may be generated by the called user or by the network. Please note that the use equipment is compatible with the call.
18	No User Responding. Also called Cause Code 16/3. Is used when a called party does not respond to a call establishment message with either an alerting or connect indication within the prescribed period of time allocated (in Q.931 by the expiry of either time T303 or T310).
19	No Answer From User (User Alerted).Is used when a user has provided an alerting indication but has not provided a connect indication within a prescribed period of time. Note: This cause is not necessarily generated by the customer premise equipment, but may be generated by internal network timers.
20	Subscriber Absent. Is used when a mobile station has logged off, radio contact is not obtained with a mobile station or if a personal telecommunication user is temporarily not addressable at any user-network interface.
21	Call Rejected. Indicates that the equipment sending this cause does not wish to accept this call, although it could have accepted the call because the equipment sending this cause is neither busy nor incompatible. This cause may also be generated by the network, indicating that the call was cleared due to a supplementary service constraint. The diagnostic field may contain additional information about the supplementary service and reason for rejection.

Table A-4. ISDN cause codes (continued)

Code	Cause
22	Number Changed. Is returned to a calling party when the called party number indicated by the calling party is no longer assigned. The new called party number may optionally be included in the diagnostic field. If the network does not support this cause, cause no: 1, unallocated (unassigned) will be used instead.
23	Reverse charging rejected
24	Call suspended
25	Call resumed
26	Non-Selected User Clearing. Indicates that the user has not been awarded the incoming call.
27	Destination Out Of Order. Indicates that the destination cannot be reached because the interface to the destination is not functioning correctly. The signaling message was unable to be delivered because of a hardware failure.
28	Invalid Number Format (Address Incomplete). Indicates that the called party cannot be reached because the called party number is not in a valid format or is not complete.
29	Facilities Rejected. Is returned when a facility requested by the user cannot be provide by the network.
30	Response To Status Enquiry. Included in the STATUS message when the reason for generating the STATUS message was the prior receipt of a STATUS ENQUIRY.
31	Normal, Unspecified. Is used to report a normal event only when no other cause in the normal class applies.
33	Circuit out of order
34	No Circuit/Channel Available. Indicates that there is no appropriate circuit/channel presently available to handle the call. Note: If you receive this call, try another data-service, such as dropping from a 64K to 56K data rate.
35	Call Queued. Indicates that the call has been queued for service by the next available device.
37	Degraded service
38	Network Out Of Order. Indicates that the network is not functioning correctly and that the conditions are likely to last a relatively long period of time. A call that is attempted soon afterwards will most likely not connect successfully.

Table A-4. ISDN cause codes (continued)

Code	Cause
39	Permanent Frame Mode Connection Out-Of-Service. Is included in a STATUS message to indicate that a permanently established frame mode connection is out-of-service (e.g. due to equipment or section failure) [see Annex A/Q.933]
40	Permanent Frame Mode Connection Operational. Is included in a STATUS message to indicate that a permanently established frame mode connection is operational and capable of carrying user information. [see Annex A/Q.933]
41	Temporary Failure. Indicates that the network is not functioning correctly and that the condition is not likely to last a very long period of time. A call that is attempted almost immediately afterwards will most likely connect successfully.
42	Switching Equipment Congestion. Indicates that the switching equipment generating this cause is experiencing a period of high traffic.
43	Access Information Discarded. Indicates that the network could not deliver access information, low layer compatibility, high layer compatibility, or sub-address as indicated in the diagnostic.
44	Requested Circuit/Channel Not Available. Is returned when the circuit or channel indicated by the requesting entity cannot be provided by the other side of the interface.
45	Pre-empted
46	Precedence Call Blocked. Indicates that there are no preemptable circuits or that the called user is busy with a call of equal or higher preemptable level.
47	Resource Unavailable, Unspecified. Is used to report a resource unavailable event only when no other cause in the resource unavailable class applies.
49	Quality Of Service Not Available. Is used to report that the requested Quality of Service cannot be provided (delay can't be supported).
50	Requested facility not subscribed. Indicates that the requested supplementary service could not be provided due to user oversight. This cause code is often caused by the CPE being configured for the wrong switch type.
51	Reverse charging not allowed
52	Outgoing calls barred. Indicates that because of call screening provided by the network, the calling user is not permitted to make a call.
53	Outgoing Calls Barred Within CUG. Indicates that although the calling party is a member of the CUG for the outgoing CUG call, outgoing calls are not allowed for this member of the CUG.
54	Incoming calls barred. Indicates that the called user will not accept the call delivered in the SETUP message.

Table A-4. ISDN cause codes (continued)

Code	Cause
55	Incoming Calls Barred Within CUG. Indicates that although the calling party is a member of the CUG for the incoming CUG call, incoming calls are not allowed for this member of the CUG.
56	Call waiting not subscribed
57	Bearer Capability Not Authorized. Indicates that the user has requested a bearer capability which is implemented by their equipment but the user is not authorized to use.
58	Bearer Capability Not Presently Available. Indicates that the user has requested a bearer capability which is implemented by the equipment which generated this cause but which is not available at this time.
62	Inconsistency In Outgoing Information Element. Indicates an inconsistency in the designated outgoing access information and subscriber class
63	Service Or Option Not Available, Unspecified. Is used to report a service or option not available event only when no other cause in the service or option not available class applies.
65	Bearer Capability Not Implemented. Indicates that the equipment sending this cause does not support the bearer capability requested.
66	Channel Type Not Implemented. Indicates that the equipment sending this cause does not support the channel type requested
67	Transit network selection not implemented
68	Message not implemented
69	Requested Facility Not Implemented. Indicates that the equipment sending this cause does not support the requested supplemental service.
70	Only Restricted Digital Information Bearer Capability Is Available. Indicates that on equipment has requested an unrestricted bearer service but that the equipment sending the cause only supports the restricted version of the requested bearer capability.
79	Service Or Option Not Implemented, Unspecified. Is used to report a service r option not implemented but only when no other cause in this class applies.
81	Invalid Call Reference Value. Indicates that the equipment sending this cause has received a message with a call reference which is not currently in use on the user-network interface.
82	Identified Channel Does Not Exist. Indicates that the equipment sending this cause has received a request to use a channel not activated on the interface for a call. For example, if the user only subscribed to channels 1 to 12 and channel 13 through 23 is requested by either side, this cause is generated.

Table A-4. ISDN cause codes (continued)

Code	Cause
83	A Suspended Call Exists, But This Call Identify Does Not. Indicates that a call resume has been attempted with a call identity which differs from that in use for any presently suspended call(s).
84	Call Identity In Use. Indicates that the network has received a call resume request. The call resume request contained a call identity information element which presently does not indicate any suspended call within the domain of interfaces over which calls may be resumed.
85	No Call Suspended. Indicates that the network has received a call resume request containing a Call identity information element which presently does not indicate any suspended call within the domain of interfaces over which calls may be resumed.
86	Call Having The Requested Call Identity Has Been Cleared. Indicates that the network has received a call resume request. The request contained a call identity information element which once indicated a suspended call, however, that the call was cleared while suspended (either a network time-out or remote user).
87	User Not A Member Of CUG. Indicates that the called user for the incoming CUG call is not a member of the specified CUG or that the calling user is an ordinary subscriber calling a CUG subscriber.
88	Incompatible Destination. Indicates that the equipment sending this cause has received a request to establish a call which has low layer compatibility, high layer compatibility, or other compatibility attributes (e.g. data rate) which cannot be accommodated.
89	Nonexistent abbreviated address entry
90	Non-Existent CUG. Indicates that the specified CUG does not exist.
91	Invalid Transit Network Selection. Indicates that a transit network identification was received which is of an incorrect format as defined in Annex C/Q.931
92	Invalid facility parameter
93	Mandatory information element is missing
95	Invalid Message, Unspecified. Is used to report an invalid message event only when no other cause in the invalid class applies.
96	Mandatory Information Element Is Missing. Indicates that the equipment sending this cause has received a message which is missing an information element which must be present in the message before that message can be processed.

Table A-4. ISDN cause codes (continued)

Code	Cause
97	Message Type Non-Existent Or Not Implemented. Indicates that the equipment sending this cause has received a message with a message type it does not recognize either because this is a message not defined or defined but not implemented by the equipment sending this cause.
98	Message Not Compatible With Call State Or Message Type Non-Existent Or Not Implemented. Indicates that the equipment sending this cause has received a message such that the procedures do not indicate that this is a permissible message to receive while in the call state, or a STATUS message was received indicating an incompatible call state.
99	Information Element / Parameter Non-Existent Or Not Implemented. Indicates that the equipment sending this cause has received a message which includes information element(s)/parameter(s) not recognized because the information element(s)/parameter name(s) are not defined or are defined but not implemented by the equipment sending the cause. This cause indicates that the information element(s)/parameter(s) were discarded. However, the information element is not required to be present in the message in order for the equipment sending the cause to process the message.
100	Invalid Information Element Contents. Indicates that the equipment sending this cause has received an information element which it has implemented; however, one or more fields in the information elements are coded in such a way which has not been implemented by the equipment sending this cause.
101	Message Not Compatible With Call State. Indicates that a message has been received which is incompatible with the call state.
102	Recovery On Timer Expiry. Indicates that a procedure has been initiated by the expiry of a timer in association with Q.931 error handling procedures.
103	Parameter Non-Existent Or Not Implemented - Passed On. Indicates that the equipment sending this cause has received a message which includes parameters not recognized because the parameters are not defined or are defined but not implemented by the equipment sending this cause.
110	Message With Unrecognized Parameter Discarded. Indicates that the equipment sending this cause has discarded a received message which includes a parameter that is not recognized.
111	Protocol Error, Unspecified. Is used to report a protocol error event only when no other cause in the protocol error class applies.
127	Interworking, Unspecified. Indicates that there has been interworking which does not provide causes for actions. The precise cause for a message which is being sent cannot be ascertained.

Table A-5 lists the cause codes for the ITR6 switch type.

Table A-5. ISDN cause codes for ITR6 switch type

ITR6 Code	Cause
1	Invalid call reference value.
3	Bearer service not implemented. (Service not available in the A-exchange or at another position in the network, or no application has been made for the specified service.)
7	Call identity does not exist. (Unknown call identity).
8	Call identity in use. (Call identity has already been assigned to a suspended link.)
10	No channel available. (No useful channel available on the subscriber access line—only local significance.)
16	Requested facility not implemented. (The specified FAC code is unknown in the A-exchange or at another point in the network.)
17	Request facility not subscribed. (Request facility rejected because the initiating or remote user does not have appropriate authorization.)
32	Outgoing calls barred. (Outgoing call not possible because of access restriction that has been installed.)
33	User access busy. (If the total made up of the number of free B channels and the number of calling procedures without any defined B channel is equal to four, any new incoming calls will be rejected from within the network. The calling party receives a DISC with a cause user access busy, which indicates the first busy instance, and a busy signal.)
34	Negative CUG comparison. (Link not possible because of negative CUG comparison.)
35	Nonexistent CUG. (This CUG does not exist.)
37	Communication as semipermanent link not permitted.
48 - 50	Not used. (Link not possible because, for example, RFNR check is negative.)
53	Destination not obtainable. (Link cannot be established in the network because of incorrect destination address, services, or facilities.)
56	Number changed. (Number of B-subscriber has changed.)
57	Out of order. (Remote TE not ready.)
58	No user responding. (No TE has responded to the incoming SETUP or call has been interrupted, absence assumed—expiry of call timeout T3AA.)

Table A-5. ISDN cause codes for ITR6 switch type (continued)

ITR6 Code	Cause
59	User busy. (B-subscriber busy)
61	Incoming calls barred. (B-subscriber has installed restrictions against incoming link, or the requested service, not supported by the B-subscriber)
62	Call rejected. (To A-subscriber: Link request actively rejected by B-subscriber, by sending a DISC in response to an incoming SETUP. To a TE during the phase in which an incoming call is being established: The call has already been accepted by another TE on the bus.)
89	Network congestion. (Bottleneck situation in the network; for example, all-trunks-busy, no conference set free.)
90	Remote user initiated. (Rejected or cleared down by remote user or exchange.)
112	Local procedure error. (In REL: Call cleared down as a result of local errors, for example, invalid messages or parameters, expiry of timeout. In SUS REJ: The link must not be suspended because another facility is already active. In RES REJ: No suspended call available. In FAC REJ: No further facility can be requested because one facility is already being processed, or the specified facility cannot be requested in the present call status.)
113	Remote procedure error. (Call cleared down because of error at remote end.)
114	Remote user suspended. (The call has been placed on hold or suspended, at the remote end.)
115	Remote user resumed. (Call at remote end is no longer on hold, suspended, or in the conference status.)
127	User Info discarded locally. (The USER INFO message is rejected locally. This cause is specified in the CON message.)

Common problems and their solutions

This section lists problems you might encounter and describes ways to resolve them. It categorizes common problems as general problems, configuration problems, hardware configuration problems, ISDN interface problems, and problems indicated by the LEDs.

General problems

Calls fail between AIM ports

The following first-level diagnostic commands can help in troubleshooting calls between AIM ports:

- For a local loopback toward an application at its AIM-port interface, use the Local LB command in the Port Diag menu.
- For a loopback toward an application at its remote-end AIM interface, use the DO Beg/End Rem LB command.
- For a channel-by-channel error measurement, use the DO Beg/End BERT command.
- To resynchronize a multichannel call, use the DO Resynchronize command.

To use a DO command, you must be in a profile or status window specific to an AIM port with a call online. For information about the Local LB command and about each DO command, see the *MAX Reference Guide*.

DO menus do not allow most operations

When the list of DO commands appears, many operations might not be available if the right profile has not been selected. Because the MAX can manage a number of calls simultaneously, you might need to select a specific Connection profile, Port profile, or Call profile in order to see certain DO commands. For example, to dial from a Call profile or a Connection profile, you must move to the Call profile (Host/6 > Port *N* Menu > Directory) or the Connection profile and press Ctrl-D 1.

Note that you cannot dial if Operations=No for the control port. If a call is already active, DO 2 (Hang Up) appears instead of DO 1 (Dial). If the T1 or E1 line is not available, Trunk Down appears in the message log and you cannot dial.

POST takes more than 30 seconds to complete

In earlier versions of the software, the MAX downloaded the required code and immediately commenced with AT POST (which sends the string AT to each modem and waits for the modem to respond with "OK"). With the current software, the MAX downloads the modem code, waits for the modems to checksum the downloaded code, and then verifies that the checksum matches before continuing. If the checksum does not match, the MAX downloads the code again, up to two more times. If the checksum still does not match after three download attempts, the MAX fails the entire slot card.

This feature helps to reduce the POST failure rates for the 12MOD cards. The 12MOD digital modem slot card boots every time the MAX power-cycles, and requires boot-up configuration data from the MAX. If the first boot-up fails, the MAX makes two further attempts to download the code for the MAX unit's 12MOD digital 12-modem slot card.

Configuration problems

The most common problems result from improperly configured profiles.

The MAX cannot dial out on a T1 or E1 line

To verify that the configured profile is correctly configured:

- 1 Make certain that you have entered the correct phone number to dial.
- 2 Verify that the Data Svc parameter specifies a WAN service available on your line.
If you request a WAN service that is not available on your line, the WAN rejects your request to place a call.
- 3 Check whether the channels using the requested WAN service are busy.
If these channels are busy, an outgoing call might be routed to channels for which you did not request the specified WAN service. Check the Data Svc, Call-by-Call, and PRI # Type parameter values in the profile.
- 4 Determine whether you have correctly set the parameters controlling Dynamic Bandwidth Allocation.

For detailed information, see the *Network Configuration Guide* for your MAX.

Some channels do not connect

You might encounter a problem in which the Line Status menu shows that the MAX is calling multiple channels simultaneously, but only some of the channels connect. In this case, an international MAX placed the call, or the call was from the U.S. to another country. In some countries, setting the Parallel Dial parameter in the System profile to a value higher than 1 or 2 violates certain dialing rules, and only some of the channels can connect during call setup. Try reducing the Parallel Dial parameter value to 2. If the problem persists, try reducing it to 1.

Data is corrupted on some international calls

You might notice that the data appears to be corrupted on single- or multichannel calls dialed from the U.S. to another country. On some international calls, the data service per channel is not conveyed by the WAN to the MAX answering the call. You must therefore set Force 56=Yes in the Call profile. If you do not, the MAX incorrectly thinks that the call uses 64-Kbps channels.

Only the base channel connects

You might encounter a problem in which the first channel of an inverse multiplexing or MP+ call connects, but the call then clears or does not connect on the remaining channels.

The most common error in defining Line *N* profiles is specifying incorrect phone numbers. The MAX cannot successfully build inverse multiplexing or MP+ calls if the phone numbers in the Line *N* profile of the called unit are incorrect. The phone numbers that you specify in the Line *N* profile are the numbers local to your unit. Do not enter the phone numbers of the MAX you are calling. Enter those numbers in the Call profile, Destination profile, or Connection profile.

In addition, when you are using E1 or T1 lines, any phone numbers you specify must correspond to those channels within the circuit that are available for data transmission. For

example, if channels 13-21 are allocated to a particular slot, you must specify the phone numbers for channels 13-21 in the Line *N* profile. Switched data channels do not have to be contiguous within the circuit.

No Channel Avail error message

If the error message No Channel Avail appears in the message log display when the MAX tries to place a call, check the Line *N* profile configuration. This message can also indicate that the lines' cables have been disconnected or were installed incorrectly.

Restored configuration has incorrect RADIUS parameters

On earlier RADIUS Servers, the submenu consisted of three clients (specific host addresses) and one Server Key for all three clients. If the MAX supports the new RADIUS Server, the restoration of the MAX configuration will cause a problem, because the new RADIUS Server allows up to nine addresses (host or net) and a Server Key for each address. When you restore configurations with the old Client Address list, the subnet mask assigned to the clients will be the default subnet mask of the address type given (for example, 128.50.1.1 will get a subnet mask of 16) and not the previous 32-bit (single host) address. In addition, the Server Key will not automatically be set. You must set the Server Key manually for each client in the RADIUS Server submenu.

Hardware configuration problems

If you cannot communicate with the MAX through the VT100 control terminal, you might have a problem with terminal configuration, the control port cable, or the MAX hardware.

Cannot access the VT100 interface

If no data is displayed on the VT100 interface, verify that the unit completes all of the Power-On Self Tests. Proceed as follows:

- 1 Verify that the MAX and your terminal are set at the same speed.
- 2 Locate the LED labeled Fault.
- 3 Switch on the MAX.

The Fault LED should remain off except during the power-on self tests. If you are using the VT100 interface, press Ctrl-L to refresh the screen.

If the Fault LED remains on longer than a minute, there is a MAX hardware failure. A blinking Fault LED also indicates a hardware failure. Should these situations arise, contact Ascend Customer Service.

Fault LED is off but no menus are displayed

If the unit passed its Power-On Self Tests and you still cannot communicate with the VT100 interface, type Ctrl-L to refresh the screen. If you still do not see any data, check the cabling between the MAX and your terminal as follows:

- 1 Check the pin-out carefully on the 9-pin cable.
The control terminal plugs into the HHT-VT100 cable or the 9-pin connector labeled Control on the back of the MAX. If you are connecting to an IBM PC-like 9-pin serial

connector, a straight-through cable is appropriate. Otherwise, you might need a 9-to-25 pin conversion cable.

2 Check the flow control settings on your VT100 terminal.

If you are not communicating at all with the MAX, see whether you can establish communication after you have turned off all transmit and receive flow control at your terminal or terminal emulator.

3 Determine whether you need a null-modem cable converter.

Though generally not needed, occasionally a null-modem cable converter is required for a few of the large numbers of different cable and terminal configurations that are available.

Random characters appear in the VT100 interface

If random or illegible characters appear on your display, you probably have a communications settings problem. Specify the following settings:

- 9600 bps data rate
- 8 data bits
- 1 stop bit
- No flow control
- No parity

If you have changed the data rate through the Port profile, make certain that your VT100 terminal matches that rate.

A Power-On Self Test fails

If the start-up display indicates a failure in any part of the POST, an internal hardware failure has occurred with the unit. In this case, contact Ascend Customer Service.

AIM-port interface problems

You can test the AIM port interface in one of two ways:

- A local loopback test
- Through true end-to-end communications

Many codecs or other AIM devices support some use of loopback. For example, when the MAX is in loopback mode and is connected to a codec, users see their own images through the codec. Likewise, most bridge/router devices recognize and report a diagnostic message when a packet is sent out and received by the same module. More often than not, the codec must be configured explicitly to accept the loopback from the communications device.

Local loopback testing is the best aid when troubleshooting the AIM-port interface (the interface between the codec and the MAX). All of the symptoms and operations described in this section assume you are working from the local loopback diagnostics menu. Unless otherwise specified, the AIM-port interfaces in this section can include the Ascend Remote Port Modules (RPMs).

The first and most critical aspect of the AIM port interface is the cable or cables connecting the codec to the MAX. If you are unsure about the cabling required, contact Ascend Customer Service.

The MAX reports data errors on all calls

Data errors on all calls can indicate that you have installed faulty host interface cables or cables not suited to the application. Information on host interface cabling requirements is found in the *Hardware Installation Guide* for your MAX.

Calls cannot be made, answered, or cleared using control leads

If you have purchased or built your own cables, verify that the pin-out is the same as the MAX pin-out for compatibility. The *Hardware Installation Guide* for your MAX lists the host interface pin-outs.

Frequently, a DB-25 breakout box is useful for monitoring control leads and for making quick changes to the cabling. However, because the host interface is running V.35 or RS-422 signal levels, you must verify that the breakout box is passive. That is, you must verify that the breakout box is not regenerating RS-232 level signals.

The codec indicates that there is no connection

The codec expects one or more of its control lines to be active. If no lines are active, toggle the various outputs available on the local loopback diagnostics menu. If there is still no connection, verify that you have installed the host cables correctly as described in the *Hardware Installation Guide* for your MAX. If the cabling is installed correctly, examine the host interface cable pin-outs as described in *Hardware Installation Guide*.

The codec does not receive data

If the codec does not receive data:

- 1 Verify that the codec is configured to accept a loopback at the communications device. Frequently, a codec requires certain control lines to be active during data transfer. Therefore, you might want to toggle the various host interface output lines, especially Data Set to Ready (DSR) and Carrier Detect (CD), to ensure that they are active.
- 2 If there is still no data transfer, your cable might not provide one or more control lines required by the host. Refer to your equipment documentation for a description of the pins that it requires to be active. The following control lines are generally the most important ones:
 - Carrier Detect (CD)
 - Clear To Send (CTS)
 - Data Set Ready (DSR)
- 3 If you are convinced that the control lines are in their correct states, but there is still no data transfer, you might have a clocking problem. The MAX provides both the transmit data clocks and the receive data clocks to your equipment through the host interface. The codec must be configured to accept the clocks from the MAX.
- 4 Check your cable length.
If the cable length exceeds the recommended distances, you should be using terminal timing. Alternatively, you might need to install RPMs.
- 5 Check the data rate.

You can adjust the data rate from the local loopback diagnostics menu by choosing the number of channels. Some applications cannot work above or below a certain data rate. For example, some high performance codecs cannot operate at data of rates less than 384 Kbps. In such cases, adjust the number of channels of data being looped back.

The codec cannot establish a call when Data Transmit Ready (DTR) is active

You might notice that the Port profile is set to establish calls when DTR is active, but the codec cannot establish a call. If the codec is going to originate the calls directly by using control-lead dialing, the call origination and clearing mechanisms must be configured for compatibility between the MAX and the codec. To verify a compatible configuration from the local loopback diagnostics menu:

- 1 Disable each of the MAX output control lines except DSR.
 To disable an output control line, toggle it to be Inactive (-). At this time, the codec should indicate that there is no connection.
- 2 Request an outgoing call from your equipment and monitor the Port Leads status menu of the active ports in the call.
 One or more of the control line inputs should become active and remain active for some period of time. If the DTR leads input do not change state, your cable is not properly configured. In this case, you must change the cable so that it routes the appropriate host output signal to the DTR input of the MAX. The MAX must use the DTR lead to establish outgoing calls.
- 3 Once you have made any changes required for verifying that the DTR lead becomes active when the MAX requests the call, configure the Port profile to expect the DTR input.
 In the Port profile, set Dial Call to DTR Active.

Calls initiated by control-lead toggling are cleared too soon

If the MAX clears a call initiated by control-lead toggling before it completely establishes the call, and the call is cleared almost immediately, the Port profile probably has a configuration error. To find the source of the problem, proceed as follows:

- 1 While monitoring the Port Leads status menu of the AIM ports used in the call, place an outgoing call from the codec.
- 2 Watch the DTR input carefully while the MAX is establishing the call.
 If the DTR input becomes Active (+) and then thereafter returns to Inactive (-), the MAX is using DTR as a pulse to place the call. Make sure that the Clear parameter in the Port profile is not set to DTR Inactive. (Set Clear to DTR Inactive only when the application maintains DTR positive during the call.)
- 3 While your equipment is still dialing the call, toggle the value of the CD output signal to indicate to your equipment that the call completed. At this time, watch the control leads very carefully. Make certain that any control leads that toggle while the call is being established are not used in the Clear parameter to clear the call. This type of configuration error is the most likely cause of a call being cleared almost immediately.

The codec cannot clear a call

If a codec-initiated call cannot be cleared, the call cannot be cleared from the codec, the Port profile probably has a configuration error. To verify the source of the problem, proceed as follows:

- 1 While monitoring the Port Leads status menu of the AIM ports used in the call, place an outgoing call from your equipment.
- 2 Once the host has requested the outgoing call, toggle the CD output to Active (+). The codec should recognize that the call is online.
- 3 Make a request to clear the call from the codec.
- 4 Watch the control leads very carefully as one or more of the input control lines toggle. Generally, either DTR or RTS is the line that toggles. Record whether the control lead input goes to Active (+) or Inactive (-) when the call is cleared; then, check that the value of the Clear parameter in the Port profile matches the action that the codec takes when the call is cleared.

ISDN PRI and BRI interface problems

Problems sometimes encountered with ISDN PRI and BRI interfaces include calls not dialed or answered reliably, Net/BRI lines not dialing or answering calls, apparent logical-link failures, and WAN calling errors in netbound Net/BRI calls.

Calls are not dialed or answered reliably

If calls are not dialed or answered reliably:

- 1 Check your cabling.
The first and most critical aspect of the interface is the physical cable connecting the MAX to the line or terminating equipment. Typically, WAN interface cabling problems appear immediately after installation. If you are unsure about the cabling required, contact Ascend Customer Service. The *Hardware Installation Guide* for your MAX describes the general PRI and BRI interface requirements and lists cabling pin-outs.
- 2 If the cabling is not the problem and the MAX is a T1 unit, check that the value of the Buildout parameter or the Length parameter in the Line profile matches the actual distance in your configuration.
The MAX displays the Buildout parameter if its interface to the T1 line is equipped with an internal CSU. Its enumerated values can be 0 DB, 7.5 DB, 15 DB, and 22.5 DB. Contact your carrier representative to determine which value to choose.
If the line interface is not equipped with an internal CSU, the Length parameter is displayed. It can specify a cable length, of 1-133, 134-266, 267-399, 400-533, or 534-655 in feet, which should correspond to the distance between the MAX and the WAN interface equipment, typically a CSU or multiplexer.

Note: T1/PRI ports not equipped with internal CSUs require an external CSU or other equipment approved for the metallic interface between the MAX and the WAN facility.

The Net/BRI lines do not dial or answer calls

Do not connect the MAX unit's Net/BRI ports directly to U-interface BRI lines. The MAX unit's Net/BRI ports require carrier-approved Network Terminating 1 (NT1) equipment between the MAX and BRI lines. Note that Net/BRI outbound calls require the use of trunk groups.

No Logical Link status

If you notice that the status of a Net/BRI line in the Line Status display is No Logical Link, you might or might not have a problem.

In some countries outside the U.S., it is common for no logical link to exist before the MAX places a call. In the U.S., when you first plug a line into the MAX or switch power on, the central office switch can take as long as 15 minutes to recognize that the line is now available. You might have to wait that long for the line state to change to Active (A). The physical link can exist without a logical link up on the line.

If you wait longer than 15 minutes and the line is still not available:

- 1** Determine whether all the ISDN telephone cables are wired straight through.
If you are running multipoint (passive bus) on your switch, all of the ISDN telephone cables must be wired straight through. If any of the cables are wired to cross over, you will not be able to place calls.
- 2** Verify that 100% termination is provided on each ISDN line.
- 3** Determine whether you have correctly specified the Service Profile Identifiers (SPIDs) in the Line *N* profile for each line. If the SPIDs are not correctly specified, the line status might indicate No Logical Link. Check with your system manager or carrier representative to obtain the SPID or SPIDs for your line. To specify your SPIDs, use the Pri SPID and Sec SPID parameters in the Line *N* profile.

WAN calling errors occur in outbound Net/BRI calls

Should you encounter a problem in which the Call Status window immediately indicates a WAN calling error when the MAX places a call on a Net/BRI module. Proceed as follows:

- 1** Check the value of the Data Svc parameter in the Call or Connection profile.
Try both the 64K and 56K options for Data Svc, to see whether using a different value solves the problem.
- 2** Verify that you are using the correct dialing plan.
Depending on how the BRI lines are configured, you might need to type four, seven, or ten digits to communicate with the remote end.
Four-digit dialing involves the last four digits of your phone number. For example, if your phone number is (415) 555-9015, four-digit dialing requires that you enter only the last four digits: 9015. Seven-digit dialing specifies that you dial the digits 5559015, and ten-digit dialing requires 4155559015.
If you are sending the incorrect number of digits, the MAX cannot route the call. Ask your carrier representative for the correct dialing plan, or simply try all of the possibilities.
- 3** Ask your carrier representative to verify explicitly that the line is capable of supporting the call types you are requesting.

ISDN PRI and BRI circuit-quality problems

Circuit-quality problems sometimes encountered on ISDN PRI and BRI lines include excessive data errors or handshaking on calls to AIM ports and scrambling of inbound data during AIM Static calls.

Excessive data errors on calls to AIM ports

If you encounter a problem where the MAX reports excessive data errors on some calls to AIM ports, run a Byte Error Rate Test (BERT), which counts data errors that occur on each channel during a call to a AIM port. The BERT checks the data integrity from the MAX at one end of the call to the MAX at the other end.

If you have verified that the MAX is correctly installed and configured, and you have previously placed calls without excessive errors, use the DO Beg/End BERT command to run the BERT. Do not clear the call before running the BERT. You can run a BERT only under the following conditions:

- A call is active.
- The Call Type parameter is set to AIM, FT1-B&O, or FT1-AIM.
- The Call Mgm parameter is set to Manual, Dynamic, or Delta.

You can also set the Auto BERT parameter in the Call profile to run an automatic BERT. If the BERT indicates very high errors on some of the channels, clear the call and redial. When redialed, the call might take a different path, correcting the excessive error problem.

Excessive handshaking on calls to AIM ports

Handshaking is a normal and momentary occurrence during call setup and when the MAX increases or decreases bandwidth. If there is trouble in the circuits that carry the call, frequent handshaking can occur. If the trouble is serious enough to degrade the quality of the call, the MAX disconnects. If handshaking is continuous for over a minute, the problem is probably not due to the quality of the line, and you should call Ascend Customer Service.

Inbound data is scrambled during an AIM Static call

Because an AIM Static call does not have a management channel, it is possible for data scrambling to occur because of WAN slips, a type of timing error. Slips are a very infrequent occurrence. If you encounter such problems, clear the call and redial.

Problems indicated by the LEDs

The LEDs can indicate that a secondary line is disabled, that the line is in a Red Alarm state, or that the D channel is not communicating with the UAN

LEDs are not lit for the secondary E1 or T1 line

If no LEDs related to the secondary line are illuminated, the line is disabled in the Line *N* profile. You can enable the secondary line by modifying the Line *N* profile.

The E1 or T1 line is in a Red Alarm state

If the Alarm LED and the Line Status menu indicate that the line is in a Red Alarm state, the MAX cannot establish proper synchronization and frame alignment with the WAN. This behavior is normal for as long as 30 seconds after a PRI line is first plugged into the MAX.

If the Red Alarm condition persists for longer than 30 seconds:

- 1 Check the value of the Framing Mode parameter in the Line *N* profile.
Change the value to the other available option and check to see whether the Red Alarm condition goes away within 30 seconds.
- 2 If the Red Alarm state persists, check the cabling.
You might have a crossover cable installed when a straight-through cable is required, or vice versa. If the MAX is connected through bantam plugs, reverse the transmit and receive plugs. Then allow the MAX to attempt to establish synchronization for an additional 30 seconds.
- 3 You can eliminate the cabling as a possible cause by replacing the connection with a loopback plug. The LS LED should go off immediately, followed by the RA LED in about 30 seconds.

A PRI line is in use and the Alarm LED blinks

A blinking Alarm LED means that the physical configuration of the E1 or T1 line is correct but the D channel is not communicating with the WAN. To resolve this problem:

- 1 Verify with your carrier representative that the D channel is channel 16 (E1) or 24 (T1).
- 2 If the D channel number is correct, check the value of the Line Encoding parameter in the Line profile. When B8ZS encoding is in use, a non-inverted D channel is established. If AMI encoding is selected, an inverted D channel is established. Check the line translations provided by your carrier representative and set the line encoding to match the inversion requirements.
- 3 Determine whether your WAN interface or the MAX T1 unit is equipped with a CSU.
If the WAN interface or the MAX is not equipped with a CSU, the ALARM LED blinks. Check whether you have specified the proper Length or Buildout value in the Line profile.
- 4 Check whether the D channel is in service.
If no equipment has been plugged into the line for a short period of time (five to ten minutes), the D channel is taken out of service. You might need to ask your carrier to put the D channel back into service.

Problems in accessing the WAN

Problems in accessing the WAN can include channels not being dialed or used and outgoing calls failing to connect.

Only some channels are dialed for AIM or BONDING calls

If the MAX dials only some of the channels when making an AIM or BONDING call, proceed as follows:

- 1 Verify that there are enough channels enabled for switched services in the Line *N* profile to meet the requirements of the Parallel Dial parameter in the System profile.
Most WAN providers can place a limited number of simultaneous calls from a single E1 or T1 line. If more concurrent attempts are made than the WAN can support, the WAN applies a congestion tone (a fast busy signal).
- 2 Try adding bandwidth once the call is up.
If you can add bandwidth, the solution is to adjust the Parallel Dial parameter in the System profile. A value of 5 works for almost all WAN providers, although some support

substantially more. If adding bandwidth does not work, the problem is most likely within the individual channel translations. In this case, call your carrier representative.

The MAX never uses some channels

If the MAX never uses some channels, proceed as follows:

- 1 If you are making AIM or BONDING calls, verify that the affected channels are enabled for switched services in the Line *N* profile.
- 2 If you have an E1 unit, check whether it has been connected recently to a device that does not support the full 31 channels. If so, the switch might take the unused channels out of service. This situation can arise on either the local or the remote end.
- 3 If you have a T1 unit, check whether it has been connected recently to a device that does not support the full 23 channels. If so, the switch might take the unused channels out of service. This situation can arise on either the local or the remote end.
- 4 Verify that the channels enabled in your Line *N* profile correspond to the channels enabled in the circuit. If only some of the channels in the circuit are available for data calls, you must specifically enable those channels in your Line *N* profile.
- 5 If you place a call and some channels are always skipped, call your carrier representative.

An outgoing call using inband signaling fails to connect to the remote end

If the T1 or E1 line is configured for inband signaling and outbound calls fail to connect:

- 1 Make sure that your Line *N* profile is properly configured for wink-start or idle-start. The Rob Ctl parameter in the Line *N* profile determines which of these call-control mechanisms the MAX uses. Check with your carrier representative to find out which inband signaling your line supports.
- 2 If the Line *N* profile is configured correctly and you still cannot place an outgoing call, check the service state of the line.
Frequently, if a T1 or E1 line has been unplugged for an extended duration, the switched services available on the line are taken out of service. Once you install the MAX, you might need to ask your carrier representative to have the line reactivated. If this is the case, leave the MAX on all the time, even when you are not using it. Otherwise, you will have to call your carrier to reactivate the line each time the unit is switched off and on.
- 3 Ask your carrier representative whether the line is configured for DTMF dialing. The line must support this type of dialing to recognize digits being dialed.

Incoming call routing problems

Routing problems occur when a call is connected to the answering MAX but cannot be routed to one of its slots.

Call status drops back to IDLE

You might notice that after the Call Status window reports ANSWERING and HANDSHAKING, it drops back to IDLE. This condition might not indicate a problem. It can indicate that the call was initially answered and that when its routing was checked, the target AIM port was busy or disabled. Handshaking does not occur on calls to the MAX unit's

internal router, but calls can initially be answered and then quickly cleared during normal operation, such as during the receipt of an incorrect password.

Dual-port call status drops back to IDLE

If you are trying to make a dual-port call, and the Call Status menu reports ANSWERING and HANDSHAKING, and then drops back to IDLE, check the status of both ports specified in the Dual Ports, Port 1/2 Dual, Port 3/4 Dual, or Port 5/6 Dual parameter of the answering MAX. If either port in the pair is busy, the call cannot be routed to that pair.

AIM or BONDING call status drops back to IDLE

If you are trying to make an AIM or BONDING call, and the Call Status window reports ANSWERING and HANDSHAKING, then drops back to IDLE, check that the routing parameters are configured correctly. If they are not, an AIM, BONDING, or AIM/DBA call might be routed to a port that cannot support these types of calls.

Bridge/router problems

Problems with a bridge or router can include the uncertainty of link quality and the MAX hanging up after answering an IP call.

The link is of uncertain quality

When running File Transfer Protocol (FTP), the data transfer rate appears in bytes per second. Multiply this rate times 8 to get the bits per second. For example, suppose that you are connected to Detroit on a 56-Kbps B channel and that FTP indicates a 5.8 Kbyte/s data rate. In this case, the link is running at $5.8 \times 8 = 46.8$ Kbps, or approximately 83% efficiency. Many factors can affect efficiency, including the load on the FTP server, the round-trip delay, the overall traffic between endpoints, and the link quality.

You can check link quality in the WAN Stat status window, or by running a Ping between the same endpoints. Dropped packets hurt the link's efficiency, as does round-trip delay. Random round-trip delay indicates heavy traffic, a condition that also drops the efficiency of the link.

The MAX hangs up after answering an IP call

If the MAX hangs up after answering an IP call, proceed as follows:

- 1 If you are running PPP, verify that you have entered the proper passwords.
- 2 Verify that Auth is set to PAP or CHAP.
- 3 If you are routing IP over PPP, verify that the calling device gives its IP address

Some calling devices supply their names, but not their IP addresses. However, you can derive an IP address if the calling device is listed in a local Connection profile or on a RADIUS authentication server. Try enabling PAP or CHAP for the Recv Auth parameter so that the MAX matches the caller's name to the Station parameter in a Connection profile and gets the corresponding LAN Adrs.

MAX Diagnostic Command Reference

B

This appendix provides all available information about the MAX diagnostic commands. The information is organized for quick reference, and does not include tutorials. All commands are listed alphabetically.

Under most circumstances, diagnostic commands are not required for correct operation of the MAX, and in some circumstances might produce undesirable results. Please use the following information with caution. Contact Ascend Technical Support with any questions or concerns.

Note: Every attempt has been made to confirm that this chapter correctly describes the functionality and output of the MAX diagnostic commands. But while diagnostic mode can be a very valuable troubleshooting tool for anyone, its primary focus is on the requirements of Ascend's development engineers. For this reason, Ascend does not guarantee the completeness of the list of commands or of the cataloging of functionality from release to release.

Using MAX diagnostic commands

To be allowed access to diagnostic mode, you must set the Field Service privilege to Yes in the active Security profile. (If you have any questions about how to activate Security profiles, see the *MAX Security Supplement*.)

Use one of the following two methods to access diagnostic mode:

- From the MAX VT100 interface, display the DO menu by pressing Ctrl-D. Then press D or select D=Diagnostics.
- From the MAX VT100 interface, type the following key sequence in rapid succession:

`Esc [Esc =`

(Press the Escape key, followed by the Left Bracket key, then the Escape key again, followed by the Equals key.)

You must press all four keys within one second for the MAX to recognize the escape sequence.

To display an abbreviated list of the most commonly used commands in diagnostic mode, enter a question mark:

`MAX>?`

To display a complete listing, append **ascend** to the question mark:

`MAX>? ascend`

To exit diagnostic mode, enter **quit**.

Because most diagnostic commands are designed to give a developer information about specific aspects of MAX functionality, you might find it helpful to use commands in combination to troubleshoot different problems.

For example, when troubleshooting modem-related issues, you might want to use ModemDrvState, ModemDiag, and MDialout (if modem dial-out is supported on your MAX) to get all modem-related information for your calls.

Using several commands simultaneously not only gives you a clearer picture of what is happening, but also shows you a chronological timeline of the events.

Command reference

Following are the MAX diagnostic commands in alphabetic order:

?

Description: Displays an abbreviated list of the most commonly used diagnostic commands and a brief description of each command. Append the `ascend` modifier to display the complete list of commands.

Usage: `? [ascend]`

Syntax element	Description
<code>ascend</code>	List all commands.

Example:

```
MAX> ?
? -> List all monitor commands
clr-history -> Clear history log
ConnList -> Display connection list information
ether-display -> ether-display <port #> <n>
fatal-history -> List history log
fclear -> clear configuration from flash
FiltUpdate -> Request update of a connection
frestore -> restore configuration from flash
fsave -> save configuration to flash
help -> List all monitor commands
nslookup -> Perform DNS Lookup
priDisplay -> priDisplay <n>
quit -> Exit from monitor to menus
reset -> Reset unit
tloadcode -> load code from tftp host
trestore -> restore configuration from tftp host
tsave -> save configuration to tftp host
wanDisplay -> wanDisplay <n>
wanDSess -> wandsess <sess <n>> (display per session)
wanNext -> wanNext <n>
```

wanOpening -> wanOpening <n> (displays packets during opening/negotiation)

AddrPool

Description: Displays messages related to dynamic address pooling. The command is a toggle that alternately enables and disables the debug display.

Usage: Enter **addrpool** at the MAX prompt.

Example: Following are several examples of output displayed from **addrpool**.

With 18 addresses currently allocated from a pool:

```
ADDRPOOL: lanAllocate index 0 inuse 18
```

The address 208.147.145.155 was just allocated:

```
ADDRPOOL: allocate local pool address [208.147.145.155]
```

The following message appeared when the address 208.147.145.141 was to be freed because the user of that address had hung up. The MAX must find the pool to which the pool address belonged, then free the address so it is available for another user:

```
ADDRPOOL: found entry by base [208.147.145.141] entry  
[208.147.145.129]  
ADDRPOOL: free local pool address [208.147.145.141]
```

The following messages shows that a new pool is created. Under Ethernet > Mod Config > WAN Options, Pool #1 Start is set to 192.168.8.8, and Pool #1 Count is set to 4:

```
ADDRPOOL: Deleting addrPool  
ADDRPOOL: New Addr pool rc = 0  
addrPool index 1 ip [192.168.8.8] count 4
```

The following message appeared when the Pool #1 Count parameter for an existing pool was changed from 4 to 3:

```
ADDRPOOL: Deleting addrPool  
ADDRPOOL: New Addr pool rc = 0  
addrPool index 1 ip [192.168.8.8] count 3
```

In the events reported by the following display, a second pool is created. Under Ethernet > Mod Config > WAN Options, Pool #2 Start is set to 192.168.10.8, and Pool #2 Count is set to 10:

```
ADDRPOOL: Deleting addrPool  
ADDRPOOL: New Addr pool rc = 0  
addrPool index 1 ip [192.168.8.8] count 4  
ADDRPOOL: New Addr pool rc = 0  
addrPool index 1 ip [192.168.8.8] count 4  
addrPool index 2 ip [192.168.10.1] count 10
```

The second pool is then deleted:

```
ADDRPOOL: Deleting addrPool  
ADDRPOOL: New Addr pool rc = 0  
addrPool index 1 ip [192.168.8.8] count 4
```

ARPTable

Description: Displays the MAX unit's Address Resolution Protocol (ARP) table. The MAX uses the ARP table to associate known IP addresses with physical hardware addresses.

Usage: Enter **arptable** at the command prompt.

Example:

MAX> **arptable**

	ip address	ether addr	if	rts	pkt	ref	insert
DYN	206.30.33.11	00A0244CCE04	0	0	0	1	281379
DYN	206.30.33.254	00605C4CA220	0	0	0	1	281303
DYN	206.30.33.21	00059A403B47	0	0	0	1	281179
DYN	206.30.33.15	00A0247C2A72	0	0	0	1	281178

The ARP table displays the following information:

Column	Description
	Unnamed first column indicates how the address was learned, dynamically (DYN) or by specification of a Bridge Address (STA).
ip address	Network address contained in ARP requests.
ether addr	Media Access Control (MAC) address of the host identified by ip address. Also referred to as the hardware address.
if	Interface on which the MAX received the ARP request.
rts	Routes pointing to the address.
pkt	Number of packets queued.
ref	Number of times that the address was used.
insert	Time at which this entry was inserted into the ARP table.

Avm

Description: Displays a report on the status of the availability of modems in the MAX. Each time you enter **avm**, you get a snapshot of current modem states and the recent history for each modem. The command is particularly helpful in troubleshooting modem connection problems, for which you must focus on the ability of individual modems to successfully connect with dial-in users.

A call is noted as successful if modem handshaking (training) and authentication are successful.

A call is noted as bad if modem handshaking fails at any point in the initial call set-up, or if the dial-in user does not successfully log in.

The **dir** parameter indicates the direction of the last call into each modem. It can have the following settings:

- 1—Call direction unknown.
- 2—Call was outgoing.
- 3—Call was incoming.

A modem is moved to the *suspect* list if its first four calls are bad, or if it experiences eight bad calls in a row. Modems on the *suspect* list may still be used if all *free* modems are in use. Any subsequent successful call to a *suspect* modem places that modem back on the *free* list.

Note: A call that has been categorized as bad does not necessarily indicate a modem problem with the MAX. Poor line quality, software problems with the calling modem, wrong numbers, and forgotten passwords all can generate calls that appear as bad calls but that have nothing to do with modems on the MAX.

Usage: Enter **avm** at the command prompt.

Example: In the following display, an 8-mod modem card is located in slot 8 of the MAX. Modems 8:5 and 8:6 are in use. Modems 8:2, 8:3, 8:4, 8:7, and 8:8 are idle and available to accept calls. Modem 1 has been disabled by the V.34 Modem > Modem Diag > Modem #1 parameter.

```
MAX> avm
Modems on free list:
Modem 8:4, 70 calls, 6 bad, last 32 calls = ffdffbfcdir=3
Modem 8:8, 54 calls, 1 bad, last 32 calls = ffffffffdir=3
Modem 8:3, 63 calls, 1 bad, last 32 calls = fffbffffdir=3
Modem 8:2, 74 calls, 1 bad, last 32 calls = ffffffffdir=3
Modem 8:7, 64 calls, 2 bad, last 32 calls = ffbffbfcdir=3
Modems on suspect list:
Modem 8:1, 57 calls, 0 bad, last 32 calls = fffffff0dir=3
Modems on disabled list:
Modems on dead list:
Modems on busy list:
Modem 8:5, 65 calls, 2 bad, last 32 calls = ffffffffdir=3
Modem 8:6, 58 calls, 1 bad, last 32 calls = ffffffffdir=3
```

Looking at modem 4 on slot 8 (designated 8:4), the eight-digit hexadecimal number has to be converted to binary to indicate how many of the last 32 calls were successful:

```
ffdffbfcd = 111111111011111111101111111100
```

The zeroes show that modem 8:4 has had four unsuccessful calls, including the last two calls. After the hexadecimal number, dir=3 indicates that the last call was an incoming call.

BRIDisplay

Description: Displays messages related to the D-channel signaling for any BRI slot cards installed on the MAX. The command is available only if you have loaded a version of MAX software that supports BRI slot cards.

If you enter the command while traffic through your MAX is heavy, the resulting amount of output can make it tedious to find the information you are looking for. The screen might even display the message **----- data lost -----**, which just means that not all the output can be displayed on the screen. You might prefer to use the BRIDisplay command during a period of low throughput.

Usage: `bridisplay n`

where **n** is the number of octets to display per frame. Specifying a value of zero disables the logging of the messages.

Example:

```
MAX> bridisplay 4
BRI-XMIT-7:   : 4 octets @ B04EE520
[0000]: 00 B3 01 01
BRI-RCV-7:   : 4 octets @ B0539A80
[0000]: 02 B3 01 01
BRI-XMIT-7:   : 4 octets @ B0529560
[0000]: 02 B3 01 01
BRI-RCV-7:   : 4 octets @ B05608A0
[0000]: 00 B3 01 01
```

Callback

Description: Displays messages related to the callback functionality of the MAX. You can use the command to display, for example, sessions queued for callback. The command is a toggle that alternately enables and disables the debug display.

With the callback feature enabled, the MAX hangs up after receiving an incoming call that matches the specifications in the Connection profile. The MAX then uses the Dial # specified in the Connection profile to call back the device at the remote end of the link.

You can use the callback command to tighten security by ensuring that the MAX connection to known destinations only. The command can also help you troubleshoot detailed areas of the callback process.

Usage: Enter **callback** at the command prompt.

Example: Following are several examples of output displayed by the Callback command.

```
MAX> callback
CALLBACK debug is now ON
```

The following message appears as the MAX prepares to call back the remote end:

```
CALLBACK: processing entry topeka
```

The MAX then dials the remote end:

```
CALLBACK: initiate call to topeka
```

When the call has been made and is being negotiated:

```
CALLBACK: new state WAITING
```

If callback failed and will be retried:

```
CALLBACK: new state FAILED
```

If callback is never successful, the call is marked for removal from the callback list and the following message appears:

```
CALLBACK-FAILED: topeka marked as failed
```

After the remote end is called back, its entry is removed from the Callback list so that the MAX can reallocate and use the resources. The following message appears:

```
CALLBACK: deleting entry topeka
```

To terminate the display:

```
MAX> callback  
CALLBACK debug is now OFF
```

ClockSource

Description: Displays the source of clocking for the MAX. Clock slips can cause connectivity problems, particularly for analog users. If you use the Net/T1 > Line Config > Line # > Clock Source parameter to move the clock source, you can use this diagnostic command to validate your changes.

Note: You need to reboot the MAX to enable any changes to the Clock Source parameter. Also, if more than one line has Clock Source set to Yes, remember that the clock source will be derived from the first line that syncs. If you want to ensure that a particular line is the source, make sure it has Clock Source set to Yes and that all other lines have Clock Source set to No.

Usage: Enter **clocksource** at the command prompt.

Example: In the following example, the clock source is taken from the first T1/PRI line, designated `dsl 0`. `Dsl#` indicates the maximum number of possible sources for the clock. The source can be on Net/T1 slot cards or Net/BRI slot cards. This MAX has three T1/PRI lines configured, so there are three possible external sources for the clock. `LstSel` is further validation that the clock is being derived from `Dsl#0`. After Now, a 2 indicates that layer 2 is up for that line and is available as the clock source.

```
MAX> clocksource  
Clock source is dsl 0  
Dsl#      012345678901234567890123456789012345678901234567890123456789  
LstSel    a????????????????????????????????????????????????????????  
Now       222-----
```

Clr-History

Description: Clears the fatal-error history log.

Usage: Enter **clr-history** at the command prompt. To display the log before clearing it, enter the fatal-history command.

Example:

```
MAX> fatal-history  
OPERATOR RESET:  Index: 99  Load: ti.m40 Revision: 5.0A  
Date: 02/13/1997.      Time: 04:22:47  
DEBUG Reset from unknown in security profile 1.  
SYSTEM IS UP:  Index: 100  Load: ti.m40 Revision: 5.0A  
Date: 02/13/1997.      Time: 04:23:50  
MAX> clr-history
```

The log is now empty:

```
MAX> fatal-history  
MAX>
```

See Also: Fatal-History

CoreDump

Description: Enables or disables the ability of the MAX to send the contents of its memory (core) to a specified UNIX host. When you use the function, the core file created can be several megabytes in size. Also, the UNIX host must be running the `ascendump` daemon, which is available by contacting Ascend Technical Support.

The CoreDump command is a particularly useful tool for Ascend's development engineering, and Technical Support occasionally requests its use to help troubleshoot specific issues.

You can include the `now` option to instruct the MAX to dump its core immediately. You can include the `enable` option to direct the MAX to dump its core when it has logged an entry to the fatal error log.



Caution: This command causes active connections to be disconnected and the MAX to reboot after its memory (core) has been dumped. Do not use the command unless specifically requested to do so by an Ascend representative.

Usage: `coredump [enable] [disable] [now] ip address`

where:

- **enable** instructs the MAX to dump its core to the specified IP address when an entry is logged to the fatal-error log.
- **disable** cancels the command if it has been enabled.
- **now** instructs the MAX to dump its core immediately to the specified IP address.

Example: Following are examples of entering the CoreDump command, and possible response messages:

```
MAX> coredump enable 1.1.1.1  
coredump over UDP is enabled locally only with server 1.1.1.1  
MAX> coredump disable 1.1.1.1  
coredump over UDP is disabled locally only with server 1.1.1.1  
MAX> coredump  
coredump over UDP is disabled locally only with server 1.1.1.1  
MAX> coredump enable 200.200.28.193  
coreDump: Sending arp request...  
coreDump: Sending arp request...  
coreDump: Sending arp request...  
coreDump aborted: Can't find ether address for first hop to  
200.200.28.193
```

Ether-Display

Description: Displays the contents of Ethernet packets.

If you enter the command while traffic through your MAX is heavy, the resulting amount of output can make it tedious to find the information you are looking for. The screen might even display the message **----- data lost -----**, which just means that not all the output can be displayed on the screen. You might prefer to use the Ether-Display command during a period of low throughput.

Usage: `ether-display port 0-# n`

Syntax element	Description
<code>port 0-#</code>	The range of Ethernet ports on which received or transmitted packets should be displayed. Use zero only to indicate that Ethernet packets for all ports should be displayed.
<code>n</code>	The number of octets to display from each Ethernet packet.

Example: To display the first 12 octets of each Ethernet packet for all ports:

```
MAX> ether-display 0 12
Display the first 12 bytes of ETHER messages
ETHER XMIT: 105 octets @ B07BE920
[0000]: 00 40 C7 5A 64 6C 00 C0 7B 0C 01 59
ETHER RECV: 64 octets @ B077EE70
[0000]: 00 C0 7B 0C 01 59 00 40 C7 5A 64 6C
ETHER XMIT: 219 octets @ B07BE920
[0000]: 00 40 C7 5A 64 6C 00 C0 7B 0C 01 59
ETHER RECV: 64 octets @ B077F4C0
[0000]: 00 C0 7B 0C 01 59 00 40 C7 5A 64 6C
MAX> ether-display 0 0
ETHER message display terminated
```

Fatal-History

Description: Displays the MAX fatal-error log. Each time the MAX reboots, it logs a fatal-error message to the fatal-error history log. The fatal-error log also includes Warnings, for which the MAX did not reset. Development engineers use Warnings for troubleshooting purposes. A Warning indicates that the MAX detected an error condition but recovered from it. The number of entries in this log is limited by available flash space, and the errors rotate on a First-In, First-Out (FIFO) basis. You can use the Clr-History command to clear the log.

Note: If your MAX experiences a fatal-error reset or Warning, contact Ascend Technical Support immediately.

Definitions of fatal errors:

The following reset is the result of an Assert. This problem can be either hardware or software related. Contact Ascend Technical Support if you experience an FE1 reset.

```
FATAL_ASSERT = 1
```

The following reset results from an out-of-memory condition, sometimes termed a memory leak:

```
FATAL_POOLS_NO_BUFFER = 2
```

Other resets include:

FATAL_PROFILE_BAD =	3
FATAL_SWITCH_TYPE_BAD =	4
FATAL_LIF_FATAL =	5
FATAL_LCD_ERROR =	6
FATAL_ISAC_TIMEOUT =	7
FATAL_SCC_SPURIOUS_INT =	8

The preceding reset is caused by a processor exception error.

FATAL_EXEC_INVALID_SWITCH =	9
FATAL_EXEC_NO_MAIL_DESC =	10

The preceding reset occurs if the MAX tries to allocate a mail message and there are none left. A reset of this type is usually due to a memory leak.

FATAL_EXEC_NO_MAIL_POOL =	11
FATAL_EXEC_NO_TASK =	12
FATAL_EXEC_NO_TIMER =	13
FATAL_EXEC_NO_TIMER_POOL =	14
FATAL_EXEC_WAIT_IN_CS =	15
FATAL_DSP_DEAD =	16
FATAL_DSP_PROTOCOL_ERROR =	17
FATAL_DSP_INTERNAL_ERROR =	18
FATAL_DSP_LOSS_OF_SYNC =	19
FATAL_DSP_UNUSED =	20
FATAL_DDD_DEAD =	21
FATAL_DDD_PROTOCOL_ERROR =	22
FATAL_X25_BUFFERS =	23
FATAL_X25_INIT =	24
FATAL_X25_STACK =	25
FATAL_ZERO_MEMALLOC =	27
FATAL_NEG_MEMALLOC =	28
FATAL_TASK_LOOP =	29

The preceding reset is caused by a software loop.

FATAL_MEMCPY_TOO_LARGE =	30
FATAL_MEMCPY_NO_MAGIC =	31
FATAL_MEMCPY_WRONG_MAGIC =	32
FATAL_MEMCPY_BAD_START =	33
FATAL_IDEC_TIMEOUT =	34
FATAL_EXEC_RESTRICTED =	35
FATAL_STACK_OVERFLOW =	36
FATAL_OPERATOR_RESET =	99

The preceding entry is logged to the fatal-error table when the MAX has been manually reset, either in diagnostic mode (with the Reset or NVRAMclear commands), through the user interface, or through MIF.

Instead of a standard stack backtrace, the message includes the active Security profile index. On the MAX the Default profile is number 1, and the Full Access profile is number 9. 0 indicates an unknown security profile.

The reset is logged immediately before the MAX goes down.

FATAL_SYSTEM_UP = 100

As a complement to entry 99, the preceding entry is logged as the MAX is coming up. For a normal, manual reset, a fatal error 99 should appear, followed by a fatal error 100.

Warning messages

Warnings are not the result of reset conditions. The MAX logs Warnings when it detects a problem and recovers. Following are the Warnings, in numeric order:

ERROR_BUFFER_IN_USE	101
ERROR_BUFFER_WRONG_POOL	102
ERROR_BUFFER_WRONG_HEAP	103
ERROR_BUFFER_NOT_MEMALLOC	104

Warning 104 can be logged under different conditions (for example, double freeing memory or a low-memory condition).

ERROR_BUFFER_BAD_MEMALLOC	105
ERROR_BUFFER_BOGUS_POOL	106
ERROR_BUFFER_BOGUS_HEAP	107

Memory management code (or other modules) detected that the buffer header of what should have been a free buffer had been corrupted by the previous overwrite.

ERROR_BUFFER_NEG_MEMALLOC	108
---------------------------	-----

Warning 108 is logged when a negative length request is made to the memory allocation code.

ERROR_BUFFER_ZERO_MEMALLOC	109
----------------------------	-----

Warning 109 is similar to Warning 108, except that the a zero length request is made to the memory allocation code.

ERROR_BUFFER_BOUNDARY	110
ERROR_BUFFER_TOO_BIG	111

Warning 111 occurs when a software routine has tried to allocate a block of memory greater than 64KB.

ERROR_BUFFER_NULL	112
ERROR_BUFFER_SEGCOUNT_ZERO	113
ERROR_BUFFER_TRAILER_MAGIC	114
ERROR_BUFFER_TRAILER_BUFFER	115
ERROR_BUFFER_TRAILER_LENGTH	116
ERROR_BUFFER_TRAILER_USER_MAGIC	117
ERROR_BUFFER_WRITE_AFTER_FREE	118
ERROR_BUFFER_NOT_IN_USE	119
ERROR_BUFFER_MEMCPY_MAGIC	120
ERROR_BUFFER_MEMCPY_MAGIC_NEXT	121
ERROR_BUFFER_MIN	101
ERROR_BUFFER_MAX	121
ERROR_LCD_ALLOC_FAILURE	145

Warning 145 occurs when a memory-copy routine was called but the source buffer was much larger than expected.

MAX Diagnostic Command Reference

Fatal-History

ERROR_MEMCPY_TOO_LARGE	150
ERROR_MEMCPY_NO_MAGIC	151
ERROR_MEMCPY_WRONG_MAGIC	152
ERROR_MEMCPY_BAD_START	153
ERROR_WAN_BUFFER_LEAK	154

Warning 154 is caused by an error in the WAN driver.

ERROR_TERMSRV_STATE	160
ERROR_TERMSRV_SEMA4	161
ERROR_STAC_TIMEOUT	170
ERROR_EXEC_FAILURE	175

Warning 175 occurs because the kernel temporarily does not have available memory to spawn a task.

ERROR_EXEC_RESTRICTED	176
ERROR_EXEC_NO_MAILBOX	177
ERROR_EXEC_NO_RESOURCES	178
ERROR_CHAN_MAP_STUCK	180

Warning 180 is caused by a missing channel on a T1/PRI line.

ERROR_CHAN_DISPLAY_STUCK	181
ERROR_NEW_CALL_NO_DISC_REQ	182

Warning 182 indicates that a Disconnect message to the Central Office (CO) was not sent. The problem can be caused by conditions on the MAX or at the CO. When the MAX encounters the condition, it assumes the CO is correct, and answers the call.

ERROR_NEW_CALL_NO_DISC_RESP	183
ERROR_DISC_REQ_DROPPED	184
ERROR_SPYDER_BUFFER	185
ERROR_SPYDER_DESC	186
ERROR_TCP_SBCONT_TOO_BIG	190
ERROR_TCP_SEQUENCE_GAP	191
ERROR_TCP_TOO_MUCH_DATA	192
ERROR_TCP_TOO_MUCH_WRITE	193
ERROR_TCP_BAD_OPTIONS	194
ERROR_OSPF_BASE	200

Usage: Enter ***fatal-history*** at the command prompt.

Example:

```
MAX> fatal-history
OPERATOR RESET:  Index: 99  Load: mhpelbip Revision: 4.6Cp22
Date: 02/24/1997.      Time: 16:08:43
DEBUG Reset from unknown in security profile 1.
OPERATOR RESET:  Index: 99  Load: ebiom.m40 Revision: 5.0A
Date: 02/24/1997.      Time: 16:09:35
NVRAM was rebuilt
SYSTEM IS UP:  Index: 100  Load: ebiom.m40 Revision: 5.0A
Date: 02/24/1997.      Time: 16:10:04
```

See Also: Clr-History

FClear

Description: Clears Flash memory on the MAX. When the MAX boots, it loads the code and configuration from Flash memory into Dynamic Random Access Memory (DRAM). If you want to return your MAX to its factory-set defaults, you need to perform an FClear.

Usage: Enter **fclear** at the command prompt.

Example:

```
MAX> fclear
.
```

See Also: FSave

FRestore

Description: Restores a configuration from Flash memory and loads it into DRAM on the MAX.

Note: The MAX performs an FRestore when it boots. You need to execute the command if you have made changes to the current configuration and want to restore the configuration stored in Flash memory.

Usage: Enter **frestore** at the command prompt.

FSave

Description: Stores the current configuration into Flash memory.

Note: When you load code with the TloadCode command, an FSave is performed automatically before the code is uploaded. When the box boots after the upload, the MAX will load the configuration stored in Flash rather than be reset to factory default settings.

Usage: Enter **fsave** at the command prompt.

Example:

```
MAX> fsave
.....
.
MAX>
```

Heartbeat

Description: Displays information related to multicast heartbeat functionality. The command is a toggle that alternately enables and disables the debug display.

Usage: Enter **heartbeat** at the command prompt.

Example: Following are several examples of output displayed by the Heartbeat command.

```
HB: Sending SNMP Alarm count
HB: Checking Number of HeartBeats received
HB: HeartBeats received x
HB: Changing to Alarm Mode, HeartBeats Received x Expected y
```

HB: HeartBeat group address changed
 HB: Heart beat received with invalid UDP port
 HB: Heart beat received from invalid source
 HB: Received HeartBeat packet

Help

Description: Displays a list of the most commonly used diagnostic commands and a brief description of each command. You can append the `ascend` modifier to display the complete list of commands.

Usage: `help [ascend]`

Syntax element	Description
<code>ascend</code>	List all commands.

Example:

```
MAX> help
? -> List all monitor commands
clr-history -> Clear history log
ConnList -> Display connection list information
ether-display -> ether-display <port #> <n>
fatal-history -> List history log
fclear -> clear configuration from flash
FiltUpdate -> Request update of a connection
frestore -> restore configuration from flash
fsave -> save configuration to flash
help -> List all monitor commands
nslookup -> Perform DNS Lookup
priDisplay -> priDisplay <n>
quit -> Exit from monitor to menus
reset -> Reset unit
tloadcode -> load code from tftp host
trestore -> restore configuration from tftp host
tsave -> save configuration to tftp host
wanDisplay -> wanDisplay <n>
wanDSess -> wandsess <sess <n>> (display per session)
wanNext -> wanNext <n>
wanOpening -> wanOpening <n> (displays packets during
opening/negotiation)
```

See Also: ?

IPXripDebug

Description: Displays incoming and outgoing IPX RIP traffic. The command is a toggle that alternately enables and disables the debug display.

Usage: Enter `ipxripdebug` at the command prompt.

Example:

```
MAX> ipxripdebug
```

```
IPX-RIP state display is ON
```

The following message appears as the MAX sends an IPX RIP packet announcing its route:

```
IPXRIP: 10000a17 announced 0 routes on interface 1000:
```

Next, a Pipeline 50 has dialed the MAX. The MAX receives a RIP route from the Pipeline:

```
IPXRIP: received response from ac1b0001:00c07b5e04c0 (1 nets).
```

The following message indicates that the MAX is delaying sending a RIP packet in order to prevent the interpacket arrival time from being closer than busy/slow routers can handle. An IPX router should never violate the minimum broadcast delay.

```
IPX-RIP: too soon to send on interface 1000.
```

The following messages indicate received and sent RIP updates:

```
IPXRIP: 10000a81 announced 0 routes on interface 1000:
```

```
IPXRIP: received response from ac1b0001:00c07b6204c0 (1 nets).
```

```
IPXRIP: 10000aa6 announced 0 routes on interface 1000:
```

```
IPXRIP: received response from ac1b0001:00c07b5504c0 (1 nets).
```

```
IPXRIP: 10000abc announced 0 routes on interface 1000:
```

MdbStr

Description: Modifies the default modem AT command strings used by the modems on the MAX for both incoming and for outgoing calls. With older software, you could not modify the AT command for modems on the MAX. You could affect the string in minor ways by modifying the V42/MNP, Max Baud, and MDM Trn Lvl parameters located in Ethernet > Mod Config > TServe Options.

The MdbStr command also allows you to return the string to its factory default settings.

The modem chip in the MAX supports AT commands of up to 56 characters in length. To fully support all possible functionality, each AT command is sent as two separate strings. You can modify one or both strings.

Note: The AT command string initializes the modems it affects. When you change the AT command string, you are changing the functionality of the modems. Please use the MdbStr command carefully.

Following are the two default strings for the MAX:

- AT&F0&C1V0W1X4
- AT%C3\N3S2=255S95=44S91=10+MS=11,1,300,33600A

Usage: `mdbstr [0] [1] [2] [AT command string]`

Example: You can modify each portion of the AT command string as follows:

Override the existing first string with a new string:

```
mdbstr 1 AT&F0&C1V1W1
```

Override the second portion of the AT command string:

```
mdbstr 2 AT%C3\N3S2=255S95=44S91=10+MS=11,1,300,14400A
```

Return both strings to their factory default settings:

```
mdbstr 0
```

ModemDiag

Description: Displays diagnostic information about each modem as the modem's call is cleared. The command is a toggle that alternately enables and disables the diagnostic display.

With ModemDiag enabled, at the end of each modem call the command initiates an AT&V1 call and displays the following variables with their current values:

Usage: Enter **modemdiag** at the command prompt.

Variable	Description
TERMINATION REASON	LINK DISCONNECT—The remote side disconnected the call. LOCAL REQUEST—The MAX initiated a disconnect because of poor line quality. CARRIER LOSS GSTN CLEARDOWN—Global Switched telephone network (GSTN) initiated the disconnect. NO ERROR CORRECTION INCOMPATIBLE PROTOCOL EXCESSIVE RETRANSMISSIONS DTR LOSS INACTIVITY TIMEOUT INCOMPATIBLE SPEEDS BREAK DISCONNECT KEY ABORT
LAST TX data rate	Last data rate at which the modem on the MAX was transmitting.
HIGHEST TX data rate	Highest data rate at which the modem on the MAX was transmitting.
LAST RX data rate	Last data rate at which the modem on the MAX was receiving.
HIGHEST RX data rate	Highest data rate at which the modem on the MAX was receiving.
Error correction PROTOCOL	Negotiated error correction protocol.
Data COMPRESSION	Negotiated data compression protocol.
Line QUALITY	Probes are sent by each modem to determine the quality of the line and the connection. The range for this variable is 0 to 128. The lower the number, the better the perceived line quality.

Variable	Description
Receive LEVEL	Representation of the attenuation (weakening) of the modem signal, which is measured in decibels. The decibel rating is translated into a number between 0 and 128 for inclusion in this report. The lower the number, the lower the attenuation of the modem signal.
Highest SPX Receive State	Number relating to an internal DSP state machine in the modem code. Has no practical use for most users.
Highest SPX Transmit State	Number relating to an internal DSP state machine in the modem code. Has no practical use for most users.

Example:

```
MAX> modemdiag
TERMINATION REASON..... LINK DISCONNECT
LAST TX data rate..... 26400 BPS
HIGHEST TX data rate..... 26400 BPS
LAST RX data rate..... 24000 BPS
HIGHEST RX data rate..... 24000 BPS
Error correction PROTOCOL... LAPM
Data COMPRESSION..... V42Bis
Line QUALITY..... 032
Receive LEVEL..... 017
Highest SPX Receive State... 67
Highest SPX Transmit State.. 67

TERMINATION REASON..... LINK DISCONNECT
LAST TX data rate..... 28800 BPS
HIGHEST TX data rate..... 31200 BPS
LAST RX data rate..... 28800 BPS
HIGHEST RX data rate..... 28800 BPS
Error correction PROTOCOL... LAPM
Data COMPRESSION..... V42Bis
Line QUALITY..... 032
Receive LEVEL..... 017
Highest SPX Receive State... 85
Highest SPX Transmit State.. 87
```

MDialout

Description: Displays messages related to modem dialout. You can use the command in conjunction with the diagnostic command ModemDrvState to get detailed information about outbound modem calls.

The command is a toggle that alternately enables and disables the debug display.

Usage: Enter **mdialout** at the command prompt.

Example: A modem on the MAX prepares to make an outbound modem call, but never receives a dialtone:

```
MAX> mdialout
```

```
MDIALOUT-2/4: >> CURR state=Await_Off_Hook, NEW event=Event_Off_Hook
MDIALOUT-2/4: connected to DSP!
MDIALOUT-2/4: rqst tone (14) via channelIndex 0
MDIALOUT-2/4: tone generation started.
MDIALOUT-2/4: >> CURR state=Await_Dial_Tone, NEW
event=Event_Dialtone_On
MDIALOUT-2/4: decode timer started.
MDIALOUT-2/4: << NEW state=Await_1st_Digit
MDIALOUT-2/4: enabling tone search, channel index=0, timeslot=0
MDIALOUT-2/4: << NEW state=Await_1st_Digit
MDIALOUT-2/4: >> CURR state=Await_1st_Digit, NEW event=Event_On_Hook
MDIALOUT-2/4: stopping decode timer.
MDIALOUT-2/4: rqst tone (15) via channelIndex 0
MDIALOUT-2/4: disabling tone search, channel index=0
MDIALOUT-2/4: disconnected from DSP.
MDIALOUT-2/4: << NEW state=Await_Off_Hook
MDIALOUT-2/4: >> CURR state=Await_Off_Hook, NEW event=Event_Close_Rqst
MDIALOUT-?/? : << NEW state= <DELETED>
```

ModemDrvDump

Description: Displays information about the status of each modem.

Usage: Enter `modemdrvdump` at the command prompt.

Example: Following is a message about modem 0 (the first modem) in the modem card in slot 3 on the MAX. The numbers in brackets indicate number of calls with unexpected open requests, unexpected Rcode events, unexpected release events and unexpected timeouts:

```
MODEMDRV-3/0: Unexp Open/Rcode/Rlsd/TimOut=[0,0,0,0]
```

ModemDrvState

Description: Displays communication to and from the modem driver on the MAX. You can see which buffers are allocated and which AT command strings are being used to establish modem connections.

You can also determine whether data is received from the modem in an understandable format. If line quality is poor, the modem driver attempts to parse incoming data from the modem, but it might not be successful.

The command is a toggle that alternately enables and disables the diagnostic display.

Note: Once a connection is negotiated, the modems exchange a series of numerical result codes. You can see and decipher these result codes to determine the negotiated connection rate and error correction/compression protocols. Following is a list of several result codes and their meanings:

- 0 - OK
- 1 - CONNECT (300 bps)
- 2 - RING
- 3 - NO CARRIER
- 4 - ERROR
- 5 - CONNECT 1200

6 - NO DIALTONE
7 - BUSY
8 - NO ANSWER
9 - CONNECT 0600
10 - CONNECT 2400
11 - ONNECT 4800
12 - CONNECT 9600
13 - CONNECT 7200
14 - CONNECT 12000
15 - CONNECT 14400
16 - CONNECT 19200
17 - CONNECT 38400
18 - CONNECT 57600
22 - CONNECT 1200/75 (Models with v.23 support only)
23 - CONNECT 75/1200 (Models with v.23 support only)
24 - DELAYED
25 - CONNECT 14400
32 - BLACKLISTED
33 - FAX
34 - FCERROR
35 - DATA
40 - CARRIER 300
43 - CONNECT 16800 (V.34 ONLY)
44 - CARRIER 1200/75 (Models with v.23 support only)
45 - CARRIER 75/1200 (Models with v.23 support only)
46 - CARRIER 1200
47 - CARRIER 2400
48 - CARRIER 4800
49 - CARRIER 7200
50 - CARRIER 9600
51 - CARRIER 12000
52 - CARRIER 14400
66 - COMPRESSION: CLASS 5 (MNP 5)
67 - COMPRESSION: V.42BIS (BTLZ)
69 - COMPRESSION: NONE
70 - PROTOCOL: NONE
77 - PROTOCOL: LAP-M (V.42)
80 - PROTOCOL: ALT (MNP)
81 - PROTOCOL: ALT - CELLULAR (MNP 10) +FC +FCERROR
85 - CONNECT 19200 (V.34 ONLY)
91 - CONNECT 21600 (V.34 ONLY)
99 - CONNECT 24000 (V.34 ONLY)
103 - CONNECT 26400 (V.34 ONLY)
107 - CONNECT 28800 (V.34 ONLY)
151 - CONNECT 31200 (V.34 ONLY)
155* - CONNECT 33600 (V.34 ONLY)

Usage: Enter **modemdrvstate** at the command prompt.

Example: A modem call comes into the MAX, and a modem call is cleared from the MAX.

```
MAX> modemdrvstate
MODEMDRV debug display is ON
```

Modem 1 on the modem card in slot 3 has been assigned to answer an incoming modem call:

```
MODEMDRV-3/1: modemOpen modemHandle B04E3898, hdlcHandle  
B026809C, orig 0
```

The modem is idle, so it is available to answer the call:

```
MODEMDRV-3/1: _processOpen/IDLE
```

The next two lines show the MAX modem sending the first string. The second line shows that a buffer needs to be allocated for sending the command out the WAN.

```
MODEMDRV: Answer String, Part 1 - AT&F0E0  
MODEMDRV-3/1: _hdlcBufSentFnc: buffer = 2E12EAE0, status = SENT
```

Buffers are allocated for data being received from the WAN:

```
MODEMDRV-3/1: _hdlcBufRcvdFnc: data=2E13ADF0, len=8,  
parseState[n,v]=[0,0], status= RCVD  
MODEMDRV-3/1: _hdlcBufRcvdFnc: data=2E13BA20, len=5,  
parseState[n,v]=[0,0], status= RCVD
```

The MAX modem receives OK from the calling modem:

```
MODEMDRV-3/1: data =OK
```

The same process is repeated for strings 2 and 3:

```
MODEMDRV-3/1: _processTimeout/DIAL_STR2  
MODEMDRV: Answer String, Part 2 - AT&C1V0W1X4  
MODEMDRV-3/1: _hdlcBufSentFnc: buffer = 2E12EAE0, status = SENT  
MODEMDRV-3/1: _hdlcBufRcvdFnc: data=2E13C038, len=2,  
parseState[n,v]=[0,0], status= RCVD  
MODEMDRV-3/1: data = 0  
MODEMDRV-3/1: _processTimeout/DIAL_STR3  
MODEMDRV: Answer String, Part 3 -  
AT%C3\N3S2=255S95=44S91=10+MS=11,1,300,33600A
```

Now, result codes are processed to clarify the characteristics of the connection. The MAX modem sends a result code of 52, or CARRIER 14400, and the MAX modem receives the same speed from the calling modem:

```
MODEMDRV-3/1: _hdlcBufSentFnc: buffer = 2E12EAE0, status = SENT  
MODEMDRV-3/1: data = 5  
MODEMDRV-3/1: _hdlcBufRcvdFnc: data=2E13ADF0, len=2, pars-  
eState[n,v]=[5,0], status= RCVD  
MODEMDRV-3/1: data = 2  
MODEMDRV-3/1: decode= 52
```

Result codes 77 and 67 indicate that V.42 error correction and V.42bis error compression, respectively, have been successfully negotiated.

```
MODEMDRV-3/1: _hdlcBufRcvdFnc: data=2E13B408, len=1,  
parseState[n,v]=[2,0], status= RCVD  
MODEMDRV-3/1: data = 7  
MODEMDRV-3/1: _hdlcBufRcvdFnc: data=2E13BA20, len=8,  
parseState[n,v]=[5,0], status= RCVD  
MODEMDRV-3/1: data = 7
```



```
MODEMDRV-3/1: decode= 77  
MODEMDRV-3/1: decode= 67
```

At this point the modem call is up, and the modem driver has completed its task. From here, the call will be passed to Ethernet resources:

```
MODEMDRV-3/1: _processRcodeEvent/AWAITING RLSD, mType=5, RLSD=0  
MODEMDRV-3/1: _processRlsdChange/AWAITING RLSD = 1
```

Following is the normal sequence of steps for a modem call that is cleared (by either modem). Modem 5 on the modem card in slot 7 of the MAX is freed from the previous call and is reinitialized (so it is available for the next call).

```
MODEMDRV-7/5: modemClose modemHandle B04E6F38  
MODEMDRV-7/5: _closeConnection:ONLINE, event=3  
MODEMDRV-7/5: _processTimeout/INIT
```

NSLookup

Description: Similar to the UNIX nslookup command. When you specify a host name, a DNS request is forwarded. If the host is found, the corresponding IP address is displayed.

Usage: nslookup *host_name*

Example:

```
MAX> nslookup host1  
Resolving host host1.  
IP address for host drawbridge is 1.1.1.1.  
  
MAX> nslookup 198.4.92.1  
Resolving host 198.4.92.1.  
  
MAX> nslookup  
Missing host name.  
  
MAX> nslookup nohost  
Resolving host nohost.  
Unable to resolve nohost!
```

NVRAMClear

Description: Clears Nonvolatile Random Access Memory (NVRAM). The current system configuration is stored in NVRAM.

Note: A copy of the configuration may also be stored in Flash memory. If you clear NVRAM, the MAX resets and initializes itself with the configuration it detects in Flash memory. To return your MAX to its factory default settings, you must first use the FClear command to clear the configuration in Flash then use NVRAMClear.

Usage: Enter **nvramclear** at the command prompt.

See Also: FClear

PPPDump

Description: Very similar to the WANDisplay diagnostic command. But PPPDump strips out escape characters that are present for asynchronous PPP users (who are dialing in with modems). The escape characters are necessary because of the asynchronous nature of the data stream. Stripping them out simply clarifies the presentation of the data.

If you enter the command while traffic through your MAX is heavy, the resulting amount of output can make it tedious to find the information you are looking for. The screen might even display the message ----- data lost -----, which just means that not all the output can be displayed on the screen. You might prefer to use the PPPDump command during a period of low throughput.

Usage: `pppdump n`

where **n** is the number of octets to display per frame. Specifying a value of 0 (zero) disables the logging of data.

Example:

Consider the following frames, which were logged by the WANDisplay 64 command:

```
7E FF 7D 23 C0 21 7D 21 7D 21 7D 20 7D 37 7D 22 7D 26 7D 20 7D
2A 7D 20 7D 20 2D 7D 23 7D 26 3A AA 7E
7E FF 7D 23 C0 21 7D 21 7D 21 7D 20 23 7D 20 7D 24 7D 20 7D 20
7D 22 7D 7E
```

To get the data stream without escape characters, the 0x7D bytes need to be stripped, and the byte following each 0x7D byte needs to be decremented by 0x20.

With PPPDump, the MAX automatically convert and displays the data as follows:

```
7E FF 03 C0 21 01 01 00 17 02 06 00 0A 00 00 2D 03 06 3A AA 7E 7E
FF 03 C0 21 01 01 00 23 00 24 00 00 02 7E
```

See Also: WANDisplay, WANNNext, WANOpen

PPPFISM

Displays changes to the PPP state machine as PPP users connect. The command is a toggle that alternately enables and disables the diagnostics display.

Usage: Enter `pppfism` at the command prompt.

Example: The following display shows the complete establishment of a PPP session.

```
MAX> pppfism
PPPFISM state display is ON
PPPFISM-97: Layer 0   State INITIAL      Event OPEN...
PPPFISM-97: ...New State STARTING
PPPFISM-97: Layer 0   State STARTING     Event UP...
PPPFISM-97: ...New State REQSENT
PPPFISM-97: Layer 1   State INITIAL      Event UP...
PPPFISM-97: ...New State CLOSED
PPPFISM-97: Layer 2   State INITIAL      Event UP...
PPPFISM-97: ...New State CLOSED
```

```

PPPFSM-97: Layer 3      State INITIAL      Event UP...
PPPFSM-97: ...New State CLOSED
PPPFSM-97: Layer 4      State INITIAL      Event UP...
PPPFSM-97: ...New State CLOSED
PPPFSM-97: Layer 5      State INITIAL      Event UP...
PPPFSM-97: ...New State CLOSED
PPPFSM-97: Layer 6      State INITIAL      Event UP...
PPPFSM-97: ...New State CLOSED
PPPFSM-97: Layer 7      State INITIAL      Event UP...
PPPFSM-97: ...New State CLOSED
PPPFSM-97: Layer 8      State INITIAL      Event UP...
PPPFSM-97: ...New State CLOSED
PPPFSM-97: Layer 9      State INITIAL      Event UP...
PPPFSM-97: ...New State CLOSED
PPPFSM-97: Layer 0      State REQSENT      Event RCONFREJ...
PPPFSM: irc_new scr 4
PPPFSM-97: ...New State REQSENT
PPPFSM-97: Layer 0      State REQSENT      Event RCONFACK...
PPPFSM-97: ...New State ACKRECD
PPPFSM-97: Layer 0      State ACKRECD      Event RCONFREQ...
PPPFSM-97: ...New State ACKRECD
PPPFSM-97: Layer 0      State ACKRECD      Event RCONFREQ...
PPPFSM-97: Layer 1      State CLOSED      Event OPEN...
PPPFSM-97: ...New State REQSENT
PPPFSM-97: ...New State OPENED
PPPFSM: PAP Packet
PPPFSM-97: Layer 6      State CLOSED      Event OPEN...
PPPFSM-97: ...New State REQSENT
PPPFSM-97: Layer 4      State CLOSED      Event OPEN...
PPPFSM-97: ...New State REQSENT
PPPFSM-97: Layer 4      State REQSENT      Event RCONFREQ...
PPPFSM-97: ...New State REQSENT
PPPFSM: ccp Packet code 1
PPPFSM-97: Layer 6      State REQSENT      Event RCONFREQ...
PPPFSM-97: ...New State REQSENT
PPPFSM: ccp Packet code 2
PPPFSM-97: Layer 6      State REQSENT      Event RCONFACK...
PPPFSM-97: ...New State ACKRECD
PPPFSM-97: Layer 4      State REQSENT      Event RCONFACK...
PPPFSM-97: ...New State ACKRECD

```

PPPIF

Description: Displays messages relating to each PPP connection. This command is particularly useful in troubleshooting negotiation failures. To help in troubleshooting PPP issues, you might want to use PPPIF in conjunction with PPPDump.

Usage: Enter **pppif** at the command prompt.

Example:

```
MAX> pppif
PPPIF debug is ON
PPPIF: open: routeid 285, incoming YES
```

The following message indicates a modem call:

```
PPPIF-110: ASYNC mode
```

Link Compression Protocol (LCP) is negotiated:

```
VJ Header compression is enabled.
PPPIF-110: vj comp on
```

PAP authentication is configured on the MAX and required for access:

```
PPPIF-110: _initAuthentication
PPPIF-110: auth mode 1
PPPIF-110: PAP auth, incoming
PPPIF-110: bypassing async layer
```

LCP has been successfully negotiated and established. Authentication is next:

```
PPPIF-110: Link Is up.
PPPIF-110: pppMpNegUptimeout last 0 layer 0
PPPIF-110: pppMpNegUptimeout last 0 layer 0
PPPIF-110: LCP Opened, local 'Answer', remote ''
PPPIF-110: _openAuthentication
PPPIF-110: pppMpNegUptimeout last 0 layer 1
PPPIF-110: Auth Opened
PPPIF-110: Remote hostName is 'my_name'
```

PAP Authentication was successful. Compression Control Protocol (CCP) is negotiated next, along with IP Network Control Protocol (IPNCP):

```
PPPIF-110: opening CCP
PPPIF-110: pppMpSendNeg Pkt
PPPIF-110: pppMpNegTimeout layer 6
```

The user is given the address 1.1.1.1 from pool 0:

```
PPPIF-110: using address from pool 0
PPPIF-110: Allocated address [1.1.1.1]
PPPIF-110: opening IPNCP:
PPPIF-110: pppMpSendNeg Pkt
PPPIF-110: pppMpNegTimeout layer 4
PPPIF-110: pppMpSendNeg Pkt
PPPIF-110: pppMpSendNeg Pkt
PPPIF-110: pppMpNegUptimeout last 0 layer 6
PPPIF-110: pppMpNegUptimeout last 0 layer 4
PPPIF-110: pppMpSendNeg Pkt
PPPIF-110: pppMpSendNeg Pkt
PPPIF-110: pppMpNegUptimeout last 0 layer 4
PPPIF-110: IPNCP Opened to
PPPIF-110: pppMpSendNeg Pkt
PPPIF-110: pppMpNegUptimeout last 0 layer 6
PPPIF-110: CCP Opened
```

IPNCP and CCP have been successfully negotiated. The PPP session has been completely established.

PPPInfo

Description: Displays information about established PPP sessions. Has little practical use other than as a tool for developmental engineering.

Usage: `pppinfo index [all]`

Example:

Syntax element	Description
<i>index</i>	Selects a particular PPP information table.
<i>all</i>	Displays information about embedded structures.

Example:

```
MAX> pppinfo 1
Ncp[LCP]           = B02B396C
Ncp[AUTH]          = B02B39BC
Ncp[CHAP]          = B02B3A0C
Ncp[LQM]           = B02B3A5C
Ncp[IPNCP]         = B02B3AAC
Ncp[BNCP]          = B02B3AFC
Ncp[CCP]           = B02B3B4C
Ncp[IPXNCP]        = B02B3B9C
Ncp[ATNCP]         = B02B3BEC
Ncp[UNKNOWN]       = B02B3C3C
Mode               = async
nOpen pending     = 0
LocalAsyncMap      = 0
RemoteAsyncMap     = 0
Peer Name          = N/A
Rmt Auth State     = RMT_NONE
aibuf              = 0
ipcp               = B03E502C
vJinfo             = 0
localVjInfo        = 0
bncpInfo           = B03E559C
ipxInfo            = B03E55DC
remote             = no
Bad FCS            = a
```

PPTPCM

Description: Displays messages relating to the call management layer of PPTP. Messages appear as calls are routed to the PPTP server by the MAX. The command is a toggle that alternately enables and disables the diagnostic display.

Usage: Enter `pptpcm` at the command prompt.

Example: Following are messages from a successful connection:

```
PPTPCM: Connecting to host [1.1.1.1]
PPTPCM-[1.1.1.1]: Event = Local-Start-Request
PPTPCM-[1.1.1.1]: Starting local session
```

In the following message, `status = 0` indicates that this was a successful connection:

```
PPTPCM-[1.1.1.1]: Started local session; status = 0
PPTPCM-[1.1.1.1]: _receiveFunc called
PPTPCM-[1.1.1.1]: Event = Remote-Start-Reply
PPTPCM-[1.1.1.1]: Session state changed from Local-Start to Up
```

Following are messages from an unsuccessful connection:

```
PPTPCM-[2.2.2.2]: Event = Local-Start-Request
PPTPCM-[2.2.2.2]: Starting local session
PPTPCM-[0.0.0.0]: Started local session; status = -4
PPTPCM-[0.0.0.0]: EC Start failed
```

PPTPData

Description: Displays the data flowing between the PPTP client and the PPTP server. The command is a toggle that alternately enables and disables the diagnostic display.

Usage: Enter **pptpdata** at the command prompt.

Example: The first of the following messages indicates that the MAX received a positive acknowledgement from the NT server:

```
PPTPDATA-[1.1.1.1]: Received GRE ACK
```

Also, the MAX received data from the NT server that needs to be forwarded out the WAN port:

```
PPTPDATA-[1.1.1.1]: _dataFromLan
```

The MAX receives a packet from the WAN with a good Frame Check Sequence, and sends it to the PPTP server to be processed:

```
PPTPDATA-[1.1.1.1]: Good FCS. Sending packet to peer
```

The following message is a result of an unsuccessful attempt to connect to an NT PPTP server.

```
PPTPDATA-[2.2.2.2]: pptpDataSessionDown, Session not found
```

PPTPEC

Description: Displays control link messages between the PPTP client and the PPTP server. The command is a toggle that alternately enables and disables the diagnostics display.

Usage: Enter **pptpec** at the command prompt.

Example: Following are messages from a successful connection and from an unsuccessful attempt.

Successful connection:

```
PPTPEC-[1.1.1.1]: pptpECSend called
PPTPEC-[1.1.1.1]: New state = Running
```

```
PPTPEC-[1.1.1.1]: Event = Send, current state = Running
PPTPEC-[1.1.1.1]: New state = Running
PPTPEC-[1.1.1.1]: Receive callback called
PPTPEC-[1.1.1.1]: Event = Receive, current state = Running
PPTPEC-[1.1.1.1]: New state = Running
```

Unsuccessful attempt:

```
PPTPEC-[2.2.2.2]: pptpecStart called-
PPTPEC-[2.2.2.2]: Event = Start, current state = Stopped
```

PPTPSend

Description: Sends an Echo Request to the specified NT PPTP server.

Usage: `pptpsend ip_address_of_PPTP_server`

Example:

```
MAX> pptpsend 1.1.1.1
PPTPCM: Sending Echo Request to host [1.1.1.1]
```

PRIDisplay

Description: Displays the contents of WAN packets.

If you enter the command while traffic through your MAX is heavy, the resulting amount of output can make it tedious to find the information you are looking for. The screen might even display the message `----- data lost -----`, which just means that not all the output can be displayed on the screen. You might prefer to use the PRIDisplay command during a period of low throughput.

Usage: `pridisplay n`

where **n** is the number of octets to display from each WAN packet.

Example: The output from the following PRIDisplay command shows the first 64 bytes from each packet sent to or received from the WAN:

```
MAX> pridisplay 64
Display the first 64 bytes of PRI messages
PRI-RCV-0(task: B0479C00, time: 83251.39) 4 octets @ B0539620
[0000]: 02 01 01 61
PRI-XMIT-0(task: B04B3A40, time: 83251.39) 4 octets @ B050C340
[0000]: 02 01 01 49
PRI-RCV-0(task: B0479C00, time: 83261.64) 4 octets @ B052AF60
[0000]: 02 01 01 61
PRI-XMIT-0(task: B04B3A40, time: 83261.65) 4 octets @ B051EFA0
[0000]: 02 01 01 49
PRI-RCV-0(task: B0479C00, time: 83269.98) 27 octets @ B0539620
[0000]: 02 01 48 60 08 02 1A 7B 05 04 03 80 90 A2 18 04
[0010]: E9 82 83 88 70 05 C1 34 39 39 30
pridisplay 0
PRI message display terminated
```

Quit

Description: Exits diagnostic mode.

Usage: Enter **quit** at the command prompt.

RadAcct

Description: Displays RADIUS accounting information. The RadAcct command displays very few messages if RADIUS Accounting is functioning correctly. The command is a toggle that alternately enables and disables the diagnostic display.

(For troubleshooting RADIUS-related issues, the RADIF command displays more detailed information.)

Usage: Enter **radacct** at the command prompt.

Example:

```
MAX> radacct
RADACCT debug display is ON
```

A user hangs up and a stop record is generated:

```
RADACCT-147:stopRadAcct
```

The following message indicates that there is some load on the network and the sending of a stop record is delayed. This does not necessarily indicate a problem:

```
RADACCT-147:_endRadAcct: STOP was delayed
```

RadIF

Description: Displays RADIUS-related messages. RadIF is a powerful diagnostic command, because it displays RADIUS messages the MAX receives as well as messages that it sends. Output from RadIF, in conjunction with running your RADIUS daemon in diagnostic mode (using the **-x** option), gives you virtually all the information you need to clarify issues relating to user authentication.

You can also validate the IP port that you have configured (or think you have configured), and the user name that is being sent by the client.

The command is a toggle that alternately enables and disables the diagnostic display.

Usage: Enter **radif** at the command prompt.

Example: Following are messages you might see for a successful RADIUS authentication:

```
RADIF: authenticating <8:my_name> with PAP
RADIF: _radiusRequest: id 41, user name <9:my_name>
RADIF: _radiusRequest: challenge len = <0>
```

The RADIUS Daemon IP address and authentication port appear:

```
RADIF: _radiusRequest: socket 5 len 89 ipaddr 01010101 port
65534->1645
```



```
RADIF: _radCallback  
RADIF: _radCallback, buf = B05BBFA0
```

The response is sent back from RADIUS. In this case, the user my_name has passed authentication. Following is a list of the most common responses:

- 1 - Authentication Request
- 2 - Positive Acknowledgement
- 3 - Rejection
- 4 - Accounting Request
- 5 - Accounting Response
- 7 - Password Change Request
- 8 - Password Change Positive Acknowledgement
- 9 - Password Change Rejection
- 11 - Access Challenge
- 29 - Password - next code
- 30 - Password New PIN
- 31 - Password Terminate Session
- 32 - Password Expired

```
RADIF: _radCallback, authcode = 2  
RADIF: Authentication Ack
```

After authenticating a user, the RADIUS daemon sends the attributes from the user profile to the MAX. The MAX creates the user's Connection profile from these attributes, and RadIF displays them. For a complete list of attribute numbers, see the *MAX RADIUS Configuration Guide*.

```
RADIF: attribute 6, len 6, 00 00 00 02  
RADIF: attribute 7, len 6, 00 00 00 01  
RADIF: attribute 8, len 6, ff ff ff fe  
RADIF: attribute 9, len 6, ff ff ff 00  
RADIF: attribute 11, len 12, 73 74 64 2e  
RADIF: attribute 12, len 6, 00 00 05 dc  
RADIF: attribute 10, len 6, 00 00 00 00  
RADIF: attribute 13, len 6, 00 00 00 01  
RADIF: attribute 244, len 6, 00 00 11 94  
RADIF: attribute 169, len 6, 00 00 11 94  
RADIF: attribute 170, len 6, 00 00 00 02  
RADIF: attribute 245, len 6, 00 00 00 00  
RADIF: attribute 235, len 6, 00 00 00 01
```

A RADIUS Accounting Start packet is sent to the RADIUS Accounting Server (using port 1646):

```
RADIF: _radiusAcctRequest: id 42, user name <9:my_name>  
RADIF: _radiusAcctRequest: socket 6 len 82 IP cf9e400b port  
1646, ID=42  
RADIF: _radCallback  
RADIF: _radCallback, buf = B05433C0  
RADIF: _radProcAcctRsp: user:<9:my_name>, ID=42
```

RadStats

Description: Displays a compilation of RADIUS Authentication and Accounting statistics.

Usage: Enter **radstats** at the command prompt.

Example:

```
MAX> radstats
RADIUS authen stats:
```

In the following message, A denotes *authentication* and O denotes *other*. There were 612 authentication requests sent and 612 authentication responses received.

```
0 sent[A,O]=[612,15], rcv[A,O]=[612,8]
```

602 were authenticated successfully, and 18 were not:

```
timeout[A,O]=[0,6], unexp=0, bad=18, authOK=602
```

In the next message, the IP address of the RADIUS server is 1.1.1.1, and the curServerFlag indicates whether or not this RADIUS server is the current authentication server. (You can have several configured RADIUS servers, but only one is current at any one time.) 0 (zeor) indicates *no*. A 1 indicates *yes*.

```
IpAddress 1.1.1.1, curServerFlag 1
RADIUS accounting stats:
```

The next message indicates that the MAX sent 1557 Accounting packets and received 1555 responses (ACKs from the Accounting server). Therefore, the unexp value is 2. This does not necessarily indicate a problem, but might be the result of the MAX timing out a particular session before receiving an ACK from the RADIUS server. Momentary traffic load might cause this condition. The value of bad is the number of packets that were formatted incorrectly by either the MAX or the RADIUS server.

```
0 sent=1557, rcv=1555, timeout=0, unexp=2, bad=0
```

In the next message, note that the Accounting server is different from the Authentication server. The Accounting and Authentication servers do not need to be running on the same host, although they can be.

```
IpAddress 2.2.2.2, curServerFlag 1
Local Rad Acct Stats:
```

The next two messages can be used to look for traffic congestion problems or badly formatted Accounting packets. Under typical conditions, you might see a few packets whose acknowledgments fail.

The first message indicates whether any RADIUS requests have been dropped by the MAX. With this particular message, no requests were dropped. 1557 were sent successfully:

```
nSent[OK,fail]=[1557,0], nRcv=1557, nDrop[QFull,Other]=[0,0]
```

The next message indicates whether any session timeouts resulted from failure to receive a RADIUS responses were not received, causing a session timeout. The message also indicates responses that are received by the MAX but that do not match any expected responses. The MAX keeps a list of sent requests, and expects a response for each request. In the following message, one response received from the RADIUS server did not match any of the requests that the MAX had sent out. This might be caused by a corrupted response packet, or by the MAX timing out the session before the response was received.

```
nRsp[TimOut,NoMatch]=[0,1], nBackoff[new,norsp]=[0,0]
```

The following messages display a summarized list of RADIUS server statistics:

```
Local Rad Serv Stats:
unkClient=0
index 0 #Sent = 0, #SendFail=0 badAuthRcv = 0, badPktRcv = 0
```

Reset

Description: Resets the MAX, which terminates all active connections and restarts. All users are logged out and the default security level is reactivated. All active WAN lines are temporarily shut down because of the loss of signaling or framing information. As the MAX boots, it runs its Power-On Self Tests (POST).

Usage: Enter **reset** at the command prompt.

Example: To reset the unit:

```
MAX> reset
```

See Also: NVRAM

Revision

Description: Displays the serial number of the box.

Usage: Enter **revision** at the command prompt.

Example: In the following message, the MAX has a serial number of 6363077.

```
MAX> revision
revision = 0 1 10 6363077
```

SNTP

Description: Displays messages related to Simple Network Time Protocol (SNTP). The command is a toggle that alternately enables and disables the diagnostics display.

Usage: Enter **sntp** at the command prompt.

Example: Following are sample messages displayed with SNTP enabled.

The MAX accepts time from a configured NTP server. The following message appears if the MAX does not accept a supplied time:

```
Reject:li= x stratum= y tx= z
```

The following message indicates that the MAX accepts the time from a specified NTP server:

```
Server= 0 Time is b6dd82ed d94128e
```

Because the stored time is off by more than one second, it is adjusted:

```
SNTP: x Diff1= y Diff2= z
```

TelnetDebug

Description: Displays messages as Telnet connections are attempted or established. The Telnet protocol negotiates several options as sessions are established, and TelnetDebug displays the Telnet option negotiations.

The command is a toggle that alternately enables and disables the diagnostic display.

Usage: Enter **telnetdebug** at the command prompt.

Example: The following session shows the MAX terminal server establishing a successful Telnet connection with another UNIX host.

```
MAX> telnetdebug
TELNET debug is now ON
```

The far-end UNIX host has been contacted:

```
TELNET-4: TCP connect
```

For this Telnet session, the MAX will support options 24 and 1. The UNIX host should respond with either DO or WONT:

```
TELNET-4: send WILL 24
TELNET-4: recv WILL 1
```

The UNIX host will support option 1:

```
TELNET-4: repl DO 1
```

The MAX receives a request to support option 3:

```
TELNET-4: recv WILL 3
```

The MAX will support option 3:

```
TELNET-4: repl DO 3
```

The UNIX host will support option 3:

```
TELNET-4: recv DO 3
```

The UNIX host will not support option 24:

```
TELNET-4: recv DONT 24
```

The MAX will not support option 24:

```
TELNET-4: repl WONT 24
```

The UNIX host will support options 1 and 3:

```
TELNET-4: recv WILL 1
TELNET-4: recv WILL 3
```

TLoadCode

Description: Uses Trivial File Transfer Protocol (TFTP) to load software from a UNIX host into the MAX unit's flash memory. The TFTP host can be accessed from the Ethernet interface or across the WAN. The MAX needs to be reset to load the the uploaded code, since the MAX must load the code from Flash memory into DRAM.

Although the MAX might experience a small performance degradation during the file transfer, it will be fully functional during the file download process.

When you use the TLoadCode command, the current configuration of the MAX is saved to flash memory . Therefore, manual reconfiguration, which is required when loading software through the serial connection, should not be necessary.

When you execute the command, a sequence of dots appears on the screen, indicating the progress of the transfer. Each dot represents the transfer of approximately 512 bytes.

Note: If the TFTP transfer is interrupted or the checksum of the uploaded file is incorrect, the new code does not load when the MAX is rebooted. The MAX reloads its previous version of code. Also, if the new code *is* uploaded at boot time, an FRestore is performed to load the configuration that is stored in flash memory. The MAX reboots again to properly initialize the configuration.

Usage: `tloadcode name_or_ip_address_of_tftp_server filename`

Example:

```
MAX> tloadcode
usage: loadcode host file
> tloadcode 1.1.1.1 mhpt1.bin
saving config to flash
.....
.
loading code from 1.1.1.1
file mhpt1.bin...
.....
.....
.....
.....
```

TRestore

Description: Restores a saved configuration from a TFTP host to Flash memory on the MAX. You need to manually reboot the MAX to load the restored configuration from Flash memory into dynamic RAM.

Usage: `trestore name_or_ip_address_of_tftp_server filename`

Example:

```
MAX> trestore 1.1.1.1 config.txt
restoring configuration from 1.1.1.1:69
file config.txt...
```

TSave

Description: Saves the MAX configuration that is stored in flash memory to a TFTP server. You need to perform the FSave command if you want to save your currently running configuration. FSave saves the currently running configuration to flash memory.

Usage: `tsave name_or_ip_address_of_tftp_server filename`

Example:

```
MAX> tsave 1.1.1.1 config.txt
saving configuration to 1.1.1.1:69
file config.txt...
```

Update

Description: Modifies optional functionality of the MAX. To enable some options, you must obtain a set of hash codes (supplied by an Ascend representative) that will enable the functionality in your MAX. After each string is entered, the word *complete* appears, indicating that the MAX accepted the hash code.

If you enter `update` without a text string modifier, the MAX displays a list of current configuration information.

Usage: `update [text_string]`

Example:

```
MAX> update
Host interfaces: 4
Net interfaces: 4
Port 1 channels: 255
Port 2 channels: 255
Port 3 channels: 255
Port 4 channels: 255
Field features 1: 182
Field features 2: 33
Field features 3: 54
Protocols: 1

MAX> update 5 1023 12321312312312321
```

The following two messages indicate that the text strings were entered incorrectly:

```
update command: invalid arg 3!
update command: disallowed
```

The following message indicates that the MAX accepted the update string:

```
update command: command complete.
```

WANDisplay

Description: Displays all packets received from or sent to any of the WAN interfaces. Because WANDisplay output shows the raw data the MAX is receiving from and sending to the remote device, the information can be very helpful in PPP negotiation problems.

If you enter the command while traffic through your MAX is heavy, the resulting amount of output can make it tedious to find the information you are looking for. The screen might even display the message `----- data lost -----`, which just means that not all the output can be displayed on the screen.

You might prefer to use the WANDisplay command during a period of low throughput. Alternatively, depending on the types of information you need to gather, you might use WANDSess, WANOpen, or WANNext to focus the display.

Usage: `wandisplay number_of_octets_to_display_from_each_packet`

Enter `wandisplay 0` to disable the logging of this information.

Example: Following are several examples of WANDisplay output. Note that the bytes are displayed in hexadecimal format.

```
MAX> wandisplay 24
Display the first 24 bytes of WAN messages
> RECV-272:: 1 octets @ 5E138F74
[0000]: 0D
RECV-272:: 13 octets @ 5E13958C
[0000]: 0A 41 63 63 65 70 74 3A 20 69 6D 61 67
XMIT-276:: 1011 octets @ 2E12D8A4
[0000]: 7E 21 45 00 03 EE 54 2B 40 00 37 06 BA 09 CF 2B
[0010]: 00 86 D0 93 91 90 1A 0A

MAX> wandisplay 0
WAN message display terminated
```

See Also: WANDSess, WANOpen, WANNext

WANDSess

Description: Similar to WANDisplay, but WANDSess displays only incoming and outgoing packets for a specific user. WANDSess is particularly helpful for troubleshooting a MAX with several simultaneous active connections. The volume of output from commands such as WANDisplay make them not as effective for troubleshooting issues for particular users. WANDSess is a filter to let you focus your troubleshooting.

If you enter the command while traffic through your MAX is heavy, the resulting amount of output can make it tedious to find the information you are looking for. The screen might even display the message `----- data lost -----`, which just means that not all the output can be displayed on the screen. You might prefer to use the WANDSess command during a period of low throughput.

Usage: `wandsess user_name_or_profile_name number_of_octets_to_display_from_each_packet`

Enter `wandsess user_name_or_profile_name 0` to disable the logging of this information.

Example:

```
MAX> wandsess gzoller 24
RECV-gzoller:300:: 1 octets @ 3E13403C
[0000]: 7E 21 45 00 00 3E 15 00 00 00 20 7D 31 C2 D2
RECV-gzoller:300:: 15 octets @ 3E133A24
[0000]: D0 7D B3 7D B1 B3 D0 7D B3 90 02 04 03 00 35
XMIT-gzoller:300:: 84 octets @ 3E12D28C
```

```
[0000]: 7E 21 45 00 00 4E C4 63 00 00 1C 7D 31 17 5F D0  
[0010]: 93 90 02 D0 93 91 B3 00
```

Notice that the only difference in output between WANDSess and WANDisplay is that with WANDSess, the name of the user is displayed in a message. The data is identical in content, but WANDSess displays no data from any other sessions.

```
MAX> wandsess gzoller 0  
MAX>
```

WANNext

Description: Similar to WANDisplay, but WANNext displays only incoming and outgoing packets for the next successfully authenticated user. As with WANDSess, the output is the same as for WANDisplay but is filtered to include only data from a single user.

If you enter the command while traffic through your MAX is heavy, the resulting amount of output can make it tedious to find the information you are looking for. The screen might even display the message ----- data lost -----, which just means that not all the output can be displayed on the screen. You might prefer to use the WANNext command during a period of low throughput.

Usage: `wannext number_of_octets_to_display_from_each_packet`

Enter **WANNext 0** to disable the logging of this information.

WANOpening

Description: Similar to WANDisplay, but WANOpening displays only the opening incoming and outgoing packets for all users during the establishment of their PPP sessions. This command is particularly helpful if you are troubleshooting connection problems in which users seem to connect to the MAX, but are disconnected within a few seconds. Again, the output from WANOpening is very similar to WANDisplay, but displays packets for sessions only until the connection has been completely negotiated.

If you enter the command while traffic through your MAX is heavy, the resulting amount of output can make it tedious to find the information you are looking for. The screen might even display the message ----- data lost -----, which just means that not all the output can be displayed on the screen. You might prefer to use the WANOpening command during a period of low throughput.

Usage: `wanopening number_of_octets_to_display_from_each_packet`

Enter **WANOpening 0** to disable the logging of this information.

WANToggle

Description: Displays messages from the WAN drivers on the MAX, including the state of calls that have been processed by the MAX unit's calling routines but not yet sent to the Ethernet drivers.

If you enter the command while traffic through your MAX is heavy, the resulting amount of output can make it tedious to find the information you are looking for. The screen might even display the message ----- data lost -----, which just means that not all the output

can be displayed on the screen. You might prefer to use the WANToggle command during a period of low throughput.

The command is a toggle that alternately enables and disables the diagnostic display.

Usage: Enter **wantoggle** at the command prompt.

Example: Following is typical output produced by a modem call into the MAX. After the incoming call is determined to be an analog call, a modem is directed to answer it.

```
WAN-389: wanOpenAnswer
WAN-389: modem redirected back to wan
WAN-389: Startup frame received
WAN-389: Detected unknown message
WAN-389: Detected ASYNC PPP message
WAN-389: wanRegisterData, I/F 58
```

The next two messages appear when the call is cleared. The second message does not indicate a problem. It appears because the modem clears the call a split second before the software releases its resources. The software does a check on the modem, which has already been released.

```
WAN-389: wanCloseSession, I/F 58
WAN-?: no modem assoc w WanInfo
```

WDDialout

Description: Displays the specific packet that caused the MAX to dial out. The command is particularly helpful if the MAX is dialing out when it should not. You can use WDDialout information to design a filter to keep the MAX from dialing out because of a particular packet.

The command is a toggle that alternately enables and disables the diagnostic display.

Usage: Enter **wddialout** at the command prompt.

Example: The following message includes a date/time stamp, the phone number being dialed, and the packet that caused the MAX to dial out:

```
Date: 01/01/1990.      Time: 00:51:56
Cause an attempt to place call to 18185551234
WD_DIALOUT_DISP: chunk D7BA6 type OLD-STYLE-PADDED.
: 60 octets @ F3050
[0000]: 09 00 07 ff ff ff 00 05 02 e8 14 0d 00 24 aa aa
[0010]: 03 00 00 00 80 f3 00 01 80 9b 06 04 00 01 00 05
[0020]: 02 e8 14 0d 00 ff 00 f7 00 00 00 00 00 00 00 ff
[0030]: 8e 01 00 00 00 00 00 00 00 00 00 00 00 00
MAX> wddialout
WANDATA dialout display is OFF
```

PPP decoding primer

Many of the diagnostic commands display raw data. This section is designed to assist you in decoding PPP, MP, MP+ and BACP negotiations. The negotiations can be logged with the PPPDump, WANDisplay, WANDSess, WANNext, or WANOpen diagnostic commands. For more detailed information than this appendix provides, see specific RFCs. A partial list of pertinent RFCs appears at the end of this appendix.

Breaking down the raw data

An important concept to keep in mind is that each device negotiates PPP independently, so the options might be identical for each direction of the session.

During PPP negotiation, frame formats in the various protocols are very similar. They share the following characteristics:

- FF 03 which indicates a PPP frame
- A two-byte Protocol Identifier
- A one-byte Packet Format ID number
- A one-byte ID number
- A two-byte length
- Options for the protocol

Following are the most common protocols you will see in Ascend diagnostic traces:

Identifier	Description
C0 21	Link Control Protocol (LCP)
C0 23	Password Authentication Protocol (PAP)
C2 23	Challenge Handshake Authentication Protocol (CHAP)
80 21	Internet Protocol (IP)
80 29	Appletalk
80 2B	Novell's Internetwork Packet Exchange (IPX)
80 31	Bridging PDU
80 FD	Compression Control Protocol (CCP)

Following are the packet formats:

Packet Format ID	Description
01	Configure Request
02	Configure Acknowledgment

Packet Format ID	Description
03	Configure Non-Acknowledgment
04	Configure Reject
05	Terminate Request
06	Terminate Acknowledgment
07	Code Reject
08	Protocol Reject
09	Echo Request
0A	Echo Reply
0B	Discard Request

Note: If a packet received from the WAN fails the Cyclic Redundancy Check (CRC), the display is similar to the following, where RBAD denotes Received BAD:

```
RBAD-27:: 8712 octets @ 26CFE8
[0000]: fe dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd
[0010]: dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd
[0020]: dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd
[0030]: dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd
```

Annotated Traces

Following are sample traces you can use as guides to help you decode other traces.

Example of a PPP connection attempt

LCP Configure Request—MP+, MRU of 1524, MRRU of 1524 and End Point Discriminator using the device's MAC address:

```
XMIT-3:: 29 octets @ 2C2E94
[0000]: ff 03 c0 21 01 01 00 19 00 04 00 00 01 04 05 f4
[0010]: 11 04 05 f4 13 09 03 00 c0 7b 4c e0 4c
```

Following is a second LCP Configure Request from the same device. Everything in the packet is identical to the previous packet, except the ID number has incremented from 01 to 02:

```
XMIT-3:: 29 octets @ 2C2E94
[0000]: ff 03 c0 21 01 02 00 19 00 04 00 00 01 04 05 f4
[0010]: 11 04 05 f4 13 09 03 00 c0 7b 4c e0 4c
```

LCP Configure Request—CHAP authentication, Magic number

```
RECV-3:: 19 octets @ 2BEB8C
[0000]: ff 03 c0 21 01 60 00 0f 03 05 c2 23 05 05 06 4e
[0010]: 36 c9 05
```

LCP Configure Acknowledgment—The device in the following trace will be authenticated with CHAP. The Magic number is also acknowledged:

```
XMIT-3:: 19 octets @ 2C2E94
[0000]: ff 03 c0 21 02 60 00 0f 03 05 c2 23 05 05 06 4e
[0010]: 36 c9 05
```

LCP Configure Reject—MP+, MRU of 1524, MRRU of 1524 and End Point Discriminator. This rejection shows two things. First, the remote side does not support MP+ or MP, since MP+ and the MRRU were rejected. This will have to be a PPP connection. Second, since the MRU of 1524 was rejected, the default of 1500 is assumed. There must be an MRU, so a rejection of a given value only calls for use of the default value.

After the trace, the device will need to transmit another LCP Configure Request, removing all the rejected options:

```
RECV-3:: 29 octets @ 2BF1A4
[0000]: ff 03 c0 21 04 02 00 19 00 04 00 00 01 04 05 f4
[0010]: 11 04 05 f4 13 09 03 00 c0 7b 4c e0 4c
```

LCP Configure Request—Note that all values that were previously rejected are no longer in the packet:

```
XMIT-3:: 8 octets @ 2C2E94
[0000]: ff 03 c0 21 01 04 00 04
```

LCP Configure Acknowledgment:

```
RECV-3:: 8 octets @ 2BF7BC
[0000]: ff 03 c0 21 02 04 00 04
```

At this point, since both sides have transmitted LCP Configure Acknowledgments, LCP is up and the negotiation moves to the authentication phase. The device receives a CHAP challenge from the remote end:

```
RECV-3:: 21 octets @ 2BFDD4
[0000]: ff 03 c2 23 01 01 00 11 04 4e 36 c9 5e 63 6c 63
[0010]: 72 34 30 30 30
```

The device transmits its encrypted user name and password:

```
XMIT-3:: 36 octets @ 2C2E94
[0000]: ff 03 c2 23 02 01 00 20 10 49 b8 e8 54 76 3c 4a
[0010]: 6f 30 16 4e c0 6b 38 ed b9 4c 26 48 5f 53 65 61
[0020]: 74 74 6c 65
```

The remote device sends a CHAP Acknowledgment:

```
RECV-3:: 8 octets @ 2C03EC
[0000]: ff 03 c2 23 03 01 00 04
```

At this point, the negotiation moves from authentication to negotiation of Network Control Protocols (NCPs). Ascend supports Bridging Control Protocol (BCP), IPCP, IPXCP, and ATCP.

IPCP Configure Request—Van Jacobsen Header Compression, IP address of 1.1.1.1:

```
RECV-3:: 20 octets @ 2C0A04
[0000]: ff 03 80 21 01 e3 00 10 02 06 00 2d 0f 00 03 06
[0010]: 01 01 01 01
```

BCP Configure Request:

```
RECV-3:: 8 octets @ 2C101C
[0000]: ff 03 80 31 01 55 00 04
```

IPCP Configure Request—IP address of 2.2.2.2:

```
XMIT-3:: 14 octets @ 2C2E94
[0000]: ff 03 80 21 01 01 00 0a 03 06 02 02 02 02
```

IPCP Configure Reject—Van Jacobsen Header Compression. The remote device should send another IPCP Configure Request and remove the request to perform VJ Header Compression:

```
XMIT-3:: 14 octets @ 2C2E94
[0000]: ff 03 80 21 04 e3 00 0a 02 06 00 2d 0f 00
```

BCP - Protocol Reject. The local device is not configured to support bridging:

```
XMIT-3:: 8 octets @ 2C2E94
[0000]: ff 03 80 31 08 55 00 04
```

IPCP Configure Acknowledgment:

```
RECV-3:: 14 octets @ 2C1634
[0000]: ff 03 80 21 02 01 00 0a 03 06 01 01 01 01
```

IPCP Configure Request—Note that VJ Header Compression is not requested this time:

```
RECV-3:: 14 octets @ 2C1C4C
[0000]: ff 03 80 21 01 e4 00 0a 03 06 02 02 02 02
```

IPCP Configure Acknowledgment:

```
XMIT-3:: 14 octets @ 2C2E94
[0000]: ff 03 80 21 02 e4 00 0a 03 06 01 01 01 01
```

At this point, a PPP connection has been successfully negotiated. The caller was successfully authenticated by means of CHAP, and IPCP was the only successfully configured NCP. IPX, Appletalk, and bridging will not be supported during this session.

Following are two packets used in determining link quality:

LCP Echo Request packet:

```
RECV-3:: 16 octets @ 2BEB8C
[0000]: ff 03 c0 21 09 01 00 0c 4e 36 c9 05 00 00 00 00
```

LCP Echo Response:

```
XMIT-3:: 16 octets @ 2C2E94
[0000]: ff 03 c0 21 0a 01 00 0c 00 00 00 00 00 00 00 00
```

Example of MP+ call negotiation

LCP Configuration Request—MP+, MRU of 1524, MRRU of 1524, End Point Discriminator using the device's MAC address:

```
XMIT-31:: 29 octets @ D803C
[0000]: ff 03 c0 21 01 01 00 19 00 04 00 00 01 04 05 f4
[0010]: 11 04 05 f4 13 09 03 00 c0 7b 5c d3 71
```

LCP Configure Request—MP+, MRU of 1524, PAP authentication is required. MRRU of 1524, End Point Discriminator using the device's MAC address:

```
RECV-31:: 33 octets @ D4FBC
[0000]: ff 03 c0 21 01 01 00 1d 00 04 00 00 01 04 05 f4
[0010]: 03 04 c0 23 11 04 05 f4 13 09 03 00 c0 7b 53 f0
[0020]: 7a
```

LCP Configuration Acknowledgment:

```
RECV-31:: 29 octets @ D55CC
[0000]: ff 03 c0 21 02 01 00 19 00 04 00 00 01 04 05 f4
[0010]: 11 04 05 f4 13 09 03 00 c0 7b 5c d3 71
```

LCP Configuration Acknowledgment:

```
XMIT-31:: 33 octets @ D803C
[0000]: ff 03 c0 21 02 01 00 1d 00 04 00 00 01 04 05 f4
[0010]: 03 04 c0 23 11 04 05 f4 13 09 03 00 c0 7b 53 f0
[0020]: 7a
```

At this point, LCP is up. Next is the authentication phase. The local device agreed to PAP authentication, so it should transmit its user name and password. Note that they are not encrypted and can be decoded very easily.

PAP Authentication Request—User name is shown in hexadecimal and must be converted to ASCII. User name is 0x6a 0x73 0x6d 0x69 0x74 0x68 (jsmith) and password is 0x72 0x65 0x64 (red):

```
XMIT-31:: 20 octets @ D803C
[0000]: ff 03 c0 23 01 01 00 10 06 6a 73 6d 69 74 68 03 72
[0010]: 65 64
```

PAP Authentication Acknowledgment:

```
RECV-31:: 9 octets @ D5BDC
[0000]: ff 03 c0 23 02 01 00 05 00
```

Authentication is successful. Final negotiation determines protocols to be supported over the link.

Note: MP+ was negotiated, and both devices begin sending MP+ packets from this point. The data portion of the packet is identical to PPP, but there is an eight-byte MP+ header instead of the two-byte PPP header:

In the following packet, 00 3d is the designation for a Multilink packet. The fifth byte designates whether this packet is fragmented. The sixth, seventh, and eighth bytes are the sequence number, which increments by one for each packet sent or received.

Bytes nine through eleven, 80 31 01, designate as a BCP Configure Request received from the remote device:

```
RECV-31:: 20 octets @ D61EC
[0000]: ff 03 00 3d c0 00 00 00 80 31 01 01 00 0a 03 03
[0010]: 01 07 03 00
```

BCP Configure Request sent from this device:

```
XMIT-31:: 20 octets @ D803C
[0000]: ff 03 00 3d c0 00 00 00 80 31 01 01 00 0a 03 03
[0010]: 01 07 03 00
```

BCP Configure Acknowledgment:

```
XMIT-31:: 20 octets @ D864C
[0000]: ff 03 00 3d c0 00 00 01 80 31 02 01 00 0a 03 03
[0010]: 01 07 03 00
```

BCP Configure Acknowledgment:

```
RECV-31:: 20 octets @ D67FC
[0000]: ff 03 00 3d c0 00 00 01 80 31 02 01 00 0a 03 03
[0010]: 01 07 03 00
```

BCP is up and the session begins sending bridged traffic. No routed protocols were negotiated.

The following packets are sent as part of the MP+ protocol. They are sent at one-second intervals. The packets are used by each unit to validate the existence of the link. This validation gives the devices a secure way to determine whether the link is still up, even if there is no data traffic passing between the devices.

```
RECV-31:: 8 octets @ D5BDC
[0000]: ff 03 00 3d c0 00 00 05
XMIT-31:: 8 octets @ D803C
[0000]: ff 03 00 3d c0 00 00 04
RECV-31:: 8 octets @ D61EC
[0000]: ff 03 00 3d c0 00 00 06
XMIT-31:: 8 octets @ D803C
[0000]: ff 03 00 3d c0 00 00 05
```

Relevant RFCs

The following RFCs provide more detail about the protocols used in Ascend diagnostic traces.

Identifier	Title
RFC1378	PPP AppleTalk Control Protocol (ATCP)
RFC1552	PPP Internetwork Packet Exchange Control Protocol (IPXCP)
RFC1638	PPP Bridging Control Protocol (BCP)
RFC1661	Point-to-Point Protocol (PPP)
RFC1934	Ascend's Multilink Protocol Plus (MP+)
RFC1962	PPP Compression Control Protocol (CCP)
RFC1974	PPP Stac LZS Compression Protocol
RFC1989	PPP Link Quality Monitoring

Identifier	Title
RFC1990	PPP Multilink Protocol (MP)
RFC1994	PPP Challenge Handshake Authentication Protocol

Upgrading System Software

C



Caution: Periodically the procedure for uploading new software to Ascend units changes significantly. Carefully read the new software loading procedures explained in this section before upgrading your system.

This appendix explains how to upgrade your system software. It covers the following topics:

Definitions and terms	C-2
Guidelines for upgrading system software.	C-3
Guidelines for downgrading system software	C-4
Before you begin	C-5
Upgrading system software with a standard load	C-6
Upgrading system software with a fat or thin load	C-7
Upgrading system software with an extended load	C-9
Upgrading system software from versions earlier than 4.6C to version 5.0A or above	C-11
Using the serial port to upgrade to a standard or a thin load	C-12
Changing to system software that does not support V.90	C-15
System messages	C-15

Definitions and terms

This appendix uses the following terms:

Build	<p>The name of the software binary.</p> <p>For example, <code>ti.m40</code> is the MAX 4000 T1 IP-only software build. For the names of all the software builds and the features they provide see <code>/pub/Software-Releases/Max/Upgrade-Filenames.txt</code> on the Ascend FTP server.</p> <p>If possible, you should stay with the same build when upgrading. Loading a different build can cause your Ascend unit to lose its all or part of its configuration. If this happens, you must restore your configuration from a backup.</p>
Standard load	<p>Software versions 4.6Ci18 or earlier and all 4.6Cp releases. You can load these versions of software through the serial port or by using TFTP.</p> <p>TFTP is the recommended upgrade method for standard loads.</p>
Fat load	<p>4.6Ci19 to 5.0Aix and all 5.0Ap releases with a file size greater than 960 KB (for MAX units) or 448K (for Pipeline units). Before upgrading to a fat load for the first time, you must upgrade to a thin load.</p> <p>You must use TFTP to upgrade to fat loads.</p>
Thin load	<p>4.6Ci19 to 5.0Aix and all 5.0Ap releases with a file size less than 960 KB (for MAX units) or 448 KB (for Pipeline units).</p> <p>TFTP is the recommended upgrade method for thin loads.</p>
Restricted load	<p>6.0.0 or later MAX release denoted by an “r” preceding the build name. For example, <code>rti.m40</code> is the restricted load for the MAX 4000 T1 IP-only software build. Before upgrading to an extended load for the first time, you must upgrade to a restricted load. Note that after you have upgraded your system to version 6.0.0 or above, you do not need to use a restricted load to upgrade.</p> <p>A restricted load only contains essential system software and is not meant to be run in a working environment. It does not have full functionality and is to be used only to upload to an extended load. Restricted loads <i>do</i> allow you to access the unit via Telnet.</p> <p>TFTP is the recommended upgrade method for restricted loads.</p> <p>Pipeline releases do not have restricted loads.</p>
Extended load	<p>6.0.0 or later MAX release denoted by an “f” preceding the build name. You must use TFTP to upgrade to extended loads. For example, <code>fti.m40</code> is the extended load for the MAX 4000 T1 IP-only software build.</p> <p>MAX 6000 and Pipeline releases do not have extended loads.</p>

Guidelines for upgrading system software



Caution: Before upgrading, consider the following very important guidelines:

- Use TFTP to upgrade if possible. TFTP is more reliable and saves the Ascend unit configuration when you upgrade.
- You cannot load a fat load or an extended load through the serial port. You must use TFTP.
- If you are using TFTP to upgrade your software, use the `fsave` command immediately after executing the `tload` command. Failure to do so might cause your Ascend unit to lose its configuration.
- If possible, you should always stay with the same build of software when you upgrade. If you load a different version, your Ascend unit may lose its configuration. If this happens, you must restore your configuration from a backup.
- If you are upgrading to a software version 5.0A or 5.0Aix fat load for the first time, you must be on a load that supports the fat load format. All versions of software 5.0A or above support fat loads. You should perform the upgrade in two steps:
 - Upgrade to a thin load of the same build
 - Upgrade to the fat load
- If you are upgrading to a software version 6.0.0 or above, you must be on a load that supports the extended load format. All versions of software 6.0.0 or above support extended loads. You should perform the upgrade in two steps:
 - Upgrade to a restricted load of the same build
 - Upgrade to the extended load
- The MAX 6000 does not have extended or restricted loads.
- After you have upgraded your system to version 6.0.0 or above, you do not need to use a restricted load to upgrade.
- You can upgrade to a thin load or a restricted load from any version of software.
- If you are upgrading from software version 4.6C or earlier to software version 5.0A or later, see “Upgrading system software from versions earlier than 4.6C to version 5.0A or above” on page C-11 for important information before you start.

Table C-1 explains where to find the information you need to upgrade your unit.

Table C-1. Ascend system software versions

Version you are upgrading to	Use the instructions in...
Standard load (4.6Ci18 or earlier and all 4.6Cp releases)	“Upgrading system software with a standard load” on page C-6.
Fat or thin load (4.6Ci19 to 5.0Aix and all 5.0Ap releases)	“Upgrading system software with a fat or thin load” on page C-7.

Table C-1. Ascend system software versions (continued)

Version you are upgrading to	Use the instructions in...
Extended load (6.0.0 or later)	“Upgrading system software with an extended load” on page C-9.

Guidelines for downgrading system software

The MAX expects a specific organization of the parameters in a configuration file. When you upgrade a MAX, you *can* restore a configuration that was saved on an older release. The MAX enters default values for parameters if the MAX supports a parameter that is not included in the configuration file.

When you downgrade to older versions of software, the configuration might not upload completely, because older software does not support the parameters that might be in configuration files from newer releases.

You must upload a configuration that was saved from the same version of software to make sure that the MAX receives a complete configuration. If you upload a configuration from a newer version of software, you should check all parameter values to verify they are configured accurately.

If you are downgrading system software, make sure that you have a configuration saved from a MAX running with the older software and that you have console access to the MAX. Then, proceed as follows:

- 1 Use TFTP to load the system software.
- 2 Enter FCLEAR which clears the MAX unit’s flash memory.
- 3 Enter NVRAMCLEAR which clears the MAX unit’s main configuration and resets the MAX.

The MAX restarts and loads the older version of system software.

- 4 When the MAX is up, manually enter basic information being sure to include at least IP address, subnet mask, and default gateway to the Ethernet interface.

After entering you must be able to telnet to the MAX.

- 5 From the MAX unit’s VT100 interface, access the diagnostics monitor by typing the following characters in rapid succession:

Esc [Esc =

Or, press Ctrl-D to invoke the DO menu and select D=Diagnostics.

- 6 At the > prompt, use the TRestore command to restore the configuration as in the following example:

```
> trestore tftp-server router1.cfg
```

This restores the configuration named `router1.cfg` from the TFTP home directory of the server named `tftp-server`. This file must exist and be readable.

- 7 At the > prompt, enter Exit to return to the VT100 interface.

Before you begin

Make sure you perform all the tasks explained in Table C-2 before upgrading your software.

Table C-2. Before upgrading

Task	Description
If necessary, activate a Security Profile that allows for field upgrade.	If you are not sure how, see the section about Security Profiles in your documentation.
Record all of the passwords you want to retain, and save your Ascend unit's current configuration to your computer's hard disk.	For security reasons, passwords are not written to configuration files created through the serial console. A configuration file created using the Tsave command, however, <i>does</i> contain the system passwords. You can restore the Tsave configuration file using the serial console. If you chose to save your configuration using the serial console, you will have to restore your passwords manually. Restoring passwords is explained in "Using the serial port to upgrade to a standard or a thin load" on page C-12.
Obtain the correct file, either by downloading it from the FTP server or by requesting it from Ascend technical support.	<p>To ensure that you load the correct software binary, you should check the load currently installed on your unit. To do so:</p> <ol style="list-style-type: none"> 1 Tab over to the 00-100 Sys Options window. 2 Press Enter to open the Sys Options menu. 3 Using the Down-Arrow key (or Ctrl- N), scroll down until you see a line similar to the following: Load: tb.m40 4 When upgrading, obtain the file with same name from the Ascend FTP site. <p>If your unit does not display the current load or you are unsure about which load to use, contact technical support.</p>
If you are upgrading to a fat load or an extended load for the first time, you must also obtain a thin load or a restricted load of the same build, if possible.	<p>For example, if you are upgrading a MAX 4000 to 5.0Ai13 fat load (such as tbim.m40), obtain a thin load of the same build (such as 5.0A tbim.m40).</p> <p>If you are upgrading to a MAX 6.0.0 extended load, obtain a 6.0.0 restricted load. Restricted loads are designated with an "r" in the load name. (For example rtbam.m40 is a restricted load). Note that after you have upgraded your system to version 6.0.0 or above, you do not need to use a restricted load to upgrade.</p> <p>Newer Pipeline 50 or 75 units do not have fat loads and no Pipeline units have extended or restricted loads. Refer to /pub/Software-Releases/Pipeline/Upgrade-Filenames.txt to determine if you have a new Pipeline 50 or 75 unit.</p>
If you are using TFTP, make sure you load the correct binaries into the TFTP home directory on the TFTP server.	You must use TFTP to upgrade to a fat load or an extended load.

Table C-2. Before upgrading (continued)

Task	Description
If you are using the serial port, make sure you have a reliable terminal emulation program, such as Procomm Plus.	<p>If you use the serial port, you can only upgrade to a standard or a thin load. Upgrading through the serial port is not recommended.</p> <p>If you use a Windows-based terminal emulator such as Windows Terminal or HyperTerminal, disable any screen savers or other programs or applications that could interrupt the file transfer. Failure to do so might cause the software upload to halt, and can render the Ascend unit unusable.</p>

Upgrading system software with a standard load

To upgrade system software with a standard load you can use either the serial port or TFTP. TFTP is the recommended method because it preserves your Ascend unit's configuration. If you want to use the serial port to upgrade, see "Using the serial port to upgrade to a standard or a thin load" on page C-12.

Using TFTP to upgrade to a standard load

To upgrade to a standard load using TFTP, you only have to enter a few commands. But you must enter them in the correct sequence, or you could lose the Ascend unit's configuration.

To upgrade to a standard load via TFTP:

- 1 Obtain the software version you want to upgrade to and place it in the TFTP server home directory.
- 2 From the Ascend unit's VT100 interface, access the diagnostics monitor by typing the following characters in rapid succession:

`ESC [ESC =`

Or, press Ctrl-D to invoke the DO menu and select D=Diagnostics.

- 3 At the > prompt, use the Tsave command to save your configuration as in the following example:

`> tsave tftp-server router1.cfg`

This saves the configuration of your unit to the file named `router1.cfg` in the TFTP home directory of the server named `tftp-server`. This file must already exist and be writable. Normally, TFTP upgrades save the configuration. Tsave is a precaution.



Caution: The file you save with the Tsave command contains all the passwords in clear text. You should move this file from the TFTP directory to a secure location after the upgrade procedure is complete.

- 4 Enter the following command:
`tloadcode hostname filename`
where *hostname* is the name or IP address of your TFTP server, and *filename* is the name of the system software on the server (relative to the TFTP home directory).
For example, the command:

```
tloadcode tftp-server t.m40
```

loads t.m40 into flash from the machine named tftp-server.



Caution: You must use the Fsave command immediately after executing the Tload command. Failure to do so can cause your Ascend unit to lose its configuration.

- 5 Enter the following command to save your configuration to flash memory:

```
fsave
```

- 6 Enter the following command:

```
nvrwmclear
```

After the Ascend unit clears NVRAM memory, it automatically resets.

This completes the upgrade.

Upgrading system software with a fat or thin load

Upgrading to a fat or thin load is not difficult, but you must be careful to follow the correct sequence of tasks.



Caution: If you are upgrading from software version 4.6C or earlier, see “Upgrading system software from versions earlier than 4.6C to version 5.0A or above” on page C-11 for important information before upgrading.

To upgrade your system:

- 1 Obtain the software version binary you want to upgrade to and place it in the TFTP server home directory. If you are upgrading to a fat load for the first time, also obtain a thin load of the same build and place it in the same directory. (See page “Definitions and terms” on page C-2 for an explanation of fat and thin loads.)



Caution: If possible, you should stay with the same build when upgrading. Loading a different build can cause your Ascend unit to lose all or part of its configuration. If this happens, you must restore your configuration from a backup.

For example, if you are upgrading a MAX 4000 to 5.0Ai13 fat load (such as tbim.m40), obtain a thin load of the same build (such as 5.0A tbim.m40).

Note: Newer Pipeline 50 or 75 units do not have fat or thin loads, you only need to load a single software binary. Refer to

/pub/Software-Releases/Pipeline/Upgrade-Filenames.txt on the Ascend FTP site to determine if you have a new Pipeline 50 or 75 unit.

- 2 From the Ascend unit’s VT100 interface, access the diagnostics monitor by typing the following characters in rapid succession:

```
Esc [ Esc =
```

Or, press Ctrl-D to invoke the DO menu and select D=Diagnostics.

- 3 At the > prompt, use the Tsave command to save your configuration, as in the following example:

```
> tsave tftp-server router1.cfg
```

This saves the configuration of your unit to the file named `router1.cfg` in the TFTP home directory of the server named `tftp-server`. This file must already exist and be writable. Normally, TFTP upgrades save the configuration. `Tsave` is a precaution.



Caution: The file you save with the `Tsave` command contains all the passwords in clear text. You should move this file from the TFTP directory to a secure location after the upgrade procedure is complete.

- 4 At the `>` prompt, enter:

```
> tloadcode hostname filename
```

where *hostname* is the name or IP address of your TFTP server, and *filename* is the name of the system software on the server (relative to the TFTP home directory).



Caution: If you are upgrading from a standard load to a fat load, make sure you load a thin load first.

For example, the command:

```
> tloadcode tftp-server t.m40
```

loads `t.m40` into flash from the machine named `tftp-server`.



Caution: You must use the `Fsave` command immediately after executing the `Tload` command. Failure to do so may cause your Ascend unit to lose its configuration.

- 5 Enter the following command to save your configuration to flash memory:

```
fsave
```

- 6 Enter the following command:

```
nvrwamclear
```

After the Ascend unit clears NVRAM memory, it automatically resets.

- 7 If you are upgrading to a thin load, you are done. If you are upgrading to a fat load, repeat the procedure, this time uploading the fat load binary.

After a successful upgrade, one of the following messages appears.

- If the load is thin:

```
UART initialized
thin load: inflate
.....
starting system...
```

- If the load is fat:

```
UART initialized
fat load: inflate
.....
starting system...
```

This completes the upgrade if you have no errors. If the upgrade is not successful, refer to "Recovering from a failed fat load upgrade" next.

Recovering from a failed fat load upgrade

If a fat load has a CRC (cyclic redundancy check) error, the following message appears:

```
UART initialized
fat load: bad CRC!!
forcing serial download at 57600 bps
please download a "thin" system...
```

Immediately after this message appears, the serial console speed is switched to 57600 bps, and the Ascend unit initiates an Xmodem serial download. To recover from this error and load the fat system, you must first load a thin system that is fat-load aware. Proceed as follows:

- 1 Activate your Xmodem software.
- 2 After you have finished loading the fat-aware thin load, reboot the unit.
- 3 Use the Tload command to download the fat load.

When you download a fat load, messages similar to the following appear on the diagnostics monitor screen:

```
> tload 192.168.1.82 tbam.m40
saving config to flash
.....
loading code from 192.168.1.82:69
file tbam.m40..
fat load part 1:
.....
.....
fat load part 2:
.....
```

The “fat load part *n*.” messages notify you when the first and second halves of the download begin.

Upgrading system software with an extended load

Your first upgrade to an extended load requires a preliminary procedure. You must first upgrade to a restricted load. A restricted load only contains essential system software and is not meant to be run in a working environment. It does not have full functionality and is to be used only to upload to an extended load.

After you have upgraded your system to version 6.0.0 or above, you do not need to use a restricted load to upgrade. Note that the MAX 6000 and Pipeline units do not have extended loads.



Warning: You cannot upgrade to extended loads using an IP over X.25 connection because restricted loads do not have X.25 support.



Caution: If you are upgrading from software version 4.6C or earlier, see “Upgrading system software from versions earlier than 4.6C to version 5.0A or above” on page C-11 for important information before upgrading.

To upgrade your system:

Upgrading System Software

Upgrading system software with an extended load

- 1 Obtain the software-version binary you want to upgrade to and place it in the TFTP server home directory.

Extended loads are denoted by an “F” preceding the build filename.

- 2 If this is the first time you have upgraded to an extended load, obtain a restricted load of the same build and place it in the directory.

For example, if you are upgrading a MAX 4000 to an extended load (such as `ftbam.m40`), obtain a MAX 4000 restricted load (such as `rtbam.m40`).

- 3 From the Ascend unit’s VT100 interface, access the diagnostics monitor by typing the following characters in rapid succession:

`ESC [ESC =`

Or, press Ctrl-D to invoke the DO menu, and select D=Diagnostics.

- 4 At the `>` prompt, use the `Tsave` command to save your configuration, as in the following example:

```
> tsave tftp-server router1.cfg
```

This saves the configuration of your unit to the file named `router1.cfg` in the TFTP home directory of the server named `tftp-server`. This file must already exist and be writable. Normally, TFTP upgrades save the configuration. `Tsave` is a precaution.



Caution: The file you save with the `Tsave` command contains all the passwords in clear text. You should move this file from the TFTP directory to a secure location after the upgrade procedure is complete.

- 5 At the `>` prompt, enter:

```
tloadcode hostname filename
```

where *hostname* is the name or IP address of your TFTP server, and *filename* is the name of the system software on the server (relative to the TFTP home directory).



Caution: If you want to upgrade your system for the first time to a software version 6.0.0 or later, you must first upgrade your system to a restricted load. Failure to do so can cause your Ascend unit to lose its configuration.

For example, the command:

```
tloadcode tftp-server rtbam.m40
```

loads the restricted load `rtbam.m40` into flash from the machine named `tftp-server`.



Caution: You must use the `Fsave` command immediately after executing the `Tload` command. Failure to do so can cause your Ascend unit to lose its configuration.

- 6 Enter the following command to save your configuration to flash memory:

```
fsave
```

- 7 Enter the following command:

```
nvramclear
```

After the Ascend unit clears NVRAM memory, it automatically resets.

If you have downloaded the extended load, the upgrade is complete.

If you have loaded a restricted load, your system boots up in restricted mode. Restricted mode only allows you to load software. You cannot change or save profiles. While in restricted mode, the Edit menu displays the following banner:

```
* * RESTRICTED MODE * * *
```

If your system boots up in restricted mode, perform the following steps:

- 1 At the > prompt, enter:

tloadcode *hostname filename*

where *hostname* is the name or IP address of your TFTP server, and *filename* is the name of the extended load of system software on the server (relative to the TFTP home directory).

For example, the command:

```
tloadcode tftp-server ftbam.m40
```

loads the extended load *ftbam.m40* into flash from the machine named *tftp-server*.

- 2 Enter the following command:

```
nvrampclear
```

After the Ascend unit clears NVRAM memory, it automatically resets.

Your system will then boot up with the new version of software running.

Upgrading system software from versions earlier than 4.6C to version 5.0A or above

If you are upgrading from software version 4.6C or earlier to version 5.0A or later, perform the upgrade in the following order:

- 1 Load version 4.6Ci18, following the procedure in “Upgrading system software with a standard load” on page C-6.
- 2 Load version 5.0A, following the procedure in “Upgrading system software with a fat or thin load” on page C-7.
- 3 Load version 5.0Aix or 6.0.0, following the procedure in “Upgrading system software with a fat or thin load” on page C-7 (for software versions 5.0Aix) or “Upgrading system software with an extended load” on page C-9 (for software version 6.0.0).



Caution: Failure to follow this procedure might cause your Ascend unit to lose or corrupt its configuration, and could render the unit unusable.

Using the serial port to upgrade to a standard or a thin load



Caution: Uploading system software via the serial console overwrites all existing profiles. Save your current profiles settings to your hard disk before you begin upgrading system software. After the upgrade, restore your profiles from the backup file you created. Since the backup file is readable text, you can reenter the settings through the Ascend unit's user interface. To avoid having existing profiles overwritten, use TFTP to upgrade your unit.



Caution: You cannot upload a fat load or an extended load using the serial port; it must be done using TFTP.

Upgrading through the serial port consists of the following general steps:

- Saving your configuration
- Uploading the software
- Restoring the configuration

Before you begin

Before upgrading your system through the serial port, make sure you have the following equipment and software:

- An IBM compatible PC or Macintosh with a serial port capable of connecting to the Ascend unit's Console port.
- A straight-through serial cable.
- Data communications software for your PC or Mac with XModem CRC/1K support (for example, Procomm Plus, HyperTerminal for PCs or ZTerm for the Mac).



Caution: If you use a Windows-based terminal emulator such as Windows Terminal or HyperTerminal, disable any screen savers or other programs or applications that could interrupt the file transfer. Failure to do so might cause the software upload to halt, and can render the Ascend unit unusable.

Saving your configuration

Before you start, verify that your terminal emulation program has a disk capture feature. Disk capture allows your emulator to capture to disk the ASCII characters it receives at its serial port. You should also verify that the data rate of your terminal emulation program is set to the same rate as the Term Rate parameter in the System Profile (Sys Config menu).

You can cancel the backup process at any time by pressing Ctrl-C.

To save the Pipeline configuration (except passwords) to disk:

- 1 Open the Sys Diag menu.
- 2 Select Save Config, and press Enter.

The following message appears:

Ready to download - type any key to start....

- 3 Turn on the Capture feature of your communications program, and supply a filename for the saved profiles. (Consult the documentation for your communications program if you have any questions about how to turn on the Capture feature.)
- 4 Press any key to start saving your configured profiles.
Rows of configuration information appear on the screen as the configuration file is downloaded to your hard disk. When the file has been saved, your communications program displays a message indicating the download is complete.
- 5 Turn off the Capture feature of your communications program.
- 6 Print a copy of your configured profiles for later reference.

You should examine the saved configuration file. Notice that some of the lines begin with START= and other lines begin with END=. A pair of these START/STOP lines and the block of data between them constitute a profile. If a parameter in a profile is set to its default value, it does not appear. In fact, you can have profiles with all parameters at their defaults, in which case the corresponding START/STOP blocks are empty. Make sure that there are no extra lines of text or characters either before START= or after END=. If there are, delete them. They could cause problems when you try to upload the file to the Ascend unit.

Uploading the software

To upload the software:

- 1 Type the following four-key sequence in rapid succession (press each key in the sequence shown, one after the other, as quickly as possible):
`Esc [Esc -`
(Press the escape key, the left bracket key, the escape key, and the minus key, in that order, in rapid succession.) The following string of Xmodem control characters appears:
`CKCKCKCK`
If you do not see these characters, you probably did not press the four-key sequence quickly enough. Try again. Most people use both hands and keep one finger on the escape key.
- 2 Use the Xmodem file-transfer protocol to send the system file to the Ascend unit.
Your communications program normally takes anywhere from 5 to 15 minutes to send the file to your Ascend unit. The time displayed on the screen does not represent real time. Do not worry if your communication program displays several “bad batch” messages. This is normal.

After the upload, the Ascend unit resets. Upon completion of the self-test, the Ascend unit’s initial menu appears in the Edit window with all parameters set to default values. This completes the upgrade.

If the upload fails during the transfer, try downloading another copy of the binary image from the Ascend FTP server and re-loading the code to the Ascend unit. If you still have problems, contact Ascend technical support for assistance.

Restoring the configuration

Under certain circumstances, the serial-port method might not completely restore your configuration. You should therefore verify that your configuration was properly restored every time you use this method. If you have many profiles and passwords, you should consider using

TFTP to upgrade your software. (See “Using TFTP to upgrade to a standard load” on page C-6.)

To restore the configuration, you must have administrative privileges that include Field Service (such as the Full Access Profile, for example). You use the Restore Cfg command to restore a full configuration that you saved by using the Save Cfg command, or to upload more specific configuration information obtained from Ascend (for example, a single filter stored in a special configuration file).

To load configuration information through the serial port

- 1 From the Ascend unit's VT100 interface, access the diagnostics monitor by typing the following characters in rapid succession:

```
Esc [ Esc =
```

Or, press Ctrl-D to invoke the DO menu, and select D=Diagnostics.

- 2 At the > prompt, enter the Fclear command:

```
> fclear
```

- 3 At the > prompt, enter the NVRAMClear command:

```
> nvramclear
```

This causes the system to reset. When it comes back up, proceed with restoring your configuration.

- 4 Enter **quit** to exit the Diagnostic interface.

- 5 Open the Sys Diag menu.

- 6 Select Restore Cfg, and press Enter.

The following message appears:

```
Waiting for upload data...
```

- 7 Use the Send ASCII File feature of the communications software to send the configuration file to the unit. (If you have any questions about how to send an ASCII file, consult the documentation for your communications program.)

When the restore has been completed, the following message appears:

```
Restore complete - type any key to return to menu
```

- 8 Press any key to return to the configuration menus.

- 9 Reset the Ascend unit, by selecting System > Sys Diag > Sys Reset and confirming the reset.

Restoring passwords

For security reasons, passwords are not written to configuration files created through the serial console. A configuration file created using the Tsave command, however, *does* contain the system passwords. You can restore the Tsave configuration file using the serial console.

After upgrading you may have to re-enter all the passwords on your system. If you edit your saved configuration file, however, and enter passwords in the appropriate fields (by replacing the word *SECURE* in each instance), these passwords will be restored. But note that if you do choose to edit your configuration file, you must save it as text only or you will not be able to load it into your unit.

If you restored a complete configuration, the passwords used in your Security profiles have been wiped out. To reset them:

- 1 Press Ctrl-D to invoke the DO menu, select Password, and choose the Full Access profile.
- 2 When you are prompted to enter the password, press Enter (the null password).
After you have restored your privileges by entering the null password, you should immediately open the Connection profiles, Security profiles, and Ethernet profile (Mod Config menu), and reset the passwords to their previous values.

Changing to system software that does not support V.90

If the software version on the MAX supports Rockwell V.90 code, the default value for the Ethernet > Mod Config > TService Options > MDM Modulation parameter is V.90. If you downgrade to a software version on the MAX that does not support Rockwell V.90 code, you must set the MDM Modulation parameter to either K56 or V.34. In general, if you downgrade to older software versions and need to restore a configuration, you must originally have saved the configuration from a MAX running the older version of code.

System messages

Table C-3 explains the messages that can appear during your upgrade.

Table C-3. System software messages

Message	Explanation
UART initialized fat load: bad CRC!! forcing serial download at 57600 bps please download a "thin" system...	The fat load has a CRC (cyclic redundancy check) error. Immediately after this message appears, the serial console speed is switched to 57600 bps, and the Ascend unit initiates an Xmodem serial download. Load a thin load that understands the fat load format, as explained in "Upgrading system software with a fat or thin load" on page C-7.
File tbam.m40 incompatible fat load format--discarding downloaded data	You attempted to upgrade to a fat load from a version of system software that does not understand the fat load format. You must first load a thin load that is fat load aware, as explained in "Upgrading system software with a fat or thin load" on page C-7.
This load has no platform identifier. Proceed with caution.	This message can occur if you are running software version 5.0Ai11 or later and you load an earlier incremental or patch release onto your system. The message indicates that Tloadcode cannot determine which platform the code is intended for. If you are using the correct software version, you can ignore this message.

Table C-3. System software messages (continued)

Message	Explanation
This load appears not to support your network interface. Download aborted. Use 'tloadcode -f' to force.	Indicates you are attempting to load a version of code intended for a different network interface (for example, loading MAX 4000 T1 software onto a MAX 4000 E1 unit).
This load appears to be for another platform. Download aborted. Use 'tloadcode -f' to force.	Indicates you are attempting to load a version of code onto a platform for which it is not intended (for example, loading MAX 4000 software onto a MAX 2000). This is not recommended
UART initialized fat load: inflate starting system...	Indicates you have successfully loaded a fat load.
UART initialized extended load: inflate essential .++...... invalid CRC!! entering restricted mode starting system...	Indicates the extended load has failed and that your system is being brought up in restricted mode. You must reload the software as explained in “Upgrading system software with an extended load” on page C-9.
UART initialized extended load: inflate essential .++...... . invalid length!! entering restricted mode starting system...	Indicates the extended load has failed and that your system is being brought up in restricted mode. You must reload the software as explained in “Upgrading system software with an extended load” on page C-9.
UART initialized extended load: inflate essential .++...... inflate expendable..... starting system...	Indicates you have successfully loaded an extended load.
UART initialized thin load: inflate starting system...	Indicates you have successfully loaded a thin load.

Machine Interface Format (MIF)

This chapter covers the following topics:

What is MIF?	D-1
How to access MIF	D-2
MIF addresses	D-3
MIF commands	D-5
Lexical sequence of MIF types	D-8
Command line basics	D-31
Editor basics	D-31

What is MIF?

Machine Interface Format (MIF) is an Ascend-specific language that provides an alternative configuration interface for Ascend units. You can use a command line or write a MIF program that sets Ascend parameters, rather than use the configuration menus to change one parameter after another. MIF programs provide a batch-processing method of changing a configuration or performing a series of actions.

Following are the primary features of MIF:

- Command-line driven.
- Controlling computer does not have to process asynchronous events.
- Controlling computer can enable asynchronous event reporting

How to access MIF

You can access MIF with the Use MIF command, the MIF escape sequence, or a transfer command.

Use MIF command

You can start MIF from the VT100 configuration menus by selecting the Use MIF command in the Sys Diag menu:

```
00-200 Sys Diag
00-201 Restore Cfg
00-202 Save Cfg
>00-203 Use MIF
00-204 Sys Reset
00-205 Term Serv
00-206 Upd Rem Cfg
```

The MIF interface replaces the configuration menus. You can then start entering MIF commands interactively, or download an ASCII file containing a series of MIF commands by using the appropriate transfer command (such as Send Text) in your VT100 emulation program.

MIF escape sequence

You can start MIF from any location in the configuration menus by typing the following four-key sequence in rapid succession (press each key in the sequence shown, one after the other, as quickly as possible):

```
ESC [ ESC !
```

Transfer command

You can start MIF by using the appropriate transfer command (such as Send Text) in your VT100 emulation program, but that the first line in the emulation program must contain the MIF escape sequence ESC [ESC !.

MIF addresses

Each profile, parameter, DO menu item, or status window is called an *addressable entity*. Each of these entities has a unique address.

A *full address* specifies a specific entity and consists of the full syntax shown below. A *partial address* does not include the *name* attribute.

Addresses have the following syntax:

slot and port.type.entry.name

For example:

103.DIAL.1.Data Svc

The address syntax includes the following elements:

Syntax element	Description
slot	One-digit slot number of the addressed entity (1 in the example). For most addresses, the slot number of the addressed entity is identical to the first digit of the menu number in the standard user interface.
port	Two-digit port number of the addressed entity (03 in the preceding example). For most addresses, the port number of the addressed entity is identical to the second and third digits of the menu number of the standard user interface.

Syntax element	Description
type	<p>This attribute contains the type of the addressed entity. The defined types are listed below, and are described in detail in “Lexical sequence of MIF types” on page D-8.</p> <ul style="list-style-type: none">• ALARM—Line alarm indications• BRIDGE—Bridge Adrs profile• CONN—Answer and Connection profiles• DEST—Destination profiles• DIAG—System diagnostics• DIAGN—Line diagnostics• DIAL—Call profiles• DO—DO Command menu• ETHERNET—Ethernet profile• FILT—Filter profiles• FR—Frame Relay profiles• HOST2—Host-Interface profile for Host/Dual modules• HOST4—Host-Interface profile for Host/Quad modules• HOST6—Host-Interface profile for Host/6 modules• LINE—Line profiles• LMODEM—LAN Modem profiles• LOOP—Port diagnostics (loopback)• PORT—Port profile• ROUTE—Route profiles• SEC—Security profiles• STAT—Status menu• SWAN—Serial WAN profile (currently not supported)• SYS—System profile• TRAP—SNMP Traps profiles• V110—V.110 profiles
entry	<p>Identifies a specific entity, such as a profile. If there is only one entity of a particular type, as in the case of the Port profile of the DO menu, the entity’s entry is a zero. When a type includes more than one entity, as in the case of Line N profiles, 0 (zero) is the current (default) entry, 1 is the first entry saved after the current entry, and so on. An address without an entry denotes the factor-default type profile.</p>
name	<p>Identifies the name of the addressed entity.</p>

MIF commands

Use the SET command to set the value attribute. Use the GET and NEXT commands to retrieve current information in the value attribute. Following are the supported MIF commands:

- LOAD <partial address>
- SAVE <partial address>
- GET <full or edit address>
- NEXT <address>
- SET <full or edit address>=<value>

For a definition of the edit address, see “Loading and saving entities” on page D-5

MIF responses

The LOAD and SAVE commands respond with a prompt (:) if the command is valid:
:

The GET and NEXT commands return a value in the following syntax:

+ <address>=<value>

For example,

```
: GET 201.DIAL.16.Call Type  
+ 201.DIAL.16.Call Type=AIM
```

The plus-sign indicates a returned value or an error. Invalid commands return the following message:

+ ERROR

The SET command also responds with a prompt (:). When it is applied to a status or alarm entity, however, it creates a trap which is reported in the following syntax:

- <address>=<value>

For example:

```
: SET 100.ALARM.0.alarm=20  
- 100.ALARM.0.alarm=LA  
:
```

The minus-sign indicates an asynchronous report. For more information, see “MIF traps and asynchronous reports” on page D-7.

Loading and saving entities

Only entities (such as profiles) that have been loaded into the edit area can be modified. Because there is only one edit area and it can have only one profile loaded into it at a time, commands that operate on entities in the edit area can use another version of the address called the *edit address*. The edit address has the following format:

<name>

The LOAD commands loads a profile into the edit area. It uses the following syntax:

LOAD <partial address>

For example,

: LOAD 201.PORT.0

When the profile has been loaded into the edit area, you can modify it, using only the SET command, for example:

: SET Port Name=Chicago #1

When you have finished modifying the profile, save it. The SAVE command copies the profile in the edit area to the specified address. It uses the following syntax:

SAVE <partial address>

For example,

: SAVE 201.PORT.0

Getting an entity's current value

If an entity (profile) has not already been loaded into the edit area by using the LOAD command, the GET command loads the profile and then extracts the requested value.

The GET command returns the value of the addressed attribute. When the addressed attribute is a parameter in the standard user interface, the value returned by GET is a parameter value. When the addressed attribute is a status window in the standard user interface, all lines in the status window are returned.

The GET command uses the following syntax:

GET <full or edit address>

For example, the following GET command uses a full address:

: GET 201.DIAL.16.Call Type
+ 201.DIAL.16.Call Type=AIM

Or, if the profile has already been loaded into the edit area, use the following syntax:

: LOAD 201.DIAL.16
: GET Call Type
+ 201.DIAL.16.Call Type=AIM

Getting the address and value of the next entity

The NEXT command returns the address and value of the attribute with the next address. Addresses, though composed of both textual and numeric components, are ordered as if each component was a digit of a decimal number. The sequence is:

<name> within <entry>
<entry> within <type>
<type> within <port>
<port> within <slot>

The NEXT command uses the following syntax:

NEXT <full address>

For example:

```
: NEXT 000.DIAL.1.Data Svc
+ 000.DIAL.1.Base Ch Count=1
```

Modifying parameter values

If an entity (profile) has not already been loaded into the edit area by using the LOAD command, the SET command loads the profile and then replaces the specified value.

The SET command replaces the current value of the entity with the <value> given in the command. In this context, it uses the following syntax:

SET <edit address>=<value>

When the address refers to a parameter in a profile, the SET command accepts only an edit address. So, the profile must already be loaded into the edit area. For example:

```
: LOAD 201.PORT.0
: SET Port Name=Chicago #1
: SAVE 201.PORT.0
:
```

Note: The SET command does not replace the parameter's value until you use the SAVE command.

To SET an enumerated parameter (such as Yes or No), the <value> must be identical to the enumerated value in the standard Ascend user interface. However, the specified value is not case-sensitive. For example, you can use either one of these commands:

```
: SET 100.DIAGN.0.Clr Err1=Yes
: SET 100.DIAGN.0.Clr Err1=yes
```

You can also apply the SET command to status and alarm entities, as described in the next section.

MIF traps and asynchronous reports

When you apply the SET command to a status window or an alarm, it enables asynchronous reports (traps) of the requested status screen or alarms. In this context, the SET command uses the following syntax:

SET <full address>=<value>

The <value> established in the SET command sets the time period in seconds between status checks. For example,

```
: SET 100.ALARM.0.alarm=20
- 100.ALARM.0.alarm=LA
:
```

Reports are generated only whenever a change is detected in the requested status window components or whenever an alarm occurs. If the <value> in the SET command is 0, asynchronous reports are not generated.

Lexical sequence of MIF types

This section lists each MIF type with its allowed values. It uses the conventions and formats described next.

Types are listed alphabetically. The following format is used:

<address>=<value>

For example, the Remote Mgmt type can be set to Yes or No. It appears in the system profile (SYS) at the following MIF address:

000.SYS.0.Remote Mgmt

So, it is listed in this section like the following:

000.SYS.0.Remote Mgmt=Yes,No

Comments are set off by parentheses(), as shown below for the Clr Err1 type that can be SET but not read:

100.DIAGN.0.Clr Err1=Yes (write only)

If the type does not have enumerated values, the type of values it can take are given in *italics* as in the following two examples:

000.SYS.0.Name=*text*

000.SYS.0.Status 1=*XN-n00* (menu number for a status screen)

Note: The menu numbering shown in this section reflects the standard MAX whose base system slot 2 has a Host/Quad module. This differs from the MAX 4000, whose base system slot 2 has a Net/T1 module. Furthermore, the base system of the MAX 4000 has slot 9 (the Ethernet module), slot A (an Ether-Data module), and slot B (a Serial WAN module), while slots 9, A, and B do not exist on the standard MAX.

The slot and port of most addresses are given explicitly; however, in some cases they are represented by *spp*, where *s* is the slot number and *pp* is the port number. For example, either one of the following two commands may be used:

000.SYS.0.Name=*text*

spp.SYS.0.Name=*text*

ALARM

For T1/PRI and E1/PRI models:

s00.ALARM.n.alarm= (write)

DS, RA, YA, 1S, DF, LA (read)

For BRI models:

100.ALARM.n.alarm= (write)

-, X, ., P, M, D (read) (dash, X, period, P, M, D)

For Switched-56 models:

100.ALARM.*n*.alarm= (write)
– , X , . , A (read) (dash, X, period, A)

Note:

- Do not exceed 32,000 seconds when using SET to write to these addresses
- *s00*.ALARM.*n*...
s = 1 (Multiband Plus and Pipeline 100/400)
s = 1 or slot number of a T1/PRI or E1/PRI module (MAX)
n = the line number minus 1. Namely, *n*=0 is line #1, *n*=1 is line #2, etc.
- Alarm definitions for T1/PRI lines are as follows:
 - DS (Line disabled)
 - RA (Red Alarm, loss of sync)
 - YA (Yellow Alarm)
 - 1S (AIS, Blue alarm)
 - DF (No D channel)
 - LA (Link Active)
- Alarm definitions for BRI/Switched 56 lines are as follows:
 - – (Line disabled)
 - X (No physical link)
 - P (Link active, BRI point-to-point)
 - M (Link active, BRI multipoint 1)
 - D (Line active, BRI multipoint 2)
 - A (Line active, switched 56)

For example:

Report status of the “100.ALARM.0.alarm” entity every 20 seconds if change occurs:

: SET 100.ALARM.0.alarm=20
- 100.ALARM.0.alarm=LA
:

BRIDGE

s00.BRIDGE.*n*.Enet Adrs=*12-digit hexadecimal string*
.Net Adrs=*dotted decimal format*
.Connection #=*2-digit decimal string*

Note:

- This type applies to MAX equipped with the Ethernet module and Pipeline 100/400 only. It does not apply to Multiband Plus.
- *s00*.BRIDGE.*n*...
s = slot into which the Ethernet card is installed (MAX)

$s = 2$ (Pipeline 100/400) $n = 0$ to 98**CONN**

```

s00.CONN.n.Force 56=Yes,No (n=0)
.Profile Reqd=Yes,No (n=0)
.CLID Auth=Ignore,Prefer,Force (n=0)
.Assign Adrs=Yes,No (n=0)
.Encaps...MPP=Yes,No(n=0)
.Encaps...PPP=Yes,No(n=0)
.Encaps...COMB=Yes,No(n=0)
.Encaps...FR=Yes,No(n=0)
.Encaps...EU-RAW=Yes,No(n=0)
.Encaps...EU-UI=Yes,No(n=0)
.Encaps...TCP-CLEAR=Yes,No(n=0)
.Encaps...V.120=Yes,No(n=0)
.PPP options...Route IP=Yes,No (n=0)
.PPP options...Bridge=Yes,No (n=0)
.PPP options...Recv Auth=PAP,CHAP,Either,None (n=0)
.PPP options...MRU=number (n=0)
.PPP options...LQM=Yes,No (n=0)
.PPP options...LQM Min=number (n=0)
.PPP options...LQM Max=number (n=0)
.PPP options...Link Comp=Stac,None (n=0)
.PPP options...VJ Comp=Yes,No (n=0)
.PPP options...Dyn Alg=Constant,Linear,Quadratic (n=0)
.PPP options...Sec History=number (n=0)
.PPP options...Add Pers=number (n=0)
.PPP options...Sub Pers=number (n=0)
.PPP options...Min Ch Count=number (n=0)
.PPP options...Max Ch Count=number (n=0)
.PPP options...Target Util=number (n=0)
.PPP options...Idle Pct=number (n=0)
.COMB options...Password Reqd=Yes,No (n=0)
.COMB options...Interval=number (n=0)
.COMB options...Compression=Yes,No (n=0)

.Station=text (n=1 to 31)
.Active=Yes,No (n=1 to 31)
.Encaps=MPP,PPP,COMB,FR,EU-RAW,EU-UI,TCP-CLEAR (n=1 to 31)
.PRI # Type=Unknown,Intl,National,Local,Abbrev (n=1 to 31)
.Dial #=phone number (n=1 to 31)
.Calling #=phone number (n=1 to 31)
.Route IP=Yes,No (n=1 to 31)

```

.Route IPX=Yes,No (n=1 to 31)
.Bridge=Yes,No (n=1 to 31)
.Dial Brdcast=Yes,No (n=1 to 31)
.Encaps options...Send Auth=PAP,PAP-TOKEN,PAP-TOKEN-CHAP, CACHE-TOKEN, CHAP,None (n=1 to 31)
.Encaps options...Send PW=*text* (n=1 to 31)
.Encaps options...Aux Send PW=*text* (n=1 to 31)
.Encaps options...Recv PW=*text* (n=1 to 31)
.Encaps options...Base Ch Count=*number* (n=1 to 31)
.Encaps options...Min Ch Count=*number* (n=1 to 31)
.Encaps options...Max Ch Count=*number* (n=1 to 31)
.Encaps options...Inc Ch Count=*number* (n=1 to 31)
.Encaps options...Dec Ch Count=*number* (n=1 to 31)
.Encaps options...MRU=*number* (n=1 to 31)
.Encaps options...LQM=Yes,No (n=1 to 31)
.Encaps options...LQM Min=*number* (n=1 to 31)
.Encaps options...LQM Max=*number* (n=1 to 31)
.Encaps options...Link Comp=Stac,None (n=1 to 31)
.Encaps options...VJ Comp=Yes,No (n=1 to 31)
.Encaps options...Dyn Alg=Constant,Linear,Quadratic(n=1 to 31)
.Encaps options...Sec History=*number* (n=1 to 31)
.Encaps options...Add Pers=*number* (n=1 to 31)
.Encaps options...Sub Pers=*number* (n=1 to 31)
.Encaps options...Target Util=*number* (n=1 to 31)
.Encaps options...Idle Pct=*number* (n=1 to 31)
.Encaps options...Password Req=Yes,No (n=1 to 31)
.Encaps options...Interval=*number* (n=1 to 31)
.Encaps options...Compression=Yes,No (n=1 to 31)
.Encaps options...FR Prof=*text* (n=1 to 31)
.Encaps options...DLCI=*number* (n=1 to 31)
.Encaps options...Login Host=*text* (n=1 to 31)
.Encaps options...Login Port=*number* or *dotted decimal format* (n=1 to 31)
.Ip options...LAN Adrs=*dotted decimal format/subnet mask* (n=1 to 31)
.Ip options...WAN Alias=*dotted decimal format* (n=1 to 31)
.Ip options...Metric=*number* (n=1 to 31)
.Ip options...Private=Yes,No (n=1 to 31)
.Ip options...RIP=Off,Send,Recv,Both (n=1 to 31)
.Ip options...Pool=*number* (n=1 to 31)
.Ipx options...Dial Query=Yes,No (n=1 to 31)
.Ipx options...IPX ENet#=*number* (n=1 to 31)
.Ipx options...IPX Alias=*number* (n=1 to 31)
.Ipx options...Handle IPX=None,Client,Server (n=1 to 31)
.Ipx options...Netware t/o=*number* (n=1 to 31)

```
.Session options...RIP=Off,Send,Recv,Both (n=0 to 31)
.Session options...Data Filter=number (n=0 to 31)
.Session options...Call Filter=number (n=0 to 31)
.Session options...Idle=number (n=0 to 31)
.Session options...Preempt=number (n=0 to 31)
.Session options...Secondary=text (n=1 to 31) (Pipeline 25/50)
.Session options...Backup=text (n=1 to 31)
.Session options...IP Direct=dotted decimal format
.Session options...FR Direct=Yes,No (n=1 to 31)
.Session options...FR Prof=text (n=1 to 31)
.Session options...FR DLCI=number (n=1 to 31)
.Telco options...AnsOrig=Both,Ans Only,Call Only (n=1 to 31)
.Telco options...Callback=Yes,No (n=1 to 31)
.Telco options...Call Type=Switched, Nailed, Nailed/MP+ (n=1
to 31)
.Telco options...Group=number (n=1 to 31)
.Telco options...FT1 Caller=Yes,No
.Telco options...Data Svc=Voice,56KR,56K,64K,384KR,
384K,1536K,1536KR,128K,192K,256K,320K,448K,
512K,576K,640K,704K,768K,832K,896K,960K,1024K,
1088K,1152K,1216K,1280K,1344K,1408K,1472K (n=1 to 31)
.Telco options...Force 56=Yes,No (n=1 to 31)
.Telco options...Bill #=number (n=1 to 31)
.Telco options...Call-by-Call=number (n=1 to 31)
.Telco options...Transit #=number (n=1 to 31)
```

Note:

- This type applies to the MAX equipped with the Ethernet module and the Pipeline 100/400 only. It does not apply to Multiband Plus.
- *s00.CONN.n.PRI* # Type is a T1/E1/PRI parameter only
- *s00.CONN.n.Telco Options...Bill #* is a BRI, T1/PRI parameter only
- *s00.CONN.n.Telco Options...Call-by-Call* is a T1/PRI parameter only
- *s00.CONN.n.Telco Options...Transit #* is a T1/PRI or E1/PRI parameter
- *s00.CONN.n...*
s = slot into which the Ethernet card is installed (MAX)
s = 2 (Pipeline 100/400)
n = 1 to 31
- *s00.CONN.n.Data Svc* for -SW56 models must = 56K. Data Svc for -BRI models can be Voice,56KR,56K,64K only

DEST

For T1/PRI models only:

```
000.DEST.n.Name=text
.Option=1st Avail,1st Active,Any
```

```
.Dial 1#=phone number
.Call-by-Call 1=number
.Dial 2#=phone number
.Call-by-Call 2=number
.Dial 3#=phone number
.Call-by-Call 3=number
.Dial 4#=phone number
.Call-by-Call 4=number
.Dial 5#=phone number
.Call-by-Call 5=number
.Dial 6#=phone number
.Call-by-Call 6=number
```

Note:

- does not apply to Pipeline 100/400
- 000.DEST.*n*...
n = 1 to 31
- 000.DEST .*n*.Call-by-Call are PRI parameters only

DIAG

```
000.DIAG.0.Sys Reset=Yes (write only)
000.DIAG.0.UPD REM CFG=Yes (write only)
```

Note:

- The UPD REM CFG command is available only for MAX and Pipeline 100/400.

For example:

```
: SET 000.DIAG.0.Sys Reset=No
+ ERROR
: SET 000.DIAG.0.Sys Reset=Yes
(unit resets!)
```

DIAGN

```
s00.DIAGN.0.Line LB1=Yes,No
.Line LB2=Yes,No
.Clr Err1=Yes (write only)
.Clr Perf1=Yes (write only)
.Clr Err2=Yes (write only)
.Clr Perf2=Yes (write only)
```

Note:

- This type applies to MAX-T1/PRI and Multiband Plus-T1/PRI only. It does not apply to E1/PRI, BRI, or SW56 models or to Pipeline 100/400.
- s00.DIAGN.*n*...
s = 1 (Multiband Plus)

s = 1 or slot number of a T1/PRI or E1/PRI module (MAX)

For example:

```
: SET 100.DIAGN.0.LB1=No
:
```

DIAL

```
spp .DIAL .n .Name=text
     .Dial  #=phone number
     .Call Type=AIM,BONDING,1 Chnl,2 Chnl,FT1,Ft1-AIM,FT1-B&O
     .Call Mgm=Manual,Static,Dynamic,Delta,Mode 1,Mode 2
     .Data Svc=Voice,56KR,56K,64K,384KR,384K,1536K,1536KR,
     128K,192K,256K,320K,448K,512K,576K,640K,704K,
     768K,832K,896K,960K,1024K,1088K,1152K,1216K, 1280K,1344K,1408K,1472K
     .Force 56K=Yes,No
     .Base Ch Count=number
     .Inc Ch Count=number
     .Dec Ch Count=number
     .Call-by-Call=number (T1/PRI only)
     .Bill  #=number (T1/PRI only)
     .Auto-BERT=Off,15 sec,30 sec,60 sec,90 sec,120 sec
     .Bit Inversion=Yes,No
     .Fail Action=Disc,Reduce,Retry
     .PRI  # Type=Unknown,Intl,National,Local,Abbrev (T1/PRI only)
     .Transit #=number (T1/PRI only)
     .Group=number
     .FT1 Caller=Yes,No
     .B&O Restore=number (n=30 to 30000)
     .Flag Idle=Yes,No
     .Dyn Alg=Constant,Linear,Quadratic
     .Sec History=number
     .Add Pers=number
     .Sub Pers=number
     .Time Period 1...Activ=Disabled,Enabled,Shutdown
     .Time Period 1...Beg Time=hh:mm:ss
     .Time Period 1...Min Ch Cnt=number
     .Time Period 1...Max Ch Cnt=number
     .Time Period 1...Target Util=number
     .Time Period 2...Activ=Disabled,Enabled,Shutdown
     .Time Period 2...Beg Time=hh:mm:ss
     .Time Period 2...Min Ch Cnt=number
     .Time Period 2...Max Ch Cnt=number
     .Time Period 2...Target Util=number
     .Time Period 3...Activ=Disabled,Enabled,Shutdown
     .Time Period 3...Beg Time=hh:mm:ss
```

```
.Time Period 3...Min Ch Cnt=number
.Time Period 3...Max Ch Cnt=number
.Time Period 3...Target Util=number
.Time Period 4...Activ=Disabled,Enabled,Shutdown
.Time Period 4...Beg Time=hh:mm:ss
.Time Period 4...Min Ch Cnt=number
.Time Period 4...Max Ch Cnt=number
.Time Period 4...Target Util=number
```

Note:

- This type applies to MAX and Multiband Plus only. It does not apply to Pipeline 100/400.
- *spp.DIAL.n...*(Multiband Plus)
s = 0 or 2
when *s*=0, *pp* = 00
when *spp*=000, *n* = 0 through 15 (These are shared Call Profiles 17 to 32)
when *s*=2, *pp* = 01 through last serial host port
when *spp* is not 000, *n* = 0 through 16 (If *n*=0, this is the current Call Profile of serial host port *pp*. If *n* is not 0, these are stored Call Profiles 1 to 31.)
- *spp.DIAL.n...*(MAX)
s = 0 or 2 or slot number of a Host/Dual or Host/6 module
when *s*=0, *pp* = 00
when *spp*=000, *n* = 0 through 15 (These shared Call Profiles 17 to 32)
when *s*=2 or slot number, *pp* = 01 through last serial host port
when *spp* is not 000, *n* = 0 through 16 (If *n*=0, this is the current Call Profile of serial host port *pp*. If *n* is not 0, these are stored Call Profiles 1 to 31.)
- *spp.DIAL.n.Data Svc* for -SW56 models must = 56K
spp.DIAL.n.Data Svc for -BRI models can be Voice,56KR,56K,64K only
- *s00.DIAL.n.PRI # Type* is a T1/E1/PRI parameter only
- *s00.DIAL.n.Bill #* is a T1/PRI parameter only
- *s00.DIAL.n.Call-by-Call* is a T1/PRI parameter only
- *s00.DIAL.n.Transit #* is a T1/PRI only

For example:

```
: NEXT 000.DIAL.1.Data Svc
+ 000.DIAL.1.Base Ch Count=1
: GET 201.DIAL.16.Call Type
+ 201.DIAL.16.Call Type=AIM
:
```

DO

```
spp.DO.0.Dial=Yes ,No (read) Yes (write)
.Hang Up=Yes ,No (read) Yes (write)
.Answer=Yes ,No (read) Yes (write)
.Extend BW=Yes ,No (read) Yes (write)
.Contract BW=Yes ,No (read) Yes (write)
```

```
.Beg/End Rem LB=Yes ,No (read) Toggle (write)
.Beg/End BERT=Yes ,No (read) Toggle (write)
.Resynchronize=Yes ,No (read) Yes (write)
```

Note:

These commands apply only during certain conditions. For example, *spp.DO.0.Hang Up* applies only when the object specified has a call online, while *spp.DO.0.Dial* applies only to objects not having a call online. See the *MAX Reference Guide* for details on each of the DO commands.

- *spp.DO...(Multiband Plus)*
s = 2
pp = 01 through last serial host port
- *spp.DO...(Pipeline 100/400)*
spp = 200
- *spp.DO...(MAX)*
s = 2 or the slot number of a serial host or Ethernet module when *s*=2 or the slot number of a serial host module,
pp = 01 through last serial host port when *s*= the slot number of the Ethernet module, *pp* = 00
- The <value> Toggle in a SET (write) command changes the state of the addressed entity from its current state to another state, i.e., from Yes to No or from No to Yes. The SET command applied to a DO <address> causes the DO action to be invoked if active.
- The GET (read) command returns the <value> YES or NO when applied to a DO <address>. YES is returned if the item can be invoked at the time of the request (is active) and NO is returned otherwise.
- DO P (password), DO S (save), and DO L (load) are not available.

For example:

```
: NEXT 201.D0.0.Extend
+ 201.D0.0.Contract=Yes
:
```

ETHERNET

The following applies to Pipeline 100/400s and Ethernet-equipped MAX units.

```
s00.ETHERNET.0.Module Name=text (MAX only)
.Ether options...IP Adrs=dotted decimal format/subnet mask
.Ether options...2nd Adrs=dotted decimal format/subnet mask
.Ether options...RIP=Off,Send,Recv,Both
.Ether options...Ignore Def Rt=Yes,No
.Ether options...Proxy Mode=Off,Inactive,Active,Always
.Ether options...Filter=number
.Ether options...IPX Frame=802.3,802.2,SNAP,ENET II
.Ether options...IPX Net#=number
.WAN options...Dial Plan=Trunk Grp,Extended (MAX only)
.WAN options...Ans 1#=Phone number (MAX only)
```


.WAN options...Ans 2#=*Phone number* (MAX only)
.WAN options...Ans 3#=*Phone number* (MAX only)
.WAN options...Ans 4#=*Phone number* (MAX only)
.WAN options...Pool Start #1=*dotted decimal format*
.WAN options...Pool Count #1=*number*
.WAN options...Pool Start #2=*dotted decimal format*
.WAN options...Pool Count #2=*number*
.WAN options...Pool Only=Yes,No
.SNMP options...Read Comm=*text*
.SNMP options...R/W Comm=*text*
.Tserv options...TS Enabled=Yes,No
.Tserv options...Passwd=*text*
.Tserv options...Banner=*text*
.Tserv options...Prompt=*text*
.Tserv options...Term Type=*text*
.Tserv options...PPP=Yes,No
.Tserv options...SLIP=Yes,No
.Tserv options...SLIP BOOTP=Yes,No
.Tserv options...V42/MNP=Yes,No
.Tserv options...Telnet=Yes,No
.Tserv options...Def Telnet=Yes,No
.Tserv options...Clear Call=Yes,No
.Tserv options...Binary Mode=Yes,No
.Tserv options...Initial Scrn=Cmd,Menu
.Tserv options...Toggle Scrn=Yes,No
.Tserv options...Security=None,Partial,Full
.Tserv options...3rd Prompt=*text*
.Tserv options...Remote Conf=Yes,No
.Tserv options...Host #1 Addr=*dotted decimal format*
.Tserv options...Host #1 Text=*text*
.Tserv options...Host #2 Addr=*dotted decimal format*
.Tserv options...Host #2 Text=*text*
.Tserv options...Host #3 Addr=*dotted decimal format*
.Tserv options...Host #3 Text=*text*
.Tserv options...Host #4 Addr=*dotted decimal format*
.Tserv options...Host #4 Text=*text*
.Tserv options...Immed Telnet=Yes,No
.Tserv options...PPP Delay=Yes,No
.Tserv options...7-Even=Yes,No
.Tserv options...Login Case=L/P, l/p, L/p, l/P
.Tserv options...Ppp Info=Yes,No
.Tserv options...Clr Scrn=Yes,No
.Tserv options...Silent=Yes,No
.Bridging=Yes,No
.IPX Routing=Yes,No

.Shared Prof=Yes,No
.Telnet PW=*text*
.RIP Policy=Split Hrzn,Poison Rvrs
.RIP Summary=Yes,No
.ICMP Redirects=Accept,Ignore
.DHCP Spoofing=Yes ,No (Pipeline 50/25 only)
.Spoof Adr=*dotted decimal format/subnet mask* (Pipeline 50/25 only)
.Renewal Time=*number* (Pipeline 50/25 only)
.DNS...Domain Name=*text*
.DNS...Pri DNS=*dotted decimal format*
.DNS...Sec DNS=*dotted decimal format*
.DNS...Pri WINS=*dotted decimal format*
.DNS...Sec WINS=*dotted decimal format*
.Acct...Acct= None,RADIUS
.Acct...Acct Host #1=*dotted decimal format*
.Acct...Acct Host #2=*dotted decimal format*
.Acct...Acct Host #3=*dotted decimal format*
.Acct...Acct Port=*number*
.Acct...Acct Timeout=*number*
.Acct...Acct Key=*number*
.Acct...Sess Timer=*number*
.Auth...Auth= None,TACACS,RADIUS,RADIUS/LOGOUT
.Auth...Auth Host #1=*dotted decimal format*
.Auth...Auth Host #2=*dotted decimal format*
.Auth...Auth Host #3=*dotted decimal format*
.Auth...Auth Port=*number*
.Auth...Auth Timeout=*number*
.Auth...Auth Key=*number*
.Auth...Auth Pool=Yes,No
.Auth...Auth Req=Yes,No
.Auth...APP Server=Yes,No
.Auth...APP Host=*dotted decimal format*
.Auth...APP Port=*number*
.Log...Syslog=Yes,No
.Log...Log Host=*dotted decimal format*
.Log...Log Facility=Local0,Local1,Local2,Local3,Local4, Local5,Local6,Local 7
.Modem Ringback=Yes,No

The following applies to Ethernet-equipped Multiband Plus-T1/PRI and -E1/PRI. (Ethernet IF does not apply to the Multiband Plus.)

300.ETHERNET.0.Ether options...Ethernet IF=AUI,COAX,UTP
.Ether options...IP Adrs=*dotted decimal format/subnet mask*
.Ether options...Def Rte=*dotted decimal format*
.Ether options...RIP=Off,Recv
.SNMP options...Read Comm=*text*

```
.SNMP options...R/W Comm=text
.Syslog=Yes,No
.Log Host=dotted decimal format
.Log Facility=Local0,Local1,Local2,Local3,Local4,Local5, Local6,Local 7
```

Note:

- s00.ETHERNET... (MAX models)
s = any slot into which the Ethernet expansion module is installed.
- s00.ETHERNET... (Multiband Plus-T1/PRI or -E1/PRI models)
s = 3
- s00.ETHERNET... (Pipeline 100/400 models)
s = 2
- Passwd, PPP, SLIP, Initial Scrn, Toggle Scrn, Security, Remote Conf, Host #N Addr, Host #N Text in the Tserv Options menu apply to the MAX and Pipeline 100/400 only.

For example:

```
: GET 200.ETHERNET.0.MODULE NAME
200.ETHERNET.0.MODULE NAME=Tom's Pipeline
:
```

FILT=<type>

```
s00 . FILT . n . Name=text
.In Filter 01...Valid=Yes,No
.In Filter 01...Type=Generic,Ip
.In Filter 01...Generic...Forward=Yes,No
.In Filter 01...Generic...Offset=number
.In Filter 01...Generic...Length=number
.In Filter 01...Generic...Mask= hexadecimal string
.In Filter 01...Generic...Value= hexadecimal string
.In Filter 01...Generic...Compare= ==, !=
.In Filter 01...Generic...More=Yes,No
.In Filter 01...Ip...Forward=Yes,No
.In Filter 01...Ip...Src Mask=dotted decimal format
.In Filter 01...Ip...Src Adrs=dotted decimal format
.In Filter 01...Ip...Dst Mask=dotted decimal format
.In Filter 01...Ip...Dst Adrs=dotted decimal format
.In Filter 01...Ip...Protocol=number
.In Filter 01...Ip...Src Port Cmp=None,Less,Eq,Gr,Neq
.In Filter 01...Ip...Src Port #=number
.In Filter 01...Ip...Dst Port Cmp=None,Less,Eq,Gr,Neq
.In Filter 01...Ip...Dst Port #=number
.In Filter 01...Ip...TCP Estab=Yes,No
.Out Filter 01...Valid=Yes,No
.Out Filter 01...Valid=Yes,No
.Out Filter 01...Type=Generic,Ip
```

```

.Out Filter 01...Generic...Forward=Yes,No
.Out Filter 01...Generic...Offset=number
.Out Filter 01...Generic...Length=number
.Out Filter 01...Generic...Mask= hexadecimal string
.Out Filter 01...Generic...Value= hexadecimal string
.Out Filter 01...Generic...Compare= ==, !=
.Out Filter 01...Generic...More=Yes,No
.Out Filter 01...Ip...Forward=Yes,No
.Out Filter 01...Ip...Src Mask=dotted decimal format
.Out Filter 01...Ip...Src Adrs=dotted decimal format
.Out Filter 01...Ip...Dst Mask=dotted decimal format
.Out Filter 01...Ip...Dst Adrs=dotted decimal format
.Out Filter 01...Ip...Protocol=number
.Out Filter 01...Ip...Src Port Cmp=None,Less,Eql,Gtr,Neq
.Out Filter 01...Ip...Src Port #=number
.Out Filter 01...Ip...Dst Port Cmp=None,Less,Eql,Gtr,Neq
.Out Filter 01...Ip...Dst Port #=number
.Out Filter 01...Ip...TCP Estab=Yes,No

```

(.In/Out Filter 02 thru 12... same as .In/Out Filter 01...)

Note:

- This type applies to the MAX equipped with an Ethernet module and the Pipeline 100/400 only. It does not apply to the Multiband Plus.
- *s00.FILT.n...*
s = slot into which the Ethernet card is installed (MAX)
s = 0 (Pipeline 100/400)
n = 0 to 15

FR

```

s00.FR.0.Name=text
.Active=Yes,No
.Call Type=Nailed,Switched
.Nailed Grp=number
.Data Svc=Voice,56KR,56K,64K,384KR,
384K,1536K,1536KR,128K,192K,256K,320K,448K,
512K,576K,640K,704K,768K,832K,896K,960K,1024K,
1088K,1152K,1216K,1280K,1344K,1408K,1472K
.PRI # Type=Unknown,Intl,National,Local,Abbrev
.Dial #=number
.Bill #=number
.Call-by-Call=number
.Transit #=number
.Link Mgmt=T1.617D,None
.N391=number

```

.N392=*number*
.N393=*number*
.T391=*number*
.N392=*number*
.MRU=*number*

Note:

- This type applies to the MAX equipped with the Ethernet module and the Pipeline 100/400 only. It does not apply to the Multiband Plus.

HOSTN

HOST2 applies to Multiband Plus and MAX only.

s00.HOST2.0.Module Name=*text* (MAX only)
.Dual Port=No Dual,1&2 Dual
.Palmtop=Full,Restrict
.Palmtop Port #=*number*
.Palmtop Menus=Standard,Limited,MIF

HOST4 applies to Multiband Plus only.

200.HOST4.0.Dual Port=No Dual,1&3 Dual,2&4 Dual,All Dual
.F Palmtop=Full,Restrict
.F Palmtop Port #=*number*
.F Palmtop Menus=Standard,Limited,MIF
.L Palmtop=Full,Restrict
.L Palmtop Port #=*number*
.L Palmtop Menus=Standard,Limited,MIF
.R Palmtop=Full,Restrict
.R Palmtop Port #=*number*
.R Palmtop Menus=Standard,Limited,MIF

HOST6 applies to MAX only.

s00.HOST6.0.Module Name=*text*
.Port 1/2 Dual=Yes,No
.Port 3/4 Dual=Yes,No
.Port 5/6 Dual=Yes,No

Note:

- This type applies to the MAX and Multiband Plus only. It does not apply to the Pipeline 100/400.
- s00.HOST2... (MAX)
s = 2 or any slot in which a Host/Dual serial host expansion module is installed.
- s00.HOST2... (Multiband Plus)
s = 2
- s00.HOST4... (Multiband Plus)
s = 2

- *s00*.HOST6... (MAX)
s = any slot in which a Host/6 serial host expansion module is installed.

LINE

For models that interface to T1/PRI lines:

```

s00 . LINE . n . Name=text
      .2nd Line=Disabled,D&I,Trunk
      . 2nd Line=Yes ,No  (E1 Models only)
      .Line 1...Sig Mode=Inband,ISDN,PBX T1,ISDN_NFAS
      .Line 1...NFAS_ID num=number
      .Line 1...Rob Ctl=Wink-Start,Idle-Start,Inc-W-200,Inc-W-400, Loop-Start
      .Line 1...Switch Type=AT&T,NTI,GloBanD,Japan,NI-2
      .Line 1...Framing Mode=D4,ESF
      .Line 1...Encoding=AMI,B8ZS,None
      .Line 1...FDL=None ,AT&T ,ANSI ,Sprint  (Not Pipeline 100/400)
      .Line 1...Length=1-133,134-266,267-399,400-533,534-655
      .Line 1...Buildout=0 db,7.5 db,15 db,22.5 db
      .Line 1...Clock Source=Yes,No
      .Line 1...PBX Type=Voice,Data,Leased 1:1
      .Line 1...Delete Digits=number
      .Line 1...Add Number=
      .Line 1...Call-by-Call=number
      .Line 1...Ans #=phone number
      .Line 1...Ans Service=Voice,56KR,56K,64K,384KR,384K,
      1536K,1536KR,128K,192K,256K,320K,448K,512K,576K,
      640K,704K,768K,832K,896K,960K,1024K,1088K,1152K,
      1216K,1280K,1344K,1408K,1472K
      .Line 1...Ch 1=Unused,Switched,D&I,Nailed,D-channel
      .Line 1...Ch 1 #=number
      .Line 1...Ch 1 Slot=number  (MAX only)
      .Line 1...Ch 1 Prt/Grp=number
      .Line 1...Ch 1 TrnkGrp=number

      (.Line 1...Ch 2 thru Ch 23 same as Ch 1)

      .Line 1...Ch 24=Unused,Switched,D&I,Nailed,D-channel, NFAS-Prime,NFAS-Second
      .Line 1...Ch 24 #=number
      .Line 1...Ch 24 Slot=number  (MAX only)
      .Line 1...Ch 24 Prt/Grp=number
      .Line 1...Ch 24 TrnkGrp=number

```

(.Line 2... same as Line 1...)

For models that interface to BRI lines:

```

100 . LINE . n . Name=text

```

```
.Switch Type=AT&T,NTI,NI1,FRANC,U.K.,JAPAN,BELGI,AUSTR,SWISS,
GERMAN,DUTCH, NET 3
.Line 1...Enabled=Yes,No
.Line 1...LinkType=P_T_P,Multi_P
.Line 1...B1 Usage=Unused,Switched,Nailed
.Line 1...B1 Prt/Grp=number
.Line 1...B2 Usage=Unused,Switched,Nailed
.Line 1...B2 Prt/Grp=number
.Line 1...Pri Num=phone number
.Line 1...Pri SPID=number
.Line 1...Sec Num=phone number
.Line 1...Sec SPID=number
```

(.Line 2... thru .Line 8... same as Line 1...)

For models that interface to Switched-56 lines:

```
100.LINE.n.Name=text
.Line 1...Enabled=Yes,No
.Line 1...Ch Usage=Unused,Switched,Nailed
.Line 1...Phone Num=phone number
.Line 1...Port/Grp=number
```

(.Line 2... thru .Line 7... same as Line 1...)

For models that interface to E1/PRI lines:

```
s00.LINE.n.Name=text
.Line 1...Sig Mode=ISDN,None,DPNSS
.Line 1...Switch Type=NTI,French,German,GloBanD,Net 5, Australian,DASS
2,ISDX,ISLX,MERCURY
.Line 1...L2=A END,B END
.Line 1...L3=X END,Y END
.Line 1...NL Value=number
.Line 1...LoopAvoidance=number
.Line 1...Framing Mode=G.703,2DS
.Line 1...Clock Source=Yes,No
.Line 1...Ch 1=Unused,Switched,Nailed
.Line 1...Ch 1 #=number
.Line 1...Ch 1 Slot=number (MAX only)
.Line 1...Ch 1 Prt/Grp=number
.Line 1...Ch 1 TrnkGrp=number
```

(.Line 1...Ch 2 to Ch 15 and Ch 17 to Ch 31 same as Ch 1)

```
.Line 1...Ch 16=D-channel
```

.Line 1...Ch 16 #=N/A
 .Line 1...Ch 16 Slot=N/A
 .Line 1...Ch 16 Prt/Grp=N/A
 .Line 1...Ch 16 TrnkGrp=N/A

(.Line 2... same as Line 1...)

Note:

- *s00.LINE.n...* (MAX)
s = 1 or any slot in which a WAN (line) module is installed.
n = 0 through 3, where 0 is the current Line Profile.
- *s00.LINE.n...* (Multiband Plus and Pipeline 100/400)
s = 1
n = 0 through 3, where 0 is the current Line Profile.
- B1 Prt/Grp, B2 Prt/Grp, Ch x Prt/Grp, Port/Grp, =*number* (software 4.4B and later) or *character* (software 4.4 and earlier)

For example:

```
: LOAD 100.LINE.1
:
```

LMODEM

LMODEM applies to the Pipeline 100/400 and MAX models with digital modems only.

```
s00.LMODEM.0.Module Name=text
.Ans 1#=phone number
.Ans 2#=phone number
.Ans 3#=phone number
.Ans 4#=phone number
```

Note:

- *s00.LMODEM...* (MAX)
s = any slot in which a LAN modem (digital modem) module is installed.
- *s00.LMODEM...* (Pipeline 100/400)
s = 3

LOOP

```
spp.LOOP.0.Local LB=Yes,No
.DSR=Active,Inactive (read) Toggle (write)
.RI=Active,Inactive (read) Toggle (write)
.CD=Active,Inactive (read) Toggle (write)
.DLO=Active,Inactive (read) Toggle (write)
.PND=Active,Inactive (read) Toggle (write)
.ACR=Active,Inactive (read) Toggle (write)
.Inc Ch Count=Yes (write only)
```


.Dec Ch Count=Yes (write only)
.Rate=64K, 56K (read) Toggle (write)

Note:

- This type applies to the MAX and Multiband Plus only. It does not apply to the Pipeline 100/400.
- *spp*.LOOP... (MAX)
s = 1 or any slot in which a serial host expansion module is installed.
pp = 01 through last serial host port.
- *spp*.LOOP... (Multiband Plus)
s = 1
pp = 01 through last serial host port.
- Active/Inactive and 64K/56K are <value>s only for read commands such as GET.
- Toggle is a <value> only for write commands such as SET.
- "SET *spp*.LOOP.0.Local LB=Yes" must be commanded before any other LOOP commands, such as RI, CD, etc.
- The <value> Toggle in a SET command changes the state of the addressed entity from its current state to another state, i.e., from Active to Inactive or from Inactive to Active.

For example:

```
: SET 202.LOOP.0.DSR=Toggle
+ ERROR
: SET 202.LOOP.0.Local LB=Yes
: SET 202.LOOP.0.DSR=Toggle
:
```

PORT

```
spp.PORT.0.Port Name=text
. Ans 1#=phone number
. Ans 2#=phone number
. Ans 3#=phone number
. Ans 4#=phone number
.Idle=None,Call
.Dial=Terminal,DTR Active,RS-366 Ext1,RS-366 Ext2,V.25bis,
V.25bis-C,X.21 Ext1,X.21 Ext2,X.21 Ext1-P
.Answer=Auto,DTR Active,DTR+Ring,V.25bis,V.25bis-C,Terminal,
X.21,P-Tel Man,None
.Clear=DTR Inactive,DTR Active,RTS Inactive,RTS Active,
Terminal
.Term Timing=Yes,No
.RS-366 Esc=*,#,5,6,7,9,0,00
.Early CD=Answer,Originate,Both,No
.DS0 Min Rst=Monthly,Daily,Off
.Max DS0 Mins=number
```

.Max Call Mins=*number*

Note:

- This type applies to the MAX and Multiband Plus only. It does not apply to the Pipeline 100/400.
- *spp*.PORT... (MAX)
s = 1 or any slot in which a serial host expansion module is installed.
pp = 01 through last serial host port.
- *spp*.PORT... (Multiband Plus)
s = 1
pp = 01 through last serial host port.

For example:

```
: LOAD 201.PORT.0
: SET 201.PORT.0.Port Name=Chicago #1
+ ERROR
: SET Port Name=Chicago #1
: SAVE 200.PORT.0
+ ERROR
: SAVE 201.PORT.0
:
```

ROUTE

```
s00 .ROUTE .n .Name=text
.Active=Yes,No
.Dest=text in dotted decimal format/subnet mask
.Gateway=text in dotted decimal format
.Metric=number
.Private=Yes,No
```

Note:

- This type applies to the MAX equipped with the Ethernet module and the Pipeline 100/400 only. It does not apply to the Multiband Plus.
- *s00*.ROUTE.*n*...
s = slot into which the Ethernet card is installed (MAX)
s = 2 (Pipeline 100/400)
n = 0 to 63
- If *n* = 0, Name=Default and Dest=0.0.0.0/0
- MAX Models must have the Ethernet expansion module option

SEC

```
000 .SEC .n .Name=text
.Passwd=*SECURE*
.Operations=Yes,No
```

.Edit Security=Yes,No
.Edit System=Yes,No
.Edit Line=Yes,No
.Edit All Port=Yes,No (Multiband Plus and MAX only)
.Edit Own Port=Yes,No (Multiband Plus and MAX only)
.Edit All Calls=Yes,No
.Edit Com Call=Yes,No (Multiband Plus and MAX only)
.Edit Own Call=Yes,No (Multiband Plus and MAX only)
.Edit Cur Call=Yes,No (Multiband Plus and MAX only)
.Sys Diag=Yes,No
.All Port Diag=Yes,No (Multiband Plus and MAX only)
.Own Port Diag=Yes,No (Multiband Plus and MAX only)
.Download=Yes,No
.Upload=Yes,No
.Field Service=Yes,No

Note:

- 000.SEC.*n*...
 n = 0 thru 8 (The default security profile is 0.)
- The command SAVE cannot be applied to a security profile address.

For example:

: SAVE 000.SEC.8
:

STAT

For all models:

000.STAT.0.Sys Options=
 n.Message Log= (*n* =0 thru 31)
 0.Port Info=
 0.CDR=

For T1/PRI and E1/PRI models only:

*s*00.STAT.0.Line 1 Stat=
 0.Line 2 Stat=
 0.Line Errors=
 n.FDL1=(*n*=0 thru 96) (not E1/PRI or Pipeline)
 n.FDL2=(*n*=0 thru 96) (not E1/PRI or Pipeline)
 0.Net Options=

(*s*=1 for Pipeline 100/400 and Multiband Plus. *s*=1 or any other slot in which a T1/PRI module is installed in a MAX.)

For BRI and Switched-56 models only:

100.STAT.0.Line 1 Stat=
 0.Line Errors=

0.Net Options=

For the MAX and Multiband Plus models only:

```
spp.STAT.0.Call Status=
  n.Message Log= (n=0 thru 31)
0.Statistics=
0.Port Opts=
0.Session Err=
0.Port Leads=
```

s=2 for Multiband Plus. *s*=2 or any other slot in which a serial host module is installed in a MAX. *pp*=01 through the last serial host port.

For models with Ethernet interface:

```
s00.STAT.0.Sessions= (does not apply to Multiband Plus)
  0.Routes= (does not apply to Multiband Plus)
  0.WAN Stat= (does not apply to Multiband Plus)
0.Ether Stat=
0.Ether Opt=
0.Dyn Stat=
```

s=2 for Pipeline 100/400. *s*=3 for Multiband Plus. *s*=slot of a MAX in which the Ethernet module is installed.

Note:

- *n* can range from 0 through 96 for the FDL Status Screens. If *n* is 0, the last 24 hours are reported. 1 through 96 refer to the 15 minute time intervals occurring during the last 24 hours, with 1 being the most recent interval.
- Do not exceed 32,000 seconds when using SET to write to these addresses
- The GET command returns a multiple-line <value> when applied to a Status Screen <address>. Output from a status request is almost identical to the status display using the native mode user interface. The difference is that displays that would scroll (000.STAT.0.Sys Option, 100.STAT.0.Line Errors, etc.) have all lines listed. Each line of the multi-line response is separated by a <CR><LF> pair. Multi-line output is indicated by starting the value field of the response with a <CR><LF> pair.
- When you apply SET to CDR, all events that occurred during the time period are displayed. This is unlike other traps generated by SET. For example, SET 201.STAT.0.Port Leads=20 compares the Port Info screen at the beginning to the end of the 20 sec. time period; and if there is a difference, only the current Port Leads is displayed.

For example:

```
: GET 100.STAT.0.Line Errors
+ 100.STAT.0.Line Errors=
+ 01-005 Ln1 Ln2
+10 -
+2 10 -
:
```

: SET 000.STAT.0.CDR=1

For example:

: GET 600.STAT.0.Line 2 Stat
(Get status of line #2 in the module in slot 6.)

For example:

: GET 202.STAT.0.Call Status
(Get call status of serial host port #2.)

SYS

```
000.SYS.0.Name=text
  .Location=text (Ethernet interface required)
  .Contact=text (Ethernet interface required)
  .Date=mm/dd/yy
  .Time=hh:mm:sec
  .Term Rate=300,1200,2400,4800,9600,19200,38400,57600
  .Palmtop Rate=300,1200,2400,4800,9600,19200,38400,57600
  .Console=Standard,Limited,MIF
  .Remote Mgmt=Yes,No
  .Parallel Dial=number
  .Single Answer=Yes,No (MAX and Multiband Plus only)
  .Sub-Adr=TermSel,Routing,None (T1/E1/BRI models only)
  .DM=number (T1/E1/BRI models only)
  .LAN=number (T1/E1/BRI models only)
  .Serial=number (T1/E1/BRI models only)
  .V110=number (MAX models only)
  .Use Trunk Grps=Yes,No (T1/PRI only)
  .Excl Routing=Yes,No (MAX and Multiband Plus only)
  .Auto Logout=Yes,No
  .Idle Logout=number
  .DS0 Min Rst=Monthly,Daily,Off
  .Max DS0 Mins=number
  .High BER=10 ** -3,10 ** -4,10 ** -5 (T1/PRI or E1/PRI only)
  .High BER Alarm=Yes,No (T1/PRI or E1/PRI only)
  .No Trunk Alarm=Yes,No (T1/PRI or E1/PRI only)
  .Delay Dual=Yes,No (MAX and Multiband Plus only)
  .Edit=XN-n00 (menu number for an edit screen)
  .Status 1=XN-n00 (menu number for a status screen)
  .Status 2=XN-n00 " "
  .Status 3=XN-n00 " "
  .Status 4=XN-n00 " "
  .Status 5=XN-n00 " "
  .Status 6=XN-n00 " "
  .Status 7=XN-n00 " "
```

```
.Status 8=XN-n00 " "
```

Note:

- Palmtop Rate applies only to the MAX and Multiband Plus
- MAX 4000 does not have a Palmtop Port.

For example:

```
: GET 000.SYS.0.Name
+ =kansas BRI
```

TRAP

```
s00.TRAP.n.Name=text
n.Alarm=Yes,No
n.Port=Yes,No
n.Security=Yes,No
n.Comm=dotted decimal format
n.Dest=dotted decimal format
```

Note:

- This type applies to the MAX equipped with the Ethernet module and the Pipeline 100/400 only. It applies to the Multiband Plus if equipped with Ethernet interface.
- *s00.TRAP.n...*
s = slot into which the Ethernet card is installed (MAX)
s = 2 (Pipeline 100/400)
s = 3 (Multiband Plus)
n = 0 to 7

V110

V110 applies to MAX models with V.110 modules only.

```
s00.V110.0.Module Name=text
.Ans 1#=phone number
.Ans 2#=phone number
.Ans 3#=phone number
.Ans 4#=phone number
```

Note:

- *s00.V110...* (MAX)
s = any slot in which a V.110 module is installed.

Command line basics

This section gives a quick overview of command-line processing in MIF.

- **Command Line Length**
The maximum command line is limited to 76 characters. Data entered after the 76th character is ignored and not echoed to the screen. The line is not terminated until a Line Termination is entered.
- **Command Echo**
All data entered by the user except the line termination character will be echoed back to the user, character by character.
- **Line Terminations**
Lines are terminated by either a Return (ASCII <CR>), or a Line Feed (ASCII <LF>), or both. When either is first received, the sequence <CR>-<LF> is echoed. An <LF> following a <CR> does not result in an additional <CR>-<LF> being echoed. The Line Termination character may be entered at any point on the line; the entire line is accepted.
- **Prompt**
The display of a prompt is an explicit acknowledgment that the previous entry has been processed and that the system is now ready to process the next request. The default prompt is a colon (:).
- **Output Indicators**
To make it easier for a computer program to parse, all output lines are prefixed with either an output indicator, namely plus (+) or minus (-). There are two indicators used.
The plus indicator (+) is used when the output is a response to a previous command. Multi-line responses start each line with the output indicator.
The minus indicator (-) is used when the output is the result of an asynchronous event.

Editor basics

When modifying an entity in the edit area, the following line-editing conventions are supported:

- **Line History**
The last 10 lines entered are kept. Whenever a line is entered the oldest kept line is thrown away. The stack is initialized empty at power up. Previous lines can be selected using the line selection characters. When a previous line is selected, the newly edited line replaces the selected line. That line becomes the newest line.
- **Line Selection Characters**
There are two line selection characters, one to walk backwards through the Line History and another to walk forward through the Line History. When the oldest entry is selected while walking backwards through the line history, the next backward selection selects the newest line entered. When the newest entry is selected while walking forward through the line history, the next forward selection selects the oldest line.
The backward line selection character is either a VT100 up arrow (the Escape sequence ESC-[-A) or the control character ^P. The P is mnemonic for Previous.
The forward line selection character is either a VT100 down arrow (the escape sequence ESC-[-B) or the control character ^N. The N is mnemonic for Next.

If you enter a Line selection character while editing a line, the current line is replaced by the current line -- any edits in progress are lost.

The cursor is positioned at the end of the selected line.

- **Cursor movement**

The cursor can be moved within a line by entering the Cursor Left character or the Cursor Right character. The Cursor Left character is ignored when the cursor is at the first character of a line. The Cursor Right character is ignored when the cursor is one position to the right of the last character of the line.

The Cursor Left character is either a VT100 left arrow (the escape sequence ESC-[-D) or the control character ^B. The B is mnemonic for Backward.

The Cursor Right character is either a VT100 right arrow (the escape sequence ESC-[-C) or the control character ^F. The F is mnemonic for Forward.

- **Line Editing**

The current line can be edited until the Line Termination character is entered. Line editing is always in “insert” mode; the character typed will be entered before the cursor and any characters starting from the cursor to the end of the line will be shifted right one position. If the insertion causes the line to exceed the maximum line length the last (rightmost) character is dropped. Cursor movement and line selection commands are processed as described above. The backspace character deletes the character behind the cursor. When a backspace is received at the beginning of a line it is ignored.

Example environments

This appendix discusses example environments, including graphic representations of the environment, a conceptual discussion of the environment, and portions of saved configurations displaying applicable parameters from Ascend units. This appendix covers the following topics:

IP-routing environment	E-2
IP-routing and AppleTalk-routing environment	E-6

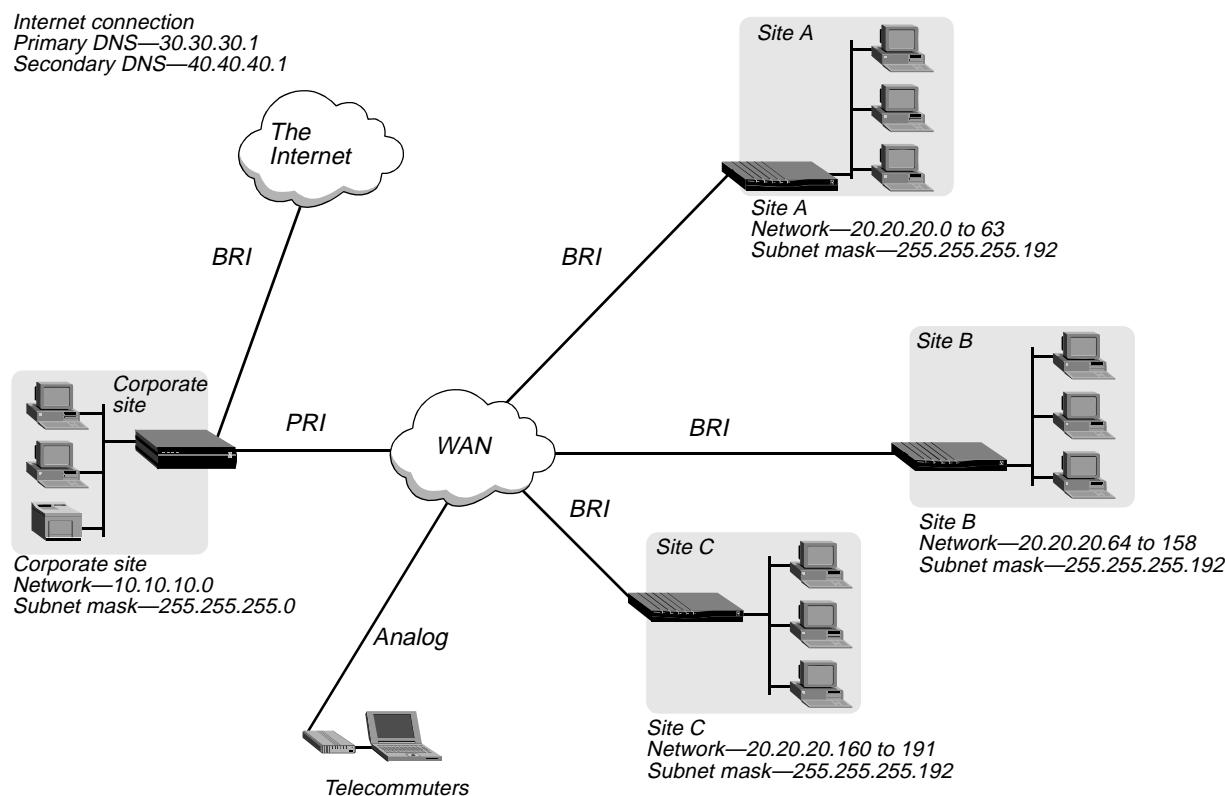
Note: Future revisions of this manual will contain additional examples. Please send suggestions to techpubs@ascend.com.

IP-routing environment

Figure E-1 illustrates the main office and three remote offices of Smith Company. All sites support IP routing. Twelve dial-in analog circuits are available for employees to dial into the corporate office while traveling. The remote sites and dial-in users access the Internet by way of the corporate office.

The corporate site belongs to the 10.10.10.0 network. The remote sites share subnetted segments of the 20.20.20.0 network. The corporate site maintains a 128k link to the Internet, and also reserves twelve connections available for employees to dial into while traveling. The MAX dynamically assigns up to ten dial-in users with IP addresses from a pool that begins with the address 10.10.10.40.

Figure E-1. Example IP-routed environment



MAX configuration

Following is a section of the saved configuration from the MAX at the corporate site:

```
START=ROUTE=500=0
Name=Default
Active=Yes
Gateway=30.30.56.18
Metric=1
Private=Yes
END=ROUTE=500=0
START=ROUTE=500=1
```

```
Name=SiteA
Dest=20.20.20.0/26
Gateway=20.20.20.1
END=ROUTE=500=1
START=ROUTE=500=2
Name=SiteB-1
Dest=20.20.20.64/26
Gateway=20.20.20.65
END=ROUTE=500=2
START=ROUTE=500=3
Name=SiteB-2
Dest=20.20.20.128/27
Gateway=20.20.20.65
END=ROUTE=500=3
START=ROUTE=500=4
Name=SiteC
Dest=20.20.20.160/27
Gateway=20.20.20.161
END=ROUTE=500=4
START=CONN=500=0
Profile Reqd=Yes
Assign Adrs=Yes
Encaps...ARA=Yes
PPP options...Recv Auth=Either
END=CONN=500=0
START=CONN=500=1
Station=SiteA
Active=Yes
Dial #=918885551212
Ip options...LAN Adrs=20.20.20.1/26
Telco options...AnsOrig=Ans Only
END=CONN=500=1
START=CONN=500=2
Station=SiteB
Active=Yes
PRI # Type=Unknown
Dial #=95551212
Ip options...LAN Adrs=20.20.20.65/26
END=CONN=500=2
START=CONN=500=3
Station=SiteC
Active=Yes
PRI # Type=Unknown
Dial #=913335551212
Ip options...LAN Adrs=20.20.20.161/27
END=CONN=500=3
START=CONN=500=4
Station=mega
Active=Yes
PRI # Type=Unknown
Dial #=95553333
Ip options...LAN Adrs= 30.30.227.33/27
```

Example environments

IP-routing environment

```
Ip options...WAN Alias=30.30.56.18
Ip options...IF Adrs=30.30.227.58/27
Session options...Idle=0
Telco options...Data Svc=64K
END=CONN=500=4
START=ETHERNET=500=0
Ether options...IP Adrs=10.10.10.230/24
Ether options...Proxy Mode=Active
WAN options...Pool#1 start=10.10.10.40
WAN options...Pool#1 count=10
TServ options...TS Enabled=Yes
TServ options...PPP=Yes
TServ options...Telnet=Yes
TServ options...Modem Dialout=Yes
TServ options...Immediate Modem=Yes
Telnet PW=*SECURE*
END=ETHERNET=500=0
START=SYSTEM=0=0
Name=corp
END=SYSTEM=0=0
```

Pipeline configuration

Following is a section of the saved configuration from the Pipeline unit at the Site C:

```
START=SYSTEM=0=0
Name=SiteC
END=SYSTEM=0=0
START=ROUTE=200=0
Name=Default
Active=Yes
Gateway=10.10.10.230
Metric=1
Private=Yes
END=ROUTE=200=0
START=CONN=200=0
Profile Reqd=Yes
PPP options...Route IP=Yes
PPP options...Route AppleTalk=Yes
PPP options...Bridge=No
PPP options...Recv Auth=Either
END=CONN=200=0
START=CONN=200=1
Station=corp
Active=Yes
Dial #-9915655551212
Route IP=Yes
Bridge=No
Dial brdcast=No
Encaps options...Send Auth=CHAP
Encaps options...Send PW=*SECURE*
```

```
Encaps options...Recv PW=*SECURE*
Encaps options...Base Ch Count=2
Encaps options...Min Ch Count=2
Ip options...LAN Adrs=10.10.10.230/24
Session options...Idle=0
Telco options...AnsOrig=Call Only
Telco options...Call Type=Perm/Switched
Telco options...Data Svc=64K
END=CONN=200=1
START=ETHERNET=200=0
Ether options...IP Adrs=20.20.20.161/27
Ether options...RIP=Off
Ether options...Proxy Mode=Active
END=ETHERNET=200=0
```

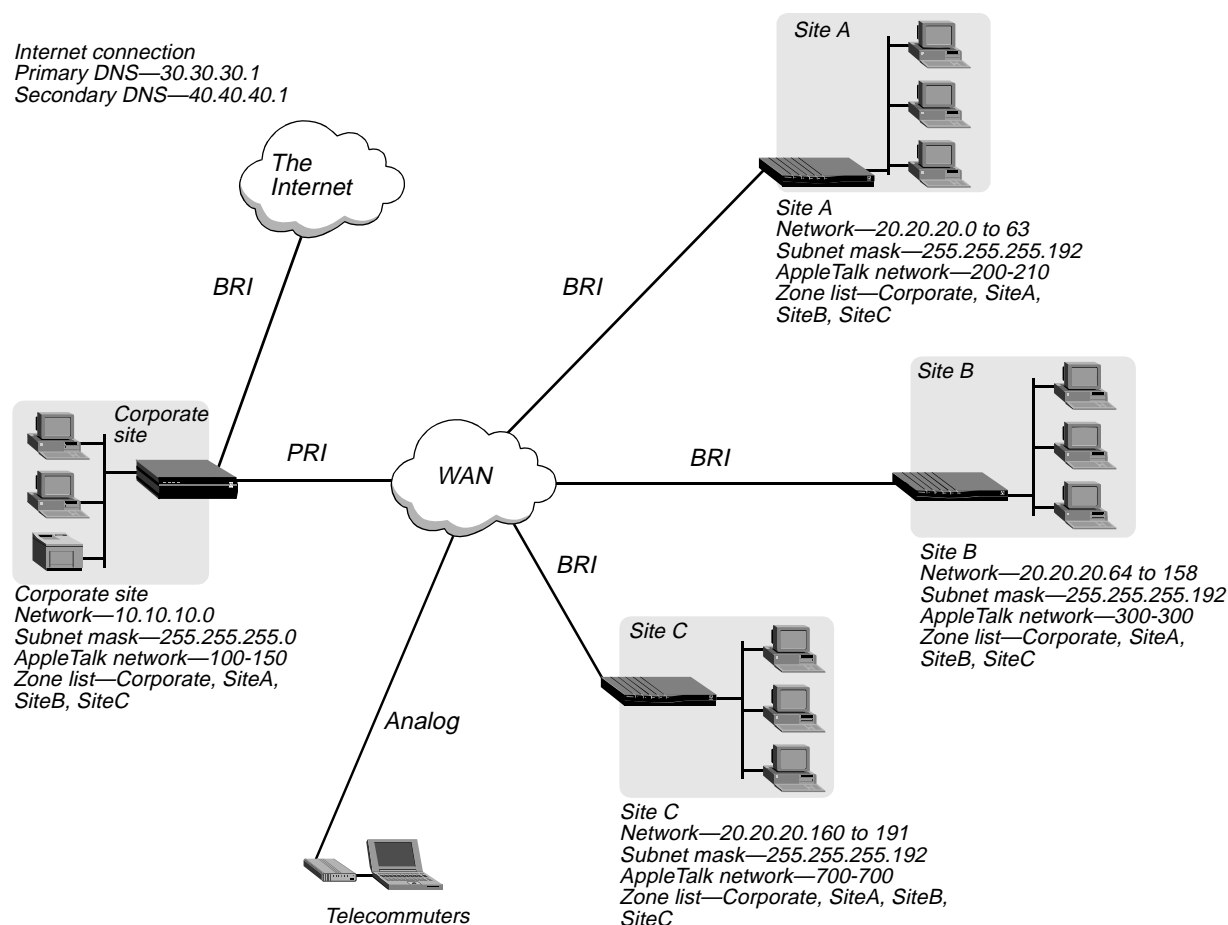
IP-routing and AppleTalk-routing environment

As another example, Smith Company adds AppleTalk devices to the network and sets up an AppleTalk-routed environment, illustrated in Figure E-2. All sites support IP routing and AppleTalk routing. Twelve dial-in analog circuits are available for employees to dial into the corporate office while traveling. The remote sites and dial-in users access the Internet by way of the corporate office.

For the company's IP-routed environment, the corporate site belongs to the 10.10.10.0 network. The remote sites share subnetted segments of the 20.20.20.0 network. The corporate site maintains a 128 kbps link to the Internet, and also reserves twelve connections available for employees to dial into while traveling. The MAX dynamically assigns up to ten dial-in users with IP addresses from a pool that begins with the address 207.107.84.40.

Four zones are created for the company's AppleTalk-routed environment: Corporate, SiteA, SiteB, and SiteC. Devices that share the Ethernet segment with the MAX unit belong to network 100-150. Devices that share the Ethernet segment with the SiteA Pipeline belong to network 200-210. Devices that share the Ethernet segment with the SiteB Pipeline belong to network 300-300. Devices that share the Ethernet segment with the SiteC Pipeline belong to network 700-700.

Figure E-2. Example IP-routed environment



MAX configuration

Following is a section of the saved configuration from the MAX at the corporate site:

```
START=ROUTE=500=0
Name=Default
Active=Yes
Gateway=30.30.56.18
Metric=1
Private=Yes
END=ROUTE=500=0
START=ROUTE=500=1
Name=SiteA
Dest=20.20.20.0/26
Gateway=20.20.20.1
END=ROUTE=500=1
START=ROUTE=500=2
Name=SiteB-1
Dest=20.20.20.64/26
Gateway=20.20.20.65
END=ROUTE=500=2
START=ROUTE=500=3
Name=SiteB-2
Dest=20.20.20.128/27
Gateway=20.20.20.65
END=ROUTE=500=3
START=ROUTE=500=4
Name=SiteC
Dest=20.20.20.160/27
Gateway=20.20.20.161
END=ROUTE=500=4
START=CONN=500=0
Profile Req'd=Yes
Assign Adrs=Yes
Encaps...ARA=Yes
PPP options...Route AppleTalk=Yes
PPP options...Recv Auth=Either
END=CONN=500=0
START=CONN=500=1
Station=SiteA
Active=Yes
Dial #=918885551212
Route AppleTalk=Yes
Bridge=Yes
Ip options...LAN Adrs=20.20.20.1/26
AppleTalk options...Zone Name=SiteA
AppleTalk options...Net Start=200
AppleTalk options...Net End=210
Telco options...AnsOrig=Ans Only
END=CONN=500=1
START=CONN=500=2
Station=SiteB
Active=Yes
```

Example environments

IP-routing and AppleTalk-routing environment

```
PRI # Type=Unknown
Dial #=95551212
Route AppleTalk=Yes
Ip options...LAN Adrs=20.20.20.65/26
AppleTalk options...Zone Name=SiteB
AppleTalk options...Net Start=300
AppleTalk options...Net End=300
END=CONN=500=2
START=CONN=500=3
Station=SiteC
Active=Yes
PRI # Type=Unknown
Dial #=913335551212
Route AppleTalk=Yes
Ip options...LAN Adrs=20.20.20.161/27
AppleTalk options...Zone Name=SiteC
AppleTalk options...Net Start=700
AppleTalk options...Net End=700
END=CONN=500=3
START=CONN=500=4
Station=mega
Active=Yes
PRI # Type=Unknown
Dial #=95553333
Ip options...LAN Adrs= 30.30.227.33/27
Ip options...WAN Alias=30.30.56.18
Ip options...IF Adrs=30.30.227.58/27
Session options...Idle=0
Telco options...Data Svc=64K
END=CONN=500=4
START=ETHERNET=500=0
Ether options...IP Adrs=10.10.10.230/24
Ether options...Proxy Mode=Active
WAN options...Pool#1 start=10.10.10.40
WAN options...Pool#1 count=10
TServ options...TS Enabled=Yes
TServ options...PPP=Yes
TServ options...Telnet=Yes
TServ options...Modem Dialout=Yes
TServ options...Immediate Modem=Yes
AppleTalk=Yes
Telnet PW=*SECURE*
AppleTalk...Zone Name=Corporate
AppleTalk...AppleTalk Router=Seed
AppleTalk...Net Start=100
AppleTalk...Net End=150
AppleTalk...Default Xone=Corporate
AppleTalk...Zone Name #1=SiteB
AppleTalk...Zone Name #2=SiteA
AppleTalk...Zone Name #3=SiteC
END=ETHERNET=500=0
START=SYSTEM=0=0
```



```
Name=corp
END=SYSTEM=0=0
```

Pipeline configuration

Following is a section of the saved configuration from the Pipeline unit at the Site C:

```
START=SYSTEM=0=0
Name=SiteC
END=SYSTEM=0=0
START=ROUTE=200=0
Name=Default
Active=Yes
Gateway=10.10.10.230
Metric=1
Private=Yes
END=ROUTE=200=0
START=CONN=200=0
Profile Reqd=Yes
PPP options...Route IP=Yes
PPP options...Route AppleTalk=Yes
PPP options...Bridge=No
PPP options...Recv Auth=Either
END=CONN=200=0
START=CONN=200=1
Station=corp
Active=Yes
Dial #=9915655551212
Route IP=Yes
Route AppleTalk=Yes
Bridge=No
Dial brdcast=No
Ip options...LAN Adrs=10.10.10.230/24
AppleTalk options...Zone Name=Corporate
AppleTalk options...Net Start=100
AppleTalk options...Net End=150
Session options...Idle=0
Telco options...AnsOrig=Call Only
Telco options...Call Type=Perm/Switched
Telco options...Data Svc=64K
END=CONN=200=1
START=ETHERNET=200=0
Ether options...IP Adrs=20.20.20.161/27
Ether options...RIP=Off
Ether options...Proxy Mode=Active
AppleTalk=Yes
AppleTalk...Zone Name=SiteC
AppleTalk...AppleTalk Route=Seed
AppleTalk...Net Start=700
AppleTalk...Net End=700
AppleTalk...Default Zone=SiteC
```

Example environments

IP-routing and AppleTalk-routing environment

```
AppleTalk...Zone Name #1=Corporate
AppleTalk...Zone Name #2=SiteA
AppleTalk...Zone Name #3=SiteB
END=ETHERNET=200=0
```

Index

? command, B-2
100ST LED, A-4
ITR6, A-4
ITR6 cause codes, numerical list, A-11
ITR6 switch type, 1-21
7-bit ASCII mode, 1-10
8-bit Binary mode, 1-10

A

A Fail LED, A-3
Abandon Call and Retry (ACR), 3-10, 4-27
access security, and SNMP, 6-1
accounting server, 6-12
accumulated errors, displaying, 4-30
ACE server, 1-17
ACR. *See* Abandon Call and Retry
ACT LED, A-3
active AIM call, displaying, 4-7
active calls LED, A-2
active WAN interfaces, 5-11
Added Bandwidth message, 4-20
adding RIP routes, and OSPF, 5-28
address pool, updating, 3-4
address pooling, diagnostics, B-3
address syntax, attributes of, D-3
address, displaying MAC, 4-11
addresses
 edit, D-5
 MIF, D-3
 of next entity, D-6
AddrPool command, B-3
administrative configuration, example of, 1-5
administrative permissions, 1-1
administrative privileges, 1-1
age, of routes, 5-12
AIM, A-14
 port interface problems, solving, A-17
AIM call, displaying active, 4-7
AIM host-interface status, 4-26
AIM module, 4-19

AIM port, 4-19, 4-27, 4-31
AIM port, and loopback test, 3-9
AIM ports, A-22
AIM ports, displaying status of, 4-15
AIS, A-2
Alarm, 6-4
alarm events, 6-4
 coldStart (RFC-1215 trap-type 0), 6-4
 eventTableOverwrite (ascend trap-type 16), 6-5
 linkDown (RFC-1215 trap-type 2), 6-5
 linkUp (RFC-1215 trap-type 3), 6-5
 warmStart (RFC-1215 trap-type 1), 6-4
Alarm LED, 3-4, A-2
ALARM MIF type, D-8
alarm relay, 1-5
all ones, 4-16, A-2
ALU. *See* Average Line Utilization
amount of delay, displaying, 4-32
ANSI T1-601, 3-7
Answer, as user, 1-23
APP Server utility, 1-17
ARP cache, 5-17
ARP-directed (RFC 1433), xix
ARPTable command, B-4
Ascend Connect codes, 4-37
Ascend Disconnect codes, 4-34
Ascend enterprise MIB, 6-1
Ascend Events Group, 6-2
ascendump daemon, B-8
ASCII mode, 1-10
assert, B-9
Assigned to port message, 4-20
asynchronous reports, generating, D-7
AT, A-14
AT command strings, B-15
AT commands, 1-13
AT&V1, B-16
authenticationFailure (RFC-1215 trap-type 4), 6-6
Auto Logout parameter, 1-4
automatic updating, of DNS table, 5-16
autotype function, 3-2

Index

B

Average Line Utilization, 4-11, 4-32
Avm command, B-4
awaiting codes, modem status, 1-21
awaiting DCD, modem status, 1-21

B

B Fail LED, A-3
Backoff Q full, 6-11
Backoff Q full message, explained, 4-38
back-panel alarm relay, 1-5
bandwidth
 how to decrease, 2-6
 how to increase, 2-7
bandwidth utilization, displaying, 4-10
banner, updating, 3-3
B-channel status, displaying, 4-6
BCP (RFC 1638), xix
BERT, 6-10
BERT, performing a, 2-4
Binary mode, 1-10
Bit Error Rate Test (BERT), 6-10
bit-error rate, 1-4
bits, M1, 3-7
block error status display, 3-8
block error totals, 3-8
block errors, 3-7
block errors, displaying, 4-6
block errors, obtaining, 3-7
Blue alarm, 4-16
BRIDGE MIF type, D-9
bridge/router problems, solving, A-25
bridging links, displaying active, 4-31
BRIDisplay command, B-5
BRI/LT diagnostics, 5-2
BRI/LT driver, maintenance functions, 3-7
bundle ID, 1-23
Busy, 4-21
byte errors, 4-30

C

Call Detail Reporting (CDR), 4-9, 4-32
 defined, 4-9
call disconnect
 syslog messages, 6-9
Call Disconnected message, 4-21
call establishment, and syslog messages, 6-8

Call profile
 displaying current, 4-7
call quality
 displaying, 4-32
Call Refused message, 4-21
Call Request (CRQ), 4-28
call routing state diagram, incoming, 5-7
Call Status window, 4-7
Call Terminated message, 4-4, 4-20
callback, 6-11
callback diagnostics, B-6
Callback Pending message, 4-20
Call-by-Call parameter, 1-14
call-close (CL) message, 4-33
called number, and show calls command, 1-21
called-party number
 displaying, 4-10
CalledPartyID, 1-21
CallID, 1-21
CallingPartyID, 1-21
calls
 clearing all, 3-3
 manually placing/clearing, 2-2
 routing, inbound
 illustrated, 5-7
canceller, echo, 3-7
cancelling loopback, 3-8
Carrier Detect (CD), 3-10, 4-28
carrier registers, 4-13
Cause Code, 4-23
cause codes
 disconnect and progress, 4-33
 X.25, 5-47
CCITT Blue Book Q.931, 1-20
CCP (RFC 1962), xix
CD. *See* Carrier Detect
CDR. *See* Call Detail Reporting
channel status
 displaying, 4-16
channels
 displaying call, 4-8
CHAP
 RFC 1994, xix
checksum, 3-8, A-14
checksum, control, 3-8
CIDR
 RFC 1519, xix
circuit information
 displaying, 5-44
 set circuit active circuit-1 command, 5-44
 set circuit command, 5-44

-
- circuit information, *continued*
 - set circuit inactive circuit-2 command, 5-45
 - show fr circuits command, 5-44
 - circuit, turning off Frame Relay, 5-44
 - classic MAX, A-3
 - Classless Inter-Domain Routing (CIDR)
 - RFC 1519, xix
 - clear cause codes, and X.25, 5-47
 - Clear dn timer statistics command, 1-7
 - CLID, 4-23
 - CLID, and show calls command, 1-21
 - clock rate, host, 3-10
 - ClockSource command, B-7
 - Close command, 1-7
 - Clr Err1, 3-5
 - Clr Err2, 3-6
 - Clr NEBE, 3-9
 - Clr Perf1, 3-5
 - Clr Perf2, 3-6
 - Clr-History command, B-7
 - CLU. *See* Current Line Utilization
 - codec, A-18, A-19
 - codes, disconnect and progress, 6-12
 - COL LED, A-3
 - coldStart (RFC-1215 trap-type 0), 6-4
 - Combinet, 4-31
 - Comm, 6-4
 - commands, B-28
 - ?, B-2
 - AddrPool, B-3
 - ARPTable, B-4
 - Avm, B-4
 - BRIDisplay, B-5
 - ClockSource, B-7
 - Clr-History, B-7
 - Coredump, B-8
 - Ether-Display, B-8
 - Fatal-History, B-9
 - FClear, B-13
 - for MIF support, D-5
 - FRestore, B-13
 - FSave, B-13
 - Heartbeat, B-13
 - Help, B-14
 - iproute add, 5-12
 - iproute delete, 5-13
 - iproute show, 5-10
 - ipxping, 5-23
 - IPXRipDebug, B-13, B-14
 - MdbStr, B-15
 - MDialout, B-17
 - ModemDiag, B-16
 - ModemDrvDump, B-18
 - commands, *continued*
 - ModemDrvState, B-18
 - NSLookup, B-21
 - NVRAMClear, B-21
 - PPPDump, B-22
 - PPPFISM, B-22
 - PPPIF, B-23
 - PPPInfo, B-25
 - PPTPCM, B-25
 - PPTPData, B-26
 - PPTPEC, B-26
 - PPTPSend, B-27
 - PRIDisplay, B-27
 - RadAcct, B-28
 - RadIF, B-28
 - RadStats, B-29
 - Reset, B-31
 - Revision, B-31
 - set circuit, 5-44
 - set circuit active circuit-1, 5-44
 - set circuit inactive circuit-2, 5-45
 - show dn timer, 5-17
 - show fr ?, 5-42
 - show fr circuits, 5-44
 - show fr dlci, 5-43
 - show fr lmi (link management information), 5-43
 - show fr stats, 5-42
 - show icmp, 5-18
 - show igmp ?, 5-40
 - show igmp clients, 5-41
 - show igmp groups, 5-40
 - show igmp stats, 5-41
 - show ip, 5-18
 - show ip address, 5-20
 - show ip routes, 5-10
 - show ip stats, 5-20
 - show mrouter ?, 5-40
 - show mrouter stats, 5-42
 - show netware networks, 5-25
 - show netware servers, 5-24, 5-25
 - show netware stats, 5-24
 - show pools, 5-22
 - show udp listen, 5-21
 - SNTP, B-31
 - TelnetDebug, B-32
 - TLoadCode, B-32
 - TSave, B-33
 - Update, B-34
 - WANDisplay, B-34
 - WANDSess, B-35
 - WANNext, B-36
 - WANOpening, B-36
 - WANToggle, B-36
 - WDDialout, B-37
 - commands, AT, 1-13
 - commands, displaying set, 1-11
-

Index

D

commands, displaying terminal-server, 1-6
commands, DO, 1-1
 description of, 2-1
 DO Answer (DO 3), 2-3
 DO Beg/End BERT (DO 7), 2-3
 DO Beg/End Rem LB (DO 6), 2-4
 DO Beg/End Rem Mgm (DO 8), 2-5
 DO Close TELNET (DO C), 2-6
 DO Contract BW (DO 5), 2-6
 DO Diagnostics (DO D), 2-6
 DO Dial (DO 1), 2-7
 DO ESC (DO 0), 2-7
 DO Hang Up (DO 2), 2-8
 DO Load (DO L), 2-8
 DO Menu Save (DO M), 2-8
 DO Password (DO P), 2-9
 DO Resynchronize (DO R), 2-10
 DO Save (DO S), 2-10
 DO Termserv (DO E), 2-10
 Extend BW (DO 4), 2-7
commands, network monitoring, 1-7
community name, 6-4
community strings, setting, 6-2
Compressed SLIP command, 1-7
configuration
 checking, 3-3
configuration problems, solving, A-15
configuration, restoring, 3-1, B-13
configuration, storing current into flash, B-13
CONN MIF type, D-10
Connection profile, displaying current, 4-11
connections
 Ascend codes for, 4-37
connection-specific messages, 4-19
Console parameter, 1-3
consoleStateChange (ascend trap-type 12), 6-6
contact parameter, 1-3
control checksum, 3-8
control-lead dialing, 4-27
CoreDump command, B-8
Corrupt CRC, 3-8
corrupt CRC, 3-7
cost of OSPF route, 5-26
counter, FEBE, 3-9
counter, NEBE, 3-9
CRC, corrupt, 3-7
CRCs, inverted, 3-8
CSLIP command, 1-7, 1-8
CSU repeater, 3-4
CSU, determining if the MAX has installed, 4-25
Ctrl-C, 1-13

current configuration, storing into flash, B-13
current Connection profile, displaying, 4-11
Current Line Utilization (CLU), 4-11, 4-32

D

D4, 3-5, 4-12
D4-framed lines, and error events, 3-5
daemon, syslog, 4-32, 6-7
Data Carrier Detect, 4-27
Data LED, A-2
Data Line Occupied (DLO), 3-10, 4-28
data rate
 displaying, 4-9
 loopback, 3-10
Data Set Ready (DSR), 3-9, 4-28
Data Svc parameter, 1-14
Data Terminal Ready (DTR), 4-28
date
 system, setting, 1-3
D-channel failure, 4-16
D-channel signalling, diagnostics, B-5
Dec Ch Count, 3-10
default modem AT string, modifying, B-15
default password, 1-2
delay
 synchronization, displaying, 4-31
Dest, 6-4
DEST MIF type, D-12
DIAG MIF type, D-13
DIAGN MIF type, D-13
diagnostic commands
 ?, B-2
 AddrPool, B-3
 ARPTTable, B-4
 Avml, B-4
 BRIDisplay, B-5
 ClockSource, B-7
 Clr-History, B-7
 CoreDump, B-8
 Ether-Display, B-8
 Fatal-History, B-9
 FClear, B-13
 FRestore, B-13
 FSave, B-13
 Hearbeat, B-13
 Help, B-14
 IPXRipDebug, B-13, B-14
 MdbStr, B-15
 MDialout, B-17
 ModemDiag, B-16

diagnostic commands, *continued*

- ModemDrvDump, B-18
- ModemDrvState, B-18
- NSLookup, B-21
- NVRAMClear, B-21
- PPPDump, B-22
- PPPFSM, B-22
- PPPIF, B-23
- PPPInfo, B-25
- PPTPCM, B-25
- PPTPData, B-26
- PPTPEC, B-26
- PPTPSend, B-27
- PRIDisplay, B-27
- Quit, B-28
- RadAcct, B-28
- RadIF, B-28
- RadStats, B-29
- Reset, B-31
- Revision, B-31
- SNTP, B-31
- TelnetDebug, B-32
- TLoadCode, B-32
- TSave, B-33
- Update, B-34
- WANDisplay, B-34
- WANDSess, B-35
- WANNNext, B-36
- WANOpening, B-36
- WANToggle, B-36
- WDDialout, B-37

diagnostic field values

- X.25, 5-48

Diagnostic mode

- access to, B-1

diagnostic tests, 3-3

diagnostics

- accessing diagnostic interface, 2-6
- BRI/LT, 5-2
- E1 line, 5-2
- IDSL, 5-4
- port, 5-4
- T1 line, 5-1
- X.25, 5-48

diagram, incoming call routing, 5-7

DIAL MIF type, D-14

dialed number

- displaying, 4-10

dialing

- a Call or Connection Profile, 2-7
- manually, 2-2

Digit Present (DP), 4-27

digital modem

- disabling, 3-11

digital modem, disabling, 3-10

direct routes, 5-11

Directed ARP (RFC 1433), xix

DIS_LOCAL_ADMIN, 1-23

disable modem value, 3-11

disable modem+chan value, 3-11

Disabled link, 4-16

disabling a modem, 3-10

disconnect cause codes, 4-33

disconnect codes, 6-12

disconnects, Ascend codes for, 4-34

disk capture feature, 3-2

displaying

- IP routing table, 5-10

DLCI, 5-43

DLCI status

- displaying, 5-43

DLO. *See* Data Line Occupied

DNS table, local, 5-16

Dnstab command, 1-7

DO Answer (DO 3), 2-3

DO Beg/End BERT (DO 7), 2-3

DO Beg/End Rem LB (DO 6), 2-4

DO Beg/End Rem Mgm (DO 8), 2-5

DO Close TELNET (DO C), 2-6

DO commands, 1-1

DO Contract BW (DO 5), 2-6

DO Diagnostics (DO D), 2-6

DO Dial (DO 1), 2-7

DO ESC (DO 0), 2-7

DO Extend BW (DO 4), 2-7

DO Hang Up (DO 2), 2-8

DO Load (DO L), 2-8

DO menu, B-1

DO Menu Save (DO M), 2-8

DO menu, exiting, 2-7

DO menus, A-14

DO MIF type, D-15

DO Password command, 1-16

DO Resynchronize (DO R), 2-9

DO Save (DO S), 2-10

DO Termserv (DO E), 2-10

DO Toggle (DO T), 2-10

download permission, and Save Cfg command, 3-2

DS0 Min Rst parameter, 1-4

DS0 minute, 1-4, 6-10

DS1 MIB, 6-7

dsl #, B-7

DSR. *See* Data Set Ready

DSX signal-conditioning module, 3-4

Index

E

DTR, loss of, 1-4
Dual Port req'd message, 4-21
Dual-terminal, 4-18
Dyn Stat window, 4-10
dynamic address pooling, diagnostics, B-3
Dynamic Random Access Memory (DRAM), B-13

E

E1 diagnostics, 5-2
echo canceller, 3-7
echo_request packet, 5-15
echo_response packets, 5-16
edit address, described, D-5
Edit parameter, 1-5
editing, basics for entity, D-31
electrical link, displaying condition of, 4-6
embedded operations channel (EOC), 3-7
enable modem value, 3-11
ending a call, 2-8
enterprise MIB, Ascend, 6-1
entities
 current value of, D-6
 defining, D-3
 line-editing conventions for, D-31
 loading and saving, D-5
EOC Address, 5-4
EOC. *See* embedded operations channel
equal-cost gateways, 5-26
error buffers, FEBE and NEBE, 4-6
error events, 6-4
error events, and D4-framed lines, 3-5
error events, displaying, 4-13
error information, 4-20
error log, fatal, B-7, B-9
error message, and self-test, 1-15
error messages
 did not negotiate MPP, 1-16
 ITR6 switch type cause codes, numerical list, A-11
 bad digits in phone number, 1-15
 call failed, 1-15
 call terminated packets sent packets received, 1-15
 cannot establish connection for, 1-16
 cannot find profile for, 1-16
 cannot handshake, 1-15
 Cannot open session, 1-12
 DL TEI ASSIGNED, 1-19
 DL TEI REMOVED, 1-19
 far end does not support remote management, 1-16
 far end rejected session, 1-16

error messages, *continued*
 frame-count must be in the range 1-65535, 1-15
 ISDN cause codes, numerical list, A-4
 management session failed, 1-16
 NL ANSWER REQUEST, 1-19
 NL CALL CLEARED WITH CAUSE, 1-19
 NL CALL CLEARED WITH CAUSE 16, 1-20
 NL CALL CLEARED/L1 CHANGE, 1-19
 NL CALL CONNECTED, 1-19
 NL CALL FAILED/BAD PROGRESS IE, 1-19
 NL CALL FAILED/T303 EXPIRY, 1-19
 NL CALL REJECTED/BAD CALL REF, 1-19
 NL CALL REJECTED/BAD CHANNEL ID, 1-19
 NL CALL REJECTED/INVALID CONTENTS, 1-19
 NL CALL REJECTED/NO VOICE CALLS, 1-19
 NL CALL REJECTED/OTHER DEST, 1-19
 NL CALL REQUEST, 1-19
 NL CLEAR REQUEST, 1-19, 1-20
 no connection
 host reset, 1-11
 host unreachable, 1-11, 1-12
 net unreachable, 1-11, 1-12
 no phone number, 1-15
 not authorized, 1-16
 PH ACTIVATED, 1-19
 PH DEACTIVATED, 1-19
 profile for does not specify MPP, 1-16
 telnet, 1-11
 test aborted, 1-15
 unit busy, 1-15
 Unit busy. Try again later., 1-11
 unknown items on command-line, 1-15
 unknown option, 1-15
 unknown value, 1-15
 wrong phone number, 1-15
error totals, 3-8
error-register statistics, 4-13
errors
 block, 3-7
 byte, 4-30
 channel-by-channel, 4-15
 displaying accumulated, 4-30
 displaying frame, 4-4
 displaying line, 4-6
 obtaining block, 3-7
errors, avoiding transmission, 1-4
errors, displaying block, 4-6
escape character, default rlogin, 1-12
ESF, 4-12
Ether Opt status window, 4-11
Ether Stat window, 4-11
Ether-Data card, 6-8
Ether-Display command, B-8
ethernet frames, displaying number of, 4-11
ethernet interface, 5-11

ethernet interface, displaying, 4-11
ethernet interface, displaying statistics for, 4-4
Ethernet interface, status message, 4-20
ETHERNET MIF type, D-16
ethernet traffic, displaying, B-8
Ethernet up message, 4-20
Ethernet window, 4-12
events, alarm or error, 6-4
events, types of, 4-20
eventTableOverwrite (ascend trap-type 16), 6-5
Experience with the OSPF protocol
 RFC 1246, xx
expiration, multicast membership, 5-41

F

Facilities Data Link (FDL), 4-12
Facility Data Link (FDL), 3-4
Fan LED, A-3
Far End Hung Up message, 4-21
far-end block error (FEBE), 3-7
fatal error history log, B-7
fatal error log, B-9
Fatal-History command, B-9
Fault LED, A-2
fault led, 3-3
FClear command, B-13
FDL statistics window, 4-12
FDL. *See* Facilities Data Link
FDL.*See* Facility Data Link
FDX LED, A-4
feature, disk feature, 3-2
features, displaying, 4-5
FEBE counter, clearing, 3-9
FEBE error buffers, 4-6
FEBE. *See* far-end block error
Field Service privilege, B-1
FILT=<type> MIF type, D-19
finger command, 5-16
Finger requests, responding to, 1-5
Firewall-Friendly FTP (RFC 1579), xx
firewalls (RFC 1579), xx
flash memory, clearing, B-13
forwarding address, advertising, 5-27
FR MIF type, D-20
FR Stat window, 4-14
Frame, 6-7
frame errors, displaying, 4-4

Frame Relay
 circuit information
 set circuit active circuit-1 command, 5-44
 set circuit command, 5-44
 set circuit inactive circuit-2 command, 5-45
 show fr circuits command, 5-44
 DLCI, 5-43
 DLCI status
 show fr dlci command, 5-43
 link management information, show fr lmi, 5-43
 monitoring connections, 5-42
 RFC 1586, xx
 statistics, show fr stats command, 5-42
Frame Relay circuit, turning off, 5-44
Frame Relay MIB, 6-7
Frame Relay profile, 1-17
Frame Relay, monitoring, 5-42
frame-count, 1-14
frames, displaying received, 4-4
frames, displaying transmitted, 4-4
framing bits, 3-5
FRestore command, B-13
FSave command, B-13
FT1-B&O call, 4-19
FT1-B&O calls, 4-32
Full Access profile, 1-2

G

gateways, equal-cost, 5-26
general problems, solving, A-14
German ITR6, 1-21, 5-6, A-4
glare, 4-21
graceful call disconnect, 6-9
Guidelines for Running OSPF Over Frame Relay
 Networks
 RFC 1586, xx

H

Handshake Complete message, 4-20
handshaking, 4-27, B-4
hanging up a call, 2-8
Hangup command, 1-6
hardware address, displaying, 4-11
hardware configuration problems, solving, A-16
hash table, 5-40
HDLC channel, 6-8
Heartbeat command, B-13
Help command, 1-6, B-14

help information, displaying, 1-6
hidden routes, 5-28
High BER alarm parameter, parameters
 High BER alarm, 1-4
High BER parameter, 1-4
high-bit-error alarm, setting, 1-4
histograms, input and output, 5-18
historical performance, displaying, 4-13
host port, and Session Err window, 4-30
host ports, displaying status, 4-15
Host/.. Status window, 4-15
Host/6, 4-19
Host/Dual, 4-19
HOSTN MIF type, D-2, D-21, D-24

I

ICMP
 RFC 1256, xix
 statistics, 5-18
ICMP echo_request packet, 5-15
ICMP Router Discovery Messages (RFC 1256), xix
Idle Logout parameter, parameters
 Idle Logout, 1-4
Idle parameter, 1-16
idle, modem status, 1-21
IDSL
 diagnostics, 5-4
ie0, 5-11
inactive WAN interfaces, 5-11
Inc Ch Count, 3-10
Incoming Call message, 4-20
Incoming call routing state diagram, 5-7
incoming calls
 routing problems, solving, A-24
Incoming Glare message, 4-21
Incomplete Add message, 4-20
Index 100, 3-3
Index 99, 3-3
informational log messages, 4-20
initializing, modem status, 1-21
InOctets, 1-21, 5-6
installed modules, checking, 3-3
interface
 terminal-server, 1-1
interface, displaying ethernet, 4-11
interfaces, active WAN, 5-11
Internal Error message, 4-21

Internet Control Message Protocol, *see* ICMP.
 displaying statistics on, 5-18
inverse multiplexing, 6-8
inverted CRCs, 3-8
IP activity, displaying statistics, 5-20
IP address pool status, displaying, 5-22
IP address pool, updating, 3-4
IP information, displaying, 5-18
IP Mobility (RFC 2002), xix
IP routing
 table, 5-11
IP routing table
 fields, 5-11
IP static routes, updating, 3-3
IP Version 4 (RFC 1812), xix
IPCP (RFC 1332), xix
iproute add command, 5-12
Ipoute command, 1-7
iproute delete command, 5-13
iproute show command, 5-10
IPX address, server, 5-24
IPX RIP traffic, displaying, B-14
IPXping, 5-23
Ipxping command, 1-7
ipxping command, 5-23
IPXRipDebug command, B-13, B-14
ISDN
 call information, 5-6
 cause codes, numerical list, A-4
 PRI and BRI circuit-quality problems, solving, A-21
 PRI and BRI interface problems, solving, A-20
ISDN calls, displaying information on, 5-6
ISDN D-channel X.25 support, 5-47
ISDN line, monitoring, 1-19
ISDN messages, information on, 1-20
ISDN, show command, 1-19

J

Japan NTT, 5-6
Japan NTT switch type, 1-21

K

K56Flex modem cards, numbering of, 1-20
Keep alive, 4-16
Kill command, 1-7
kill command, 1-23

L

- LAN security error message, 4-21
- LAN session down message, 4-20
- LAN session up message, 4-4, 4-20
- latent routes, 5-28
- LED, Alarm, 3-4
- LEDs, A-1, A-3
 - MAX back panel, illustrated, A-3
 - MAX front panel, illustrated, A-1
 - Power, A-3
 - problems, solving, A-22
 - Redundant MAX front panel, illustrated, A-3
- LEDs, described, A-2
- Line, 3-4, 3-6
- Line 1 Stat window, 4-16
- Line 2 Stat window, 4-16
- line diagnosis, functions, 3-7
- Line Errors status window, 4-15
- line errors, displaying, 4-6
- Line LB1, 3-4, 3-6
- line loopback test, 3-4
- LINE MIF type, D-22
- line quality, B-5
- Line Status (Net/BRI) window, 4-17
- line status, displaying, 4-3
- line utilization
 - displaying, 4-31
- lines, displaying status, 4-16
- lines, specifying outgoing, 1-14
- Link active, 4-16
- LINK LED, A-4
- link quality, displaying, 4-11
- link uptime, displaying, 4-11
- linkDown (RFC-1215 trap-type 2), 6-5
- linkUp (RFC-1215 trap-type 3), 6-5
- lmi command (link management information), 5-43
- lo0, 5-11
- location paramater, 1-3
- load name in Sys Options window, 4-5
- load, displaying, software load, displaying, 1-22
- loading a saved or edited profile, 2-8
- loading, entities, D-5
- Local command, 1-6
- local DNS table, 5-16
- Local LB, 3-9
- Local LB command, A-14
- Local LB menu, 3-9
- local loopback test, 3-9
- local mode, going to, 1-6
- local terminal server session, starting, 3-3
- locating slow, 5-13
- log facility, syslog, 6-7
- log messages
 - working with, 4-1
- log window, message, 4-4
- log, fatal error, B-7, B-9
- logging out of the MAX, 2-9
- Logical Link status, A-21
- login service, 6-11
- LOOP MIF type, D-24
- loopback, 3-7, 4-27, 5-4, A-14
- loopback command, 3-8
- loopback counters, 4-6
- loopback function, cancelling, 3-8
- loopback interface, 5-11
- loopback menu, 3-9
- loopback route, 5-12
- loopback route, private, 5-12
- loopback serial data rate, 3-10
- loopback test, 3-4, 3-9
- loopback, LED, A-2
- loopback, restrictions, 3-8
- Loss of Sync, 4-16
- loss of sync, A-2
- loss of T1 framing, 3-3
- LQM, xix

M

- M1, M2, and M3 bits, 3-7
- MAC address, 4-39, 4-43
- MAC address, displaying, 4-11
- Machine Interface Format, 3-2
- Machine Interface Format (MIF), 1-4
 - command support for, D-5
 - lexical sequence for types of, D-8
- Machine Interface Format (MIF) commands
 - for address/value of next entity, D-6
 - for entity current value, D-6
 - generating traps/asynchronous reports, D-7
 - loading/saving entities, D-5
 - modifying parameter values, D-7
 - responses to, D-5
- Machine Interface Format, *see* Use MIF
- Main Edit menu, 1-1
- management, remote, 1-4
- Max DS0 Mins parameter, 1-4

Index

M

Max Rel Delay value, 4-32
MAX reset, using SNMP, 6-2
MAX, classic, A-3
maxTelnetAttempts (ascend trap-type 15), 6-6
MBID, 4-23
MdbStr command, B-15
mdialout, B-2
MDialout command, B-17
mdoem AT commands, 1-13
membership, multicast, 5-41
memory contents, dumping, B-8
memory, clearing flash, B-13
Menu command, 1-7, 1-8
menu mode, terminal server, 1-8
menu,Main Edit, 1-1
message
 Added Bandwidth, 4-20
Message Log display, 4-32
message log window, displaying, 4-4
messages
 Assigned to port, 4-20
 Backoff Q full, 4-38
 Busy, 4-21
 Call Disconnected, 4-21
 Call Refused, 4-21
 Call Terminated, 4-20
 Callback Pending, 4-20
 Dual Port req'd, 4-21
 Ethernet up, 4-20
 Far End Hung Up, 4-21
 Handshake Complete, 4-20
 Incoming Call, 4-20
 Incoming Glare, 4-21
 Incomplete Add, 4-20
 Internal Error, 4-21
 LAN security error, 4-21
 LAN session down, 4-20
 LAN session up, 4-20
 Moved to secondary, 4-20
 Network Problem, 4-22
 No Chan Other End, 4-22
 No Channel Avail, 4-22
 No Connection, 4-22
 No Phone Number, 4-22
 No port DS0 Mins, 4-22
 No System DS0 Mins, 4-22
 Not Enough Chans, 4-22
 Not FT1-B&O, 4-22
 Outgoing Call, 4-20
 Port use exceeded, 4-20
 RADIUS config error, 4-21
 Remote Mgmt Denied, 4-22
 Removed Bandwidth, 4-21
 Request Ignored, 4-22

messages, *continued*
 Requested Service Not Authorized, 4-21
 Sys use exceeded, 4-21
 working with status/log, 4-1
 Wrong Sys Version, 4-22
messages, connection-specific, 4-19
messages, information on ISDN, 1-20
messages, syslog, 6-8
messages, warning, B-11
MIB, 6-1
MIB II, 6-1
MIB-II, 6-7
MIBs, supported, 6-7
 RFC 1213, 6-7
 RFC 1315, 6-7
 RFC 1317, 6-7
 RFC 1406, 6-7
 RFC 1696, 6-7
MIF, 3-2
MIF (Machine Interface Format)
 command line processing for, D-31
 described, D-1
MIF commands
 basics for processing, D-31
MIF types
 ALARM, D-8
 BRIDGE, D-9
 CONN, D-10
 DEST, D-12
 DIAG, D-13
 DIAGN, D-13
 DIAL, D-14
 DO, D-15
 ETHERNET, D-16
 FILT=<type>, D-19
 FR, D-20
 HOSTN, D-2, D-21, D-24
 LINE, D-22
 LOOP, D-24
 PORT, D-25
 ROUTE, D-26
 SEC, D-26
 STAT, D-27
 SYS, D-29
 TRAP, D-30
 V110, D-30
MIF. *See* Machine Interface Format
MIF. *See* Machine Interface Format
modem
 disabling, 3-11
 opening session, 1-7
Modem #n, 3-11
modem AT command strings, B-15
modem AT string, modifying, B-15

modem availability, diagnostics, B-4
 modem cards, numbering, 1-20
 Modem Diag status window, 4-25
 modem dialout, displays, B-17
 Modem MIB, 6-7
 modem quiescence, 3-11
 modem sessions, displaying active, 4-3
 modem status, 1-21
 modem status characters, 4-24
 modem status, displaying, 1-20
 modem window, 4-23
 modem, disabling, 3-10
 modemdiag, B-2
 ModemDiag command, B-16
 ModemDrvDump command, B-18
 modemdrvstate, B-2
 ModemDrvState command, B-18
 ModemSlot, 3-10
 Moved to primary message
 messages
 Moved to primary, 4-20
 Moved to secondary message, 4-20
 MP (RFC 1990), xix
 MPP Bundle, 1-23
 Multiband simulation, and disabled commands, 1-6
 Multicast
 related RFCs, xx
 RFC 1458, xx
 RFC 1584, xx
 Multicast (RFC 1949), xx
 multicast activity, displaying, 5-41
 multicast clients, displaying, 5-41
 Multicast Extensions to OSPF
 RFC 1584, xx
 multicast forwarding table, displaying, 5-40
 multicast heartbeat, B-13
 multicast routing, 5-40
 multipath routing, 5-26
 Multipoint, 4-18

N

Name Server (RFC 1877), xix
 name, system, 1-3
 near-end block error (NEBE), 3-7
 NEBE counter, clearing, 3-9
 NEBE error buffers, 4-6
 NEBE. *See* near-end block error
 Net Options status window, 4-25

Net/BRI status, 4-25
 Net/T1 status window, 4-25
 NetWare stations, 5-23
 network monitoring commands, 1-7
 Network Problem message, 4-22
 network-specific information, show commands to
 monitor, 1-18
 next-hop router, 5-11
 NFAS D channels, 3-5
 NFAS D channels, swaps primary/secondary, 3-5
 NFAS signaling, 3-5
 NIX man pages, 4-32
 No Chan Other End message, 4-22
 No Channel Avail message, 4-22
 No Connection message, 4-4, 4-22
 No Phone Number message, 4-22
 No port DSO Mins message, 4-22
 No System DSO Mins message, 4-22
 No Trunk Alarm parameter, 1-5
 Not Enough Chans message, 4-22
 Not FT1-B&O message, 4-22
 NSLookup command, B-21
 NSSA (RFC 1587), xx
 NT1, returning to normal, 3-9
 NTT switch type, 1-21
 Number of remaining allocated addresses, 5-23
 NVRAMClear command, B-21

O

On Internet Authentication (RFC 1704), xx
 online. The call is up, modem status, 1-21
 Open command, 1-7
 Operator Reset, 3-3
 optional features, displaying, 4-5
 OSPF
 RFC 1245, xx
 RFC 1246, xx
 OSPF (RFC 1583), xx
 OSPF MIB (RFC 1850), xx
 OSPF NSSA Option
 RFC 1587, xx
 OSPF protocol analysis
 RFC 1245, xx
 OSPF route, cost, 5-26
 OSPF Version 2
 RFC 1583, xx
 OSPF Version 2 Management Information Base (RFC
 1850), xx

Index

P

Outgoing Call message, 4-20
outgoing lines, specifying for self-test, 1-14
OutOctets, 1-21, 5-6
out-of-service LED, A-2
output, verbose, 5-15

P

packet count, displaying, 5-19
packet filtering
 related RFCs, xx
packet size, 5-15
PAD
 service signals, 5-47
PAD connections, 5-45
PAD sessions, displaying, 5-45
Parallel Dial parameter, 1-4
parameters
 Auto Logout, 1-4
 Call-by-Call, 1-14
 Console, 1-3
 contact, 1-3
 Data Svc, 1-14
 DSO Min Rst, 1-4
 Edit, 1-5
 High BER, 1-4
 Idle, 1-16
 location, 1-3
 Max DSO Mins, 1-4
 No Trunk Alarm, 1-5
 Parallel Dial, 1-4
 PRI # Type, 1-14
 Remote Mgmt, 1-4
 R/W Comm, 6-2
 Security, 6-2
 Single Answer, 1-4
 Status, 1-5
 Term Rate, 1-3
 Transit #, 1-14
parameters, modifying values of MIF command, D-7
parameters, system administration, 1-2
password challenges, displaying, 1-17
password mode, disabling, 1-17
password mode, entering, 1-17
password mode, putting the terminal server in, 1-17
password security, SNMP, 6-1
password, default, 1-2
passwords, and Save Cfg command, 3-1
PDU, 6-3
performance registers
 clearing line #1 in, 3-5
 clearing line #2 in, 3-6
performance-register statistics, 4-13
permissions, administrative, 1-1
permissions, activating administrative, 1-2
phone number
 testing, 1-6
ping, 5-15, 5-16
Ping command, 1-7
PND. <emphasis> See Present Next Digit
Point-to-point, 4-18
Point-to-Point Protocol
 RFC 1661, xix
pool, updating, 3-4
Port, 6-4
port, 6-8
port diagnostics, 5-4
port diagnostics, performing, 5-4
Port Info status window, 4-26
Port Leads status window, 4-27
PORT MIF type, D-25
port number, UDP, 5-21
Port Opts information, listed, 4-29
Port Opts status window, 4-28
Port state change events, 6-5
port status, displaying V.110, 1-22
Port use exceeded message, 4-20
portAcrPending (ascend trap-type 10), 6-6
portCarrier (ascend trap-type 8), 6-6
portCollectDigits (ascend trap-type 5), 6-5
portConnected (ascend trap-type 7), 6-6
portDTENotReady (ascend trap-type 11), 6-6
portDualDelay (ascend trap-type 1), 6-5
portHaveSerial (ascend trap-type 3), 6-5
portInactive (ascend trap-type 0), 6-5
portLoopback (ascend trap-type 9), 6-6
PortN Stat window, 4-29
portRinging (ascend trap-type 4), 6-5
portUseExceeded (ascend trap-type 13), 6-6
portWaiting (ascend trap-type 6), 6-5
portWaitSerial (ascend trap-type 2), 6-5
POST, A-14
POST. <emphasis> See power-on self test
POSTs (power-on self tests), 3-3
power LED, A-2
power-on self test (POST), 3-3
PPP, 4-31
PPP (RFC 1661), xix
PPP Bridging Control Protocol (RFC 1638), xix
PPP Challenge Handshake Authentication Protocol (RFC 1994), xix

PPP command, 1-7, 1-8
 PPP Compression Control Protocol (RFC 1962), xix
 PPP in HDLC-like Framing (RFC 1662), xix
 PPP Internet Protocol Control Protocol (RFC 1332), xix
 PPP Internet Protocol Control Protocol Extensions for
 Name Server Addresses (RFC 1877), xix
 PPP Link Quality Monitoring (RFC 1989), xix
 PPP Multilink Protocol (RFC 1990), xix
 PPP Stac LZS Compression Protocol (RFC 1974), xix
 PPP Vendor Extensions (RFC 2153), xix
 PPPDump command, B-22
 PPPFSM command, B-22
 PPPIF command, B-23
 PPPInfo command, B-25
 PPTPCM command, B-25
 PPTPData command, B-26
 PPTPEC command, B-26
 PPTPSend command, B-27
 preference value, for route, 5-11
 preferences, route, 5-28
 Present Next Digit (PND), 3-10
 PRI # Type parameter, 1-14
 PRI interface, displaying stats for, 4-12
 PRI, and maximum bit-error rate, 1-4
 PRIDisplay command, B-27
 private loopback route, 5-12
 privileges
 administrative, 1-1
 assigning required, 1-16
 Problems accessing the WAN, solving, A-23
 profile, Full Access, 1-2
 progress codes, 4-33, 6-12
 protocol data unit (PDU), 6-3
 protocols
 multiple IP routing, 5-10
 show commands to monitor, 1-18

Q

Q.931, 1-20
 quality of the link, displaying, 4-11
 quality, displaying call, 4-32
 quality, monitoring transmission, 3-8
 queue, backoff, 6-11
 queued packets, UDP, 5-21
 quiescing a modem, 3-11
 Quit, B-28
 Quit command, 1-6, B-28

R

radacct, 6-12
 RadAcct command, B-28
 RadIF command, B-28
 RADIUS accounting server, 6-12
 RADIUS Backoff Q full, 6-11
 RADIUS config error message, 4-21
 RADIUS configuration, updating, 3-4
 RADIUS server
 opening connection to, 3-3
 radiusd, 6-12
 RadStats command, B-29
 raw TCP hosts
 specifying, 1-9
 rawTcp parameter, 1-9
 received frames
 displaying, 4-4
 Red Alarm, 4-16, A-2
 registers, carrier and user, 4-13
 relay, alarm, 1-5
 remaining allocated addresses, explained, 5-23
 Remote command, 1-6, 1-16
 remote command, 1-15
 remote login
 terminating, 1-12
 remote management, 1-4
 at remote end of an AIM call, 2-5
 session, opening, 1-6
 session, starting, 1-15
 session, terminating, 1-16
 session, timing out, 1-16
 Remote Mgmt Denied message, 4-22
 Remote Mgmt parameter, 1-4
 remote u interface, 3-7
 Removed Bandwidth message, 4-21
 Report of IAB Workshop (RFC 1636), xx
 reports, generating MIF, D-7
 Request Ignored message, 4-22
 Request to Send (RTS), 4-28
 Requested Service Not Authorized message, 4-21
 required privileges
 assigning, 1-16
 Requirements for IP Version 4 Routers (RFC 1812), xix
 Requirements for Multicast Protocols (RFC 1458), xx
 resent Next Digit (PND), 4-28
 Reset command, B-31
 reset, system, 3-3
 reset, using SNMP, 6-2
 restarting MAX, 3-3

Index

S

Restore Cfg, 3-1
Resume command, 1-7
resynchronizing a call in progress, 2-10
Revision command, B-31
RFC 1213, 6-7
RFC 1288, 1-5
RFC 1288, finger command, 5-16
RFC 1315, 6-7
RFC 1317, 6-7
RFC 1406, 6-7
RFC 1696, 6-7
RFCs
 IP routing, xix
 OSPF, xx
 PPP, xix
 RFC 1974, xix
RI. <emphasis> See Ring Indicate
Ring Indicate (RI), 3-10, 4-28
RIP routes, how OSPF adds, 5-28
RIP traffic, IPX, B-14
rlogin
 terminating session, 1-12
Rlogin command, 1-7
rlogin command, 1-11
rlogin, default escape character, 1-12
round-trip statistics, statistics, round-trip, 5-16
route
 adding, 5-12
 age, 5-12
 calls, inbound (illustrated), 5-7
 deleting, 5-13
 preferences, displayed, 5-11
route age, 5-12
ROUTE MIF type, D-26
Route preferences, 5-28
route, loopback private, 5-12
routers, 5-13
Routes status window, 4-29
routes, hidden, 5-28
Routing in a Multi-provider Internet (RFC 1787), xix
routing links
 active, displaying, 4-31
routing state diagram, call routing, 5-7
routing, multipath, 5-26
routing, third-party, 5-27
Rq Corrupt CRC, 3-9
Rq Uncorrupt CRC, 3-9
RS232 MIB, 6-7
RS-366, 4-27, 4-28
RS-366 output signal, 3-10

RS-422, 4-29
RS-449, 4-29
RS-449 Host I/F, 4-29
R/W Comm, 6-2
R/W Comm parameter, 6-2

S

SAFWORD server, 1-17
Save Cfg, 3-2
Save Cfg command, and download permission, 3-2
saving, loaded entries, D-5
Scalable Multicast Key Distribution (RFC 1949), xx
Sealing Current, 5-3
SEC MIF type, D-26
Secure Access Manger firewall, 4-38
Secure Operation of the Internet (RFC 1281), xx
Security, 6-4
security
 events, 6-6
 related RFCs, xx
 RFC 1245, xx
 SNMP, 6-1
security configuration, and SNMP, 6-2
Security Considerations for IP Fragment Filtering
 RFC 1858, xx
Security parameter, 6-2
self-test error messages, 1-15
self-test, phone number self-test, 1-13
Send commands, listing, 1-11
serial data rate, loopback, 3-10
serial number, displaying, 4-5
Serial WAN status window, 4-30
server, accounting, 6-12
session
 terminal server, starting, 3-3
 user, terminating, 1-7
Session Err status window, 4-30
session ID, and kill command, 1-23
Sessions status window, 4-31
sessions, displaying active, 4-3
set all command, settings, displaying current, 1-17
set circuit active circuit-1 command, 5-44
set circuit command, 5-44
set circuit inactive circuit-2 command, 5-45
Set command, 1-6
set command, 1-16
set commands, SNMP, 6-2
set commands, displaying, 1-11

-
- set fr commands, 1-17
 - set password command, 1-17
 - set term command, terminal type, specifying, 1-17
 - settings, displaying current, 1-11
 - show, 5-43
 - show calls command, 1-21
 - Show command, 1-6
 - show commands, 1-17
 - Show dn timer command, 1-18
 - Show dn timer statistics command, 1-18
 - show dn timer command, 5-17
 - show fr ? command, 5-42
 - show fr circuits command, 5-44
 - show fr dlci command, 5-43
 - show icmp command, 5-18
 - show igmp ? command, 5-40
 - show igmp clients command, 5-41
 - show igmp groups command, 5-40
 - show igmp stats command, 5-41
 - show ip address command, 5-20
 - show ip command, 5-18
 - show ip routes command, 5-10
 - show ip stats command, 5-20
 - show ISDN command, 1-19
 - show ISDN output, 1-19
 - show modems command, 1-13, 1-20
 - show mrouting ? command, 5-40
 - show mrouting stats command, 5-42
 - show network networks command, 5-25
 - show network servers command, 5-24, 5-25
 - show network stats command, 5-24
 - show pad command, 5-45
 - show revision command, revision, displaying, 1-22
 - show udp listen command, 5-21
 - show uptime command, 1-21
 - show V.110s command, 1-22
 - show x25 command, 5-45
 - Signaling System 7, A-4
 - signaling, NFAS, 3-5
 - Simple Network Time Protocol (SNTP) (RFC 2030), xix
 - Simple Network Time Protocol (SNTP), 1-3
 - Single Answer parameter, 1-4
 - Site Security Handbook (RFC 1244), xx
 - SLIP command, 1-7, 1-8
 - slow routers, locating, 5-13
 - SNMP
 - configuring access security, 6-1
 - configuring security, 6-2
 - enforcing security, 6-2
 - SNMP, *continued*
 - management, 6-1
 - resetting the MAX, 6-2
 - security, 6-1
 - setting traps, 6-3
 - trap parameters, 6-3
 - traps, 6-3
 - verifying MAX reset, 6-2
 - SNMP set commands, enabling, 6-2
 - SNMP trap, 6-3
 - SNMP trap configuration, 6-4
 - SNTP command, B-31
 - SNTP, RFC 2030, xix
 - SNTP. *See* Simple Network Time Protocol
 - socket number, UDP, 5-21
 - source of clocking, B-7
 - Stac LZS compression (RFC 1974), xix
 - STAT MIF type, D-27
 - state diagram, incoming call routing, 5-7
 - static routes, updating, 3-3
 - Statistics window, 4-31
 - status display, block error, 3-8
 - status messages
 - working with, 4-1
 - Status parameter, 1-5
 - status window, 1-1
 - activating, 4-2, 4-5
 - customizing appearance of, 4-5
 - default, 4-1
 - scrolling information, 4-2
 - status/log messages. *See also* error messages
 - stored configuration
 - restoring, 3-1
 - strings, setting community, 6-2
 - superframe, 3-8
 - format, 3-5
 - super-user, 1-2
 - Switch D Chan, 3-5
 - switch type
 - 1TR6, A-4
 - German and Japanese, 5-6
 - synchronization delay
 - displaying, 4-31
 - SYS MIF type, D-29
 - Sys Options window, 4-5, 4-40
 - information listed, 4-41
 - Sys use exceeded message, 4-21
 - sysAbsoluteStartupTime, 6-2
 - Syslog, 4-32
 - syslog daemon, 4-32, 6-7
 - syslog messages, meanings, 6-8

Index

T

- syslog, disconnect and progress codes, 6-12
- system administration parameters, 1-2
- system date
 - setting, 1-3
- System Is Up, 3-3
- system memory
 - checking, 3-3
- system name, 1-3
- System Reset, 3-3
- System Status window, 4-19, 4-42
- system time
 - setting, 1-3
- system uptime, 4-41
 - displaying, 4-5
- systemUseExceeded (ascend trap-type 14), 6-6

T

- T1 connections
 - checking, 3-3
- T1 diagnostics, 5-1
- T1 framing loss, 3-3
- T1 line, determining quality, 3-4
- TACACS+, 6-11
- tag, 5-26
- target address, 5-11
- TCP command, 1-7, 1-12
- TCP packets, displaying statistics, 5-22
- Telnet and raw TCP hosts
 - mixing, 1-8
- Telnet command, 1-7
- telnet command, 1-10
- Telnet commands, sending standard, 1-11
- telnet connection, opening, 1-11
- telnet error messages, 1-11
- Telnet hosts
 - specifying, 1-8
 - updating list, 3-3
- Telnet session
 - closing, 1-11
 - commands, 1-11
- Telnet sesssion
 - terminating, 1-23
- TelnetDebug command, B-32
- Term Rate parameter, 1-3, 3-2
- Term Serv, 3-3
- terminal server banner
 - updating, 3-3
- terminal server commands
 - displaying, 1-6
- terminal server interface, 1-1, 1-6
- terminal server menu mode, 1-8
- terminal server session
 - closing, 1-6
 - displaying active, 4-31
 - starting, 1-6, 3-3
- test
 - line loopback, 3-4
- Test command, 1-6
- test command, 1-13
- test frames, displaying, 4-6
- test, loopback, 3-8
- tests, diagnostic, 3-3
- third-party routing, 5-27
- time
 - system, setting, 1-3
- Time-To-Live (TTL), 5-13
- TLoadCode command, B-13, B-32
- token security card, 5-12
- totals,block error, 3-8
- Traceroute (RFC 1393), xix
- Traceroute command, 1-7, 5-13
- Traceroute Using an IP Option (RFC 1393), xix
- training, B-4
- Transit # parameter, 1-14
- transmission errors
 - avoiding, 1-4
- transmission quality, monitoring, 3-8
- transmitted frames, displaying, 4-4
- Transparent mode, 1-10
- trap, 6-3
- TRAP MIF type, D-30
- traps, generating MIF, D-7
- troubleshooting
 - 1TR6 switch type cause codes, numerical list, A-11
 - AIM port interface problems, A-17
 - bridge/router problems, A-25
 - configuration problems, A-15
 - general problems, A-14
 - hardware configuration problems, A-16
 - incoming call routing problems, A-24
 - ISDN cause codes, numerical list, A-4
 - ISDN PRI and BRI circuit-quality problems, A-21
 - ISDN PRI and BRI interface problems, A-20
 - problems accessing the WAN, A-23
- TSave command, B-33
- type of service, IPX, 5-25
- type, specifying terminal, 1-17

U

- u interface, remote, 3-7
- UDP packets
 - displaying statistics, 5-21
- Uncorrupt CRC, 3-9
- unexpected call disconnect, and syslog messages, 6-9
- UNIX, 5-16, 6-7, B-8
- UnRq Corrupt CRC, 3-8
- Upd Rem Cfg, 3-3
- Update command, B-34
- updating, of DNS table, 5-16
- uptime in status window, 4-5
- uptime, displaying, 1-21, 4-5
- uptime, displaying link, 4-11
- uptime, system, 4-41
- Use MIF, 3-2, 3-3
- user error event register, clearing line, 3-5
- user performance registers, 4-13
- user session
 - terminating, 1-7
- U-superframe, 3-7
- utilization
 - line, displaying, 4-31

V

- V.110 cards, displaying status, 1-22
- V.110 port status, displaying, 1-22
- V.25 bis, 4-27
- V.25 output signal, 3-10
- V.25 signal, 3-9
- V.25bis, 4-42
- V.35, 4-29
- V.35 Host I/F, 4-29
- V110 MIF type, D-30
- values
 - getting entity current, D-6
 - modifying MIF command parameter, D-7
 - of next entity, D-6
- verbose output, 5-15
- virtual connect session
 - closing, 1-7
- virtual connection, suspending of, 1-13
- virtual connection, terminating, 1-13
- VT100 interface, initial screen, 1-1
- VT100 menus
 - returning to, 1-7

W

- WAN interface
 - active, 5-11
 - displaying, 4-25
- WAN interface, inactive, 5-11
- WAN lines, displaying status, 4-16
- WAN links, displaying active, 4-4
- WAN port, display in information on, 1-19
- WAN Stat window, 4-43
- WANDisplay command, B-34
- WANDSess command, B-35
- wanidle0, 5-11
- wanN, 5-11
- WANNNext command, B-36
- WANOpeing command, B-36
- WANToggle command, B-36
- warmStart (RFC-1215 trap-type 1), 6-4
- warning messages, B-11
- WDDialout command, B-37
- window
 - Call Status, 4-7
 - Dyn Stat, 4-10
 - Ether Opt status, 4-11
 - Ether Stat, 4-11
 - Ethernet, 4-12
 - FDL statistics, 4-12
 - FRStat, 4-14
 - Host/..Status, 4-15
 - Line 1 Stat, 4-16
 - Line 2 Stat, 4-16
 - Line Errors status, 4-15
 - Line Status (Net/BRI), 4-17
 - Modem Diag status, 4-25
 - PortN Stat, 4-29
 - System Status, 4-42
- windows, status *See* status window, 1-1
- Wrong Sys Version message, 4-22

X

- X.21, 4-27, 4-29, 4-42
- X.25, 5-45
 - clear cause codes, 5-47
 - diagnostic field values, 5-48
 - diagnostics, 5-48
 - PAD service, monitoring, 5-45

Y

Yellow Alarm, 4-16, A-2

yellow fault led, 3-3