MAX 800 Series Administration Guide

Ascend Communications, Inc.
Part Number: 7820-0618-001
For software version 7.0.0

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

Figures

Tables

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 BRI lines, how to remove digital modems from service, and how to display call information. The chapter also discusses administering and managing TCP/IP and IPX 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, “Example environments,” discusses example environments, including an IP-routing environment and an IP-routing/AppleTalk environment.

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 ***`italics`***—see *Italics*, below). If you could enter the characters but are not specifically instructed to, they do not appear in boldface.
Italics	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

For information about IPX routing, see:

- 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 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 800 Series documentation set consists of the following manuals:

- *NavisConnect User's Guide*
- MAX *800 Series Administration Guide (this guide)*
- MAX *800 Series Hardware Installation Guide*
- MAX *800 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

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 as 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
      Remote Mgmt=Yes
      Auto Logout=No
      Idle Logout=0
      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
         Log CallInfo=None
         Log Call Progress=No
```

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

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

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.

Log out parameters

The Auto Logout parameter specifies whether to log out and go back to default privileges upon loss of Data Transmit Ready (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.

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.

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
```

```
iproute         Manage IP routes. Type ‘iproute ?’ for
                help
dnstab          Displays help information about the DNS
                table. Type 'dnstab ?' for help
slip            SLIP command
cslip           Compressed SLIP command
ppp             PPP command
menu            Host menu interface
telnet          telnet [ -a|-b|-t ] <host-name> [
                <port-number> ]
tcp             tcp <host-name> <port-number>
ping            ping <host-name>
ipxping         ipxping <host-name>
traceroute      Trace route to host.  Type 'traceroute -?'
                for help
rlogin          rlogin [ -l user -ec ] <host-name> [ -l
                user ]
open            open < modem-number | slot:modem-on-slot >
resume          resume virtual connect session
close           close virtual connect session
pptp            pptp <server-name>
l2tp            l2tp <server-name>
ara             ARA command
```

Returning to the VT100 menus

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

```
quit            Closes terminal server session
hangup          Closes terminal server session
local           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:

```
iproute             Manage IP routes.  Type ’iproute ?’ for help
ping                ping <host-name>
ipxping             ipxping <host-name>
traceroute          Trace route to host.  Type ’traceroute -?’ 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:

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

where

- **`–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 node.
- **`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 1-10. 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 [-1username]
```

where:

- -e*char* 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.
- **-l*username*** 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 oyu 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
```

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* 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` *N1* `packets sent` *N2* `packets received`	This message indicates the number of packets sent (*N1*) and received (*N2*).
`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` *option*	The command-line contained the option specified by *option*, which is invalid.
`unknown value` *value*	The command-line contained the value specified by *value*, which is invalid

Message	Explanation
`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.

Message	Explanation
`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
```

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 SAFEWORD 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 SAFEWORD 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 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 uptime    Display system uptime
show revision  Display system revision
show sessid    Display current and base session id
```

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 tcp
show dnstab
show netware
```

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 CCITTT Blue Book Q.931 or other ISDN specifications.

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
```

VT100 Interface DO Commands

2

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=Termserv
 D=Diagnostics
```

To execute a DO command, press and release the the Ctrl-D, 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.

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=Termserv
 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.

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.

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 Mgmt 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.

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.)

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.
- 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.*

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.*

Termserv (DO E)

The DO Termserv 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 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 is 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 messag`e 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.

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.

VT100 Interface Status Windows

4

This chapter describes the MAX unit's status windows.

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

```
|--------------------| |--------------------|
|00-200 22:17:52     | | 90-100 Sessions    |
|>M31  Line   Ch     | | >  1 Active        |
| Call Terminated    | |  0 mth             |
|                    | |                    |
|--------------------| |--------------------|
|90-400 Ether Stat   | |90-300 WAN Stat     |
|>Rx Pkt:    3486092 | |>Rx Pkt:     184318^|
| Tx Pkt:      10056 | | Tx Pkt:     159232 |
| Col:          3530 | | CRC:          0v   |
|--------------------| |--------------------|
|80-000 Modem Stat   | |mth                 |
| 12345678           | | Qual Good 26:05:41 |
| ......--           | | 64K     1 channels |
|                    | | CLU   0%  ALU   0% |
|--------------------| |--------------------|
|60-100 2468         | |00-100 Sys Option   |
|  Link DDD          | |>Security Prof: 1  ^|
|  B1   *--.         | | Software +7.0.0+   |
|  B2   ---.         | | S/N: 12345678      |
|--------------------| |--------------------|
```

Navigating the status windows

To scroll the information in a status window or execute a context-specific DO command, you must make the status window active by pressing 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 Edit window (the menu).

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 4-5.

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:

```
|--------------------| l--------------------|
|90-100 Sessions     | |00-200 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.

The system message log provides a log of up to 32 of the most recent system events.

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.

The Ether Stat window shows the current count of received frames, transmitted frames, and frames with errors at the Ethernet interface.

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.

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 4-5.*)*

For example, the MAX displays line-status windows for the T1 (or E1) lines in Slot 1 as windows 1 and 2 by default. To instruct it to use status windows 3 and 4 to display line-status windows for the T1 (or E1) lines in Slot 2, proceed as follows:

1 Open the System profile.

2 Specify the number identifying line 1 in slot 2 by setting the Status 3 parameter:

```
Status 3=20-100
```

3 Specify the number identifying line 2 in slot 2 by setting the Status 4 parameter:

```
Status 4=20-200
```

4 Close the System profile.

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.

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, press the TAB key to activate a status window, then press the arrow keys to access the System > CDR window. This screen shows the 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 screen window number and title.

The second line displays the time the event occurred in this format:

year: *month* : *day* : *hour* : *minute* : *second*

The third line displays describes the CDR event. It shows an event description, event ID, the data service in use, and the slot-port address on which the event occurred, in that order.

- CDR event description

  The event description uses these abbreviations:

  – OR for Originated (outgoing call)

  – AN for Answered (incoming call)

  – AP for Assigned to Port or module (incoming call)

  – CL for Cleared

  – OF for 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.
- The 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.
- The slot-port address on which the 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 Dialed Number Information Service (DNIS) from your WAN provider. In some cases, the called-party number is not delivered, such as when the MAX is behind some PBXs.

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

Dyn Stat window

The Dyn Stat window shows the name, quality, bandwidth, and bandwidth utilization of each online multi-channel PPP connection with dynamic bandwidth management. To display the Dynamic Status window, press the TAB key to activate a status window, then press the arrow keys to access the Ethernet > Dyn Stat window.

This screen shows the Dyn Stat display for the 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 multi-channel 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 (Dyn Stat).

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 last line displays these values:

- CLU (Current Line Utilization)

  CLU is 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

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

The following illustration shows the Ether Opt display for the 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 Ethernet I/F parameter in the *MAX Reference Guide.*

Ether Stat window

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 Ethernet Status window, press the TAB key to activate a status window, then press the arrow keys to access the Ethernet > Ether Stat window.

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

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

This 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. It lists those windows that display the status of the Ethernet interface. This screen shows the Ethernet window:

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

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 a line status window, press the TAB key to activate a status window, then press the arrow keys to access the Host/BRI (or Net/BRI) > Line Status window.

For example, when a Net/BRI module is installed in slot 4:

```
40-100 12345678    O
Link   PPP-----
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 following one-character abbreviations to characterize the overall state of the line (see Table 4-1).

Table 4-1. 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 channel usage parameter in the Line 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 describe the state of the B1 and B2 channels, respectively, using the indicators shown in Table 4-2.

Table 4-2. 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 marked Unused in the channel usage parameter of the Line 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 a 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 for an AIM module, press the TAB key to activate a status window, then press the arrow keys to access the Host/Dual > Port*n* Stat > Messages window.

System message logs

The Message Log for the system provides a log of system events. It is listed in the System status window. This example shows a Message Log (System) record 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. See “Log messages.” The fourth line contains connection-specific messages. See Table 4-5.

Log messages

Table 4-3 shows the informational messages that can appear in the Message Log windows:

Table 4-3. Informational log messages

Message	**Description**
Added Bandwidth	The MAX has added bandwidth to an active call.
Assigned to port	The MAX has determined the assignment of an incoming call to 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.
LAN session down	This message appears before Call Terminated if a PPP, MP+, or Combinet session is terminated
LAN session up	This message appears after Incoming Call if a PPP, MP+, or Combinet session is established
Outgoing Call	The MAX has dialed a call.
Removed Bandwidth	The MAX has removed bandwidth from an active call.
RADIUS config error	The MAX has detected an error in the configuration of a RADIUS user entry.
Requested Service Not Authorized	This message appears in the terminal server interface if the user requests a service not authorized by the RADIUS server.

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

Table 4-4. 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.
Far End Hung Up	The remote end terminated the call normally.

Table 4-4. Warning log messages (continued)

Message	**Description**
Incoming Glare	The MAX could not place a call because it saw an incoming “glare” 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 Line profile parameters.
Internal Error	Call setup failed because of a lack of system resources. If this type of error occurs, notify Ascend customer support.
LAN security error	This warning 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 Auth Timeout parameter in the *MAX Reference Guide*.
Network Problem	The call setup was faulty because of problems within the WAN or in the Line 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.
Not Enough Chans	A request to dial multiple channels or to increase bandwidth could not be completed because there were not enough channels available.
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.
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 4-5 shows connection messages that can appear on the fourth line of the Message Log windows:

Table 4-5. Message indicators

Indicator	**Description**
MBID	The MBID parameter 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	This parameter specifies the number of channels added to or removed from a call. It 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	This parameter 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 Combinet 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 CLID (calling line ID). When the CLID appears, the MBID does not.

Modem window

The Main Status Menu contains an entry for each modem card. When you select the modem entry for a card, the Modem Status menu displays. On this menu, each modem is correlated with a display character. To display the Modem Status window for an modem module, press the TAB key to activate a status window, then press the arrow keys to access the V.34 Modem > Modem Status window.

For example, this is a Modem Stats 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 contains a status indicator. The status indicators are described in Table 4-6.

Table 4-6. Modem status characters

Indicator	Mnemonic	Description
.	Nothing	This modem is non-existent.
f	Failed	This modem failed the POST (Power-On Self Test). The modem is unavailable for use.
-	Not used	The modem is not in use.
a	Waiting to go active	The modem has been instructed to dial or answer a call, and the unit is waiting for RLSD (Received Line Signal Detector) to go active.
A	Active	RLSD has already gone 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	The modem is re-initializing after being reset.
q	Open request	The modem is re-initializing after being reset and an open request is waiting to be processed when re-initialization completes.
Q	Open request for virtual connection	The modem is re-initializing after being reset and an open request for Virtual Connection is waiting to be processed when re-initialization completes.
d	Dialing	The first part of the dial string has been sent. This unit is pausing for the modem to read and process the second part before sending it.
v	Virtual connection	A virtual connection session is active on modem. No call is active yet.
o	out of service in interface	The user has disabled the modem from the MAX configuration interface. The modem is unavailable for calls.
O	Out of service	The user has disabled the modem from the MAX configuration interface. The modem is unavailable for calls and a B-channel is set to OutOfService.

Routes window

The Routes window displays the current routing table. To display the Routes window, press the TAB key to activate a status window, then press the arrow keys to access the Ethernet > Routes window.

The following screen shows a Routes window:

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

Note: Press the Down Arrow key to view the next route, or Up Arrow key to view 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 this 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 4-7.

Table 4-7. Routes window values

Value	Description
LAN Active	This active route has a destination on the local subnet.
WAN Active	This active route has a destination off the local subnet.
LOOP Active	This active route has this MAX as a router and destination. No data packets are propagated.
LAN Inactive	This inactive route has a destination on the local subnet.
WAN Inactive	This 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 been connected does not affect the active or inactive status of the route

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. This 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 4-8 lists the session status characters that can appear.

Table 4-8. 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` indicates 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. This screen shows the Statistics display for the first port of an AIM card installed in slot 7:

```
71-300 Albuquerqu+ 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.

- Good means that no errors have been detected during the transmission of the call.
- Fair means that some errors have been detected in transmission.
- Marg means that a significant number of errors have been detected; in this case, reliable transmission is not guaranteed and resynchronization is recommended.

- Poor means that the MAX may 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. Otherwise, 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 Albuquerqu+ O
 Qual Good 2=Poor
 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 specifies 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 these 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 is set to Dynamic and Call Type is set to 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. This host is specified by the Log Host parameter in the Ethernet profile. The log host saves the system status messages in a Syslog file. These messages are derived from two sources—the Message Log display and the CDR display.

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

- Level 4 (warning) and Level 5 (informational) Syslog messages

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

  ASCEND: *slot-n port-n | line-n, channel-n, text-1, 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.

  Text-2 specifies the system name, IP address, or MAC address of the remote end of a session for the “LAN session up” and “LAN session down” messages (text-1).

- Level 5 (notice) 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 this format:

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

  – The *call-event-ID* specifies the event ID in the CDR display.

  – The *event-description* is a description of the CDR event.

  – The *slot-n port-n* address indicates the AIM port, which is suppressed when it is not applicable or unknown.

  – *Data-svcK* indicates the data service in use.

  – *Phone*-n is the phone number.

  Because the Syslog host adds the date, type, and name of all Syslog messages from the MAX, that data is not included in the message format. Some example Syslog entries follow:

```
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 cause 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 reason, progress code, and login host is appended to each CL message. The disconnect cause code uses this format:

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

  Name is the name of a profile. It can contain up to 64 characters. A name containing more than 64 characters is truncated, and '+' is added to the truncated name. The name appears for incoming calls only.

  Xxxx is the disconnect cause 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 4-9 list the Ascend Disconnect codes.

Table 4-9. Ascend disconnect cause codes

Code	Description
0	No reason.
1	The event was not a disconnect.
2	The reason for the disconnect is unknown. This code can appear when the remote connection goes down.

Table 4-9. Ascend disconnect cause codes (continued)

Code	Description
3	The call has disconnected.
4	Calling-Line ID (CLID) authentication has failed.
These codes can appear if a disconnect occurs during the initial modem connection.	
10	The modem never detected Data Carrier Detect (DCD).
11	The modem detected DCD, but became inactive.
12	The result codes could not be parsed.
These codes are related to immediate Telnet and raw TCP disconnects during a terminal server session.	
20	The user exited normally from the terminal server.
21	The user exited from the terminal server because the idle timer expired.
22	The user exited normally from a Telnet session.
23	The user could not switch to SLIP or PPP because the remote host had no IP address or because the dynamic pool could not assign one.
24	The user exited normally from a raw TCP session.
25	The login process ended because the user failed to enter a correct password after three attempts.
26	The raw TCP option is not enabled.
27	The login process ended because the user typed Ctrl-C.
28	The terminal server session has ended.
29	The user closed the virtual connection
30	The virtual connection has ended.
31	The user exited normally from an Rlogin session
32	The user selected an invalid Rlogin option.
33	The MAX has insufficient resources for the terminal server session.
These codes concern PPP connections.	
40	PPP LCP negotiation timed out while waiting for a response from a peer.
41	There was a failure to converge on PPP LCP negotiations.

Table 4-9. Ascend disconnect cause codes (continued)

Code	Description
42	PPP PAP authentication failed.
43	PPP CHAP authentication failed.
44	Authentication failed from the remote server.
45	The peer sent a PPP Terminate Request.
46	LCP got a close request from the upper layer while LCP was in an open state.
47	LCP closed because no NCPs were open.
48	LCP closed because it could not determine to which MP bundle it should add the user.
49	LCP closed because the MAX could not add any more channels to an MP session.
These codes are related to immediate Telnet and raw TCP disconnects, and contain more specific information that the Telnet and TCP codes listed earlier in this table.	
50	The Raw TCP or Telnet internal session tables are full.
51	Internal resources are full.
52	The IP address for the Telnet host is invalid.
53	The MAX could not resolve the hostname.
54	The MAX detected a bad or missing port number.
The TCP stack can return these disconnect codes during an immediate Telnet or raw TCP session.	
60	The host reset the TCP connection.
61	The host refused the TCP connection.
62	The TCP connection timed out.
63	A foreign host closed the TCP connection.
64	The TCP network was unreachable.
65	The TCP host was unreachable.
66	The TCP network was administratively unreachable.
67	The TCP host was administratively unreachable.
68	The TCP port was unreachable.

Table 4-9. Ascend disconnect cause codes (continued)

Code	Description
These are additional disconnect codes.	
100	The session timed out because there was no activity on a PPP link.
101	The session failed for security reasons.
102	The session ended for callback.
120	One end refused the call because the protocol was disabled or unsupported.
150	RADIUS requested the disconnect.
160	The allowed retries for V.110 synchronization have been exceeded.
170	PPP authentication has timed out.
180	The call disconnected as the result of a local hangup.
185	The call disconnected because the remote end hung up.
190	The call disconnected because the T1 line that carried it was quiesced.
195	The call disconnected because the call duration exceeded the maximum amount of time allowed by the Max Call Mins or Max DS0 Mins parameter on the MAX.

Table 4-10 lists the Ascend Connect codes.

Table 4-10.Ascend Connect codes

Code	Explanation
0	No progress.
1	Not applicable.
2	The progress of the call is unknown.
10	The call is up.
30	The modem is up.
31	The modem is waiting for DCD.
32	The modem is waiting for result codes.
40	The terminal server session has started up.
41	The MAX is establishing the TCP connection.

Table 4-10.Ascend Connect codes (continued)

Code	Explanation
42	The MAX is establishing the immediate Telnet connection.
43	The MAX has established a raw TCP session with the host. This code does not imply that the user has logged into the host.
44	The MAX has established an immediate Telnet connection with the host. This code does not imply that the user has logged into the host.
45	The MAX is establishing an Rlogin session.
46	The MAX has established an Rlogin session with the host. This code does not imply that the user has logged into the host.
60	The LAN session is up.
61	LCP negotiations are allowed.
62	CCP negotiations are allowed.
63	IPNCP negotiations are allowed.
64	Bridging NCP negotiations are allowed.
65	LCP is in the Open state.
66	CCP is in the Open state.
67	IPNCP is in the Open state.
68	Bridging NCP is in the Open state.
69	LCP is in the Initial state.
70	LCP is in the Starting state.
71	LCP is in the Closed state.
72	LCP is in the Stopped state.
73	LCP is in the Closing state.
74	LCP is in the Stopping state.
75	LCP is in the Request Sent state.
76	LCP is in the ACK Received state.
77	LCP is in the ACK Sent state.
80	IPXNCP is in the Open state.
90	V.110 is up.

Table 4-10.Ascend Connect codes (continued)

Code	Explanation
91	V.110 is in the Open state.
92	V.110 is in the Carrier state.
93	V.110 is in the Reset state.
94	V.110 is in the Closed state.

- The backoff queue error message in the Syslog file

  Accounting records are kept until they are acknowledged by the accounting server. Up to 100 unacknowledged records are stored in the backoff queue. If the unit never receives an acknowledgment to an accounting request, it will eventually run out of memory. In order to keep this situation from the occurring, the unit deletes the accounting records and displays this error message in 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 are incorrect. The Accounting Key must match the value assigned in the RADIUS clients file or the TACACS+ configuration file.

  – You are using the Livingston server instead of the Ascend server.

- Syslog messages generated by packets seen by a Secure Access Manager firewall

  Syslog messages may be generated for packets seen by the firewall if specified by SAM. By default, SAM will cause a Syslog message to be generated for all packets blocked by a firewall. Syslog messages created by firewalls will use the standard format:

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

  – `date` indicates the date the message was logged by `syslog`.

  – `time` indicates the time the message was logged by `syslog`.

  – `router name` indicates the router this message was sent from.

  – `interface` is the name of the interface (`ie0`, `wan0`, and so on) or *call* if the packet is logged by the call filter as it brings up the link.

  – The `message` format has a number of fields, one or more of which may be present.

  The message fields appear in this order:

  ```
  protocol local direction remote length frag log tag
  ```

  – `protocol` is the four-hexadecimal-digit Ether Type, or one of the following network protocol names: arp, rarp, ipx, appletalk. For IP protocols, it is 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, it will also include the ICMP Code and Type ([`Code`]/[`Type`]/icmp).

– For non-IP packets, *local* is the source Ethernet MAC address of transmitted packets and the destination Ethernet MAC address of received packets. On a non-bridged WAN connection, the two MAC addresses will be all zeros. For IP protocols, it is the IP source address of transmitted packets and the IP destination address of received packets. In the case of TCP or UDP, it will also include the TCP or UDP port number ([*IP-address*];[*port*]).

– *direction* is an arrow (<- or ->) showing the direction in which the packet was traveling (receive and send, respectively).

– For non-IP protocols, *remot*e has the same format as *local* non-IP packets but shows the destination Ethernet MAC destination address of transmitted packets and the source Ethernet MAC address of received packets. For IP protocols, it has the same format as *local* but shows the IP destination address of transmitted packets and the IP source address of received packets.

– *length* is the length of the packet in octets (8-bit bytes).

– *frag* is used to report "frag" if the packet has a non-zero IP offset or the IP More-Fragments bit is set in the IP header.

– *log* is used to report one or more messages based upon the packet status or packet header flags. The packet status messages include:

corrupt—the packet is internally inconsistent

unreach—the packet was generated by an "unreach=" rule in the firewall

!pass—the packet was blocked by the data firewall

bringup—the packet matches the call firewall

!bringup—the packet did not match the call firewall

TCP flag bits that will be displayed include syn, fin, rst.

syn is only displayed for the initial packet, which has the SYN flag and not the ACK flag set.

– *tag* contains any user defined tags specified in the filter template used by SAM.

Sys Options window

The Sys Options window provides a read-only list that identifies your MAX and names each of the features with which it has been equipped. This screen shows the Sys Options window:

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

The Sys Options window can contain the following information.:

Table 4-11.Sys Options information

Option	Description
Security Prof: 1, Security Prof: 2...	Indicates 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 *uptime*	Indicates the system uptime in this format:
	`Up: days:hours:minutes:seconds`
	For example:
	`Up: 13:12:18:26`
	The Days value *turns over* every 999 days. If the unit stays up continuously for 1000 days, the initial field will contain a 0 and will begin incrementing again.

MAX 800	Indicates the Ascend unit.
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 if the MAX can place calls over switched circuits.
MAX Link Installed or MAX Link Not Inst	Indicates if the MAX Link option is installed.
Dyn Bnd Installed or Dyn Bnd Not Inst	Indicates if Dynamic Bandwidth Allocation functionality is available.
ISDN Sig Installed or ISDN Sig Not Inst	Indicates whether or not ISDN signaling is installed.
MAX Dial Installed or MAX Dial Not Inst	Indicates if the MAX Dial client software option is installed.
AuthServer: *a.b.c.d*	Indicates the IP address of the current RADIUS authentication server for this unit.
AcctServer: *a.b.c.d*	Indicates the IP address of the current RADIUS accounting server for this unit.

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.

This 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 indicates 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. An CRC error indicates a frame containing at least one data error.

Network Administration

5

Administering WAN lines and calls

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

- 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.*

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:

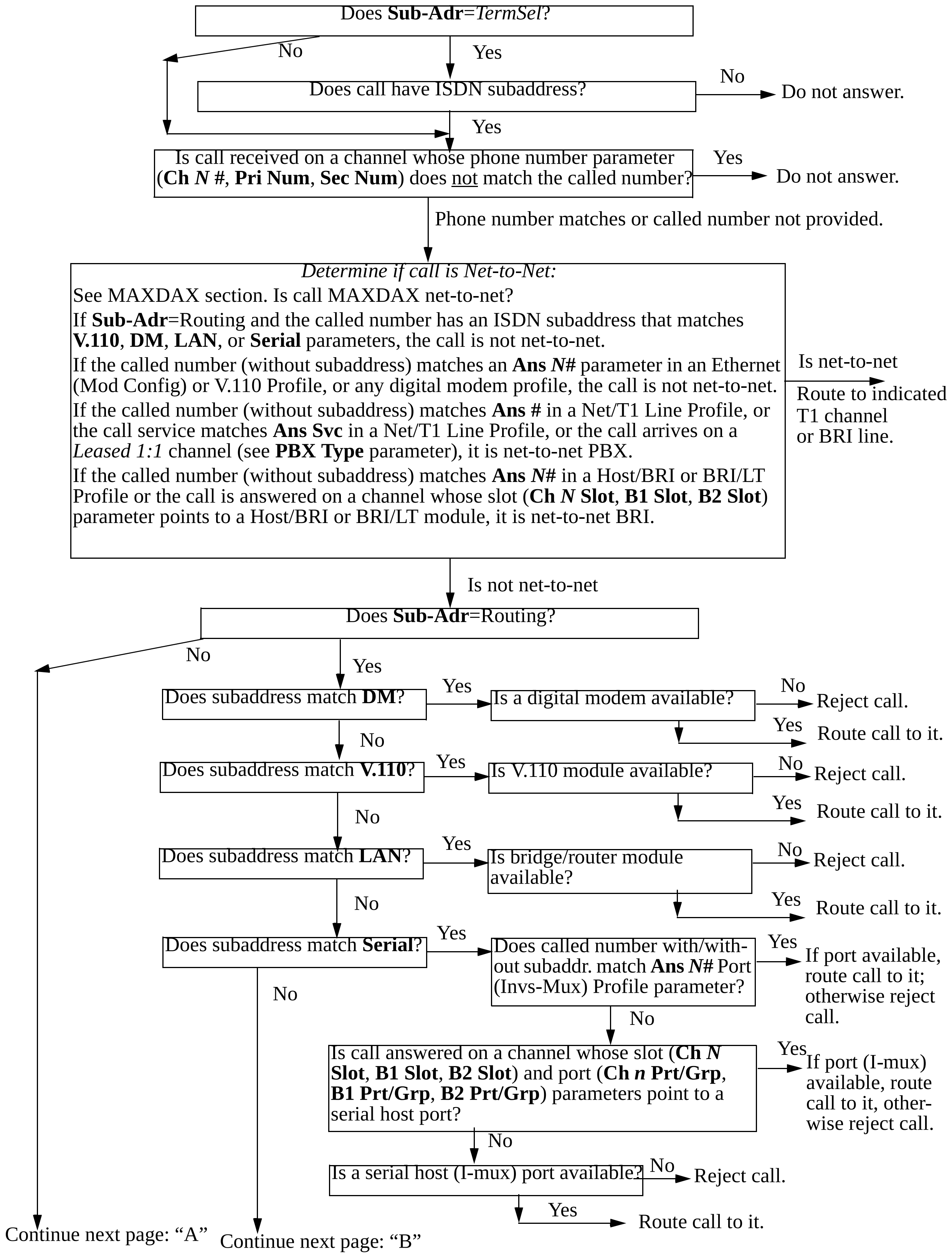
Value	**Result**
`enable modem`	Enables disabled modems. This is the default value.
`disable modem`	Places the modem on the disabled list. When an active connection drops, the card becomes available for maintenance.
`enable modem+chan`	Enables the modem and a disabled B channel.
`disable modem+chan`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

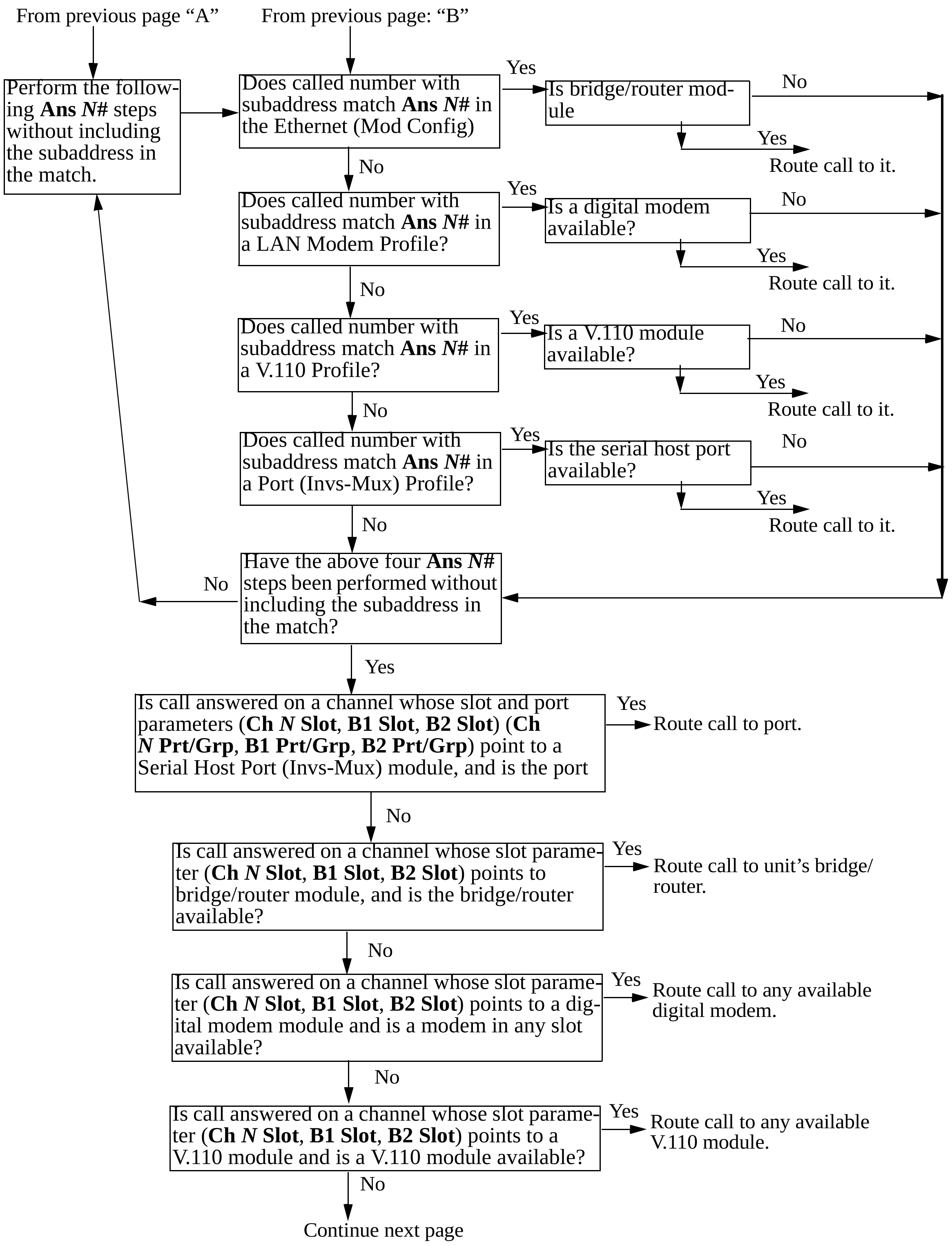
To quiesce a modem slot, use the ModemSlot command. You can set one of the following values:

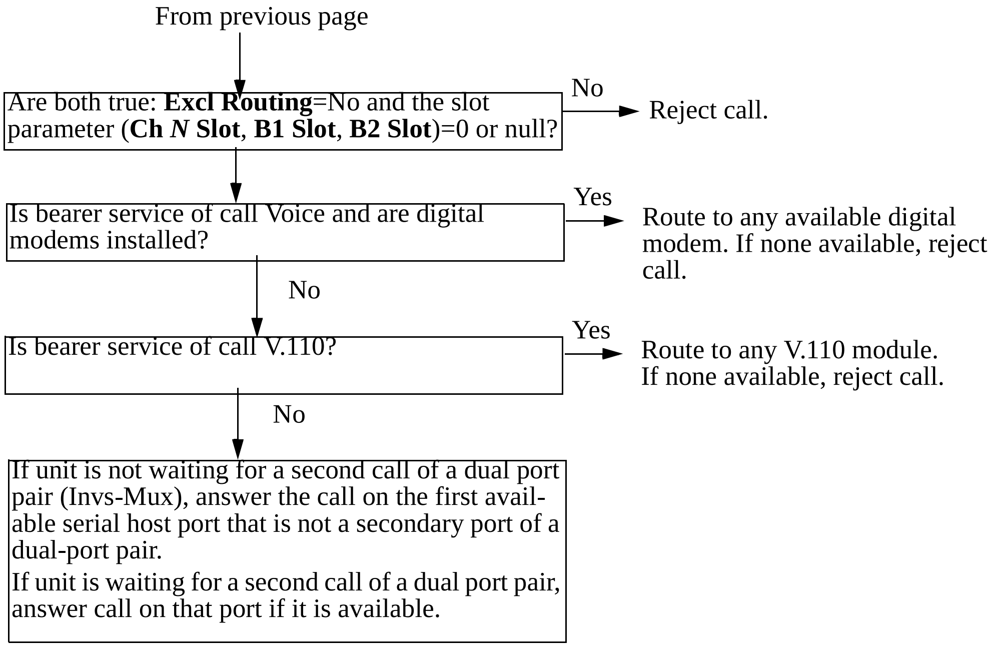
Value	**Result**
`enable slot`	Enables disabled modems on the slot. This is the default value.
`disable slot`	Places all modems that are not active on the disabled list. When the active connections drop, the card becomes available for maintenance.
`enable slot+chan`	Restores the slot card and channels 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.
`disable slot+chan`	Disables all modems on the slot, along with an equal number of B channels.

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*.


Does **Sub-Adr**=*TermSel*?
No
Yes
Does call have ISDN subaddress?
No
Do not answer.
Yes
Is call received on a channel whose phone number parameter (**Ch *N* #**, **Pri Num**, **Sec Num**) does not match the called number?
Yes
Do not answer.
Phone number matches or called number not provided.
Determine if call is Net-to-Net:
See MAXDAX section. Is call MAXDAX net-to-net?
If **Sub-Adr**=Routing and the called number has an ISDN subaddress that matches **V.110**, **DM**, **LAN**, or **Serial** parameters, the call is not net-to-net.
If the called number (without subaddress) matches an **Ans *N*#** parameter in an Ethernet (Mod Config) or V.110 Profile, or any digital modem profile, the call is not net-to-net.
If the called number (without subaddress) matches **Ans #** in a Net/T1 Line Profile, or the call service matches **Ans Svc** in a Net/T1 Line Profile, or the call arrives on a *Leased 1:1* channel (see **PBX Type** parameter), it is net-to-net PBX.
If the called number (without subaddress) matches **Ans *N*#** in a Host/BRI or BRI/LT Profile or the call is answered on a channel whose slot (**Ch *N* Slot**, **B1 Slot**, **B2 Slot**) parameter points to a Host/BRI or BRI/LT module, it is net-to-net BRI.
Is net-to-net
Route to indicated T1 channel or BRI line.
Is not net-to-net
Does **Sub-Adr**=Routing?
No
Yes
Does subaddress match **DM**?
Yes
Is a digital modem available?
No
Reject call.
Yes
Route call to it.
No
Does subaddress match **V.110**?
Yes
Is V.110 module available?
No
Reject call.
Yes
Route call to it.
No
Does subaddress match **LAN**?
Yes
Is bridge/router module available?
No
Reject call.
Yes
Route call to it.
No
Does subaddress match **Serial**?
Yes
Does called number with/without subaddr. match **Ans *N*#** Port (Invs-Mux) Profile parameter?
Yes
If port available, route call to it; otherwise reject call.
No
No
Is call answered on a channel whose slot (**Ch *N* Slot**, **B1 Slot**, **B2 Slot**) and port (**Ch *n* Prt/Grp**, **B1 Prt/Grp**, **B2 Prt/Grp**) parameters point to a serial host port?
Yes
If port (I-mux) available, route call to it, otherwise reject call.
No
Is a serial host (I-mux) port available?
No
Reject call.
Yes
Route call to it.
Continue next page: “A”
Continue next page: “B”


From previous page "A"
From previous page: "B"
Perform the following **Ans *N#*** steps without including the subaddress in the match.
Does called number with subaddress match **Ans *N#*** in the Ethernet (Mod Config)
Yes
Is bridge/router module
No
Yes
Route call to it.
No
Does called number with subaddress match **Ans *N#*** in a LAN Modem Profile?
Yes
Is a digital modem available?
No
Yes
Route call to it.
No
Does called number with subaddress match **Ans *N#*** in a V.110 Profile?
Yes
Is a V.110 module available?
No
Yes
Route call to it.
No
Does called number with subaddress match **Ans *N#*** in a Port (Invs-Mux) Profile?
Yes
Is the serial host port available?
No
Yes
Route call to it.
No
No
Have the above four **Ans *N#*** steps been performed without including the subaddress in the match?
Yes
Is call answered on a channel whose slot and port parameters (**Ch *N* Slot**, **B1 Slot**, **B2 Slot**) (**Ch *N* Prt/Grp**, **B1 Prt/Grp**, **B2 Prt/Grp**) point to a Serial Host Port (Invs-Mux) module, and is the port
Yes
Route call to port.
No
Is call answered on a channel whose slot parameter (**Ch *N* Slot**, **B1 Slot**, **B2 Slot**) points to bridge/router module, and is the bridge/router available?
Yes
Route call to unit's bridge/ router.
No
Is call answered on a channel whose slot parameter (**Ch *N* Slot**, **B1 Slot**, **B2 Slot**) points to a digital modem module and is a modem in any slot available?
Yes
Route call to any available digital modem.
No
Is call answered on a channel whose slot parameter (**Ch *N* Slot**, **B1 Slot**, **B2 Slot**) points to a V.110 module and is a V.110 module available?
Yes
Route call to any available V.110 module.
No
Continue next page


From previous page
Are both true: **Excl Routing**=No and the slot parameter (**Ch *N* Slot**, **B1 Slot**, **B2 Slot**)=0 or null?
No
Reject call.
Is bearer service of call Voice and are digital modems installed?
Yes
Route to any available digital modem. If none available, reject call.
No
Is bearer service of call V.110?
Yes
Route to any V.110 module. If none available, reject call.
No
If unit is not waiting for a second call of a dual port pair (Invs-Mux), answer the call on the first available serial host port that is not a secondary port of a dual-port pair.
If unit is waiting for a second call of a dual port pair, answer call on that port if it is available.

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.

- `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:

- `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 `techpubs`:

```
ascend% traceroute techpubs
```

```
traceroute to techpubs (10.65.212.19), 30 hops MAX, 0 byte packets
 1  techpubs.eng.ascend.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 techpubs (10.65.212.19), 60 hops MAX, 0 byte packets
 1  techpubs.eng.abc.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 `-i` option, or milliseconds, using the `-I` 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 `-I` option, or seconds, using the `-i` 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 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 5-1 shows an example of a DNS table on a MAX.

Figure 5-1. 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 Outpacket
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 *Network Configuration Guide* 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 *`Network Configuration Guide`* for your MAX.
`Octets`	Total number of bytes processed by the interface.

Field	Description
`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 5-5.

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 packetsize] 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 CFFF1234:000000000001
```

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 (EE000001:000000000001): 12 data bytes
52 bytes from (EE000001:000000000001): ping_id=0 time=0ms
52 bytes from (EE000001:000000000001): ping_id=1 time=0ms
52 bytes from (EE000001:000000000001): ping_id=2 time=0ms
?
--- novl1 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 Netware Pings command. For example:

```
ascend% show netware 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 Netware Stats command. For example:

```
ascend% show netware 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 Netware Servers command. For example:

```
ascend% show netware 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: *`network number`*:*`node number`*:*`socket number`*

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  00000000000  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.

SNMP and Syslog Configuration

6

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 Mgr*N* and WR Mgr*N* 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 Mgr*N* parameters. Leave the WR Mgr*N* 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.
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 `ConsoleEntry` 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 datestamp 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, *xxxxxxxxxxx* —The MAX has received a call on channel *`m`* of line *`n`*. The MAX has assigned it an identification number of *`xxxxxxxxxxx`*. 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, *xxxxxxxxxxx*—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, *xxxxxxxxxxx*—The call has connected.

call *n* AN slot *x* port *`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 6-11.

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.

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.

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 reattempts. 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.

Disconnect code	Description
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.
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.

Disconnect code	Description
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.
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.

Disconnect code	Description
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.
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.

Progress code	Description
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.
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

This appendix contains the following sections:

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 1TR6 (Germany), see Table A-2.

Table A-1 lists the numeric cause codes and provides a description of each.

Table A-1. ISDN cause codes

Code	Cause
0	Valid cause code not yet received
1	Unallocated (unassigned) number
2	No route to specified transit network (WAN)
3	No route to destination
4	Send special information tone
5	Misdialed trunk prefix
6	Channel unacceptable
7	Call awarded and being delivered in an established channel
8	Prefix 0 dialed but not allowed
9	Prefix 1 dialed but not allowed
10	Prefix 1 dialed but not required

Table A-1. ISDN cause codes (continued)

Code	Cause
11	More digits received than allowed, but the call is proceeding
16	Normal clearing
17	User busy
18	No user responding
19	No answer from user (user alerted)
21	Call rejected
22	Number changed
23	Reverse charging rejected
24	Call suspended
25	Call resumed
26	Nonselected user clearing
27	Destination out of order
28	Invalid number format (incomplete number)
29	Facility rejected
30	Response to STATUS ENQUIRY
31	Normal, unspecified
33	Circuit out of order
34	No circuit/channel available
35	Destination unattainable
37	Degraded service
38	Network (WAN) out of order
39	Transit delay range cannot be achieved
40	Throughput range cannot be achieved
41	Temporary failure
42	Switching equipment congestion
43	Access information discarded

Table A-1. ISDN cause codes (continued)

Code	Cause
44	Requested circuit channel not available
45	Pre-empted
46	Precedence call blocked
47	Resource unavailable, unspecified
49	Quality of service unavailable
50	Requested facility not subscribed
51	Reverse charging not allowed
52	Outgoing calls barred
53	Outgoing calls barred within Call User Group (CUG)
54	Incoming calls barred
55	Incoming calls barred within CUG
56	Call waiting not subscribed
57	Bearer capability not authorized
58	Bearer capability not presently available
63	Service or option not available, unspecified
65	Bearer service not implemented
66	Channel type not implemented
67	Transit network selection not implemented
68	Message not implemented
69	Requested facility not implemented
70	Only restricted digital information bearer capability is available
79	Service or option not implemented, unspecified
81	Invalid call reference value
82	Identified channel does not exist
83	A suspended call exists, but this call identity does not
84	Call identity in use

Table A-1. ISDN cause codes (continued)

Code	Cause
85	No call suspended
86	Call having the requested call identity has been cleared
87	Called user not member of CUG
88	Incompatible destination
89	Nonexistent abbreviated address entry
90	Destination address missing, and direct call not subscribed
91	Invalid transit network selection (national use)
92	Invalid facility parameter
93	Mandatory information element is missing
95	Invalid message, unspecified
96	Mandatory information element is missing
97	Message type nonexistent or not implemented
98	Message not compatible with call state, or message type nonexistent or not implemented
99	Information element nonexistent or not implemented
100	Invalid information element contents
101	Message not compatible with call state
102	Recovery on timer expiry
103	Parameter nonexistent or not implemented, passed on?
111	Protocol error, unspecified
127	Internetworking, unspecified

Table A-2 lists the cause codes for the 1TR6 switch type.

Table A-2. ISDN cause codes for 1TR6 switch type

1TR6 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.)

Table A-2. ISDN cause codes for 1TR6 switch type (continued)

1TR6 Code	Cause
58	No user responding. (No TE has responded to the incoming SETUP or call has been interrupted, absence assumed—expiry of call timeout T3AA.)
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

DO menus do not allow most operations

When the list of DO commands appears, many operations might not be not 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.

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.

ISDN BRI interface problems

Problems sometimes encountered with ISDN BRI interfaces include calls not dialed or answered reliably, BRI lines not dialing or answering calls, apparent logical-link failures, and WAN calling errors in netbound BRI calls.

Calls are not dialed or answered reliably

If calls are not dialed or answered reliably, 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.

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 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.

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 5.8x8=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 guide 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
`ascend`	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 = ffdffbfc dir=3
Modem 8:8, 54 calls, 1 bad, last 32 calls = ffffffff dir=3
Modem 8:3, 63 calls, 1 bad, last 32 calls = fffbffff dir=3
Modem 8:2, 74 calls, 1 bad, last 32 calls = ffffffff dir=3
Modem 8:7, 64 calls, 2 bad, last 32 calls = ffbfffbf dir=3
Modems on suspect list:
Modem 8:1, 57 calls, 0 bad, last 32 calls = ffffff00 dir=3
Modems on disabled list:
Modems on dead list:
Modems on busy list:
Modem 8:5, 65 calls, 2 bad, last 32 calls = fffffffd dir=3
Modem 8:6, 58 calls, 1 bad, last 32 calls = ffffffff dir=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:

```
ffdffbfc = 11111111110111111111101111111100
```

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
```

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
port 0-#	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.
n	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. 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 111occurs 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.

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: mhpe1bip 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>
```

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
`ascend`	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: Modfies 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.

Variable	Description
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.
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
19DEMDRV-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, WANNext, WANOpen

PPPFSM

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 **`pppfsm`** at the command prompt.

Example: The following display shows the complete establishment of a PPP session.

```
MAX> pppfsm
PPPFSM state display is ON
PPPFSM-97: Layer 0   State INITIAL     Event OPEN...
PPPFSM-97: ...New State STARTING
PPPFSM-97: Layer 0   State STARTING    Event UP...
PPPFSM-97: ...New State REQSENT
PPPFSM-97: Layer 1   State INITIAL     Event UP...
PPPFSM-97: ...New State CLOSED
PPPFSM-97: Layer 2   State INITIAL     Event UP...
PPPFSM-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: pppMpNegUntimeout last 0 layer 0
PPPIF-110: pppMpNegUntimeout last 0 layer 0
PPPIF-110: LCP Opened, local ’Answer’, remote ’’
PPPIF-110: _openAuthentication
PPPIF-110: pppMpNegUntimeout 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: pppMpNegUntimeout last 0 layer 6
PPPIF-110: pppMpNegUntimeout last 0 layer 4
PPPIF-110: pppMpSendNeg Pkt
PPPIF-110: pppMpSendNeg Pkt
PPPIF-110: pppMpNegUntimeout last 0 layer 4
PPPIF-110: IPNCP Opened to
PPPIF-110: pppMpSendNeg Pkt
PPPIF-110: pppMpNegUntimeout 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: ppinfo *index* [all]

Example:

Syntax element	Description
index	Selects a particular PPP information table.
all	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 acknowledgment 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.

Successsful 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]
```

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:

```
timout[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, timout=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
```

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 ouput 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
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

Identifier	Description
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
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)

Identifier	Title
RFC1934	Ascend's Multilink Protocol Plus (MP+)
RFC1962	PPP Compression Control Protocol (CCP)
RFC1974	PPP Stac LZS Compression Protocol
RFC1989	PPP Link Quality Monitoring
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.

- Definitions and terms
- Guidelines for upgrading system software
- Before you begin
- Upgrading system software with a standard load
- Upgrading system software with a fat or thin load
- Upgrading system software with an extended load
- Upgrading system software from versions earlier than 4.6C to version 5.0A or above
- Using the serial port to upgrade to a standard or a thin load
- Changing to system software that does not support V.90
- System messages

This appendix explains how to upgrade your system software.

Definitions and terms

This document uses the following terms:

Build

The name of the software binary.

For example, `ti.m40` is the MAX 4000 T1 IP-only software build. For the names of all the software builds and the features they provide see `/pub/Software-Releases/Max/Upgrade-Filenames.txt` on the Ascend FTP server.

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.

Standard load

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.

TFTP is the recommended upgrade method for standard loads.

Fat load

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.

You must use TFTP to upgrade to fat loads.

Thin load

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).

TFTP is the recommended upgrade method for thin loads.

Restricted load

6.0.0 or later MAX release denoted by an “r” preceding the build name. For example, rti.m40 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.

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 *do* allow you to access the unit via Telnet.

TFTP is the recommended upgrade method for restricted loads.

Pipeline releases do not have restricted loads.

Extended load

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, `fti.m40` is the extended load for the MAX 4000 T1 IP-only software build.

MAX 6000 and Pipeline releases do not have extended loads.

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.
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, *does* 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-11.

Table C-2. Before upgrading (continued)

Task	Description
Obtain the correct file, either by downloading it from the FTP server or by requesting it from Ascend technical support.	To ensure that you load the correct software binary, you should check the load currently installed on your unit. To do so: **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. If your unit does not display the current load or you are unsure about which load to use, contact technical support.
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.	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`). 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. 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.
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.
If you are using the serial port, make sure you have a reliable terminal emulation program, such as Procomm Plus.	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. 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.

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-11.

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 following command loads `t.m40` into flash from the machine `tftp-server`.:

   ```
   tloadcode tftp-server t.m40
   ```

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:

   ```
   nvramclear
   ```

   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-1 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:

   ```
   nvramclear
   ```

   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:

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:

```
nvramclear
```

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 > TServ 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 understand 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.
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.

Table C-3. System software messages (continued)

Message	Explanation

`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.

Example environments

D

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 these topics:

Note: Future revisions of this manual will contain additional examples. Please send suggestions to `techpubs@ascend.com`.

IP-routing environment

Figure D-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.

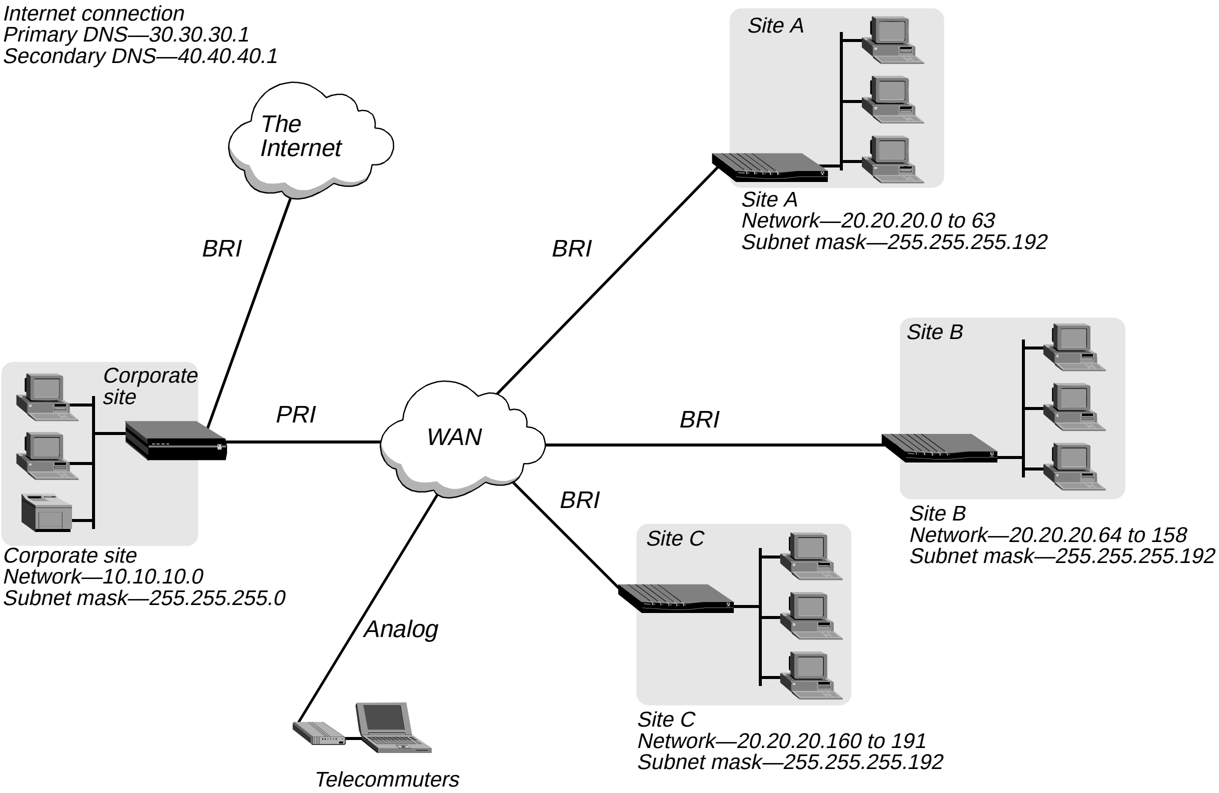


Figure D-1. Example IP-routed environment

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
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
```

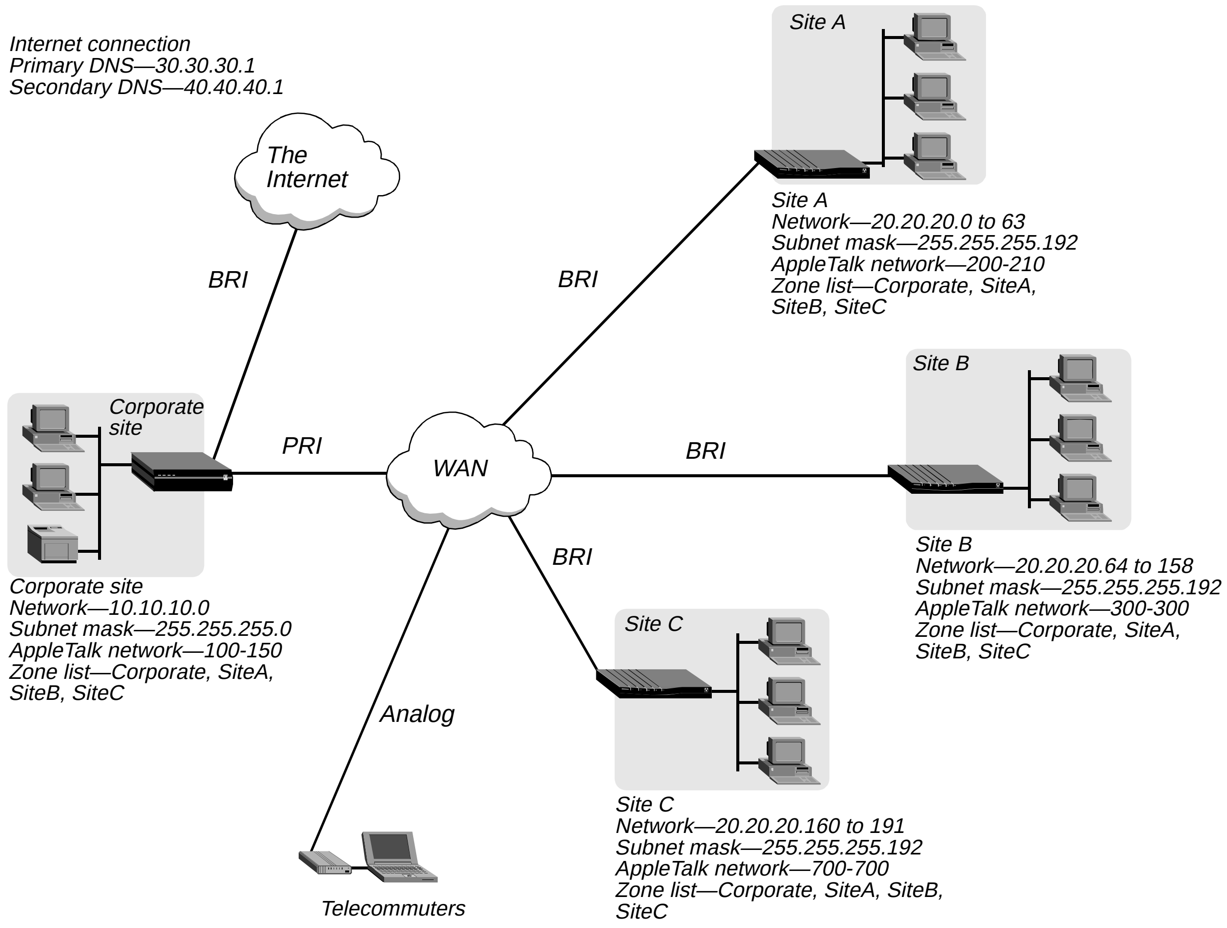
IP-routing and AppleTalk-routing environment

As another example, Smith Company adds AppleTalk devices to the network and sets up an AppleTalk-routed environment, illustrated in Figure D-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 belongs 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 D-2. Example IP-routed environment


Internet connection
Primary DNS—30.30.30.1
Secondary DNS—40.40.40.1
The Internet
BRI
Site A
Site A
Network—20.20.20.0 to 63
Subnet mask—255.255.255.192
AppleTalk network—200-210
Zone list—Corporate, SiteA, SiteB, SiteC
BRI
Site B
Corporate site
PRI
WAN
BRI
Site B
Network—20.20.20.64 to 158
Subnet mask—255.255.255.192
AppleTalk network—300-300
Zone list—Corporate, SiteA, SiteB, SiteC
BRI
Corporate site
Network—10.10.10.0
Subnet mask—255.255.255.0
AppleTalk network—100-150
Zone list—Corporate, SiteA, SiteB, SiteC
Site C
Analog
Site C
Network—20.20.20.160 to 191
Subnet mask—255.255.255.192
AppleTalk network—700-700
Zone list—Corporate, SiteA, SiteB, SiteC
Telecommuters

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...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
```

```
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
AppleTalk...Zone Name #1=Corporate
AppleTalk...Zone Name #2=SiteA
AppleTalk...Zone Name #3=SiteB
END=ETHERNET=200=0
```

Index