Lucent Technologies
Bell Labs Innovations

MAX™
Administration Guide

Ordering Information

You can order the most up-to-date product information and computer-based training online at http://www.lucent.com/ins/bookstore.

Feedback

Lucent Technologies appreciates your comments, either positive or negative, about this manual. Please send them to techpubs@ascend.com.

Lucent Technologies

Customer Service

To obtain product and service information, software upgrades, and technical assistance, visit the eSight™ Service Center at `http://www.esight.com`. The center is open 24 hours a day, seven days a week.

Finding information and software

The eSight Service Center at `http://www.esight.com` provides technical information, product information, and descriptions of available services. Log in and select a service. The eSight Service Center also provides software upgrades, release notes, and addenda. Or you can visit the FTP site at `ftp://ftp.ascend.com` for this information.

Obtaining technical assistance

The eSight™ Service Center at `http://www.esight.com` provides access to technical support. You can obtain technical assistance through email or the Internet, or by telephone.

If you need to contact Lucent Technologies for assistance, make sure that you have the following information available:

- Active contract number, product name, model, and serial number
- Software version
- Software and hardware options
- If supplied by your carrier, service profile identifiers (SPIDs) associated with your line
- 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 Lucent product
- Type of computer you are using
- Description of the problem

Obtaining assistance through email or the Internet

If your services agreement allows, you can communicate directly with a technical engineer through Email Technical Support or eSight Live chat. Select one of these sites when you log in to `http://www.esight.com`.

Calling the technical assistance center (TAC)

If you cannot find an answer through the tools and information on eSight or if you have a very urgent need, contact TAC. Access the eSight Service Center at `http://www.esight.com` and click `Contact Us` below the Lucent Technologies logo for a list of telephone numbers inside and outside the United States.

You can alternatively call (800) 272-3634 for a menu of Lucent services, or call (510) 769-6001 for an operator. If you do not have an active services agreement or contract, you will be charged for time and materials.

Table of Contents

Figures

Tables

About This Guide

The *MAX™ Administration Guide* is intended to help you as you measure, maintain, administer, and troubleshoot the performance of MAX 6000, MAX 3000, and MAX 800 units. A reference to a specific MAX model always accompanies information that applies only to that model. For example, if a description indicates *MAX 6000*, then that information applies only to MAX 6000 units. If a description indicates *MAX*, then that information applies to the MAX 6000, MAX 3000, or MAX 800 unit that is configured to support the feature being described.

To assure continuing satisfactory performance of a MAX unit make use of its indicator lights, the VT100 interface, the terminal-server command-line interface (CLI), DO commands, SNMP, and the Syslog.

⚠️ **Warning:** Before installing or operating your MAX unit, be sure to read the safety instructions in the *Edge Access Safety and Compliance Guide*. For information specific to your unit, see the "Safety-Related Electrical, Physical, and Environmental Information" appendix in your unit's hardware installation guide.

Navigation and usage of all the user interfaces are described in the *Hardware Installation and Basic Configuration Guide* for your unit. You will continue to apply that information as you use this guide.

The flexibility of the True Access™ Operating System (TAOS) software and hardware architecture of the MAX base unit allows you to introduce services as you need them. The MAX offers flash memory, slot cards, and software upgradable protocol support. You can upgrade the features that the MAX unit supports by changing the version of TAOS software running on the unit. The flexiblity of the system software and hardware architecture also results in support for over 15 WAN protocols. The MAX also supports several virtual private networking, several modem, and several bandwidth management protocols. Although the flexibility of the unit's TAOS software and hardware architecture can make the tasks quite complicated, this guide intends to help you discern how best to assure satisfactory performance. Use this guide to gather information about the performance of the MAX unit and to eliminate problems that you may discover.

Note: This manual describes the full set of features for MAX 6000, MAX 3000, and MAX 800 units. Some features might not be available with earlier versions or specialty loads of the software.

What you should know

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

*   Internet or telecommuting concepts

•   WAN concepts

•   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 monospace 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 boldface.
|	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 appear 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.
⚠ **Warning:**	Warns of danger of electric shock.

The MAX documentation set

The MAX documentation set is available on the Documentation Library CD-ROM included with your MAX unit. You can order additional copies of the documentation on CD-ROM or paper from the online bookstore or you can view the documentation online. Go to `http://www.lucent.com/ins/doclibrary` for more information about these options.

The MAX documentation set consists of the following manuals:

*   The *Edge Access Safety and Compliance Guide*
*   The *MAX Administration Guide* (This volume)
*   The *Hardware Installation and Basic Configuration Guide* for your MAX 6000, MAX 3000, or MAX 800 unit
*   The *Network Configuration Guide* for your MAX 6000, MAX 3000, or MAX 800 unit
*   The *MAX Reference*
*   The *MAX Security Supplement*
*   The *TAOS Glossary*
*   The *TAOS RADIUS Guide and Reference*

Administering MAX Hardware

1

From the moment you turn on the power and the MAX unit initiates a power-on self test (POST), you can gather information that allows you to troubleshoot the MAX. Once the MAX is running, you can interpret the indicator lights that the unit includes on its front panel and back-panel. These indicator lights, combined with performance indicators, can lead you to discover hardware and other issues such as problems with the configuration, the Ascend Inverse Multiplexing (AIM) port, related Codec devices, and cables.

For E1, T1, and BRI interface-related information see Chapter 5, "Administering E1 and T1 Services" and Chapter 6, "Administering ISDN."

Troubleshooting POST

A Power-on self test (POST) is a diagnostic test the MAX unit performs when it first starts up or after it completes a system reset. During a POST, the unit checks system memory, configuration, installed cards, compression hardware, and T1 connections.

If the start-up display indicates a failure in any part of the POST, an internal hardware failure has occurred with the unit.

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 unit and your terminal are set at the same speed.

2 Locate the indicator light labeled Fault.

3 Switch on the MAX unit.

Interpreting indicator lights

The MAX 6000, MAX 3000, and MAX 800 series each have a unique set of front panel indicator and back-panel indicator lights that display information about modems, power (including redundant power), fault-tolerance, data-link, and Alarm events.

MAX 6000

The MAX 6000 unit's front-panel indicator lights indicate the status of the system, the PRI interface, and the data transfer in active sessions. Figure 1-1 shows the location of the indicator lights on the front panel of a MAX 6000 unit.

Figure 1-1. MAX 6000 front panel
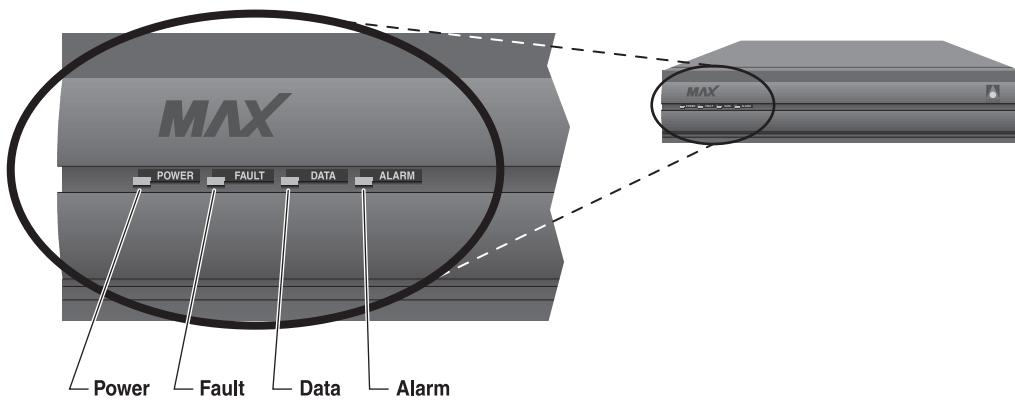
Table 1-1 describes each indicator light located on the front panel of a MAX 6000 unit.

Table 1-1. MAX 6000 front-panel indicator lights

Light	Description
Power	On when the MAX 6000 unit's power is on.
Fault	On in one of two cases: • Hardware self-test in progress. • Hardware failure. When a hardware self-test is in progress, the indicator light stays on. If any type of hardware failure occurs, the indicator light flashes. If the failure is isolated to an expansion card, the MAX 6000 unit might continue to function without the expansion card.
Data	On when calls are active.

Table 1-1. MAX 6000 front-panel indicator lights (continued)

Light	Description
Alarm	On indicates a WAN alarm or a trunk out of service (during line loopback diagnostics, for example). WAN alarms include Loss of Sync, Red Alarm, Yellow Alarm, and All Ones (or AIS).
	For more information about the Alarm indicator light, see"Troubleshooting a Red Alarm" on page 5-2 and "Troubleshooting a blinking Alarm" on page 5-4.

The MAX 6000 unit's front panel indicator lights convey information about the power supplies and the status of the unit's fans. Figure 1-2 shows the location of the indicator lights on the front panel of a Redundant MAX 6000 unit.

Figure 1-2. Redundant MAX 6000 front panel
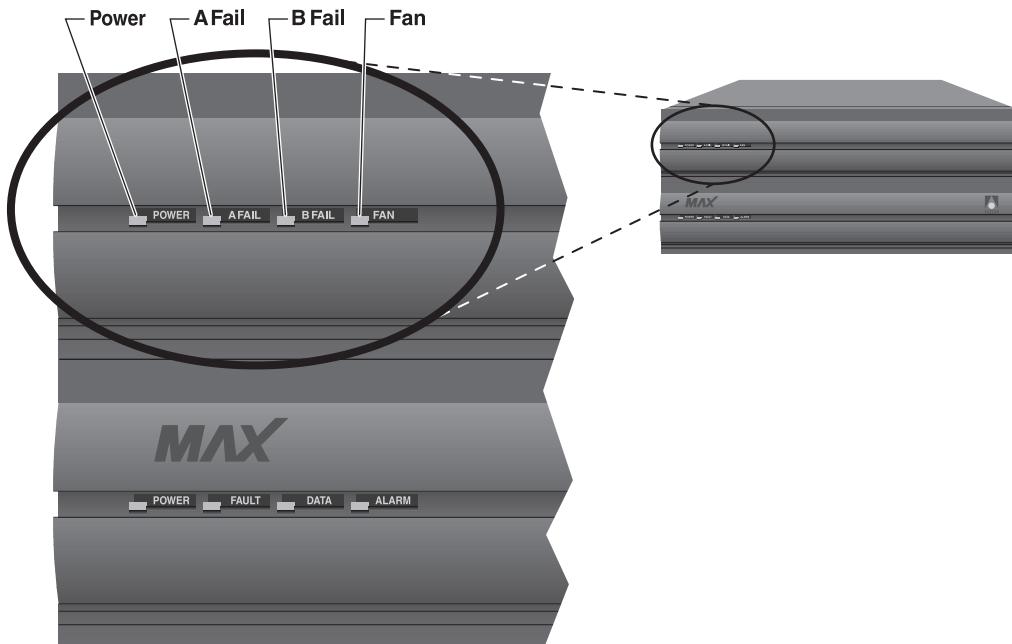
Table 1-2describes each indicator light on the front panel of a Redundant MAX 6000 unit.

Table 1-2. Redundant MAX 6000 front panel lights

Light	Description
Power	On when the Redundant MAX power supply is on.
A Fail	On only if one or more of the voltages from side A of the power supply has failed (+12, +5, +3.3, -12, -5.)

Table 1-2. Redundant MAX 6000 front panel lights (continued)

Light	Description
B Fail	On only if one or more of the voltages from side B of the power supply has failed (+12,+5, +3.3, -12, -5).
Fan	On when the fans are functioning properly (if +12 Vdc from either A or B is good). This indicator light goes off in the event of a fan failure.

For more information, see "Troubleshooting a Red Alarm" on page 5-2 and "Troubleshooting a blinking Alarm" on page 5-4.

The MAX 6000 unit's back-panel indicator lights convey information about network traffic on the unit's Ethernet interface, packet collisions on the Ethernet network, full duplex operation on the Ethernet network, 100BaseT (or 10BaseT) status, and the functional status of the Ethernet interface. Figure 1-3 shows the MAX 6000 back-panel indicator lights, which display the status of the Ethernet interface.

Figure 1-3. MAX 6000 back-panel indicator lights
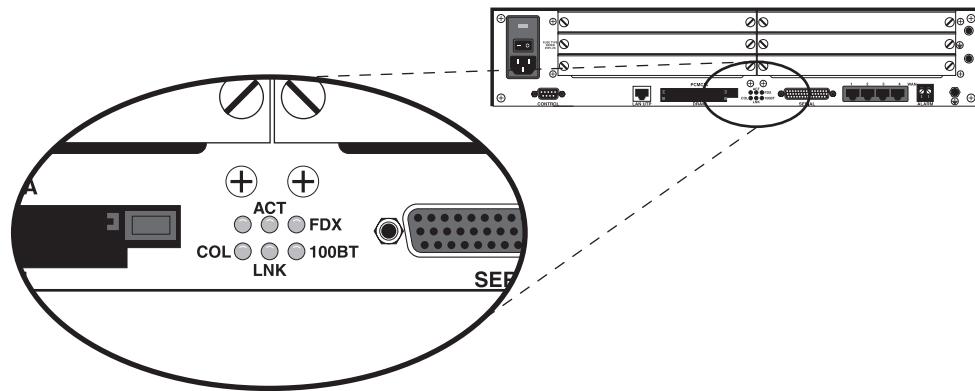
Table 1-3 describes the MAX 6000 unit's Ethernet interface indicator lights.

Table 1-3. MAX 6000 back-panel indicator lights

Light	Description
ACT (Activity)	On when the MAX is detecting activity (network traffic) on its Ethernet interface.
COL (Collisions)	On when the MAX detects packet collisions on the Ethernet.
FDX	On indicates full duplex on the Ethernet.
100BT	On indicates 100BaseT operation. Off indicates 10BaseT operation.
LINK (Link integrity)	On when the Ethernet interface is functional.

MAX 3000

The MAX 3000 unit's front panel indicator lights indicate the power, status of the system self-tests, activity on the unit's Ethernet interface, and Alarm events. Figure 1-4 shows the location of the indicator lights on the front panel of a MAX 3000 unit.

Figure 1-4. MAX 3000 front panel
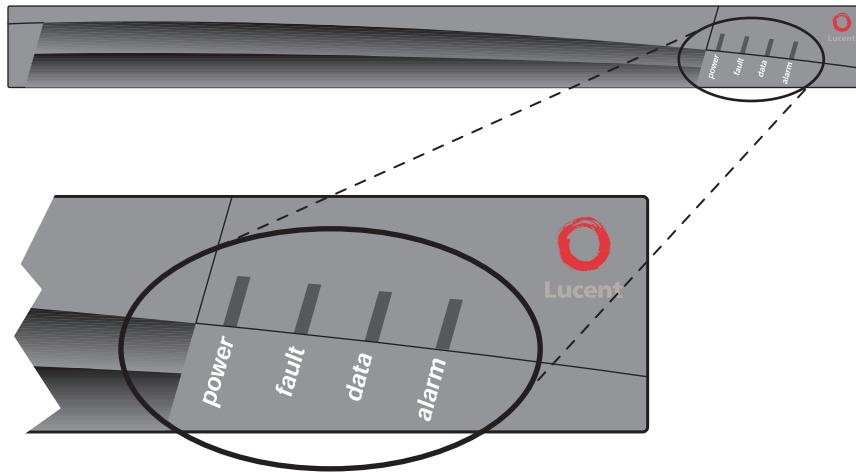
Table 1-4 describes each indicator light on the front panel of a MAX 3000 unit.

Table 1-4. MAX 3000 front-panel indicator lights

Light	Description
Power	On (green) when the MAX power is on.
Fault	On (yellow) in one of two cases: • Hardware self-test is in progress. • Hardware failure. When a hardware self-test is in progress, the light is on. If any type of hardware failure occurs, the light flashes. If the failure is isolated to an expansion card, the MAX may continue functioning without the expansion card.
Data	On (green) at power-up and thereafter if calls are active on the Ethernet interface.

Table 1-4. MAX 3000 front-panel indicator lights (continued)

Light	Description
Alarm	On (amber) at power-up. Thereafter, on indicates a WAN alarm or a trunk out of service (for example, during line loopback diagnostics). WAN alarms include Loss of Sync, Red Alarm, Yellow Alarm, and All Ones (or AIS). For more information regarding the Alarm indicator light, see "Troubleshooting a Red Alarm" on page 5-2 and "Troubleshooting a blinking Alarm" on page 5-4.

The MAX 3000 unit's back-panel indicator lights convey information about the 10 Mbps operation, 100 Mpbs operation, transmitter activity, Full Duplex Mode, Half Duplex Mode, receiver activity, and collisions. Figure 1-5 shows the MAX 3000 back-panel indicator lights.

Figure 1-5. MAX 3000 back-panel indicator lights
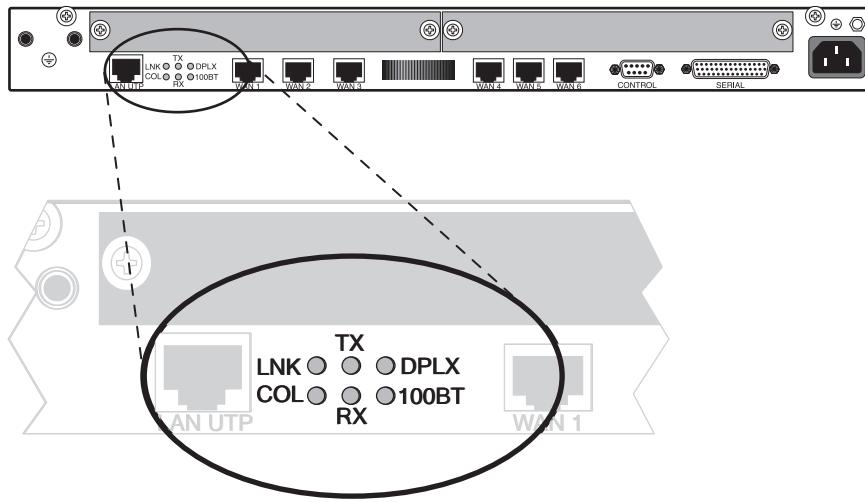
Table 1-5 describes the indicator lights on the MAX 3000 unit's back panel.

Table 1-5. MAX 3000 back-panel indicator lights

Light	Description
LNK	During 10 Mbps operation, indicates Link Valid status. During 100 Mpbs operation, indicates scrambler lock and receipt of valid Idle codes. The light is green when on.
TX	On (green) when transmitter is active.
DPLX	On (green) when the port is in Full Duplex Mode. When the light is off, the port is in Half Duplex Mode.

Table 1-5. MAX 3000 back-panel indicator lights (continued)

Light	Description
100BT	On (green) when 100 Mbps operation is selected for the UTP port.
RX	On (green) when receiver is active.
COL	On (amber) when a collision occurs.

Troubleshooting the Fault indicator light

If the MAX 3000 or MAX 6000 unit's Fault indicator light is off, the unit passed its power-on self tests and you cannot communicate with the VT100 interface, press Ctrl-L to refresh the screen. If you still do not see any data, check the cabling between the MAX unit 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 unit. 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 unit, determine if 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.

The Fault indicator light 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 indicator light remains on longer than a minute, there is a MAX hardware failure. A blinking Fault indicator light also indicates a hardware failure.

Should these situations persist, contact Lucent Technologies technical support.

MAX 800

The MAX 800 unit's front panel indicator lights convey information about the power supply, WAN activity, and installed PCMCIA cards. Table 1-6 describes the indictor lights on the front panel of a MAX 800 unit.

Table 1-6. MAX 800 front panel lights

Light	Description
Power light	The green Power light indicates when the unit has been turned on and is receiving power.

Table 1-6. MAX 800 front panel lights (continued)

Light	Description
Traffic light	The yellow Traffic light blinks to indicate that the unit has been properly installed and is transmitting and receiving data across the network.
PCMCIA cards	Each of the eight modem slots on the MAX 800 unit's back panel has four corresponding lights on the front panel. The lights are: • ON—Power (green) • CD—Carrier Detect (red) • Rx—Receive data (yellow) • Tx—Transmit data (yellow) These four lights provide status information that corresponds to each of the eight PCMCIA cards optionally plugged into the unit.

The activity of the MAX 800 unit's indicator lights and how to interpret them depends on which type of card is in use. You can interpret them when a PCMCIA card ISDN adapter is inserted in the corresponding slot. Table 1-7 describes the PCMCIA card-related indicator lights for a MAX 800 unit.

Table 1-7. PCMCIA card-related indicator lights

Light	Descriptions
ON	Each of the ON indicator lights shows whether the corresponding modem is connected correctly and/or recognized by the MAX 800 unit. When this light is on, the modem is ready to receive data. A flashing ON light means that the MAX 800 unit does not recognize the modem but is going to attempt to receive data through it anyway and interpret the data as Hayes-compatible modem commands. This happens only when the modem is not on the approved list or is malfunctioning. You can eject the questionable modem or let the MAX 800 unit attempt to receive data through it.
CD	A CD light illuminates when an outside phone line connects to the corresponding modem. The light remains illuminated until the remote party disconnects from the line.
Rx	An RX light flashes when data is being received over the phone line through the associated modem.
Tx	A TX light flashes when data is being transmitted over the phone line through the associated modem.

The MAX 800 unit's back panel includes a link-status light that identifies the status of the 10BaseT Ethernet connection. If the light is on, a working connection exists between the MAX

10BaseT port and the Ethernet hub. Figure 1-6 shows the back panel of the MAX 800 unit, including the link status light.

Figure 1-6. MAX 800 back panel
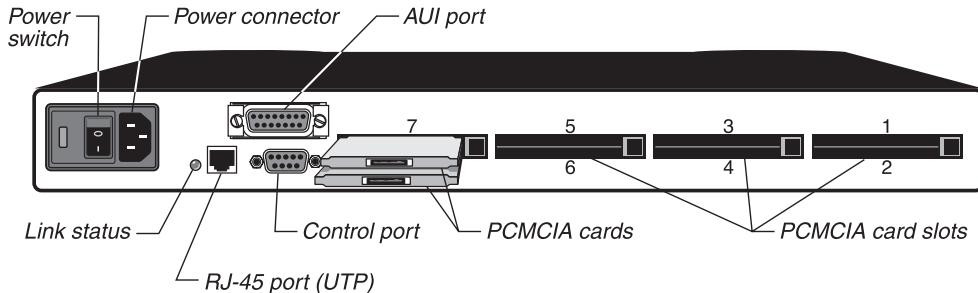
If you need more information about any component, read the description in Table 1-6.

Note: Figure 1-6 shows two PCMCIA card modems inserted in Slots 7 and 8. An ISDN terminal adapter requires two slots.

Troubleshooting the No Logical Link status

In some countries outside the U.S., it is common for no logical link to exist before the MAX unit places a call. In the U.S., when you first plug a line into the unit 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 telephone cables are wired straight through.

If you are running multipoint (passive bus) on your switch, all of the 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 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.

Troubleshooting the AIM port interface

You can connect a videoconferencing codec (coder/decoder) to a port supporting inverse multiplexing to communicate over a point-to-point link. The MAX supports two types of Inverse Multiplexing: Bandwidth ON Demand Interoperability Group (BONDING) and Ascend Inverse Multiplexing (AIM). Both types are supported by the V.35, RS-449, or X.21 port on the MAX unit. Typically, inverse-multiplexed calls are between video codecs and other devices that might need high bandwidth for serial data over the WAN.

Inverse multiplexing uses pins for controlling the data flow through the port. A device sends a signal through a pin and over the line to another device. The signal indicates the control-line state. For example, when a device sends a signal indicating that it has data to send, the control-line state is Request to Send (RTS). If the other device sends a signal to indicate that it is ready to receive data, its control-line state is Data Transmit Ready (DTR). The process of sending these synchronization signals between Inverse Multiplexing ports is called *handshakin*g. You can install two types of inverse multiplexing cards on a MAX unit: Host/AIM6 and Host/Dual. The Host/AIM6 card supports six ports and the Host/Dual card supports two ports. Both cards support of the same dialing protocols: AIM/Bonding, RS-366, V.25 bis, and X.21.

When you install a Host/AIM6 or Host/Dual card on the MAX unit, the card's ports become the default route for inbound data calls, taking precedence over the bridge/router software. Make sure that your call-routing configuration accommodates calls destined for the local Ethernet network.

Note: When you install a Host/AIM6 or Host/Dual card on a MAX unit, the card's ports become the default route for inbound data calls and take precedence over the bridge/router software. Make sure that your call-routing configuration accommodates calls destined for the local Ethernet network. For more information about configuring a MAX unit to support a Host/AIM6 or a Host/Dual card, see the *Network Configuration Guide* for your unit.

Testing the AIM port interface

Test the AIM port interface in one of two ways:

- A local loopback test
- Through true end-to-end communications

Many COder/DECoder (codec) units or other AIM devices support some use of loopback. For example, when a MAX unit is in loopback mode and is connected to a codec, users see their own configuration through the codec. Likewise, most bridge/router devices recognize and report a diagnostic message when a packet is sent out and received by the same module. More often than not, the codec must be configured explicitly to accept the loopback from the communications device.

Local loopback testing is the best tool when troubleshooting the AIM port interface (the interface between the codec and the MAX unit). All of the symptoms and operations described in this section assume you are working from the local loopback diagnostics menu. Unless otherwise specified, the AIM port interfaces in this section can include the Remote Port Modules (RPMs).

The first and most critical aspect of the AIM port interface is the cable or cables connecting the codec to the MAX unit. If you are unsure about the cabling required, contact Lucent Technologies technical support.

Calls fail between AIM ports

The following first-level diagnostic commands can help in troubleshooting calls between AIM ports:

- For a local loopback toward an application at its AIM port interface, use the Local LB command in the Port Diag menu.

- For a loopback toward an application at its remote-end AIM interface, use the DO Beg/End Rem LB command.

- For a channel-by-channel error measurement, use the DO Beg/End BERT command.

- To resynchronize a multichannel call, use the DO Resynchronize command.

To use a DO command, you must be in a profile or status window specific to an AIM port with a call online.

Excessive data errors on calls to AIM ports

Circuit-quality problems sometimes encountered on PRI and BRI lines include excessive data errors or handshaking on calls to AIM ports and scrambling of inbound data during AIM Static calls.

If you encounter a problem in which the MAX reports excessive data errors on some calls to AIM ports, run a Byte Error Rate Test (BERT), which counts data errors that occur on each channel during a call to a AIM port. The BERT checks the data integrity from the MAX unit at one end of the call to the MAX unit at the other end.

If you have verified that the MAX is correctly installed light and configured, and you have previously placed calls without excessive errors, use the DO Beg/End BERT command to run the BERT. Do not clear the call before running the BERT. Run a BERT only under the following conditions:

- A call is active.

- The Call Type parameter is set to AIM, FT1-B&O, or FT1-AIM.

- The Call Mgm parameter is set to Manual, Dynamic, or Delta.

Set the Auto BERT parameter in the Call profile to run an automatic BERT. If the BERT indicates very high errors on some of the channels, clear the call and redial. When redialed, the call might take a different path, correcting the excessive error problem.

Excessive handshaking on calls to AIM ports

Handshaking is a normal and momentary occurrence during call setup and when the MAX unit increases or decreases bandwidth. If there is trouble in the circuits that carry the call, frequent handshaking can occur. If the trouble is serious enough to degrade the quality of the call, the MAX unit disconnects. If handshaking is continuous for over a minute, the problem is probably not due to the quality of the line, and you should call Lucent Technologies technical support.

Inbound data is scrambled during an AIM Static call

Because an AIM Static call does not have a management channel, it is possible for data scrambling to occur because of WAN slips, which are a type of timing error. Slips are a very infrequent occurrence. If you should encounter such a problem, clear the call and redial.

Troubleshooting a codec

A COder/DECoder (codec) unit is a device that encodes analog data into a digital signal for transmission over a digital medium. Codecs are often used for videoconferencing.

A dual-port call is one in which a codec performs inverse multiplexing on two channels in order to achieve twice the bandwidth of a single channel. The codec provides two ports, one for each channel. Two AIM ports on the MAX unit connect a dual-port call to the codec. These ports are the primary port and the secondary port. Because the unit places the two calls in tandem and clears the calls in tandem, it considers them a single call.

The codec indicates that there is no connection

The codec expects one or more of its control lines to be active. If no lines are active, toggle the various outputs available on the local loopback diagnostics menu. If there is still no connection, verify that you have installed the host cables correctly as described in the *Hardware Installation and Basic Configuration Guide* for your MAX unit.

If the cabling is installed correctly, examine the host interface cable pin-outs which are described in the *Hardware Installation and Basic Configuration Guide* for your unit.

The codec does not receive data

If the codec does not receive data, proceed as follows:

1   Verify that the codec is configured to accept a loopback at the communications device.

Frequently, a codec requires certain control lines to be active during data transfer. Therefore, you might want to toggle the various host interface output lines, especially Data Set to Ready (DSR) and Carrier Detect (CD), to ensure that they are active.

2   Check the control line states.

If there is still no data transfer, your cable might not provide one or more control lines required by the host. Refer to the unit's *Hardware Installation and Basic Configuration Guide* for a description of the pins that it requires to be active. The following control lines are generally the most important ones:

–   Carrier Detect (CD)

–   Clear To Send (CTS)

–   Data Set Ready (DSR)

3   Make sure the codec is configured for clocking.

If you are convinced that the control lines are in their correct states, but there is still no data transfer, you might have a clocking problem. The MAX unit provides both the transmit data clocks and the receive data clocks to your equipment through the host interface. The codec must be configured to accept the clocks from the unit.

4   Check your cable length.

If the cable length exceeds the recommended distances, you should be using terminal timing. Alternatively, you might need to install Remote Port Modules (RPM).

5   Check the data rate.

Adjust the data rate from the local loopback diagnostics menu by choosing the number of channels. Some applications cannot work above or below a certain data rate. For example,

some high performance codecs cannot operate at data rates of less than 384 Kbps. In such cases, adjust the number of channels of data being looped back.

The codec cannot establish a call

You might notice that the Port profile is set to establish calls when Data Transmit Ready (DTR) is active, but the codec cannot establish a call. If the codec is going to originate the calls directly by using control-lead dialing, the call origination and clearing mechanisms must be configured for compatibility between the MAX unit and the codec. To verify a compatible configuration from the local loopback diagnostics menu:

1   Disable each of the MAX output control lines except DSR.

    To disable an output control line, toggle it to be Inactive (-). At this time, the codec should indicate that there is no connection.

2   Request an outgoing call from your equipment and monitor the Port Leads status menu of the active ports in the call.

    One or more of the control line inputs should become active and remain active for some period of time. If the DTR lead's input does not change state, your cable is not properly configured. In this case, you must change the cable so that it routes the appropriate host output signal to the DTR input of the MAX. The MAX must use the DTR lead to establish outgoing calls.

3   Once you have made any changes required for verifying that the DTR lead becomes active when the MAX requests the call, configure the Port profile to expect the DTR input.

    In the Port profile, set Dial Call to `DTR Active`.

Calls initiated by control-lead toggling are cleared too soon

If the MAX unit clears a call initiated by control-lead toggling before it completely establishes the call and the call is cleared almost immediately, the Port profile probably has a configuration error. To find the source of the problem, proceed as follows:

1   While monitoring the Port Leads status menu of the AIM ports used in the call, place an outgoing call from the codec.

2   Watch the DTR input carefully while the MAX unit is establishing the call.

    If the DTR input becomes Active (+) and thereafter returns to Inactive (-), the unit is using DTR as a pulse to place the call. Make sure that the Clear parameter in the Port profile is not set to `DTR Inactive`. (Set Clear to `DTR Inactive` only when the application maintains DTR positive during the call.)

3   While your equipment is still dialing the call, toggle the value of the CD output signal to indicate to your equipment that the call completed. At this time, watch the control leads very carefully. Make certain that any control leads that toggle while the call is being established are not used in the Clear parameter to clear the call. This type of configuration error is the most likely cause of a call being cleared almost immediately.

The codec cannot clear a call

If a call cannot be cleared from the codec, the Port profile probably has a configuration error. To verify the source of the problem, proceed as follows:

1   While monitoring the Port Leads status menu of the AIM ports used in the call, place an outgoing call from your equipment.

2   Once the host has requested the outgoing call, toggle the CD output signal to Active (+). The codec should recognize that the call is online.

3   Make a request to clear the call from the codec.

4   Watch the control leads very carefully as one or more of the input control lines toggle. Generally, either DTR or RTS is the line that toggles. Record whether the control lead input goes to Active (+) or Inactive (-) when the call is cleared.

5   Verify that the value of the Clear parameter in the Port profile matches the action that the codec takes when the call is cleared.

Troubleshooting cable issues

Data errors on all calls can indicate that you have installed faulty host interface cables or cables not suited to the application. Information on host interface cabling requirements is found in the *Hardware Installation and Basic Configuration Guide* for your unit.

If you have purchased or built your own cables, verify that the pin-out is the same as the MAX pin-out for compatibility. The *Hardware Installation Guide and Basic Configuration Guide* for your MAX unit lists the host interface pin-outs.

Frequently, a DB-25 breakout box is useful for monitoring control leads and for making quick changes to the cabling. However, because the host interface is running V.35 or RS-422 signal levels, you must verify that the breakout box is passive. That is, you must verify that the breakout box is not regenerating RS-232 level signals.

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 statsDisplay Interface Statistics
show if totalsDisplay Interface Total counts
```

To display the status and packet count of each active WAN link and each local and loopback interface, 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
```

Table 1-8 describes the output of the Show If Stats command.

Table 1-8. Output of the Show If Stats command

Field	Description
Interface	Interface name. For more information, see the *Network Configuration Guide* for your MAX unit.
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
```

Table 1-9 describes the output of the Show If command.

Table 1-9. Show If command output

Field	Description
Name	Interface name. For more information, see the *Network Configuration Guide* for your MAX unit.
Octets	Total number of bytes processed by the interface.
Ucast	Packets with a unicast destination address.
NonUcast	Packets with a multicast address or a broadcast address.
Discard	Number of packets that the interface could not process.
Error	Number of packets with CRC errors, header errors, or collisions.
Unknown	Number of packets the MAX forwarded across all bridged interfaces because of unknown or unlearned destinations.
Same IF	Number of bridged packets whose destination is the same as the source.

Using modems to perform administrative tasks

In order to isolate performance issues related to modems, you can disable specified digital modems and modem slots. A digital modem is an internal device in a MAX unit that enables it to communicate over a digital line with a station connected to an analog line. Incoming modem calls and incoming digital calls come over the same digital line. The MAX unit can accept an incoming call from the network either as a pure digital stream or as a digital stream encoded by Pulse Coded Modulation (PCM). A PCM-encoded digital stream contains a digitized version of the analog waveform sent by a device attached to a modem. The MAX unit can also convert outgoing data into analog waveforms, convert these waveforms to a PCM-encoded digital stream, and send them to the network over a digital line. The network presents the data to the receiving modem in analog form over an analog line. The data looks exactly as it would appear if it had been sent by an analog-based modem.

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

To disable a modem or a modem slot, access the V.90 S56 II Modem (or `K56 Modem-16`)> Mod Config menu.

To disable a particular modem, use the Modem #*N* parameter, where *N* is the modem number from 1 to 30. Set one of the following values:

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

To quiesce an entire modem slot, use the ModemSlot parameter. Set one of the following values:

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

Booting from a FAT-formatted PCMCIA card

The Windows and DOS operating systems use a File Allocation Table (FAT) to keep track of the parts of files stored on devices such as hard disks and Personal Computer Memory Card International Association (PCMCIA) cards. If you administer more than one MAX 6000 unit, use a Windows or DOS operating system, and have access to a FAT-formatted PC card you can boot the units from the PCMCIA card. Only the MAX 6000 supports this feature.

In order to start one or more MAX 6000 units from a FAT-formatted PCMCIA card, you must obtain the TAOS software you want to use for booting, load it on the formatted PCMCIA card, and reset the unit. However, before you boot the MAX 6000 from a PCMCIA card, you must obtain the following two files from the Lucent Technologies FTP site. You need the following two file types:

- The TAOS executable file, which has the filename extension `.m60`. (If you need help to identify the specific file to place on the unit's PC card, see `/pub/Software-Releases/Max/Upgrade-Filenames.txt` on the Lucent Technologies FTP site, `ftp.ascend.com`.)

- The bootstrap loader, also called a handler, in a file named `m60handler.bin`.

Place both files in the TFTP home directory of a TFTP server with network access to the MAX unit.

Loading the software on the PCMCIA card

Use TFTP to load the TAOS executable file and the handler file on the PCMCIA card. When you load software using the MAX 6000 unit's TFTP functionality, the unit saves its configuration during the process.

Note: Your Security profile must permit use of Diagnostics mode or you must log in with the Full Access profile.

To place software on the PC card, proceed as follows:

1 Enter Diagnostics mode by pressing Ctrl-D to display the DO menu and selecting D for Diagnostics.
The > prompt appears.

2 Format the PC card for booting the MAX 6000 unit by entering the following command:

> **format -b**

The -b option reserves space for the handler file.

3 The FAT file system now includes a location for the handler file, which contains a routine that later invokes the TAOS executable file.

To load the handler software from your TFTP server directory enter the following command:

> **tloadcode -b *tftp-server-IPadr* m60handler.bin**

where

- -b specifies that the tloadcode command load the software into the space reserved for the handler file on the PC card.

- *tftp-server-IPadr* is the IP address of the TFTP server on which you have loaded the unit's binary files.

- m60handler.bin is the name of the handler file.

4 Create a boot directory named Current as follows:

> **mkdir /current**

5 Load a TAOS executable file for the unit into the boot directory as follows:

> **fload *tftp-server-IPadr* TAOSfilem60.bin**

where

- *tftp-server-IPadr* is the IP address of the TFTP server on which you have stored the MAX 6000 binary file.

- *TAOSfilem60.bin* is the name of the executable file for the MAX 6000 unit when loaded on the PC card. The name may be as long as 64 characters, but the filename extension must be .bin and the file must be put into the default /current directory, as in the example.

To boot the unit from the TAOS executable file stored on the PC card, enter the Reset command to disconnect all active connections and restart the unit:

> **reset**

This completes the process of loading the software on the PC card.

Managing files on the PC card

TAOS includes file management commands that you use on the FAT file system. Table 1-10 summarizes the PC card file management commands.

Table 1-10. Summary of PCMCIA file management commands

Task	Command and syntax
Format a PC card with the FAT file system.	`format [ -o -e -b ] [device]`
Copy the handler file or TAOS executable file from the TFTP server to the PC card.	`tloadcode [ options ]` `tftp_server_IPadr filename`
Copy a file from the TFTP server to the PC card.	`fload tftp_server_IPadr path1` `[ path2 ]`
Copy an image between the PC card and internal flash memory.	`FImageCopy [-i ∣ -p ]`
Create a directory.	`mkdir path`
Remove a file or an empty directory.	`rm path`
Move a file or directory.	`mv path1 path2`
Report the code version stored on the card.	`fVersionInfo -p`
Lists the files and directories on the card's file system.	`ls path`

DO Commands and Administrative Tasks

2

The MAX unit's user interface is a menu-driven interface accessed through a VT100 terminal or VT100 emulation software running on a PC or workstation. Most of the tasks you perform in order to configure the unit can be done by using parameters in that menu-driven interface. However, one of the first tasks that you perform as an administrator, activating administrative commands, can be performed by using DO commands. Also, use DO commands to perform other administrative tasks. DO menu commands provide ways to manage MAX units. In some cases, they duplicate functions that are accessible through other methods, such as VT100 interface menu items. The availability of a particular command depends on your location in the VT100 interface and on the Security profile in effect.

This chapter describes how to use DO commands to activate administrative permissions. This chapter also reacquaints you with the basics of using the DO commands. The last section of this chapter introduces you to testing and troubleshooting the MAX by using DO commands.

Note: Under most circumstances, diagnostic commands are not required for correct operation of the MAX unit, and in some circumstances might produce undesirable results. However, if you require information about diagnostics DO commands, see "Diagnostic Parameters and Commands" on page B-1.

For an overview of how to access and use the VT100 interface and CLI interfaces, including DO commands, refer to the *Hardware Installation and Basic Configuration Guide* for your unit. For information about Terminal Server DO commands, see Chapter 3, "Terminal-Server Administrative Tasks."

Activating administrative permissions

The DO menu is a context-sensitive list of commands that appears when you press Ctrl-D from any location in the VT100 interface. 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 Ctrl-D combination (or the DO key on the palmtop), 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.

Before you 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 unit 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 unit displays a message informing you that the password was accepted and that the unit is using the new security level:

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

If the password you enter is incorrect, the MAX unit 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.

The commands summarized in Table 2-1 are tools for managing security of MAX units.

Table 2-1. DO menu commands for activating administrative permissions

DO menu command	Function
ESC (DO 0)	Abort and exit the DO menu.
Password (DO P)	The DO Password command enables you to log into the MAX unit.

Performing basic administration

The availability of a particular DO command depends on your location in the VT100 interface and the Security profile in effect. DO commands are used for session management, call management, and testing and troubleshooting. Commands for these functions are summarized in Table 2-2 on page 2-4, Table 2-3 on page 2-6, and Table 2-4 on page 2-10.

Managing sessions

Besides aborting and exiting sessions (ESC DO 0 command), DO commands load parameter values in the current profile, save the VT100 interface menu layout, log in or log out of the unit, save the parameter values in a specified profile, and close an active Telnet session on the unit.

Using the DO Load command

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 appears:

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

If you choose the first option by pressing 0 (zero), the MAX unit 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
```

Saving the VT100 layout

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 Sys Config profile after using the DO Menu Save command.)

- Menu Save does not apply to palmtop controllers, nor does it apply when your VT100 is plugged into an Remote Port Module (RPM) or palmtop port.

Saving the profile

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.

- The Save option does not appear if you are not logged in with operational privileges.

Closing a Telnet session

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

The commands summarized in Table 2-2 are tools for managing sessions with MAX units.

Table 2-2. DO menu commands for session management

DO menu command	Function
ESC (DO 0)	Abort and exit the DO menu.
Load (DO L)	Load parameter values into the current profile.
Menu Save (DO M) 8	Save the VT100 interface menu layout.
Save (DO S)	Save parameter values in the specified profile.
Close TELNET (DO C)	Close the current Telnet session.

Copying FXS profiles with the DO Commands

The MAXPOTS FXS™ slot card provides Plain Old Telephone Service (POTS) functionality to MAX 6000 units that support T1/E1 and to MAX 3000 units that support T1/E1/BRI. The Foreign Exchange Station (FXS) designation indicates that the POTS ports provide subscriber loop functionality, including loop current, supervision, and signaling, similar to that provided by the telephone company's Central Office.

The MAXPOTS FXS slot card enables users to place calls between POTS ports and T1 trunks (inband signaling or PRI), POTS ports and E1 trunks (PRI or R2), or between two POTS ports. Up to four MAXPOTS FXS slot cards can be installed in a MAX 6000 T1 or a MAX 6000 E1. The MAXPOTS FXS card is also available on the MAX 3000 T1, E1 and BRI.

For more information about the MAXPOTS FXS slot card, see the *Network Configuration Guide* for your unit.

There are five possible slot profiles for each MAXPOTS slot card. The first profile listed in the slot's menu is always the active profile. Initially the `default` profile is active. You can save alternative configurations in the other four profiles.

To copy the active profile to one of the alternative profiles, proceed as follows:

1 From Analog FXS > FXS Config, select the active profile.
The active profile appears.

2 Press Ctrl-D to access the DO menu.
The DO menu appears.

3 Select S (Save).

4 Select the alternative profile by using the Up Arrow and, Down Arrow keys, and press Enter.
The active profile is saved to the specified alternative profile.

To activate one of the alternative profiles, copy any alternative profile to the active profile, proceed as follows:

1 From Analog FXS > FXS Config, select the alternative (101, 102, 103, or 104) profile you want to activate.
The alternative profile appears.

2 Press Ctrl-D to access the DO menu.
The DO menu appears.

3 Select L (Load).

Note: The Load option does not appear when you are in the active profile.

4 The alternative profile becomes the active profile.

Managing calls

Use DO commands to manage calls on a MAX unit. Since the availability of a particular DO command depends on your location in the VT100 interface, the Connection profile for the call must be open or selected in the list of profiles.

To manually place a call, proceed as follows.

1 Open the Connection profile for the destination you want to call.

2 Press Ctrl-D.
The DO menu appears. For example:

```
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 called number, followed by a message that the network session is up.

To manually clear a call, proceed as follows.

1   Open the Connection profile or tab to the status window that displays the information
     about 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 is terminated.

Clear a call by opening the Connection profile for the active connection or tab to the status
window in which that connection is listed, as described in the *Hardware Installation and Basic
Configuration Guide* for your unit.

The DO commands summarized in Table 2-3 are for call management.

Table 2-3. DO menu commands for call management

Command	Description
Answer (DO 3)	Answer an incoming call.
Contract BW (DO 5)	Decrease bandwidth.
Dial (DO 1)	Dial the selected or current profile.
Extend BW (DO 4)	Increase bandwidth.
Hang Up (DO 2)	Hang up from a call in progress.
Resynchronize (DO R)	Resynchronize a call in progress.

Testing and troubleshooting

Use DO commands to perform testing and troubleshooting tasks: measure bit-error rate test
(BERT), measure performance with a remote loopback test, and perform remote management
tasks. Use the DO commands discussed in the following sections when you need to analyze the
performance of a MAX unit, the network, or remote units.

Using bit-error tests

A bit-error rate (BER) is the ratio of error bits to the total number of bits transmitted. A MAX
unit can perform a bit-error rate test (BERT) by sending a known pattern of bits and counting

any errors received. The BER is one measure of the unit's, the network's and the remote unit's data transmission quality.

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

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

1 The local device sends a known data pattern over the network.

2 The responding end goes into a DS0-by-DS0 loopback mode of operation.

The signal at the remote end of the test is looped back at the application to a MAX unit interface, rather than at the network to unit interface.

3 By monitoring the data being received against the transmitted pattern, the local device counts the errors it receives on each individual DS0 channel.

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

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

Keep in mind the following additional information:

• A BERT suspends any transfer of user data in either directions.

• All commands that affect the call are disabled, except the command that ends the BERT.

• You must be in a port-specific edit menu or status window to execute the DO Beg/End BERT command.

• It is possible to run the BERT in only one direction at a time. That is, only one side can be the requester.

• To allow a MAX unit time to complete handshaking, you must wait at least 20 seconds between toggling the BERT on and off.

• The DO Beg/End BERT command does not appear if you are not logged in with operational privileges.

The statistics window and bit-error test

Ascend Inverse Multiplexing (AIM) manages the connection of two remotely located MAX units. A Statistics window is an AIM-port-specific window that provides information about line utilization and synchronization delay while a call is up. A Statistics window exists for each AIM port. For example, a Statistics window with the following contents would apply to the first port of an AIM card installed in slot 7:

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

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

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

- `Good`—No errors have been detected during the transmission of the call.

- `Fair`—Some errors have been detected in transmission.

- `Marg`—A significant number of errors have been detected. In this case, reliable transmission is not guaranteed and resynchronization is recommended.

- `Poor`—A MAX unit might drop individual channels from the call, or clear the call automatically.

Fractional T1-Backup and Overflow (FT1-B&O) is a type of call that provides automatic protection of nailed-up circuits. For FT1-B&O calls, the second line of the Statistics window might not show the call duration. When an FT1-B&O call has no bad channels, the call duration appears as usual. But if it does, the number of offline nailed-up channels appears after the call quality. The following screen shows the Statistics window of an FT1-B&O call with two channels offline:

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

(Specify FT1-B&O with the Call Type parameter. For more information about the Call Type parameter, see the *MAX Reference*.)

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

The last line displays the following values:

- `CLU`—Current line utilization. The percentage of bandwidth currently being used by the call for transmitted data, divided by the total amount of bandwidth that is available.

- `ALU`—Average line utilization. The average amount of available bandwidth used by the call for transmitted data during the current history period as specified by the Sec History and Dyn Alg parameters.

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

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

Using remote loopback

A remote loopback is a type of diagnostic test in which the MAX unit transmits a signal that is returned to the sending unit after passing through the network. This allows you to compare the returned signal and get a sense of any problems on the remote unit, the network, and the local unit. Loopbacks are often done by excluding one piece of equipment after another.

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

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

1 The serial host interface of the local MAX unit begins the remote loopback test.

2 The data loops at the serial host interface of the remote MAX unit and comes back to the local unit.

This loopback is also known as a remote data loopback, because the loopback occurs at the DTE/DCE interface. To end a remote loopback, press Ctrl-D 6 (DO 6 on the palmtop controller).

Unplugging the palmtop controller also terminates a remote loopback.

Keep in mind the following additional information:

- A remote loopback disables data flow from the remote host, but the call remains online.

- A remote loopback disables Dynamic Bandwidth Allocation (DBA).

- Only switched and nailed-up channels active during the current call are looped back.

- Drop-and-Insert channels are not looped back.

- You must be in a port-specific edit menu or status window to use the DO Beg/End LB command.

- To allow the MAX unit time to complete handshaking, you must wait at least 20 seconds between toggling the remote loopback on or off.

- When the remote device is a not a Lucent Technologies inverse multiplexer, you cannot set up a remote loopback if the network connection occurs over an ISDN line and the Call profile includes any of the following settings:

  – Call Type is set to `1 Chnl` or `2 Chnl`.

  – Call Type is set to `AIM` or `BONDING` and Call Mgm is set to `Static` or `Mode 1`.

- If the remote device is an ISDN Terminal Adapter (TA), the MAX unit cannot usually perform a remote loopback. ISDN TAs cannot recognize the loopback signal. However, most switching Channel Service Units/Data Service Units (CSU/DSUs) recognize the remote loopback signal that the MAX unit sends, and remote loopbacks are usually possible with such equipment.

- The MAX unit uses a proprietary loopback message when the AIM management subchannel is present (Call Mgm is set to `Manual`, `Dynamic`, or `Delta` in a Call profile).

- The MAX unit uses the CCITT V.54 loopback pattern when no management subchannel is present (Call Type is set to `1 Chnl` or `2 Chnl` and `Call Mgm=Static` in a Call profile).

- If the MAX unit fails to set up a remote loopback, it establishes a loopback at the local host interface that tried to establish the call.

- The DO Beg/End LB command does not appear if you are not logged in with operational privileges.

Using remote management

You can use remote management DO commands to begin and end a remote management session on the MAX unit.

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
```

`port` specifies the serial host port through which you are conducting remote management. To end an AIM remote management session, enter Ctrl-D 8 (DO 8 on the palmtop controller). 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 unit appear.

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

Keep in mind the following additional information:

*   During an AIM call, remote management adds 20 Kbps to the 0.2% overhead of the call, and to that small extent reduces the bandwidth provided to serial host devices using the connection.

*   The DO Beg/End Rem Mgm command is available for connections if the Call profile's Call Type parameter is set to FT1-AIM, FT1-B&O, or AIM (but not if Call Mgm is set to Static).

*   An error message of Remote Mgmt Denied indicates that you have tried to control a MAX unit that is not configured to allow remote management. You cannot remotely manage a device for which Remote Mgmt parameter, in the Sys Config profile, is set to No.

*   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.

The DO commands summarized in Table 2-4 are tools for testing and troubleshooting MAX units.

Table 2-4. DO menu commands for testing and troubleshooting

DO menu command	Function
Beg/End BERT (DO 7)	Starts and stops BERT, a bit error rate test.
Beg/End Rem LB (DO 6)	Starts and stops a remote loopback.
Beg/End Rem Mgm (DO 8)	Starts a remote management session.

DO Command 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 unit 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.

You cannot dial if the Operations parameter is set to 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.

In earlier versions of the software, the MAX unit 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 unit 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 unit downloads the code again, up to two more times. If the checksum still does not match after three download attempts, the unit fails the entire slot card.

This feature helps to reduce the POST failure rates for a particular modem module. The unit's modem modules boots every time the unit power-cycles, and requires boot-up configuration data from the unit. If the first boot-up fails, the unit makes two further attempts to download the code for the unit's modem modules.

Terminal-Server Administrative Tasks

3

You can enable and configure the terminal-server command-line interface from a MAX unit's VT100 interface. You access the terminal-server command-line interface through the DO command menu, the same interface that you use to specify administrative permissions, described in "Activating administrative permissions" on page 2-1. Use the terminal-server command-line interface to test the MAX unit, initiate remote management sessions, disconnect user Telnet connections, administer passwords, and display information about the unit's configuration and performance.

For introductory information about navigation and MAX user interfaces, including the terminal-server command-line interface, see the *Hardware Installation and Basic Configuration Guide* for your MAX unit.

Enabling and configuring the interface

The TSEnabled parameter, in the TServ Options profile, enables or disables terminal services. Terminal services must be enabled to support incoming calls from analog modems or V.120 terminal adapters. If you are unable to access the terminal-server command-line interface, you must verify that the TSEnabled parameter is set to `Yes`. For example:

```
90-900 Mod Config
  TServ Options...
   >TS Enabled=Yes
     Passwd=*SECURE*
     Banner=** Pipeline Terminal Server**
     Login Prompt=Login:
     Passwd Prompt=Password:
     Prompt=ascend%
```

```
Prompt Format=No
Term Type=vt100
Host #1 Service = Telnet
Host #2 Service = Rlogin
Host #3 Service = Telnet
Host #4 Service = Telnet
Host #1 Port = 50
Host #2 Port = 51
Host #3 Port = 52
Host #4 Port = 53
Host #1 User = Rangie
Host #2 User = Disco
Host #3 User = D90
Host #4 User = SII
```

Configuring the interface

Once you have enabled the terminal-server command-line interface, configure the interface with the Banner, Login Prompt, Prompt, Prompt format, and Term Type parameters in the TServ Options profile, in the Mod Config menu. By using these parameters, you control the appearance of the terminal-server command-line interface. For example, the users of the MAX unit's terminal-server command-line interface may have unique terminology that it would be helpful for you to use. Use these parameters to welcome the user to a part of your organization's network that serves a particular function, cue the user that the command-line interface serves a particular group in your organization, or that the command-line interface serves a particular class of user outside of your organization.

The terminal-server menu provides the user with the options of beginning a Telnet, PPP, Rlogin, or Raw TCP session. You can specify the PPP option anywhere in the menu. For Telnet, Raw TCP, and Rlogin, the host authenticates the session. For PPP, the MAX unit authenticates the session.

Table 3-1 summarizes the TServ Options parameters that enable you to configure the terminal-server command-line interface.

Table 3-1. TServ Options parameters

Parameter	Description

Banner	Specifies the text to be used as the terminal-server login banner. Enter up to 84 alphanumeric characters, as in the following example:
	
	`Banner=Welcome to Your Organization`
	
	Following is an example of the default banner setting:
	
	`** Pipeline Terminal Server **`

Table 3-1. TServ Options parameters (continued)

Parameter	Description

Login Prompt	Specifies the string used to prompt for a username when authentication is in use and an interactive user initiates a connection. If the Prompt Format parameter is set to `Yes`, include multiple lines in the login prompt by including carriage-return/line-feed (\n) and tab (\t) characters. To include an actual backslash character, you must escape it with another backslash. For example, you enter the string:
	
	 `Welcome to\n\t\\\Ascend Remote`
	 `Server\\\nEnter your user name:`
	
	 to display the following text as a login prompt:
	
	 `Welcome to \\Ascend Remote Server\\`
	 `Enter your user name:`

Prompt	Specifies the prompt the MAX unit displays during a terminal-server session. Specify a string containing up to 15 characters. The default is `ascend%`.
Prompt Format	Determines whether you are able to use the multiline format for the terminal-server login prompt.
Term Type	Specifies the default terminal type for Telnet and Rlogin sessions. Enter up to 15 characters. The default is `vt100`.

Configuring the Session Options profile

Connections that are idle but continue to be connected present a potential point of entry for unauthorized use of your network's resources. Administer terminal-server idle-time limits by specifying the settings of the parameters shown in Table 3-2, in the Session Options profile, which is included in the Connections profile. Specifying these parameters allows you to assure that resources are allocated to user connections that are currently active and not to those that are inactive, which helps maintain the security of the unit.

Table 3-2 summarizes the Session Options parameters that you use to configure idle-time parameters in the Session Options profile.

Table 3-2. Session Options parameters

Parameter	Description
TS Idle	Specifies the number of seconds that a terminal-server connection must be idle before the MAX unit disconnects the session.
TS Idle Mode	Specifies whether the MAX unit uses the terminal-server idle-timer and, if so, whether both the user and host must be idle before the unit disconnects the session.

Navigating to and from the interface

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

*   From the main VT100 interface 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=Termserv.

*   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 unit displays a command-line prompt. For example:

```
** Pipeline Terminal Server **
ascend%
```

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

The commands in Table 3-3 close the terminal-server command-line interface and return the cursor to the VT100 interface.

Table 3-3. Returning to the VT100 interface

Command	Description
Quit	Closes the terminal-server command-line interface session.
Hangup	Closes terminal-server command-line interface session.
Local	Go to Local mode, a data-transfer mode for calls on an X.25/T3POS network. In Local mode, error recovery is performed locally. The MAX unit does not send supervisory frames (ACKs and NAKs) across the X.25 network. The T3POS PAD is responsible for sending supervisory frames to the T3POS Data Terminal Equipment (DTE).

Testing the MAX unit

Test the MAX unit through the terminal-server command-line interface by using the Test command. Using the Test command open channels to run a test (sometimes called a *self-test*) in which the unit calls itself. The unit places the call on one channel and receives it on another channel. Here is a simple example of entering the Test command:

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

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

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

The Test command has the following format:

test phonenumber [frame-count] [optional fields]

The table below summarizes the one required and the one optional argument that you can include in your Test command

Argument	Specifies
phonenumber	The telephone 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 and specifies the number of frames to send during the test. The default is 100.

There are four optional fields that you may specify in addition to the arguments above. If you do not specify a value, the default value is that specified by the corresponding parameter in the Connection profile. For a information about valid settings for the parameters in the Connection profile, see the *MAX Reference*. The table below summarizes the four optional fields that you can include in your Test command:

Optional field	Specifies
[data-svc=*data-svc*]	A data service identical to any of the values available for the Data Svc parameter.
	A data service is provided over a WAN line and is characterized by the unit measure of its bandwidth. A data service can transmit either data or digitized voice. In a Connection profile, Data Svc specifies the type of data service the link uses.
	Note: Because FT1 calls do not include switched services, the Data Svc parameter lists only 56KR and 64K when Call Type=FT1; in this context, the Data Svc setting indicates how much bandwidth the unit routes to the host for each channel in the connection. When Call Type=FT1-B&O or Call Type=FT1-AIM, the Data Svc parameter refers to the switched channels.
[call-by-call=*T1-PRI-service*]	Any value available to the Call by Call parameter.
	In a connection profile, Call-by-Call specifies the PRI service to use when placing a call using that profile.

Optional field	Specifies
`[primary-number-type=AT&T-switch]`	Any value available to the PRI # Type parameter. The PRI # Type parameter specifies a switch type.
	PRI # Type is used for outbound calls made by the MAX on PRI lines so that the switch can properly interpret the phone number dialed. Ask your PRI provider for details on when to use each of the following settings. This parameter specifies the TypeOfNumber field in the called party's information element.
	Note: The value you specify for PRI # Type in the Dial Plan profile overrides the value of PRI # Type in the Call profile and Connection profile if you have enabled the unit's Dial Plan profiles.
`[transit-number=ECI]`	Any value available to the Transit # parameter.
	Specifies a string for use in the *transit network IE* for PRI calling when going through an Interexchange Carrier (IEC). The default (null) causes the MAX to use any available IEC for long-distance calls.
	Note: The Transit # value in the Dial Plan profile overrides the Transit # value in the Call profile or the Connection profile. This parameter does not apply to nailed connections.

Understanding test results

MAX 6000 and MAX 3000 units that support T1 (or E1) use the first available T1 (or E1) line unless you enable the Use Trunk Grps parameter in the Sys Config menu.

If you enable the Use Trunk Grps parameter in the Sys Config menu, specify the outgoing lines to be used in the test. The Use Trunk Grps parameter specifies the use of trunk groups for all network lines. When trunk groups are in use, channels must be assigned trunk group numbers to be available for outbound calls. In turn, when this parameter is set to `Yes`, channel configurations must specify trunk-group assignments. For more information about each of these parameters, see the *MAX Reference*.

The unit 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 telephone number you specified contained a character other than the numbers 0 through 9 and the characters `()[]-.`
`call failed`	The unit did not answer the outgoing call. Can indicate a wrong telephone number or a busy telephone number. Use the Show ISDN command to determine the nature of the failure.

Message	Explanation
`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 telephone 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 telephone number on the command line.
`test aborted`	The test was terminated (Ctrl-C).
`unit busy`	You attempted to start another test when one was already in progress. 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.
`wrong phone number`	A device other than the MAX answered the call. Therefore, the telephone number you specified was incorrect.

Starting remote management sessions

Multilink Protocol Plus (MP+) uses Point-to-Point Protocol (PPP) encapsulation with Lucent-specific extensions, as described in RFC 1934, to extend the capabilities of Multilink Protocol (MP). MP+ supports session and bandwidth management, enabling the MAX unit to connect to another unit by means of multiple channels. After an MP+ connection has been established with a remote station (for example, by using the DO Dial command), 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. Enter Ctrl-\ at any time to terminate the remote session. 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 2-1).

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

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

Disconnecting user Telnet connections

To disconnect a specified user's Telnet connection use the terminal-server command-line interface. Disconnect the user by specifying the session ID. The resulting disconnect code is identical to the RADIUS disconnect code, allowing you to track all administrative disconnects. To terminate a Telnet session, enter the command as follows:

kill session ID

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

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

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

```
Session 216747095 killed.
```

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

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

Using Set commands

The MAX unit supports administrative Set commands such as Set All, Set Term, and Set Password. To display all of the Set commands, enter the Set ? (command with a question mark), as in the following example:

```
ascend% set ?
```

Use the Set All command to display the current settings. For example:

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

Enable password mode

The Set Password command puts the terminal-server in password mode, in which a Security Dynamics ACE/Server or Enigma Logic SafeWord server at a secure site can display password challenges dynamically in the terminal-server command-line interface.

Dynamics ACE/Servers use ACE authentication, a form of token-card authentication in which RADIUS forwards a connection request to a Security Dynamics ACE/Server. The ACE/Server sends an Access-Challenge packet back through the RADIUS server and the MAX unit to the user who is dialing in. The user sees the challenge message, obtains the current token from the card, and enters the token. A token is a type of password that travels back through the MAX unit and the RADIUS server to the ACE/Server. The ACE/Server sends a response to the RADIUS server specifying whether the user has entered the proper user name and token. If the user enters an incorrect token, the ACE/Server returns another challenge, and the user can again attempt to enter the correct token. The server sends up to three challenges. After three

incorrect tries, the MAX terminates the call. (ACE authentication is also known as SecurID authentication.)

Enigma Logic SafeWord servers use SafeWord authentication, a form of token-card authentication in which RADIUS forwards a connection request to an Enigma Logic SafeWord server. The server sends an Access-Challenge packet back through the RADIUS server and the MAX unit to the user dialing in. The user sees the challenge message, obtains the current password from his or her token card, and enters the current password (also called a token). The token travels back through the MAX unit and the RADIUS server to the SafeWord server. The SafeWord server sends a response to the RADIUS server, specifying whether the user has entered the proper user name and token. If the user enters an incorrect token, the SafeWord server returns another challenge, and the user can again attempt to enter the correct token. The server sends up to three challenges. After three incorrect entries, the MAX unit terminates the call.

When the terminal-server is in password mode, it passively waits for password challenges from a remote Security Dynamics ACE/Server or Enigma Logic SafeWord server. The Set Password command applies only when the MAX unit uses security card authentication. Enter the command as follows:

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

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

Press Ctrl-C to return to normal terminal-server command-line interface operations and disable Password Mode.

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 command-line interface in password mode until all channels have been established.

The Ascend Password Protocol (APP) Server utility provides an alternative way to allow users to respond to dynamic password challenges obtained from hand-held security cards. The APP Server utility also enables a user to respond to password challenges received from an external authentication server, such as an ACE/Server or SafeWord server. To allow a user to supply a password from a host on the local network, you must configure the MAX unit to communicate with the APP Server utility on that host.

Using Show commands

Use Show commands to see uptime and revision information, modem and V.110 card status, Dialed Number Information Service (DNIS) activity, and information about filters.

Displaying uptime and revision

To see how long the MAX unit 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 unit stays up for 1000 consecutive days with no power cycles, the number of days displayed resets to zero and begins to increment again.

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

```
ascend% show revision
MAX-6000-L1 system revision:  tck.m60 8.0.0
```

Displaying modem status

Use the Show Modems command, in the terminal-server command-line interface, to display modem status on a MAX 6000 or MAX 3000. You use this information to determine which modems and V.110 terminal adaptors are online or offline. This can help when troubleshooting the unit.

In the Main Edit menu, you see modems that are installed in the MAX 6000 unit, as in the following example:

```
Main Edit Menu
 00-000 System
 10-000 Net/T1
 20-000 Net/T1
>30-000 K56 Modem-16
```

Enter the Show Modems command to display modem activity. For example, the following output is from a unit with a V.90 K56 II modem card in slot 7:

```
ascend% show modems

slot:item   modem    status
 7:   1      1       online
 7:   2      2       online
 7:   3      3       online
 7:   4      4       idle
 7:   5      5       idle
 7:   6      6       idle
 ...
 ...
 7:   23     23       idle
 7:   24     24       idle
```

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

```
ascend% show modems

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

```
8:6          7      idle
8:7          8      idle
8:8          9      idle
8:9         10      idle
8:12        11      idle
8:13        12      idle
```

Though there are several supported types of modems, all modems respond using the same fields of information. For example, the MAX 3000 unit supports V.90 S56 III Modem-30 and V.90 S56 III Modem-24 modems. The output of the show modems command is much the same as in the preceding example. However there are more modems and slots to display.

Table 3-4 describes each field and its output means.

Table 3-4. Output of Show Modems command

Field	Description
slot item	The slot and port number of the modem. For example, 8:1 indicates the first port on the digital modem card installed in slot 8.
modem	The SNMP interface number of each modem.
status	Modem status, which can be one of the following strings: idle—The modem is not in use. awaiting DCD—The call is up and waiting for Data Carrier Detect (DCD). DCD is a signal sent from a modem to a host, indicating that the modem is online. awaiting codes—The DCD signal has been sent, and the terminal or modem is waiting for modem result codes. online—The call is up. The modem can now send and receive data. initializing—The modem is being reset.

Displaying V.110 terminal adapter status

Use the Show V.100 command, using the terminal-server command-line interface, to display V.110 terminal adapter status on a MAX 6000 or MAX 3000, if you installed any V.110 terminal adapters on the unit. V.110 is a rate-adaptive standard based on fixed frames, that subdivides an ISDN channel so that it can carry one lower-speed data channel. V.110 terminal adapters make asynchronous calls with CCITT V.110 encapsulation. These calls require V.110 modem processing.

An asynchronous device, such as an ISDN terminal adapter, encapsulates its data in V.110. A V.110 card provides eight V.110 modems that each enable the MAX unit to communicate with an asynchronous device over synchronous digital lines.

To display the status of the MAX unit's V.110 terminal adapters, enter the Show V.110 command, as follows:

```
ascend% show v.110s
slot:item    v.110s    status
```

```
4:1          1         in use
4:2          2         in use
4:3          3         in use
4:4          4         open issued
4:5          5         carrier detected
4:6          6         session closed
4:7          7         idle
4:8          8         in use
```

V.110 terminal adapters make asynchronous calls with CCITT V.110 encapsulation. These calls require V.110 modem processing. A V.110 card provides eight V.110 modems that each enable the MAX unit to communicate with an asynchronous device over synchronous digital lines. An asynchronous device such as an ISDN modem encapsulates its data in V.110. The V.110 module in the MAX 3000 unit (only) removes the encapsulation and enables an asynchronous session (a type of terminal-server session).

Displaying call and user activity

Use the terminal-server command-line interface to display call and user activity on the MAX unit. The Show Calls command displays information about active calls on a German 1TR6 (a German ISDN switch standard) or Japanese NTT (Nippon Telephone and Telegraph) switch type. For example:

```
ascend% show calls

Call ID   Called Party ID Calling Party ID InOctets OutOctets

3         5104563434      4191234567          0        0
4         4197654321      5108888888       888888    99999
```

Table 3-5 describes the output included in each of the fields of output.

Table 3-5. Show calls output

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

Displaying active sessions

Displaying active sessions allows you to gather information about active sessions on the MAX unit. Use the Show Users command, in the terminal-server command-line interface, to see

information about the performance of incoming and outgoing calls. Use the command to display the identification of the line, slot, rates, service type, host information, and user.

Display the active sessions by entering the Show Users command as in the following example:

```
ascend% show users

I Session    Line: Slot: Tx      Rx      Service    Host        User
O ID         Chan  Port  Data    Rate    Type[mpID] Address     Name
O 231849873  1:1   9:1   56K     56K     MPP[1]     10.10.68.2  jdoe
I 231849874  1:3   3:1   28800   33600   Termsrv    N/A         Modem 3:1
O 214933581  1:2   9:2   56K     56K     MPP[1]     10.10.4.9   arwp50
O 214933582  1:6   9:3   56K     56K     MPP[1]     MPP Bundle  arwp50
```

Table 3-6 summarizes the output of the Show Users command.

Table 3-6. Show Users command output

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

Table 3-6. Show Users command output (continued)

Field	Content
User Name	The station name associated with the session. Initially, the value is Answer, which is usually replaced with the name of the remote host. For terminal-server command-line interface sessions User Name is the login name. Before completion of login, the field contains the string modem x:y where x and y are the slot and port, respectively, of the modem servicing the session.

Displaying Dialed Number Information Service activity

To display Dialed Number Information Service (DNIS) activity on the MAX unit, use the terminal-server command-line interface. DNIS is a telephone company service that provides information about the called number, such as the name and location of the target user or unit. To display active DNIS sessions, enter the Show DNIS Session command:

```
ascend% show dnis session

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

In the output:

- DNIS#—Displays up to eleven digits of the DNIS number. In the case that the DNIS number contains more than eleven digits, the table displays the last eleven digits.

- Used—Indicates the number of active sessions to the specified DNIS number.

- Max—Indicates the value specified in the Ethernet > Mod Config > DNIS options submenu.

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

```
DNIS Inactive
```

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

```
ascend% show dnis statistics
```

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

In the output:

- Global—Incoming calls using unspecified resources.
- Modem—Incoming calls using modem resources.
- HDLC—Incoming calls using an High level Data Link Control (HDLC) resource.
- V110—Incoming calls using a V110 resource.
- DNIS#—Displays up to eleven digits of the DNIS number.
- Tot—indicates the number of calls received by the specified DNIS number.
- Accept—Specifies the total number of calls accepted by the specified DNIS number.

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

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

```
DNIS Inactive
```

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

```
Clearing all DNIS Statistics...
```

The commands summarized in Table 3-7 are tools for managing DNIS sessions with MAX units.

Table 3-7. DO menu commands for specific protocols

Command	Description
show dnis session	Display active DNIS sessions.
show dnis statistics	Display DNIS statistics.

Using the Show Filters command

From the terminal server, enter the Show Filters command to display a list of the filters in use by sessions active on the MAX unit and display details about individual filters. For information about configuring filters, see the *Network Configuration Guide* for your unit.

Listing the filters in use

From the terminal-server, enter the Show Filters command to display a list of the filters in use by sessions active on the MAX unit. Sessions authenticated by local profiles appear with their associated filter numbers as specified in their Connection profiles. Externally authenticated sessions, such as RADIUS sessions, have no associated filter names or numbers, so they appear with blank fields (indicated by hyphens). For example:

```
** Example Terminal Server Banner **
ascend% show filters
ID   Username Src  Data-Filter Call-Filter Ipx-Filter TOS-Filter
----------------------------------------------------------------------
000  tnt2max1  loc    0            0            0           0
001  tnt2max2  loc    1            3            1           0
002  edmax     ext    –            –            –           –
003  tnt2max4  loc    0            0            0           0
ascend%
```

The first three columns in the output provide the following information:

Column	Information
ID	Indicates an identification number for the active user.
Username	Name for the active user.
Src	Indicates the source of the profile, that is, whether it is downloaded through RADIUS (ext) or is a local profile (loc).

The filter numbers appear in the last four columns, each of which is for a particular type of filter, as follows:

Column	Type of filter
Data-Filter	Packet filter that defines which packets the MAX unit can transmit on a connection.
Call-Filter	Packet filter that defines which packets can bring up a connection or reset the idle-timer for an established link.
IPX-Filter	Service Advertising Protocol (SAP) filter. Determines which SAP advertisements the MAX unit forwards or drops.
TOS-Filter	Type-of-Service filter. Enables you to specify many of the same values as an IP filter, and also to specify a precedence and TOS value.

Displaying filter details

To display the filter details for a particular session, include the filter ID in the Show Filters command:

show filters *ID*

where *ID* is the number shown in the ID column above. For example:

```
ascend% show filters 000
Hostname:       tnt2max1
*********************************************
Data Filter
Direction: In
-----------------------------
Forward = yes
Type = Generic Filter
offset = 0
len = 8
more = no
comp-neq = yes
dummyForPadding = 0
mask = ff:ff:ff:ff:ff:ff:ff:ff:00:00:00:00
value = 12:31:23:12:30:00:00:00:00:00:00:00
*********************************************
Data Filter
Direction: Out
-----------------------------
Forward = yes
Type = Generic Filter
offset = 0
len = 0
more = no
comp-neq = no
dummyForPadding = 0
mask = 00:00:00:00:00:00:00:00:00:00:00:00
value = 00:00:00:00:00:00:00:00:00:00:00:00
*********************************************
```

```
Call Filter
Direction: In
-----------------------------
Forward = no
Type = Generic Filter
offset = 0
len = 0
more = no
comp-neq = no
dummyForPadding = 0
mask = 00:00:00:00:00:00:00:00:00:00:00:00
value = 00:00:00:00:00:00:00:00:00:00:00:00
*********************************************
Call Filter
Direction: Out
-----------------------------
Forward = no
Type = Generic Filter
offset = 12
len = 8
more = yes
comp-neq = no
dummyForPadding = 0
mask = 00:00:ff:ff:ff:00:00:00:ff:ff:00:00
value = 00:00:aa:aa:03:00:00:00:80:9b:00:00
-----------------------------
Forward = no
Type = Generic Filter
offset = 32
len = 3
more = no
comp-neq = no
dummyForPadding = 0
mask = ff:ff:ff:00:00:00:00:00:00:00:00:00

value = 04:04:04:00:00:00:00:00:00:00:00:00
-----------------------------
Forward = no
Type = Generic Filter
offset = 12
len = 2
more = yes
comp-neq = no
dummyForPadding = 0
mask = ff:ff:00:00:00:00:00:00:00:00:00:00
value = 80:9b:00:00:00:00:00:00:00:00:00:00
-----------------------------
Forward = no
Type = Generic Filter
offset = 24
len = 3
more = no
comp-neq = no
```

```
                      dummyForPadding = 0
                      mask = ff:ff:ff:00:00:00:00:00:00:00:00:00
                      value = 04:04:04:00:00:00:00:00:00:00:00:00
                      -----------------------------
                      Forward = yes
                      Type = Generic Filter
                      offset = 0
                      len = 0
                      more = no
                      comp-neq = no
                      dummyForPadding = 0
                      mask = 00:00:00:00:00:00:00:00:00:00:00:00
                      value = 00:00:00:00:00:00:00:00:00:00:00:00
                      *********************************************
                      Ipx Sap Filter
                      Direction: In

                      -----------------------------
                      Type-filter:    exclude
                      Server Type:    2123
                      Server Name:    doom
                      -----------------------------
                      Type-filter:    exclude
                      Server Type:    1116
                      Server Name:    zyst
                      -----------------------------
                      Type-filter:    include
                      Server Type:    9320
                      Server Name:    abcde
                      *********************************************
                      Ipx Sap Filter
                      Direction: Out

                      -----------------------------
                      Type-filter:    include
                      Server Type:    1112
                      Server Name:    nowhere
```

In the previous example, using the Show Filters 000 command displays Data-Filter #000, Call-Filter #3, Ipx-Filter #1, and no TOS filters. The Filters submenu, in the Ethernet menu, can include up to twelve filter profiles. When you go into the individual Filter profile, assign any combination of input or output filters up to twelve. In this example, Data-Filter #1 includes an input and an output filter. Call-Filter #3 includes one input filter and several output filters. Ipx-Filter #1 includes three input filters and one output filter.

Displaying information related to virtual routing

The following Show commands support virtual routing. If you do not specify a VRouter name on the terminal server command line, the MAX unit displays global VRouter information. If you specify a VRouter name, the unit displays information about the specified VRouter.

Command	Syntax with optional VRouter arguments
IPRoutes	`show iproutes [-r vrouterName] [dest]`
IPStats	`show ip stats [[-r] vrouterName]`
IPaddress	`show ip address [[-r] vrouterName] [all]`
ICMP	`show icmp [[-r] vrouterName]`
UDP	`show udp stats [[-r] vrouterName]`
	`show udp listen [[-r] vrouterName]`
TCP	`show tcp stats [[-r] vrouterName]`
	`show tcp connection [[-r] vrouterName]`
Pools	`show pools [[-r] vrouterName]`

For more information about administering virtual routing, see "Using VRouter-related terminal-server commands" on page 7-15.

Changing System Software Versions

4

Caution: When you upgrade a MAX unit's version of TAOS, the newer version might use a configuration file format that is incompatible with the version that preceded it. The upgrade process automatically converts the unit's configuration file to the newer format. You need a backup copy of the configuration file in the older format in case it ever becomes necessary to revert back to a previous version of TAOS. If you fail to create and save a backup copy of the configuration before your change a MAX unit's version of TAOS, you might lose all configuration information.

Caution: If possible use TFTP to change a MAX unit's version of TAOS. TFTP is the most reliable way to obtain, store, and then change the version of TAOS.

Caution: The standard software files you use to upgrade to TAOS 9.0 require additional flash memory available to the MAX 6000 unit only by way of an external PCMCIA flash card. (This does not apply to MAX 3000 and MAX 800 units.)

Before you begin to change a MAX unit's system software, you must enable the unit's Field Service and Operations parameters. You must also verify that you are staying with the same build of the software. In addition to knowing the VT100 interface, you must be prepared to use the DO Command menu, as described in Chapter 2, "DO Commands and Administrative Tasks," to access the diagnostics commands that you use to upgrade or downgrade the unit's system software.

Note: Changing the system software is an exceptional situation in this regard. Under most circumstances, diagnostics commands are not required for correct operation of the MAX unit.

Trivial File Transfer Protocol (TFTP) provides a more reliable way to obtain, store, and install the system software to your unit than is the alternative, which is through the serial port of the unit.

Preparing to change system software

As you prepare to change the system software on a MAX unit, you must verify that Field Service and Operations are enabled on the unit. When upgrading, try to stay with the same build. But you can use an alternative build to avoid having to add memory. You can use the memory provided by a MAX 6000 unit's external PCMCIA card as you change system software. No additional memory is required on a MAX 3000 or MAX 800 units.

Enabling Field Service and Operations parameters

The Field Service parameter, in the Security profile, enables or disables permission to perform Lucent-specific field service operations, such as changing the operating system software on a MAX unit. The Field Service parameter is not applicable if the Operations parameter, also in the Security profile, is set to No. Before you begin the process of changing the unit's version of TAOS, make sure that both parameters are set to Yes in the administrating Security profile. For example, the following Full Access security profile of a MAX 800 unit is correctly configured to support a change of operating system software:

```
00-300 Security
 00-303 Full Access
 >Name=Full Access
  Passwd=*SECURE*
  Operations=Yes
  Edit Security=Yes
  Edit System=Yes
  Field Service=Yes
```

Staying with the same software build

When a particular build of the system software is updated, it retains the same filename. If possible, you should always stay with the same build when you upgrade or downgrade. If you install a different build, your unit can lose its configuration. If this happens, you might need to manually restore your configuration. There can be no automated way to restore configuration data from a backup when changing builds since, if the file formats between the builds are incompatible, no suitable backup exists. For example, your MAX unit might have a T1 interface. If you are attempting to transfer a build that is appropriate for an E1 interface, the unit can display the following message:

```
This load appears not to support your network interface.
Download aborted. Use tloadcode -f to force.
```

If this happens, verify that you have selected the correct build. If the build is intended for another type of unit, that you forcing the download is not recommended.

Alternative builds for a MAX 6000 unit

With two exceptions, the builds you can use to upgrade to TAOS 9.0 require additional flash memory, which is available to the MAX 6000 unit only, by way of an external PCMCIA flash card. (The builds for MAX 3000 and MAX 800 units do not require any additional flash

memory.) To avoid using a PCMCIA flash card, you can upgrade a MAX 6000 unit with one of the following two recommended builds:

- `eik.m60` (an ultrathin load for E1 environments)
- `tik.m60` (an ultrathin load for T1 environments)

In future releases, these ultrathin builds might not be available, and use of the MAX 6000 unit's external flash memory will become a requirement. The current release includes a new feature to prevent a build that is too large from being placed in the unit's internal flash memory. If a build is too large, the unit aborts the download and displays the following message:

```
tftp download aborted due to flash write error
```

The MAX unit then restarts with its previous TAOS version and configuration intact. In releases before to TAOS 9.0, the process appeared to complete successfully although TAOS was corrupted and the configuration unusable.

The `eik.m60` and `tik.m60` builds do not include support for the following features:

- AppleTalk
- BRI
- IPX
- PHS
- POTS
- X.25

For the names of all the software builds and the features they provide, see `/pub/Software-Releases/Max/Upgrade-Filenames.txt` on the Lucent Technologies FTP server.

Using TFTP to upgrade or downgrade

If possible, use TFTP to change a MAX unit's version of TAOS. TFTP is a more reliable way to obtain, store, and then change the version of TAOS than is the alternative. Using TFTP, you can use a MAX 6000 unit's external memory to create redundant backup images, as well as to upgrade the unit's version of TAOS.

Creating redundant backup images for a MAX 6000 unit

MAX 6000 units now support two redundant copies of TAOS code on the PCMCIA flash memory card. If the first version of code becomes corrupt, the unit boots up the second version.

To create the redundant backup image, proceed as follows:

Note: The order of these two steps is not important, but the unit will be unable to recover from a failure in the primary code image until both steps have been executed.

1   Create a backup copy of the currently running binary on the PCMCIA flash card by using the `fBackupImage` debug command:

```
> fBackupImage
```

```
Preparing for image copy...
This load contains an IOP part
Copying 1797281 bytes from PCMCIA flash to PCMCIA...
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
Image copied to high PCMCIA flash successfully.
 >
```

2   Load the `lvs.m60` image into internal flash using the `tload -i` debug monitor
command to support the backup image:

```
> tload -i tftp-server lvs.m60
saving config to flash


loading code from 204.253.164.44:69
file lvs.m60...


tftp download complete. Verifying image...
Downloaded image is OK.
```

Using TFTP to upgrade

To upgrade with TFTP, you must enter the commands in the correct sequence. If you do not
enter them in the correct sequence, you could lose the MAX unit's configuration.

To use TFTP to upgrade system software, proceed as follows:

1   Locate the following and place them in the TFTP server home directory:

– The configuration that is compatible with the version of TAOS to which you will
upgrade.

– The build of the system software version to which you will upgrade.

2   From the unit's VT100 interface, press Ctrl-D to invoke the DO menu, then select
`D=Diagnostics`.

3   At the > prompt, use the `Tsave-m` command to save your current configuration in a way
that allows you to match it with the version of system software with which it is
compatible. For example, the following command saves the configuration named
`config800.cfg` from the TFTP home directory of the server named `tftp-server`:

```
tsave -m tftp-server config800.cfg
```

⚠

Caution: A MAX unit's internal flash storage is limited. Use the `tsave -m` command to assure that the configuration you save is as small as possible. You must retain the saved configuration file permanently. You will need this file if it ever becomes necessary to revert back to the earlier version after you upgrade the unit to TAOS 9.0. The file you save with the `Tsave` command contains all the passwords in clear text. Move this file from the TFTP directory to a secure location after the upgrade procedure is complete.

4   Enter the following command

> **tloadcode *hostname filename***

where ***hostname*** is the name or IP address of your TFTP server, and ***filename*** is the name of the system software on the server (relative to the TFTP home directory).

For example, the command

> **tloadcode tftp-server ebixk.m60**

loads `ebixk.m60` into flash memory from the machine named `tftp-server`.

5   Enter the following command to save your configuration to flash memory:

> `>` **fsave**

Use the command immediately after executing the `tloadcode` command.

6   Enter the following command:

> `>` **nvramclear**

After the unit clears NVRAM memory, the unit automatically resets itself two times.

This completes the upgrade to TAOS 9.0.

After installing TAOS 9.0 you will have a smaller amount of available memory than you had with the previous TAOS release. The software files stored on the flash card have gotten bigger and therefore require more memory. As new features are added to TAOS, the amount of memory used by the operating system grows. Therefore, the units running later versions of TAOS report less available memory. The reduced available memory is not a cause for concern.

Using TFTP to downgrade

To downgrade system software, you must follow the same steps as for upgrading TAOS, with one exception. Instead of using the `fsave` command, as described in step 5 in "Using TFTP to upgrade," enter the following command to restore the compatible configuration to flash memory:

trestore -f *hostname savedConfig*

where ***hostname*** is the name or IP address of your TFTP server, and ***savedConfig*** is the compatible configuration on the server (relative to the TFTP home directory).

For example, the command

trestore -f tftp-server Config803

retrieves `Config803`, a configuration compatible with TAOS 8.0.3, from the unit named `tftp-server`.

Note: The `-f` argument is necessary when downgrading. Failure to use the `-f` argument causes `trestore` to place the configuration in binary format into NVRAM, rendering the configuration unusable to the MAX unit.

Using the serial port to upgrade or downgrade

Caution: Upgrading system software through the serial console deletes 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. For security reasons, password information is not stored in backup files. If you have many passwords, you should consider using TFTP to upgrade your software. (For instructions, see "Using TFTP to upgrade or downgrade" on page 4-3.)

Before upgrading your system through the serial port, make sure you have the following equipment and software:

- An IBM-compatible PC or Macintosh system with a serial port capable of connecting to the MAX unit's Console port.
- A straight-through serial cable.
- Data communications software for your system, with terminal emulation (for example, Procomm Plus, HyperTerminal for the PC, or ZTerm for the Macintosh). Verify that the line-width settings of the communications software are set to at least 80 characters.

Saving your current profiles

Caution: If you use a Windows-based terminal emulator, such as Windows Terminal or HyperTerminal, disable any screen savers or other programs that could interrupt the file transfer. Failure to do so might cause the file transfer to halt and can render the MAX unit unusable.

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 menu's Sys Config profile. You can cancel the backup process at any time by pressing Ctrl-C.

To save the MAX unit's 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.

5   Turn off the Capture feature of your communications program.

6   Print a copy of your configured profile and examine the saved configuration file.

Upgrading system software

To upgrade the software through the MAX unit's serial port:

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 Esc key, the Left Bracket key, the 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 unit.

Your communications program normally takes anywhere from 5 to 15 minutes to send the file to the 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.

3   From the MAX unit's VT100 interface, access the diagnostics monitor by pressing Ctrl-D to invoke the DO menu, and select D=Diagnostics.

4   At the > prompt, enter the Fclear command:

> **fclear**

5   At the > prompt, enter the NVRAMClear command:

> **nvramclear**

This causes the system to reset. When it comes back up, proceed with restoring your configuration.

6   Enter **quit** to exit the Diagnostic interface.

7   Open the Sys Diag menu.

8   Select Restore Cfg, and press Enter.

The following message appears:

Waiting for upload data...

Use the Send ASCII File feature of the communications software to send the configuration file to the unit.

Note: If you are upgrading, the configuration you restore in this step is the one that you saved by following the steps in "Saving your current profiles" on page 4-6. If you are downgrading then the configuration you saved in "Saving your current profiles" is not the correct configuration to restore at this time. If you are downgrading then you must restore the configuration file you saved before you upgraded to the current version of TAOS.

If you have any questions about how to send an ASCII file, consult the documentation for your communications program.

9   When the restore has been completed, the following message appears:

Restore complete – type any key to return to menu

Press any key to return to the configuration menus.

10 Reset the unit by selecting System > Sys Diag > Sys Reset and confirming it.

Restoring passwords

Edit your configuration file and enter the word *SECURE* in each instance of a password and save it as a text-only file. When you use the restore config command, the unit's configuration file and the passwords are restored to the unit.

Note: If you do not save the configuration as a text-only file, you will not be able to transfer it into the MAX unit.

If you restored a complete configuration, one without the modifications described above, then all 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.

After the upgrade

After installing TAOS 9.0 you will have a smaller amount of available memory than you had with the previous TAOS release. The software files stored on the flash card have gotten bigger and therefore require more memory. As new features are added to TAOS, the amount of memory used by the operating system grows. Therefore, the units running later versions of TAOS report less available memory. The reduced available memory is not a cause for concern.

Restoring correct RADIUS parameters

On earlier RADIUS servers, the RADIUS Server submenu consisted of three clients (specific host addresses) and one Server Key for all three clients. If a MAX unit supports the new RADIUS Server, restoration of the unit's configuration causes 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.

If you cannot communicate with the MAX unit through the VT100 control terminal, you might have a problem with terminal configuration, the control port cable, or the MAX hardware.

Notice of discontinuance of configurable RADIUS port and ID space

In earlier versions of the system software, the default settings for User Datagram Protocol (UDP) source ports and ID spaces for communication with a RADIUS server specified the use of a unique source port for each card and a distinct ID space for both authentication and accounting requests. However, the MAX unit could be configured to use a single source port and ID space systemwide, in order to accommodate certain RADIUS server daemons that had a system-unique requirement.

Because no known RADUIS servers continue to maintain this requirement, and because increased port density makes the use of a single port and ID space undesirable, MAX units now always use port-unique source ports and always send RADIUS authentication and accounting requests with distinct RADIUS IDs. The following parameters are therefore no longer supported and have been removed from the External-Auth profile:

```
[EXTERNAL-AUTH]
rad-id-space = distinct
rad-id-source-unique = port-unique
```

The `rad-ip-space` and `rad-id-source-unique` parameters no longer appear in the External-Auth profile. If you downgrade the unit to an earlier release, the parameters revert to their default values for that release.

Administering E1 and T1 Services

5

A T1 line supports 24 64-Kbps channels, each of which can transmit and receive data or digitized voice. The line uses framing and signaling to achieve synchronous and reliable transmission. The most common configurations for T1 lines are ISDN Primary Rate Interface (T1 PRI) and unchannelized T1, including fractional T1. The MAX unit supports up to four T1 lines for up to 96 concurrent sessions.

An E1 Primary Rate Interface (E1/PRI) line consists of 32 64-Kbps channels. E1/PRI uses 30 B channels for user data, one 64-Kbps D channel for ISDN D-channel signaling, and one framing channel. The B channels can be all switched, all nailed up, or a combination of switched and nailed up. The E1/PRI line is a standard in Europe and Asia called CEPT G.703.

A T1 Primary Rate Interface (T1/PRI) line has a total bandwidth of 1.544 Mbps. T1/PRI uses 23 B channels for user data, and one 64-Kbps D channel for ISDN D-channel signaling. The B channels can be all switched, all nailed up, or a combination of switched and nailed up. The T1/PRI line is a standard in North America, Japan, and Korea. Connect this type of line to standard voice, Switched-56, Switched-64, Switched-384, Switched-1536, and MultiRate data services. Using a feature called PRI-to-TI conversion, the MAX can share the bandwidth of a T1/PRI line with a PBX.

Use the MAX unit's indicator lights to begin troubleshooting and diagnosing E1 or T1 problems. Use line diagnostics to perform tests on the unit and see the information that is displayed in the unit's status windows to determine whether or not E1 or T1 performance is meeting your standards. By verifying telephone numbers and using one VT100 interface parameter, remedy a Trunk Down state on the unit. Use the terminal-server command line interface (CLI) to test lines, reset the unit, clear calls, and display clock source. Verify

parameters in the VT 100 interface that are E1-specific, T1-specific, T1/PRI-specific, and PBX-T1-specific.

The MAX 6000 and MAX 3000 units also support unchannelized T1 services and fractional T1 services. An unchannelized T1 service uses the entire bandwidth of a T1/PRI line (1.544 Mbps) or an T1/PRI line (2.048 Mbps). Use an unchannelized line for a nailed-up connection, such as the link to a Frame Relay network. The MAX unit treats the line as though it were a single connection at a fixed speed, without individual channels. For more information, see Chapter 8, "Administering PAD, X.25, and Frame Relay."

Troubleshooting a Red Alarm

Without using any of the MAX 6000 or the MAX 3000 unit's available interfaces, the indicator lights help you begin to gather information about the performance of the unit. For example, if the Alarm indicator light indicates that the line is in a Red Alarm state, the MAX unit cannot establish proper synchronization and frame alignment with the WAN. Synchronization is a method of ensuring that the receiving end of a WAN connection can recognize characters in the order in which the transmitting end sent them, and can know where one character ends and the next begins. Without synchronization, the receiving end perceives data simply as a series of binary digits with no relation to one another. Frame alignment is a method of ensuring that the sending end of a WAN connection can recognize characters in the order in which the receiving end returns them, and can know where one character ends and the next begins.

After you plug an E1 or T1 line into the unit or change the settings that affect framing and synchronization, allow 30 seconds for the Red Alarm state to end.

Verifying enabled lines

The MAX 6000 or MAX 3000 unit that supports E1 or T1 can accommodate up to two line profiles in each of its Net/E1 or Net/T1 interfaces. If you are not using one of the MAX unit's lines and it is enabled in the Line Config menu's Line *N* profile, the unit is in a Red Alarm state. You must verify that the unused line is disabled in the Line Config menu's Line *N* profile. In the following example, the 2nd Line is unused and, therefore, disabled:

```
10-1** Factory
  Name=Factory
   >2nd Line=Disabled
    x Line 1...
    x Line 2...
```

Conversely, if you have a line that is set to Enabled and the T1/PRI services have been temporarily discontinued by the carrier, the unit is in a Red Alarm state. This could occur if you enable the integrated Channel Service Unit (CSU) on a T1/PRI port and connect the port directly to the metallic interface of the WAN without contacting your carrier for approval. To avoid harming the WAN, you must contact your carrier for approval before installation. If you disconnect or turn off the unit without prior notification, the carrier might temporarily discontinue your T1/PRI service. Verify that the port's integrated CSU in the Front End parameter is set to CSU, in the Line Config menu's Line *N* profile, then contact your T1/PRI carrier.

For more information about the CSU and troubleshooting indicator lights, see "Integrated CSU for T1/PRI" on page 5-4.

Verifying Framing Mode settings

You must contact your E1 or T1 service carrier to determine the correct setting to specify for the Framing Mode parameter, which is located in the Line Config menu's Line *N* profile. The Framing Mode parameter specifies the framing mode in use on the physical links of a T1 or E1 line.

For a T1 line, the carrier can require you to specify one of the following values:

*   `D4`—Specifies the superframe format, which consists of 12 consecutive frames, separated by framing bits. Do not use this setting with ISDN D-channel signaling (when `Signaling-Mode=ISDN`).
*   `ESF`—Specifies the Extended Superframe Format, which consists of 24 consecutive frames, separated by framing bits. The ISDN specification advises that you use ESF with ISDN D-channel signaling (when `Signaling-Mode=ISDN`).

For an E1 line, the carrier can require you to specify the following values:

*   `G703`—Specifies that the trunk interface uses CRC-4.
*   `2DS`—Specifies that the trunk interface does not use CRC-4.

Resolving cabling issues

If the MAX unit is connected through bantam connector plugs, reverse the transmit and receive plugs. Then allow the unit to attempt to establish synchronization for 30 seconds. The MAX unit uses bantam connector plugs to connect with digital circuits and digital crossover (DSX) patch panels.

Perform a line loopback test on a RJ48C connector-plug, connect: pin 1 to pin 5 and pin 2 to pin 4. When you plug this connector into the T1/PRI WAN port, the port should come out of Red Alarm state on the MAX unit, no matter what Encoding or Framing Mode settings you have specified. You should see line active (LA) in the corresponding line status window.

For more information about cables and cable specifications, see the *Hardware Installation and Basic Configuration Guide* for your unit.

Summary of Red Alarm causes and solutions

Table 5-1 summarizes potential causes for a Red Alarm and the solutions that may end the Red Alarm state.

Table 5-1. Red Alarm potential causes and solutions

Cause	Solution
Unused T1 or T1 line is enabled	If the one of the T1 or T1 lines is unused, verify that it is disabled in the Line Config menu's Line *N* profile.

Table 5-1. Red Alarm potential causes and solutions (continued)

Cause	Solution
Framing Mode parameter specifies incorrect value	Check the specified value of the Framing Mode parameter in the Line Config menu's Line *N* profile.
Cabling problems	You might have a crossover cable installed when a straight-through cable is required, or vice versa.

Troubleshooting a blinking Alarm

Without using any of the MAX 6000 or the MAX 3000 unit's available interfaces, a blinking Alarm helps you begin to gather information about the performance of the unit. For example, the indicator lights can indicate that a secondary E1/PRI or T1/PRI line is disabled.

A blinking Alarm indicator light indicates that the physical configuration of the E1/PRI or T1 line is correct but the D channel is not communicating with the WAN. A D channel carries WAN synchronization and signaling information on a T1 or T1 line. Synchronization over the D channel helps assure that data traveling over the network does not get lost or become jumbled. Signaling enables connections over telephone lines to be gracefully built and then torn down. Remedy D-channel issues by verifying information with your PRI service carrier, specifying values for several parameter settings in the Line Config profile, and verifying whether or not the unit is equipped with an integrated Channel Service Unit (CSU).

Integrated CSU for T1/PRI

If the WAN interface or the MAX unit is not equipped with an integrated CSU, the Alarm indicator light blinks. A CSU is a component of Data Circuit-terminating Equipment (DCE). A CSU connects a digital telephone line to a customer's network-access equipment. It can be built into the network interface of the network-access equipment, or it can be a separate device. The CSU terminates the connection at the user's end and processes digital signals. For information about displaying WAN interface features, such as the integrated CSU, see "Listing WAN interface features" on page 5-7.

Specify whether or not the MAX unit uses the integrated CSU by enabling or disabling the Front End parameter in the Line Config menu's Line *N* profile. In the following example, the Front End parameter specifies the front-end type of the T1 transceiver. For a T1 line, specify CSU or DSX. The CSU setting specifies a Channel Service Unit, a device that ensures that only clean signals go out on the line. For example:

```
10-103 Example profile
  Line 1...
    Sig Mode=Inband
    NFAS ID num=N/A
    Rob Ctl=Wink-Start
    Switch Type=N/A
    Framing Mode=D4
    Front End=CSU
    Encoding=AMI
    FDL=N/A
    Length=
```

```
Buildout=0 dB
Clock Source=Yes
Collect DNIS/ANI=No
Pbx Type=N/A
Delete Digits=N/A
Add Number=N/A
Front-End-Type
```

In the preceding example, the Front End parameter is set to CSU. However, for T1/PRI there is one other valid setting and for T1/PRI there are two other settings. The DSX setting specifies digital crossover interfaces for connecting DS1 and DS3 signals. The Short-Haul setting specifies that there should be no such limitation.

If you enable the internal CSU on a T1/PRI port, connect the port directly to the metallic interface of the WAN. To avoid harming the WAN, you must contact your carrier for approval before installation. Once you install the MAX unit, you must notify the carrier before disconnecting the unit from the WAN. If you disconnect or turn off the unit without prior notification, the carrier might temporarily discontinue your T1/PRI service.The MAX unit's internal CSUs are compatible with dry-loop T1/PRI lines, and with span-powered or wet-loop powered T1/PRI lines.

If you intend to use the MAX unit on T1 service lines, the unit must be one that is equipped with a CSU, otherwise the Alarm indicator light blinks. For example, MAX 6000 and the MAX 3000 units that support T1 have an integrated CSU.

During loss or power, or any other time a MAX 3000 unit resets, a relay closure connects WAN 1 to WAN 3. This feature protects the MAX 3000 unit's drop-and-insert port (WAN 3) from power interruptions.

If you enable DSX on a T1/PRI port, you cannot connect directly to the WAN. You must connect the port to other equipment that provides the interface to the WAN (for example, an external CSU). Your carrier determines the correct value for the line buildout setting of the CSU, and you specify the value during installation.

If you specify settings for an E1/PRI line, Long-Haul or Short-Haul are valid. The Long-Haul setting specifies that the unit uses120-ohm termination only.

Remedying D-channel issues

With your PRI service carrier, you verify that the D channel is in service. This is especially important if no equipment has been plugged into the line for some time. Next, your E1/PRI or T1/PRI service carrier can verify the setting that they are using for the line is appropriate for your MAX unit. For example, a MAX unit that supports T1 requires a D channel setting of 16. Finally, the T1 services carrier can verify the type of line encoding to specify in the Line Config profile's Encoding parameter.

In the MAX unit's Line Config profile, verify that you have specified values that support the type of E1/PRI or T1 services required by the unit. The Encoding parameter specifies the type of T1 line encoding that the MAX unit uses. Your carrier can tell you which type of encoding you require.

There are three possible settings. AMI, the default setting, specifies that the unit uses Alternate Mark Inversion encoding. AMI is an encoding method in which alternating positive and

---

negative voltage represents a 1, and zero voltage represents a zero. AMI includes density enforcemnt, which dictates that you cannot transmit 16 consecutive zeroes. The None setting specifies that AMI is used without applying density enforcement. B8ZS specifies that the encoding is Bipolar with 8-Zero Substitution. This is often required for ISDN lines. The B8ZS encoding method uses alternating positive and negative voltage to represent a 1, zero voltage represents a zero, and at least one bit out of every eight bits must be a 1.

After you have determined the correct setting, specify the setting by using the Encoding parameter. In the following example the PRI carrier has specified that AMI is the correct setting:

```
10-103 Example profile
  Line 1...
    Sig Mode=Inband
    NFAS ID num=N/A
    Rob Ctl=Wink-Start
    Switch Type=N/A
    Framing Mode=D4
    Front End=CSU
    Encoding=AMI
    FDL=N/A
    Length= 1-133 ft.
    Buildout=0 dB
    Clock Source=Yes
    Collect DNIS/ANI=No
    Pbx Type=N/A
    Delete Digits=N/A
    Add Number=N/A
    Front-End-Type
```

In the preceding example T1 line profile, the Length parameter specifies the cable length of the line from the CSU or other network interface unit to the MAX unit. The setting you indicate must reflect the longest line length you expect to encounter in your installation. The blinking Alarm state continues until you specify a value that is correct for your installation.

The Buildout parameter specifies the line buildout value for T1 lines connected to an internal CSU (Channel Service Unit). The buildout value is the amount of attenuation the unit should apply to the line's network interface. The amount, if any, depends on the length of the MAX unit and the repeater from which it receives the signal. If the MAX unit is too close to a repeater, you might need to specify some attenuation, to reduce the strength of the signal. Check with your carrier to determine the correct value for this parameter. This parameter is not applicable if the T1 line does not have an integrated CSU to connect to the local digital telephone system.

For more information about the integrated CSU, see "Integrated CSU for T1/PRI" on page 5-4.

Summary of blinking Alarm potential causes and possible solutions

Table 5-2 summarizes potential causes and solutions for the blinking Alarm indicator.

Table 5-2. Blinking Alarm potential causes and possible solutions

Cause	Solution
MAX unit is not equipped with a CSU	Determine whether your WAN interface or the MAX T1 unit is equipped with a CSU.
D channel is out of service	If no equipment has been plugged into the line for a short period of time (five to ten minutes), the D channel is taken out of service. You might need to ask your carrier to put the D channel back into service.
D channel setting is incorrect	Verify with your carrier representative that the D channel is channel 16 (E1) or 24 (T1).
Encoding parameter setting is incorrect	If the carrier's D channel number is correct, check the value of the Line Encoding parameter in the Line profile. When B8ZS encoding is in use, a noninverted D channel is established. If AMI encoding is selected, an inverted D channel is established. Check the line translations provided by your carrier representative and set the line encoding to match the inversion requirements.

Using Net/E1 and Net/T1 status windows

MAX 3000 and MAX 6000 units that support E1 provide you with Net/E1 status windows. The units that support T1 provide you with Net/T1 status windows. The status windows are branches of the Main Status window, in the unit's VT100 interface. Use the status windows to display WAN interface features, error and performance information, line status, and Facility Data Line (FDL) Extended Superframe (ESF) performance.

For general information about navigating status windows in the VT100 interface, see the *Hardware Installation and Basic Configuration Guide* for your unit.

Listing WAN interface features

The Net Options window lists the WAN interface features installed on the MAX unit that supports T1 (or E1). To display the Net Options window, tab to a status window, then use the arrow keys to access the Net Options window.

The following example shows the Net Options window on a MAX unit that supports T1/PRI:

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

In the preceding example, the first line shows that the type of physical interface to the WAN is a T1/PRI Network I/F. The second line shows the number of network interfaces associated with the module. The third line shows whether internal CSUs are installed for the T1 lines.

Displaying errors

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

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

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

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

```
10-300 Errors
1:       0      -
2:      33      -
3:      33      -
```

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

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

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

Displaying link and channel status

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

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

In the preceding example, the first line of the Line Stat window shows the window number followed by columns for channels 1 through 10. The second line begins with the line number, followed by the link status, which is indicated by one of the two-character abbreviations listed in Table 5-3. Following the link status is a single-character that indicates channel status. (Table 5-4 lists the channel-status indicators.) The third line has column headers for the remaining channels. The fourth line continues where the second line left off, showing the status of the remaining channels.

Note: If the MAX 3000 unit is configured for Drop-and-Insert functionality, and a Red Alarm (RA) or Loss of Synch condition is detected, the failure is conveyed to the device by sending an all ones (A1S) over Line 2. The Red Alarm indicates the line is not connected, improperly configured, experiencing a very high error rate, or is not supplying adequate WAN synchronization. The Alarm indicator light illuminates when the line is in this state. During the time this failure is active, devices connected to Line 2 cannot place calls.

Table 5-3 summarizes the link-status indicators that appear in the Line Stats window.

Table 5-3. Link-status indicators

Link status	Mnemonic	Description
LA	Link active	The line is active and physically connected.
RA	Red Alarm/Loss of Sync	The line is not connected or is improperly configured, experiencing a very high error rate, or is not supplying adequate synchronization. The Alarm indicator light illuminates when the line is in this state.
YA	Yellow Alarm	The MAX unit is receiving a Yellow Alarm pattern. The Yellow Alarm pattern is sent to the unit to indicate that the other end of the line cannot recognize the signals the unit is transmitting. The Alarm indicator light illuminates when the line is in this state.
DF	D-channel failure	The D channel for a PRI line is not currently communicating.
1S	Keep alive (all ones). Also known as Blue Alarm.	A signal is being sent from the T1 (or E1) network to the MAX unit to indicate that the T1 line is currently inoperative. The Alarm light illuminates when the line is in this state.
DS	Disabled link	The line is physically connected, but you have disabled the line in the Line *N* profile.

A single character represents the status of each channel in the line, as described in Table 5-4.

Table 5-4. 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 is set to Unused in the Line *N* profile.
*	Current	The channel is connected in a current call.
-	Idle	The channel is currently idle (but in service).
d	Dialing	The unit is dialing from this channel for an outgoing call.
r	Ringing	The channel is ringing for an incoming call.
m	Maintenance	The channel is in maintenance/backup (ISDN only).
n	Nailed	The channel is marked Nailed in the Line *N* profile.
x	Drop-and-Insert	The channel is configured for Drop-and-Insert for a DASS 2 E1 line or DPNSS E1/PRI line.
o	Out of Service	The channel is out of service (ISDN only).
s	ISDN D channel	The channel is an active D channel (ISDN only).
b	Backup ISDN D channel	The channel is the backup D channel (ISDN only).

Displaying FDL statistics

A Facilities Data Link (FDL) is a 4-Kbps digital link between a sender and the telephone company's monitors. The FDL uses Extended Superframe (ESF) framing, a framing format that consists of 24 consecutive frames, separated by framing bits. The telephone company uses an FDL to check on the quality and performance of T1 lines. It provides information at regular intervals to your carrier's maintenance devices. The MAX unit continues to accumulate ESF performance statistics in the FDL Stats windows, even if you do not choose an FDL protocol. Your carrier can tell you which FDL protocol to specify.

The FDL Stats windows are the fourth and fifth options listed in the VT100 interface's status window Net/T1 window:

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

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

```
10-500 FDL2 Stats
>Error Events...
 Current Period...
 Last 24 Hours...
 00:00...          v
```

Note: Pressing the Down Arrow key displays additional statistics.

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

Note: If your T1 service has a D4 (SF) interface, no carrier performance data is recorded. The D4 format consists of 12 consecutive frames, each one separated by framing bits. T1 lines that do not use ISDN D-channel signaling use the D4 format.

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

```
   10-500 FDL2 Stats            user registers

    03:45                       carrier registers

   ES:000005 000005
   US:000000 000000
   SS:000000 000000
   BS 000000 000000
   LF:000000 000000
   CS:000000 000000
```

You can use the Clr Perf *N* parameters in the Line Diag menu to reset the user performance registers, but only the carrier can reset the carrier registers. All performance registers are reset upon power-up or software reset.

Table 5-5 describes the FDL performance registers.

Table 5-5. FDL performance registers

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

Table 5-5. FDL performance registers (continued)

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

Fractional T1 services

Set the Call Type parameter to specify several fractional T1 settings. One of the settings, FT1-B&O, affects the information that the MAX unit displays in the Statistics window.

Fractional T1 is a nailed-up T1 line with bandwidth that might be only a fraction of the full T1 bandwidth. A nailed-up line is one that is rented from the telephone company for exclusive use, 24 hours per day, seven days per week. It is possible to lease one channel on a line from the telephone company for exclusive use, 24 hours per day, seven days per week. The connection exists between two predetermined points and cannot be switched to other locations. A nailed-up line is also called a leased line.

Fractional T1-Backup and Overflow (FT1-B&O) is a type of call that provides automatic protection of nailed-up circuits. For FT1-B&O calls, the second line of the Statistics window might not show the call duration. When an FT1-B&O call has no bad channels, the call duration appears as usual. But if it does, the number of offline nailed-up channels appears after the call quality. The following screen shows the Statistics window of an FT1-B&O call with two channels offline:

```
21-300 Albuquerqu+ O
Qual Good 00:04:01
```

```
MAX Rel Delay 10
CLU 80% ALU 77%
```

Using line diagnostics

MAX 3000 and MAX 6000 units that support E1 or T1 provide you with a set of diagnostic command parameters, in the Line Diag menu, to test the performance of the units' lines. Initiate a line loopback test, swap the status of Non-Facility Associated Signaling (NFAS) D-channels on applicable lines, clear each line's user error event registers, and clear all performance registers for each line using the options in the Line Diag menu.

A MAX 6000 unit that supports E1 or T1 lines has two slots, each of which supports two lines. Each of the unit's two Line Diag menus provide line loopback, clear event registers, and clear all performance registers parameters for two lines, as in the following example of a MAX 6000 that supports T1:

```
10-000 Net/T1
  10-200 Line Diag
   >10-201 Line LB1
      10-202 Line LB2
      10-203 Switch D chan
      10-204 Clr Err1
      10-205 Clr Perf1
      10-206 Clr Err2
      10-207 Clr Perf2
```

A MAX 3000 unit that supports E1 or T1 lines has one slot that supports two lines. However, the MAX 3000 unit can also include one drop-and-insert (North America integrated CSU) T1 line. The unit's one Line Diag menu provides line loopback, clear event registers, and clear all performance registers parameters for three lines, as in the following example of a MAX 3000 that supports E1:

```
10-000 Net/E1
  10-200 Line Diag
   >10-201 Line LB1
      10-202 Line LB2
      10-203 Line LB3
      10-204 Switch D chan
      10-205 Clr Err1
      10-206 Clr Err2
      10-207 Clr Err3
      10-208 Clr Perf1
      10-208 Clr Perf2
      10-209 Clr Perf3
```

Clearing user error event and performance registers

The Clr Err1 command clears the user error event register of Line 1, the Clr Err2 command clears the user error event register of Line 2, and the Clr Err3 command clears the user error

event register of the MAX 3000 unit's drop-and-insert Line 3. However, the Clr Err*N* commands do not clear the performance registers for the line. The Clr Perf*N* command clears all performance registers for Line *N*, restarts the current time period, and begins accumulating new performance data.

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

Initiating a line loopback test

Note: Do not activate a line loopback test when a call is active on the line because the test disrupts data flow between the codecs connected to either end of the network line.

Line LB1 is a Line LoopBack (LLB) command for Line 1 in a T1 slot, Line LB2 is a Line LoopBack command for Line 2 in a T1 slot, and so on. When you start the line loopback test for a T1 line, a remote device can test the T1 line and the MAX unit's interface to the T1 line. All signals received by the MAX unit are looped back toward the remote unit. The remote unit can determine the quality of the T1 line by comparing the sent signal to the received signal.

The LLB occurs behind the unit's Channel Service Unit (CSU) repeater, which boosts the signal on a T1 line, or Digital System Cross-connect (DSX) signal-conditioning module, which amplifies signals. Drop-and-Insert channels, which enable a single T1 line to carry both data and voice traffic, are also looped back.

Note: Do not activate LLB when a call is active on the line; doing so disrupts the data flow between the codecs connected to either end of the network line.

The unit responds to both the inband LLB signal and the Facility Data Link (FDL) LLB message. A management device can put the unit into LLB. A management device is a unit, on a T1 line, that measures the line's performance and can send management signals to other devices on the line.

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

Swapping NFAS status

The Switched D Chan parameter, in the Line Diag menu, swaps the status of the primary and secondary Non-Facility Associated Signaling (NFAS) Dchannels. It applies only to T1 lines using NFAS signaling.

NFAS is a form of out-of-band signaling that maximizes the number of PRI lines supported by the signaling of one external Dchannel. NFAS is a special case of ISDN signaling in which two or more T1 lines use the same D-channel, and add a backup Dchannel. NFAS is required for the Switched-1536 data service. Because all 24 channels of the T1 line carry user data, the Dchannel must be on another line.

Table 5-6 summarizes Net/T1 diagnostic commands available in the Line Diag menu.

Table 5-6. Net/T1 diagnostic commands

Command	Purpose
Line LB1 Line LB2 Line LB3	Test Line 1, Line 2, or Line 3 (MAX 3000 only) in a T1 slot, places a call from the MAX unit to itself over the WAN to determine the unit's ability to initiate and receive calls and to diagnose the soundness of the digital access line and WAN. Do not initiate these commands when a call is active on the line because they disrupt data flow between the codecs connected to either end of the network line.
Switch D Chan	Swaps status of the primary and secondary Non-Facility Associated Signaling (NFAS) D channels on T1 lines that use NFAS signaling.
Clr Err1 Clr Err2 Clr Err3	Clears the user error event register of Line 1, Line 2, or Line3 (MAX 3000 only).
Clr Perf1 Clr Perf2 Clr Perf3	Clears all performance registers for Line 1, Line 2, or Line 3 (MAX 3000 only), restarts the current time period, and begins accumulating new performance data.

Testing the lines

The MAX unit can run a test (sometimes called a self-test) that uses two open channels to place a call on one open channel and receive the call on another open channel. Use the Test command, in the unit's terminal-server CLI, to perform this test.

Before you begin you must check one setting in the Sys Config profile and two settings in the Line *N* profile. Verify that you have not enabled the Use Trunk Grps parameter in the Sys Config profile. The Call-by-Call parameter, in the Line Config menu's Line *N* profile, specifies the PRI service that the MAX uses when placing a call that is part of the test. Finally, verify that the unit has two available channels. Warning 180 is caused by a missing channel on a T1/PRI line. For example:

```
ERROR_CHAN_DISPLAY_STUCK          181
ERROR_NEW_CALL_NO_DISC_REQ        182
```

Remedying Trunk Down state

When the list of DO commands appears, many operations might not be not available if the right profile is not selected. Because the MAX unit 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.

You cannot dial if `Operations` is set to `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.

To verify that the profile is correctly configured:

1   Make certain that you have entered the correct telephone number to dial.

2   Verify that the Data Svc parameter specifies a WAN service available on your line.

    If you request a WAN service that is not available on your line, the WAN rejects your request to place a call.

3   Check whether the channels using the requested WAN service are busy.

    If these channels are busy, an outgoing call might be routed to channels for which you did not request the specified WAN service. Check the Data Svc, Call-by-Call, and PRI # Type parameter values in the profile.

4   Determine whether you have correctly set the parameters controlling Dynamic Bandwidth Allocation.

    For detailed information, see the *Network Configuration Guide* for your unit.

Using terminal-server commands

Terminal-server CLI commands can display information directly related to, or temporarily affecting, the performance of the unit's the E1/PRI and T1/PRI interfaces. Use the terminal-server command-line interface to test and reset the MAX unit. Verify clock source settings the MAX unit.

For more information about how to use the terminal-server command-line interface, see Chapter 3, "Terminal-Server Administrative Tasks."

Resetting the unit and clearing calls

The Sys Reset command restarts the MAX unit and clears all calls without disconnecting the device from its power source. The unit logs out all users and returns user security to its default state. In addition, the unit performs diagnostic power-on self tests (POSTs) when it restarts. A system reset of a MAX unit 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 unit to the switch is incorrect until T1 framing is reestablished, usually within 30 seconds. If you have enabled the integrated CSU on the MAX unit that you are testing, you must notify your E1/PRI or T1/PRI carrier before you turn the unit off. For more information, see "Integrated CSU for T1/PRI" on page 5-4.

Displaying the source of clocking

The Clocksource command displays the source of clocking for the MAX unit. Clock slips can cause connectivity problems, particularly for analog users. If you have used the Clock Source parameter, in the Line Config menu's Line *N* profile, use the clocksource command to validate your changes.

In the following example, the clock source is taken from the first T1/PRI line, designated dsl 0. Dsl# indicates the maximum number of possible sources for the clock. The source can be on Net/T1 slot cards. This MAX has three T1/PRI lines configured, so there are three possible external sources for the clock. LstSel is further validation that the clock is being derived from Dsl#0. After Now, a 2 indicates that Layer 2 is up for that line and is available as the clock source. For example:

```
MAX> clocksource
Clock source is dsl 0
Dsl#    01234567890123456789012345678901234567890123456789
LstSel  a?????????????????????????????????????????????????
Now     222-----------------------------------------------
```

You must reset the MAX unit to enable any changes to the Clock Source parameter. Also, if more than one line has Clock Source set to Yes, remember that the clock source will be derived from the first line with which the unit synchronizes. If you want to ensure that a particular line is the source, make sure it has Clock Source set to Yes and that all other lines have Clock Source set to No.

Specifying channels for E1 and T1

The telephone numbers that you specify in the Line *N* profile are the numbers local to your unit. Do not enter the telephone numbers of the MAX unit 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 telephone numbers you specify must correspond to those channels within the circuit that are available for data transmission. For example, if channels 13 through 21 are allocated to a particular slot, you must specify the telephone numbers for channels 13 through 21 in the Line *N* profile. Switched data channels do not have to be contiguous within the circuit.

Verifying E1 and T1 parameter settings

Verify parameter settings in the MAX unit's VT 100 interface that are E1-specific, T1-specific, T1/PRI-specific, and PBX-T1-specific. Determine if the configuration of the unit is correct for your T1 or E1 services environment. In some cases, you may need to contact your E1 or T1 service carrier for information about the correct settings you are required to specify.

E1-specific parameter settings

The VT100 interface of the MAX unit includes a NET/E1 menu. Specify E1 settings by using one E1-specific parameter in the Line Config profile and four E1-specific parameters in the Line *N* subprofiles in the Line Config profile. You must evaluate the settings of E1 parameters as you verify the proper configuration of the unit. In some cases, the correct setting that you must specify is determined by your E1 services carrier.

Table 5-7 summarizes the E1-specific parameters that are available.

Table 5-7. E1 parameters and settings

Parameter	Description
Back-to-back	Enables you to set up DASS-2 and DPNSS lines in a back-to-back connection. A crossover cable connects an E1 port of one MAX unit to an E1 port of another unit. No switch is required, and the connection is entirely local. One unit should be set up for DTE operation, and the other for DCE operation. This parameter applies only to E1 lines whose signaling mode is DPNSS. DPNSS is a standard that defines how different Private Branch Exchange (PBX) systems can operate together to produce a single virtual PBX.
L2 End	Specifies CCITT Layer 2, which is used to determine the address to send when two PBX devices are connected back-to-back. In that case, one side must act as a PBX and the other side must act as an ET.
L3 End	Specifies whether or not the MAX unit supports Layer2 Tunneling Protocol (L2TP) and, if it does, whether the unit functions as an L2TP Access Concentrator (LAC), an L2TP Network Server (LNS), or both.
LoopAvoidance	Specifies the number of transit PBX devices through which a call may be routed.
NL Value	Specifies the number of retransmissions to send on this line. The default value is required when the line connects to a DPNSS or DASS2 switch. It must be set to its default value when the line connects to a DPNSS or DASS2 switch. The default is 64.

T1-specific parameter settings

The VT100 interface of the MAX unit includes a NET/T1 menu. Specify T1 settings by using three T1-specific parameters in the Line *N* subprofiles in the Line Config profile. You must evaluate the settings of T1 parameters as you verify the proper configuration of the unit.

Table 5-8 summarizes the T1-specific parameters that are available, the location of the parameter in the VT100 interface, and whether or not the setting you specify is determined by your E1 services carrier.

Table 5-8. T1-specific parameters

Parameter	Description
Buildout	Specifies the line buildout value for T1 lines with an internal CSU (Channel Service Unit). The buildout value is the amount of attenuation the MAX unit should apply to the line's network interface in order to match the cable length from the unit to the next repeater.
	Attenuation is a measure of the power lost on a transmission line or on a portion of that line. When you specify a build-out value, the MAX unit applies an attenuator to the T1 line, causing the line to lose power when the received signal is too strong. Repeaters boost the signal on a T1 line. If the MAX unit is too close to a repeater, you need to add some attenuation.
FDL	Specifies the FDL (Facilities Data Link) protocol that the MAX unit uses. FDL is a protocol used by the telephone company to monitor the quality and performance of T1 lines. This parameter does not apply to D4-framed T1 lines.
Hunt-*n* (*N*=1–3)	These parameters indicate the hunt group numbers associated with the T1 line in a specific Line *N* profile. An SNMP manager can retrieve these numbers from Lucent Technologies devices and store them in a table that includes the devices from which information is retrieved and the hunt group numbers in their WAN Line Profiles. The numbers entered in the Hunt-*N #* parameters must be the same as the numbers that are assigned to T1 channels, creating the hunt group.

Fractional T1-specific parameters

The VT100 interface of the MAX unit that supports Host/Dual (or Host/6) modules includes a Host/Dual (or a Host/6) menu. Specify fractional T1 settings by using five fractional T1-specific parameter in the Port *N* menu's Directory profile. Evaluate the settings of fractional T1 parameters as you verify the proper configuration of the unit intended to support fractional T1 services.

Table 5-9 summarizes fractional T1-specific parameters.

Table 5-9. Fractional T1-specific parameters

Parameter	Description
FT1 Caller	Specifies whether the MAX unit initiates an FT1-AIM, FT1-B&O, or Nailed/MPP call or whether it waits for the remote end to initiate these types of calls. If the remote end has FT1 Caller set to No, set it to Yes on the local MAX unit; by the same token, if the remote end has FT1 Caller set to Yes, set it to No on the local MAX unit.

Table 5-9. Fractional T1-specific parameters (continued)

Parameter	Description
Idle	In a Port profile, this parameter is not applicable when the port's current Call profile is configured for FT1 calls. If the MAX unit uses a port for FT1-AIM or FT1-B&O calls and Idle is set to Call in the Port profile, you must set Dial to `Terminal`; if the unit uses a port for FT1-AIM or FT1-B&O calls, and Idle is set to `None` in the Port profile, you must set Dial to `DTR`. Both the local and remote ends must use the same combination of these parameters. Further, if you set Idle to `None` and Dial to `DTR`, the hosts at both ends of the connection must make DTR (Data Terminal Ready) active for the MAX unit to connect the switched channels.
Inc Ch Count	This parameter does not apply if all channels if the call type is `Nailed`. In a Call profile, this parameter applies only if the call type is `AIM`, `FT1-AIM`, `FT1-B&O`, or `BONDING` and the Call Mgm parameter is set to `Manual`, `Dynamic`, or `Mode 2`.
B&O Restore	Specifies how many seconds the MAX unit waits before restoring a nailed-up channel to an FT1-B&O call-that is, a call for which `Call Type=FT1-B&O`.
Call Mgm	Specifies the way that the MAX unit manages calls at an AIM port when `AIM`, `FT1- AIM`, `FT1-B&O`, or `BONDING` is the value for the Call Type parameter. For these types of calls, call management consists of remote management, online error monitoring, remote loopbacks, and online bandwidth control between codecs.

T1/PRI-specific parameters

The VT100 interface of the MAX unit includes a NET/T1 menu. Specify T1/PRI settings by using four T1/PRI-specific parameters in the Line *N* subprofiles in the Line Config profile. You must evaluate the settings of T1/PRI parameters as you verify the proper configuration of the unit. The correct settings for the T1/PRI-specific parameters are determined by your T1/PRI service carrier.

Table 5-10 summarizes T1/PRI-specific parameters.

Table 5-10. T1-PRI-specific parameters

Parameter	Description
Call-by-Call	In a T1 Line profile, specifies the call-by-call signaling value to set for routing calls from a local device through the MAX unit to the network. When it is set in another profile, it specifies the PRI service to use when placing a call using that profile.
Encoding	Specifies the type of T1 PRI line encoding that the MAX unit uses.

Table 5-10. T1-PRI-specific parameters (continued)

Parameter	Description
T1-PRI:PRI # Type	T1-PRI:PRI # Type is used for outbound calls made by the MAX unit on PRI lines so that the switch can properly interpret the telephone number dialed. Ask your PRI provider for details on when to use each of settings. This parameter specifies the TypeOfNumber field in the called party's information element.
	The value you specify for PRI # Type in the Dial Plan profile overrides the value of T1-PRI:PRI # Type in the Line *N* profile if you have enabled the unit's Dial Plan profiles.
	This parameter applies only to calls placed by devices terminating the inband T1 lines provided by the MAX unit in a T1-PRI conversion configuration.
T1-PRI:Num-PlanID	T1-PRI:NumPlanID is used for outbound calls made by the MAX on PRI lines so that the switch can properly interpret the telephone number dialed. Ask your PRI provider for details on when to use each of the settings. This parameter specifies NumberPlanID field in the called party's information element.
	This parameter applies only to calls placed by devices terminating the inband T1 lines provided by the MAX unit in a T1-PRI conversion configuration.
	The value you specify for NumPlanID in the Dial Plan profile overrides the value of T1-PRI:NumPlanID in the Line *N* profile if you have enabled the unit's Dial Plan profiles.

PBX-T1 specific parameters

The VT100 interface of the MAX unit includes a NET/T1 menu. Specify T1 settings by using five T1-specific parameters in the Line *N* subprofiles in the Line Config profile. You must evaluate the settings of T1 parameters as you verify the proper configuration of the unit.

Table 5-11 summarizes the T1-specific parameters that are available if the MAX unit is functioning in a PBX-T1 network environment.

Table 5-11. PBX-T1 parameters and settings

Parameter	Specifies
Add Number	Specifies a series of digits to add to the beginning of the dial-out telephone number after removing the digits specified by Delete Digits. The device connected to Line 2 (typically a PBX) dials this telephone number. This parameter applies only to T1 lines using PBX-T1 conversion. Specify any digit string that the PRI switch requires. Contact your PRI switch provider for more information about requirements.

Table 5-11. PBX-T1 parameters and settings (continued)

Parameter	Specifies
Ans #	Specifies a telephone number to be used for routing calls received on the first T1 line to the second line. This may be an add-on number. This parameter applies only to T1 lines using PBX-T1 conversion.
Ans Service	Specifies that the MAX unit routes an incoming call from Line 1 to Line 2 (the PBX) if the data service of the call matches the data service specified by Ans Service. It provides an alternative way to indicate which calls received on Line 1 should be forwarded to Line 2. If you set both Ans # and Ans Service to `null`, the MAX unit does not route incoming calls to Line 2.
	If you set `PBX Type=Data`, the MAX unit switches an incoming call on Line 1 to Line 2 only if its data service type matches the data service specified by the Ans Service parameter, and only if its telephone number matches the telephone number specified by the Ans # parameter.
Delete Digits	Specifies the number of digits deleted from the beginning of the telephone number dialed by the device connected to Line 2. Typically, a PBX (Private Branch Exchange) is connected to Line 2. A PBX is an internal telephone network in which one incoming number directs calls to various extensions and from one office to another.
	Use this parameter when the PBX used to be connected to a switch that supplied a T1 line, is now connected to the MAX unit. The PBX has to change the numbers it dials. The Delete Digits parameter converts the number the PBX dials to the number presented to the WAN switch. This parameter applies only to T1 lines using PBX-T1 conversion.
Input Sample Count	Allows the PRI-T1 conversion process to use one or two sets of Goertzel samples to do the DTMF tone detection. By default, the MAX unit uses only one sample to decode signals from robbed-bit PBXs, because come PBX devices have a tone duration less than 50ms, which does not provide enough time to compute two sets of Goertzel samples. The PRI- T1 conversion process is more accurate when the unit can use two samples. Using two samples is recommended when the tone duration is longer than 70ms. This parameter applies only to T1 lines using PBX-T1 conversion.

Troubleshooting channels

You might encounter a problem in which the Line Status menu shows that the MAX unit is calling multiple channels simultaneously, but only some of the channels connect. In this case, an international MAX unit placed the call, or the call was from the U.S. to another country. In some countries, setting the Parallel Dial parameter in the Sys Config 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.

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 unit answering the call. You must therefore set `Force 56` to `Yes` in the Call profile. If you do not, the MAX unit incorrectly thinks that the call uses 64-Kbps channels.

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 telephone numbers. The MAX unit cannot successfully build inverse multiplexing or MP+ calls if the telephone numbers in the Line *N* profile of the called unit are incorrect. The numbers that you specify in the Line *N* profile are the numbers local to your unit. Do not enter the telephone numbers of the MAX unit 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 telephone numbers you specify must correspond to those channels within the circuit that are available for data transmission. For example, if channels 13 through 21 are allocated to a particular slot, you must specify the telephone numbers for channels 13 through 21 in the Line *N* profile. Switched data channels do not have to be contiguous within the circuit.

If the error message No Channel Avail appears in the message log display when the MAX unit 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.

Administering ISDN

6

In addition to observing a MAX unit's indicator lights to gather information about the performance of the unit's ISDN adapters and links, you can display information to resolve WAN calling errors that occur in outbound Net/BRI calls and to troubleshoot BRI interface problems. You can also display ISDN (including E1 ISDN) call information and use ISDN Cause codes to troubleshoot the performance of a MAX unit.

Troubleshooting BRI interface problems

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

WAN calling errors in outbound Net/BRI calls

Should you encounter a problem in which the Call Status window immediately indicates a WAN calling error when the MAX places a call on a Net/BRI module. Proceed as follows:

1   Check the value of the Data Svc parameter in the Call or Connection profile.

    Try both the 64K and 56K options for Data Svc, to see whether using a different value solves the problem.

2   Verify that you are using the correct dialing plan.

    Depending on how the BRI lines are configured, you might need to type four, seven, or ten digits to communicate with the remote end.

    Four-digit dialing involves the last four digits of your phone number. For example, if your phone number is (415) 555-9015, four-digit dialing requires that you enter only the last four digits: 9015. Seven-digit dialing specifies that you dial the digits 5559015, and ten-digit dialing requires 4155559015.

    If you are sending the incorrect number of digits, the MAX cannot route the call. Ask your carrier representative for the correct dialing plan, or simply try all of the possibilities.

3   Ask your carrier representative to verify explicitly that the line is capable of supporting the call types you are requesting.

Calls are not dialed or answered reliably

If calls are not dialed or answered reliably, proceed as follows:

1 Check your cabling.

The first and most critical aspect of the interface is the physical cable connecting the MAX to the line or terminating equipment. Typically, WAN interface cabling problems appear immediately after installation. If you are unsure about the cabling required, contact Lucent Technologies Customer Service.

2 If the cabling is not the problem and the MAX is a T1 unit, check that the value of the Buildout parameter or the Length parameter in the Line profile matches the actual distance in your configuration.

The MAX displays the Buildout parameter if its interface to the T1 line is equipped with an internal CSU. Its enumerated values can be 0 DB, 7.5 DB, 15 DB, and 22.5 DB. Contact your carrier representative to determine which value to choose.

If the line interface is not equipped with an internal CSU, the Length parameter is displayed. It can specify a cable length, of 1-133, 134-266, 267-399, 400-533, or 534-655 in feet, which should correspond to the distance between the MAX and the WAN interface equipment, typically a CSU or multiplexer.

Note: T1/PRI ports not equipped with internal CSUs require an external CSU or other equipment approved for the metallic interface between the MAX and the WAN facility.

The Net/BRI lines do not dial or answer calls

Do not connect the MAX unit's Net/BRI ports directly to U-interface BRI lines. The MAX unit's Net/BRI ports require carrier-approved Network Terminating 1 (NT1) equipment between the MAX and BRI lines.

Note: Net/BRI outbound calls require the use of trunk groups.

Displaying E1 ISDN call information

If the E1/PRI line switch-type is German 1TR6 or Japanese NTT, display information about ISDN calls by invoking the terminal-server command line and entering the Show Calls command. For example:

```
ascend% show calls
```

The command displays statistics about current calls. For example:

```
Call ID  Called Party ID Calling Party ID InOctets OutOctets

3          5104563434         4191234567               0          0
4         4197654321        5108888888        888888   99999
```

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

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

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

Note: When an ISDN call disconnects from either a German 1TR6 switch or a Japanese NTT switch, the switch sends call billing information to the call originator as part of the call tear-down process. This information is written to the eventCallCharge (eventEntry 17) SNMP object in the Ascend Enterprise MIB events group (10). An SNMP manager can then read this object to determine the cost of the call. The eventCallCharge object is a read-only integer and is applicable only if eventType is callCleared (3). Otherwise, 0 is returned.

For more information, see Chapter 5, "Administering E1 and T1 Services."

Displaying ISDN events

The Show ISDN command enables the MAX unit 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 unit.) For example, to display information about the leftmost built-in WAN port, you would enter the following command:

```
ascend% show isdn 0
```

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

```
PH: ACTIVATED
PH: DEACTIVATED
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
```

Understanding 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 (SS7) 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 switch type is 1TR6 (Germany), see Table 6-2. Table 6-1 lists the numeric cause codes and provides a description of each.

Table 6-1. 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
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

Table 6-1. ISDN cause codes (continued)

Code	Cause
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
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)

Table 6-1. ISDN cause codes (continued)

Code	Cause
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
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

Table 6-1. ISDN cause codes (continued)

Code	Cause
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 6-2 lists the cause codes for the 1TR6 switch type.

Table 6-2. 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.)

Table 6-2. ISDN cause codes for 1TR6 switch type (continued)

1TR6 Code	Cause
32	Outgoing calls barred. (Outgoing call not possible because of access restriction that has been installed.)
33	User access busy. (If the total made up of the number of free B channels and the number of calling procedures without any defined B channel is equal to four, any new incoming calls will be rejected from within the network. The calling party receives a DISC with a cause `user access busy`, which indicates the first busy instance, and a busy signal.)
34	Negative CUG comparison. (Link not possible because of negative CUG comparison.)
35	Nonexistent CUG. (This CUG does not exist.)
37	Communication as semipermanent link not permitted.
48 - 50	Not used. (Link not possible because, for example, RFNR check is negative.)
53	Destination not obtainable. (Link cannot be established in the network because of incorrect destination address, services, or facilities.)
56	Number changed. (Number of B subscriber has changed.)
57	Out of order. (Remote TE not ready.)
58	No user responding. (No TE has responded to the incoming SETUP or call has been interrupted, absence assumed—expiration 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.)

Table 6-2. ISDN cause codes for 1TR6 switch type (continued)

1TR6 Code	Cause
112	Local procedure error. (In REL: Call cleared down as a result of local errors, for example, invalid messages or parameters, expiry of time-out. 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.)

Administering TCP/IP

7

The OSI Reference Model describes the layers of a network, details the functions of each layer, and explains how to connect communications devices on a LAN or WAN. The middle layer of the OSI Reference Model, the Transport layer, also called Layer 4, provides data transfer at the proper speed, quality, and error rate, ensuring reliable delivery. Transmission Control Protocol (TCP), a common implementation of the Transport layer, provides connection-oriented services and uses IP to deliver packets. The Network layer (Layer 3) of the OSI Reference Model provides address resolution and routing protocols. Address resolution enables the Network layer to determine a unique network address for a node. Routing protocols allow data to flow between networks and reach their proper destination. Some examples of Network layer protocols include the Internet Protocol (IP), Address Resolution Protocol (ARP), the Internet Control Message Protocol (ICMP), Routing Information Protocol (RIP), and Open Shortest Path First (OSPF). Whether you intend to manage IP, ARP, ICMP, RIP, or OSPF, you can use the MAX unit's terminal-sever command-line interface (CLI) to display protocol-specific information. In addition, you can enable Finger support and understand how IP routing and AppleTalk-routing relate.

Managing the Internet Protocol (IP)

Monitor a MAX unit's Internet Protocol (IP) routing table, route statistics, remote IP hosts, and VRouter activity in the terminal-server command-line interface (CLI).

IP-routing environment

Figure 7-1 illustrates a typical routing environment with a main office and three remote offices. All sites of the Smith Company 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 7-1. Example IP-routed environment
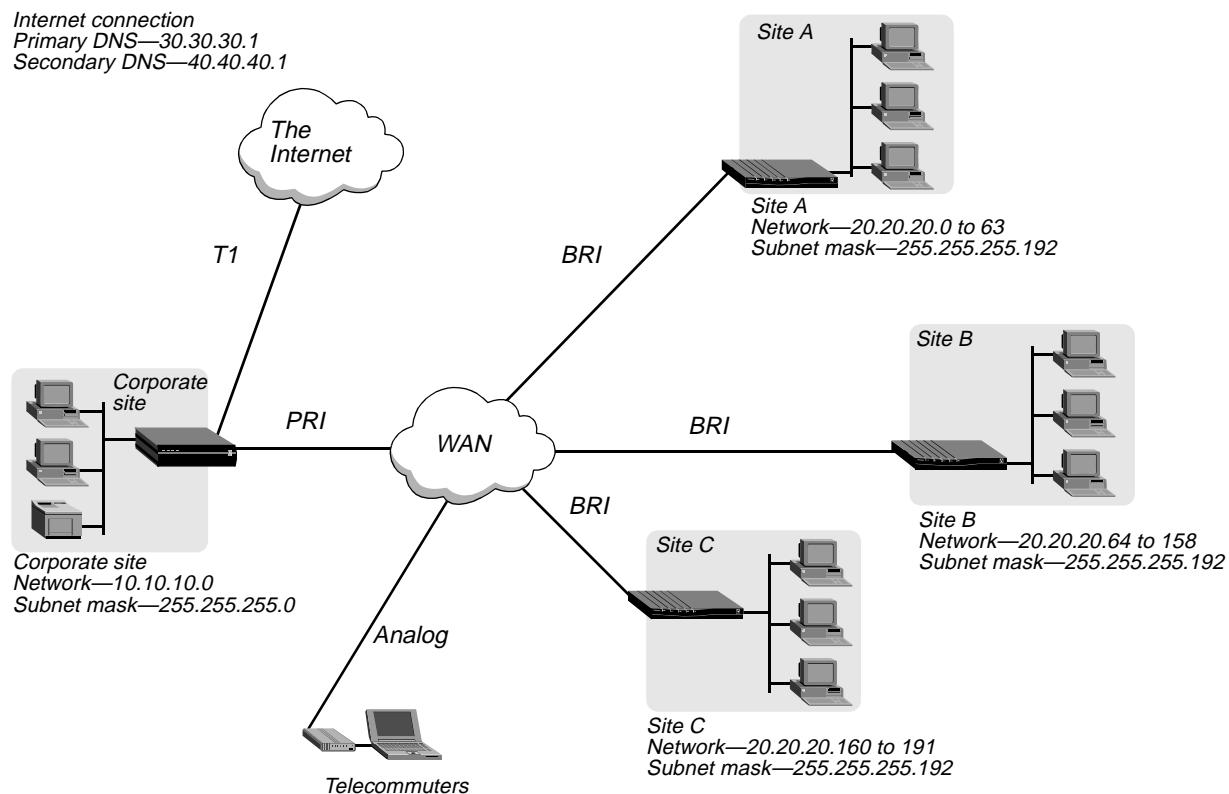
Displaying IP information

The three IP-related Show commands in the terminal-server CLI allow you to display IP statistics, IP address assignments on the unit, and IP routes. See the available commands by entering the Show IP ? command, as in the following example:

```
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
```

Using the Show IP Address command, available in the MAX unit's terminal-server CLI, you can display the IP address, destination IP address, netmask, MTU, and status of each of the unit's interfaces.

Troubleshooting IP routing

To locate slow routers or diagnose IP routing problems, you can use the Traceroute command. It traces the route an IP packet follows by launching User Datagram Protocol (UDP) probe packets with a low Time-To-Live value and then listening for an Internet Control Message Protocol (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. Table 7-1 describes the syntax elements of the Traceroute command.

Table 7-1. Traceroute command syntax elements

Element	Definition
-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 out-going probe packets. The default is 30 hops.
-p port	Sets 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, set the -p option to specify an unused port range. The default is 33434.
-q nqueries	Sets the maximum number of queries for each hop. The default is 3.
-w waittime	Sets the time to wait for a response to a query 3 seconds is the default.
host	The destination host by name or IP address.

Table 7-1. Traceroute command syntax elements (continued)

Element	Definition
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).

Example of Traceroute command usage

For example, to trace the route to a host named 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 unit 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. 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. Table 7-2 describes the annotations that can appear after the time field in a response.:

Table 7-2. Time field responses and annotations

Annotation	Definition
!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.

Table 7-2. Time field responses and annotations (continued)

Annotation	Definition
!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.

Managing the IP routing table

The MAX unit consults its internal IP routing table to determine where to forward each IP packet it processes. First, the unit tries to find a match between the packet's destination address and a Destination field in its routing table. If it finds a match, it brings up the required connection (if necessary) to reach the next-hop router specified for that route, and forwards the packet. If it does not find a match for the packet's destination address, it looks for a default route (destination address 0.0.0.0). If it finds a default route, it brings up the required connection (if necessary) and forwards the packet. If the routing table has no default route, and no route that matches a packet's destination address, the unit drops the packet.

Use the MAX unit's IProute commands, in the terminal-server CLI, to display the IP routing table and add or delete IP routes. The changes you make to the routing table by using the IProute command last only until the unit is reset. To navigate to the terminal-server CLI from the VT100 interface, select Term Serv, from the Sys Diag profile in the System menu. Press Enter and the terminal-server CLI prompt appears, as follows:

```
ascend%
```

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)
```

Use either the IProute Show command or the Show IP Routes command to display the IP routing table. For example:

```
ascend% show ip routes

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
```

In the preceding example, the first route shown is the default route with destination 0.0.0.0/0, defined through the active Connection profile. The IP Route profile for the default route specifies a preference of 1, so this route is preferred over dynamically learned routes. The default route is the route that the unit uses if it does not find a match for a packet's destination address. The unit adds dynamically assigned IP addresses to the routing table as individual host routes.

Use Table 7-3 to find a definition of the setting displayed in each field of the IP routing table:

Table 7-3. IP routing table fields and definitions

Field	Definition
Destination	Target address of a route. To send a packet to this address, the unit uses this route. 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— Internet Control Message Protocol (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

Table 7-3. IP routing table fields and definitions (continued)

Field	Definition
Pref	Preference value of the route. 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.
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.

During a session, add a static route to the MAX unit's routing table. When the unit resets, the IP route is removed. 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 unit 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 unit rejected your attempt to add a route because the routing table already contained a route, to the same destination, with a lower metric.

During a session, it is possible to remove a route from the MAX unit's routing table. When the unit resets, the route is restored. 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
```

Displaying IP route statistics

A MAX unit can perform the function of an IP router which sends IP packets from a source to a destination by multiple paths. As an IP router, the unit routes IP packets between its Ethernet interfaces and across any WAN interface configured for IP routing. Determine the Ethernet interfaces and WAN interfaces to which the unit routes packets in the IP routing table. Add and delete routes by using the unit's terminal-server command-line interface (CLI).

By using the Show IP Stats command, find information about the IP packets that the unit has received, discarded, delivered, transmitted, and reassembled. The command also allows you to display information about fragmentation on the unit. Here is an example of the results of the Show IP Stats command:

```
ascend% show ip stats
  861854 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.
     521592 packets delivered to upper layers.
     340243 transmit requests.
     0 discarded transmit packets.
     2 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.
```

Displaying IP statistics and addresses

To display the IP statistics and address 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 "Managing the IP routing table" on page 7-5.

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
```

RIP updates and IP routes

Routing Information Protocol (RIP) updates can change the metric (number of hops) for the route. RIP is a distance-vector protocol found in both the IPX and TCP/IP protocol suites. The protocol keeps a database of routing information that it gathers from periodic broadcasts by each router on a network. IPX routers broadcast RIP updates periodically and when a WAN connection is established. The MAX unit receives IPX RIP broadcasts from a remote device, adds 1 to the hop count of each advertised route, updates its own RIP table, and broadcasts updated RIP packets on connected networks in a split-horizon fashion which omits routes learned from one neighbor unit in updates sent to that neighbor unit.

IETF RFC 1058 describes the Routing Information Protocol (RIP), also known as Standard 34 (STD 0034).Routing Information Protocol. RIP is a distance-vector protocol found in both the NetWare and TCP/IP protocol suites. The protocol keeps a database of routing information that it gathers from periodic broadcasts by each router on a network.

IPX routers broadcast RIP updates periodically and when a WAN connection is established. The MAX receives IPX RIP broadcasts from a remote device, adds 1 to the hop count of each advertised route, updates its own RIP table, and broadcasts updated RIP packets on connected networks in a split-horizon fashion.

The MAX follows standard IPX RIP behavior for routers when connecting to non-Ascend units. However, when it connects to another Ascend unit configured for IPX routing, both ends of the connection immediately exchange their entire RIP tables. In addition, the MAX maintains those RIP entries as static until the unit is reset or power cycled.

The MAX recognizes network number -2 (0xFFFFFFFE) as the IPX RIP default route. When it receives a packet for an unknown destination, the MAX forwards the packet to the IPX router advertising the default route. If more than one IPX router is advertising the default route,

the unit makes a routing decision based on the hop and tick count. For example, if the MAX receives an IPX packet destined for network 77777777 and it does not have a RIP table entry for that destination, the MAX forwards the packet towards network number FFFFFFFE, if available, instead of simply dropping the packet.

IETF RFC 2453 describes Routing Information Protocol version 2 (RIP-2), also known as Standard 56 (STD 0056).

RIP updates can add back any route you remove with the IProute Delete command. The MAX unit maintains the RIP updates received from another Lucent Technologies device until you reset or power cycle the unit. However, if the RIP update comes from a non-Lucent Technologies unit, the MAX unit maintains the change to the routing table only until the WAN link is terminated.

Displaying address pool status

To view the status of the MAX unit's IP address pool enter the Show Pools command:

```
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).

Displaying DNS-related information

Domain Name System (DNS) is a TCP/IP service for centralized management of address resolution. Using DNS, you can specify a symbolic name instead of an IP address. A symbolic name consists of a user name and a domain name in the format username@domain_name. The user name corresponds to the host number in the IP address. The domain name corresponds to the network number in the IP address. A symbolic name might be steve@abc.com or joanne@xyz.edu. The domain identifier is the last part of the domain name, and identifies the type of organization to which the host belongs.

DNS maintains a database of network numbers and corresponding domain names. When you use a symbolic name, DNS translates the domain name into an IP address, and sends it over the network. When the Internet service provider receives the message, it uses its own database to look up the user name corresponding to the host number.

Displaying the local DNS fallback table

The local DNS fallback 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 fallback table contains the host name for the attempted connection, the table provides the list of IP addresses.

Create a DNS table on the local server by setting the Enable Local DNS parameter, in the Mod Config menu's DNS profile, to Yes.

```
90-C00 Mod Config

 DNS...

  >Domain Name=eng.ascend.com
   Sec Domain Name=
   Pri DNS=206.65.212.10
   Sec DNS=206.65.212.178
   Allow As Client DNS=Yes
   Pri WINS=0.0.0.0
   Sec WINS=0.0.0.0
   List Attempt=No
   List Size=N/A
   Client Pri DNS=0.0.0.0
   Client Sec DNS=0.0.0.0
   Enable Local DNS Table=Yes
   Loc.DNS Tab Auto Update=Yes
```

The MAX supports up to eight host names (or the IP addresses for each host). You can specify the host names (or the IP addresses for each host) through the terminal-server interface. 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. Following is a sample line from a DNS table:

```
1: irma 00.65.212.12* 2      Feb 10 10:40:44 00
```

In the preceding example, the first line (1:) of local DNS table describes the host named "irma." The host named "irma" has an IP address of 00.65.212.12 that was updated by a DNS query. Since the time the entry became a part of the DNS table, there have been two read events and the last read was at the specified time, on February 10, 2000.

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 in the #Read and Time of last read fields are updated when the system matches the table entry with a host name that was not found by the remote server.

Table 7-4 summarizes the output of the Show Dnstab command.

Table 7-4. Output of the Show Dnstab command

Field	Description
Name	Name of the hosts added to the DNS fallback table.
IP Address	IP Addresses added to the DNS fallback table.
# 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.

Table 7-4. Output of the Show Dnstab command (continued)

Field	Description
`Time of last read`	The time that the last read occurred.

Editing the local DNS table

Use the terminal-server `dnstab` command to edit the local DNS table. You can use three options are provided.

The Dnstab command, followed by a table entry number, displays the standard table header and table entry followed by all IP addresses in the list up to the limit specified in the List Size parameter in the Mod Config menu's DNS profile. Also, if the List Attempt parameter specifies No then unit cannot print a list. If you specify an invalid entry, the unit produces the following warning:

```
ascend% dnstab entry 9

<#> parameter must be between 1 and 8
```

The Dnstab Edit command shows the current table and queries for an entry number. After typing an entry the number is qualified and if it fails a warning is printed:

```
Enter item number (0), 0 to exit: 9

Entry # 9 does not exist and the table printout and prompt are
repeated.
```

Part of the query line is the previously edited entry number on editor's startup. Typing a 0 causes the editor to exit.

Throughout the editor the current value (or previous value in case of the item number) of the field is displayed as part of the entry prompt. By pressing Enter, instead of a new value, the value remains unchanged and the displayed value is used. If the item entry is accepted the user is prompted for the name of the entry. The current table entry name is shown as part of the prompt.

In order to clear the entry, enter the name and press Space. Names must start with an alphabetic character. Names can be local names or fully qualified names. If it is a local name then Domain Name or Sec Domain Name (if the lookup with Domain Name fails) is added before the name lookup. A periods at the end of names is ignored. (A side effect of this rule is that a string that only includes a period is considered an empty string.) Names must be less than 256 characters. If a <Return> is typed without any preceding characters then the entry remains unchanged. If no name string is present in this entry then the user does not get a chance to enter the IP address for this entry. Name entries are cleared by entering a space character, followed by <Return>. This also clears the IP address since no more name is present. The user is again prompted for an entry number. If the name is accepted it is entered into the table and the user is prompted for the IP address of the name that has just been entered.

The IP address of the current entry name is shown as part of the prompt. If you press Return, the IP address entry remains unchanged and the user is prompted for the next entry number. If

a new IP address is entered it is qualified and accepted on a good entry. If the IP address fails
the check then a message is printed, the IP address is cleared and the user is prompted for an
entry number. If the IP address is correct then is entered into the table and the editor prompts
for another entry number.

Displaying Multicast information

The terminal-server command-line interface provides commands to support IP-multicast
functionality using Internet Group Management Protocol (IGMP). To display the options,
invoke the terminal-server interface (System > Sys Diag > Term Serv) and enter the Show
IGMP and/or show Mrouting command with a question mark:

```
ascend% show igmp ?

show igmp ?Display help information
show igmp statsDisplay IGMP Statistics
show igmp groupsDisplay IGMP groups Table
show igmp clientsDisplay IGMP clients

ascend% show mrouting ?

show mrouting ?Display help information
show mrouting statsDisplay MROUTING Statistics
```

Displaying the multicast forwarding table

To display active multicast group addresses and clients (interfaces) registered for each group:

```
ascend% show igmp groups

IGMP Group address Routing Table Up Time: 0:0:22:17
Hash        Group Address     Members     Expire time    Counts
N/A       Default route      *(Mbone)     ......        2224862
10        224.0.2.250
                               2           0:3:24        3211 :: 0 S5
                               1           0:3:21         145 :: 0 S5
                             0(Mbone)      ......        31901 :: 0 S5
```

Table 7-5 describes the output of the Show IGMP Groups command.

Table 7-5. Output of the Show IGMP Groups command

Field	Description
Hash	Index to a hash table that is displayed for debugging purposes only. The Default route is not an entry in the hash table.
Group Address	IP multicast address used. The Default route is the interface on which the multicast router resides. **Note:** The IP multicast address being monitored is marked with an asterisk, meaning that this address is joined by local application.

Table 7-5. Output of the Show IGMP Groups command (continued)

Field	Description
Members	Interface ID on which the membership resides. The number 0 represents the Ethernet interface. Other numbers represent WAN interfaces, numbered according to when they became active. The interface labeled Mbone is the one on which the multicast router resides.
Expire time	Time at which this membership expires. The MAX sends out IGMP queries every 60 seconds, so the expiration time is usually renewed. If the expiration time is reached, the entry is removed from the table. Periods in this field indicates that the membership never expires.
Counts	Number of packets forwarded to the client, number of packets dropped because of a lack of resources, and state of the membership (the state is displayed for debugging purposes).

Listing multicast clients

To display a list of multicast clients, enter the Show IGMP Clients command. For example:

```
ascend% show igmp clients
IGMP Clients

Client      Version   RecvCount   CLU       ALU
  0(Mbone)     1          0          0         0
  2            1         39         68        67
  1            1      33310        65        65
```

Table 7-6 describes the output of the Show IGMP Clients command.

Table 7-6. Output of the Show IGMP Clients command

Field	Description
Client	Interface ID on which the client resides. The number 0 represents the Ethernet. Other numbers are WAN interfaces, numbered according to when they became active. The interface labeled Mbone is the one on which the multicast router resides.
Version	Version of IGMP being used.
RecvCount	Number of IGMP messages received on that interface.
CLU (CurrentLine Utilization) and ALU (Average Line Utilization)	Percentage of bandwidth utilized across this interface. If bandwidth utilization is high, some IGMP packet types will not be forwarded.

Displaying IP-multicast activity

To display the number of IGMP packet types sent and received, enter the Show IGMP Stats command. For example:

```
ascend% show igmp stats

        46 packets received.
         0 bad checksum packets received.
         0 bad version packets received.
         0 query packets received.
        46 response packets received.
         0 leave packets received.
        51 packets transmitted.
        47 query packets sent.
         4 response packets sent.
         0 leave packets sent.
```

To display the number of multicast packets received and forwarded, enter the Show Mrouting Stats commands. For example:

```
ascend% show mrouting stats

34988 packets received.
    57040 packets forwarded.
        0 packets in error.
       91 packets dropped.
        0 packets transmitted.
```

In many cases, the number of packets forwarded is greater than the number of packets received, because packets can be duplicated and forwarded across multiple links.

Using VRouter-related terminal-server commands

To support multiple virtual routers, the servers and clients you specify in the Multicast profile must be accessible to the main VRouter (virtual router).

The following terminal-server commands support virtual routing. If you do not specify a VRouter name on the command line, the MAX unit applies the command to global VRouter settings. If you specify a VRouter name, the unit applies the command to the specified VRouter. Table 7-7 describes the usage of terminal-server CLI commands that support VRouter arguments.

Table 7-7. VRouter-related terminal-server commands

Command	Usage with optional VRouter arguments

IProute	`iproute add [-r vRouterName] destination/size [gateway] [pref][metric][proto]`
	
	`iproute delete [-r vRouterName] destination/size [gateway]`

Table 7-7. VRouter-related terminal-server commands (continued)

Command	Usage with optional VRouter arguments

Traceroute	`traceroute [-n] [-v] [-m max_ttl] [-p port]`
	`[-q nqueries] [-w waittime] [-r vRouter] [-s src_addr]`
	`host-name [datasize]`

Ping	`ping [-q	-v] [-i sec	-I msec] [-s packet-size] [-r` `vRouter] [-x source_address] host-name`
Telnet	`telnet [-a	-b	-t] [-v VRouterName] [-l[e]	-r[e]]` `host-name [port-number]`

The following Show commands support virtual routing. If you do not specify a VRouter name on the terminal server command line, the MAX unit displays global VRouter information. If you specify a VRouter name, the unit displays information about the specified VRouter. Table 7-8 describes the usage of VRouter-related terminal-server commands.

Table 7-8. VRouter-related terminal-server commands

Command	Usage with optional VRouter arguments
IPRoutes	`show iproutes [-r vrouterName] [dest]`
IPStats	`show ip stats [[-r] vrouterName]`
IPaddress	`show ip address [[-r] vrouterName] [all]`
ICMP	`show icmp [[-r] vrouterName]`

UDP	`show udp stats [[-r] vrouterName]`
	
	`show udp listen [[-r] vrouterName]`

TCP	`show tcp stats [[-r] vrouterName]`
	
	`show tcp connection [[-r] vrouterName]`

Pools	`show pools [[-r] vrouterName]`

Displaying UDP packet information

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  10230 1   0   0
1  5200  50  0   532
2  7   0   32  0   0
3  1230  32  0   0
4  10220 1280  0
5  1610  64  0   0
```

The Show commands summarized in Table 7-9 to monitor specified protocols and other network-specific information:

Table 7-9. Show commands, specified protocols, and network-specific information

Command	Description
Show Fr	Display Frame relay info. Type show fr ? for help.
Show ICMP	Display Internet Control Message Protocol (ICMP) information.
Show IGMP	Display Internet Group Membership Protocol (IGMP) information. Type show igmp ? for help.
Show IP	Display Internet Protocol (IP) information. Type show ip ? for help.
Show ISDN	Display Integrated Services Digital Network (ISDN) events. Type show isdn *<line number>* for help.

Table 7-9. Show commands, specified protocols, and network-specific information (continued)

Command	Description
Show NetWare	Display IPX information. Type show netware ? for help.
Show NetWare Option [*VRoutername*]	Display IPX information related to all VRouters or a specified VRouter configured on the MAX unit.
Show OSPF	Display Open Shortest Path First (OSPF) information. Type show ospf ? for help.
Show PAD	Display X25/PAD information.
Show TCP	Display Transmission Control Protocol (TCP) information. Type show tcp ? for help.
Show UDP	Display User Datagram Protocol (UDP) information. Type show udp ? for help.
ShowX25	Display status of X.25 stack.

A single character represents the status of each channel in the line, as described in Table 7-10.

Table 7-10. T1 channel status indicators

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

If your T1 service has a D4 (SF) interface, no carrier performance data is recorded. The D4 format consists of 12 consecutive frames, each one separated by framing bits. T1 lines that do not use ISDN D-channel signaling use the D4 format.

NFAS is a special case of ISDN signaling in which two or more T1 PRI lines use the same D channel, and add a backup D channel. It is required for the Switched-1536 data service. Because all 24 channels of the T1 PRI line carry user data, the D channel must be on another line. NFAS is a form of out-of-band signaling that maximizes the number of PRI lines supported by the signaling of one, external D Channel.For more information, see Chapter 5, "Administering E1 and T1 Services."

Managing the Address Resolution Protocol (ARP)

Address Resolution Protocol (ARP) is a protocol in the TCP/IP protocol suite. By mapping an IP address to a physical (hardware) address, ARP enables a unit to identify hosts on an Ethernet LAN. In an ARP request, a remote device asks a host to provide the host's physical address so that a connection can take place. ARP requests are broadcast only on the local network.

Proxy Address Resolution Protocol (Proxy ARP) allows one unit handles address resolution requests for another device. If a remote host must respond to an ARP request, the MAX can respond on its behalf. In Proxy mode, a Connection profile assigns a local IP address to a remote host. Local hosts see the remote host as though it were on the local network. If the MAX unit is the default router on a network and is configured in proxy mode, packets destined for any of the hosts on the network go to the MAX. When calls are made to the remote host, the MAX acts on its behalf, replying to requests and forwarding packets.

Displaying and clearing the ARP cache

By mapping an IP address to a MAC (physical or hardware) address, the Address Resolution Protocol (ARP) enables a unit to identify hosts on an Ethernet LAN. In the MAX unit's terminal-server, display and reset the ARP cache to clear.

```
ascend% show arp
```

IP Address	Hardware Address	Type	Interface	RefCount
208.211.252.26	00:c0:7b:62:42:d9	Dynamic	ie0	1
208.211.252.50	00:c0:7b:8c:ed:94	Dynamic	ie0	1
208.211.252.29	00:c0:7b:5c:53:ed	Dynamic	ie0	1
208.211.252.46	00:c0:7b:6d:6f:46	Dynamic	ie0	1
208.211.252.30	00:c0:7b:5d:b2:2b	Dynamic	ie0	1
208.211.252.24	00:c0:7b:63:5e:03	Dynamic	ie0	1
208.211.252.22	00:c0:7b:5e:9e:3b	Dynamic	ie0	1
208.211.252.18	00:c0:7b:62:56:0f	Dynamic	ie0	1
208.211.252.238	00:40:9d:20:a8:2f	Dynamic	ie0	1
208.211.252.25	00:c0:7b:63:d9:6a	Dynamic	ie0	1
208.211.252.61	00:a0:24:a6:14:bd	Dynamic	ie0	1

```
208.211.252.62   00:08:c7:85:ec:f4   Dynamic   ie0                1

208.211.252.58   00:c0:05:01:0f:5b   Dynamic   ie0                1

208.211.252.59   00:c0:05:01:54:6b   Dynamic   ie0                1

208.211.252.6    00:c0:7b:62:41:f9   Dynamic   ie0             3012

208.211.252.17   00:c0:7b:62:41:f9   Dynamic   ie0           234158
```

In the preceding example, the output displays the IP address contained in the ARP requests received by the MAX unit, the MAC address of the host, and the method by which the unit learned of the address (dynamically or specified a static route. The output also displays the interface on which the unit received the ARP request and the number of times the unit consulted the entry.

To reduce the number of address resolution requests, a client normally caches resolved addresses for a (short) period of time. The ARP cache is of a finite size and would become full of incomplete and obsolete entries for devices that are not in use if it was allowed to retain the entries without check. The MAX unit periodically flushes all ARP cache entries, deleting unused entries and freeing space in the cache. It also removes information about any unsuccessful attempts to contact computers that are not currently running. To manually clear the ARP cache, use the Set ARP Clear command, as in the following example:

```
ascend% set arp clear

Clearing ARP table...

ascend%
```

Verify the settings of two parameters in the VT100 interface that relate ARP. Net Adrs, in the Ethernet menu's Bridge profile, specifies the IP address of a device at the remote end of the link. Use the Net Adrs parameter in a Bridge profile to enable the unit to respond to ARP requests while bringing up a bridged connection between two segments of the same IP network. If an ARP packet contains an IP address that matches the Net Adrs parameter, the MAX responds to the ARP request with the Ethernet MAC address specified in the Bridge profile and brings up the specified connection, in effect, using the MAX unit as a proxy for the node that actually has that address.

The Proxy Mode parameter in the Mod Config profile's Ether Options specifies under what conditions the MAX unit responds to ARP requests for remote devices. When you enable Proxy Mode, the MAX responds to the ARP request with its own MAC address. Typically, if you enable the MAX supplies IP addresses in its subnet dynamically to dial-in users.

Managing the Internet Control Message Protocol (ICMP)

Internet Control Message Protocol (ICMP) is an error-reporting mechanism integral to the TCP/IP protocol suite. Gateways and hosts use ICMP to send reports of datagram problems to the sender. ICMP also includes an echo request/reply function that tests whether a destination is available and responding.

Pinging remote IP hosts

The terminal-server Ping command is useful for verifying that the transmission path is open between the MAX unit 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 syntax elements are optional except 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. 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. 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	Specifies 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
```

Terminate the Ping exchange at any time by pressing Ctrl-C. When you press Ctrl-C, the output 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 be unable to run a TCP application (such as Telnet or FTP) to it. If you Ping a host running an earlier version of Berkeley UNIX 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.

Displaying ICMP information

Display ICMP-related information by using the Show ICMP command. Use the command to see the packets that have been received by the unit and how many of those have been received with errors. For example:

```
ascend% show icmp ?

2539 packets received.
0 packets received with errors.
Input histogram:
992 destination unreachable.
1512 redirect.
11 echo requests.
24 time exceeded.
11 packets transmitted.
0 packets not transmitted due to lack of resources.
Output histogram:
11 echo replies.
```

In the preceding example, there are 1512 redirect packets. A redirect packet instructs the receiver of the packet to override a setting in its routing table. There were also 11 Echo Requests and 11 Echo Replies. An Echo Request is a signal that determines whether a node can receive and acknowledge data transmissions. A host sends an Echo Request packet, and if the destination is properly connected and receives the request packet, it sends back an Echo Reply packet. A router can use an ICMP Redirect packet to tell a host that it is sending packets to the wrong router and to inform the host of the correct route.

Preventing ICMP security breaches

A forged ICMP Redirect packet can alter the host's routing table and compromise the security of the network. For this reason, many firewall builders prohibit ICMP traffic from their networks.

A Denial of Service (DoS) attack also uses ICMP echo request packets to deliberately interfere with network performance. Under ordinary circumstances, to determine whether a machine on the Internet is connected and responding, a host sends an ICMP Echo Request packet. If a machine receives the packet, it returns an ICMP Echo Reply packet. In a DoS attack, however, an attacker directs ICMP Echo Request packets to IP broadcast addresses from one or more remote locations. An intermediary receives an ICMP Echo Request packet directed to the IP broadcast address of its network. If the intermediary does not filter the ICMP traffic, the machines on the network receive request and send a reply. The reply packets do not use the IP address of the source machine as the source address. Instead, they contain the spoofed source

address of the intended victim. When all the machines at the intermediary's site respond to the ICMP Echo Requests, they send replies to the victim's device. An attacker can send DoS attacks to multiple intermediaries at the same time, causing all of the intermediaries to direct responses to the same victim.

Both the intermediary and victim of a DoS attack can suffer severely degraded network performance. To protect against DoS attacks, you should disable IP-directed broadcasts on the MAX unit. By disabling these broadcasts, you deny an attacker the ability to direct IP broadcast traffic onto your network. In addition, you should prevent the MAX unit from responding to ICMP packets sent to IP broadcast addresses. Because this traffic does not travel through a router to reach the machines on the local network. If someone compromises a machine on your network, he or she may try to launch an attack using the MAX as an intermediary, sending the ICMP Echo Request packet to the IP broadcast address of the local network.

The Forward Directed Bcast parameter specifies whether or not the MAX unit responds to directed-broadcast ICMP echo requests. The Reply DirectedBcast Ping parameter specifies whether the MAX unit forwards directed broadcast traffic to the Ethernet interface. Verify the configuration of the Forward Directed BCast and the Reply DirectedBcast Ping parameters in the Ethernet menu's Mod Config profile.

Managing the Routing Information Protocol (RIP)

Routing Information Protocol (RIP) is a distance-vector protocol found in both the NetWare and TCP/IP protocol suites. The protocol creates a database of routing information that it gathers from periodic broadcasts by each router on a network.

Internet Packet Exchange (IPX) routers broadcast RIP updates periodically and every time a WAN connection is established. The MAX receives IPX RIP broadcasts from a remote device, adds 1 to the hop count of each advertised route, updates its own RIP table, and broadcasts updated RIP packets on connected networks in a split-horizon fashion.

The MAX follows standard IPX RIP behavior for routers when connecting to non-Lucent units. However, when it connects to another Lucent unit configured for IPX routing, both ends of the connection immediately exchange their entire RIP tables. In addition, the MAX maintains those RIP entries as static until it is reset or power cycled.

The MAX recognizes network number -2 (0xFFFFFFFE) as the IPX RIP default route. When it receives a packet for an unknown destination, the MAX forwards the packet to the IPX router advertising the default route. If more than one IPX router is advertising the default route, the unit makes a routing decision based on the hop and tick count. For example, if the MAX receives an IPX packet destined for network 77777777 and it does not have a RIP table entry for that destination, the MAX forwards the packet towards network number FFFFFFFE, if available, instead of simply dropping the packet.

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] [-r VRoutername]
hostname
```

where:

Option	Description
hostname	Specifies the IPX address of the host, or if the host is a NetWare server, its advertised name.
-c *count*	Stops the test after sending and receiving the number of packets specified by *count*.
-i *delay*	Waits the number of seconds specified by *delay* before sending the next packet. The default is for one second.
-r *VRoutername*	Checks a supported VRouter's connectivity with another IPX host.
-s *packet-size*	Sends 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*
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
```

The output includes the following fields:

Field	Descriptions
network	IPX network number.
next router	Address of the next router, or 0 (zero) for a direct or WAN connection.
hops	Hop count to the network.
ticks	Tick count to the network.
origin	Name of the profile used to reach the network.

Note: An S or an H flag might appear next to the origin. S indicates a static route. H indicates a hidden or inactive static route. Hidden static routes occur when the router learns of a better route.

Managing the Open Shortest Path First (OSPF) protocol

Open Shortest Path First (OSPF) is the next generation Internet routing protocol. The Open in its name refers to the fact that OSPF was developed in the public domain as an open specification. The Shortest Path First portion refers to an algorithm developed by Dijkstra in 1978 for building a self-rooted shortest-path tree from which routing tables can be derived. As a link-state protocol, OSPF an take into account a variety of link conditions, such as the reliability or speed of the link, when determining the best path to a destination network. OSPF uses a link-state database of the network and propagates only changes to the database.

Displaying OSPF information

The terminal-server command-line interface provides commands for monitoring OSPF in the MAX. To display the supported commands, enter the Show OSPF command with a question mark:

```
scend% show ospf ?
show ospf ?          Display help information
show ospf size       Display OSPF size
show ospf areas      Display OSPF areas
show ospf stats      Display OSPF statistics
show ospf intf...    Display OSPF summary/detail interface information
show ospf internal   Display OSPF internal routes
show ospf lsa ...    Display OSPF detail link-state advertisements
show ospf lsdb ...   Display OSPF link-state DB summary for an area
show ospf nbrs ...   Display OSPF summary/detail neighbor information
show ospf routers    Display OSPF routers
show ospf ext        Display OSPF external AS advertisements
show ospf rtab       Display OSPF routing table
show ospf database   Display OSPF entire database summary
show ospf translator Display OSPF entire database summary
```

For additional information about supported commands, see RFC 1583.

Displaying OSPF areas

To display information about OSPF areas, enter the Show OSPF Areas command. For example:

```
ascend% show ospf area
Area ID  Authentication  Area Type #ifcs  #nets  #rtrs  #brdrs  #intnr
0.0.0.0  Simple-passwd   Normal     1      0      2      0       3
```

The output includes the following fields:

Field	Description
Area ID	Area number in dotted-decimal format.
Authentication	Type of authentication, Simple-passwd, MD5, or Null.
Area Type	Type of OSPF area: Normal, Stub, or NSSA.
#ifcs	Number of MAX interfaces specified in the area.
#nets	Number of reachable networks in the area.
#rtrs	Number of reachable routers in the area.
#brdrs	Number of reachable area border routers in the area.
#intnr	Number of reachable internal routers in the area.

Displaying general OSPF statistics

To display general information about OSPF, enter the Show OSPF Stats command. For example:

```
ascend% show ospf stats

         OSPF version:            2
         OSPF Router ID:          192.192.192.2
         AS boundary capability:  Yes
Attached areas:             1    Estimated # ext.(5) routes:   300
OSPF packets rcvd:      94565    OSPF packets rcvd w/ errs:      0
Transit nodes allocated: 3058    Transit nodes freed:         3056
LS adv. allocated:       1529    LS adv. freed:               1528
Queue headers alloc:       32    Queue headers avail:           32
# Dijkstra runs:            4    Incremental summ. updates:      0
Incremental VL updates:     0    Buffer alloc failures:          0
Multicast pkts sent:    94595    Unicast pkts sent:              5
LS adv. aged out:           0    LS adv. flushed:                0
Incremental ext.(5) updates: 0   Incremental ext.(7) updates:    0
External (type-5) LSA database -
Current state:            Normal
Number of LSAs:           1
Number of overflows:      0
```

The output includes the following fields:

Field	Description
OSPF version	Version of the OSPF protocols running.
OSPF Router ID	IP address assigned to the MAX, typically, the address specified for the Ethernet interface.
AS boundary capability	Displays Yes if the MAX functions as an ASBR or No if it does not.
Attached areas	Number of areas to which this MAX attaches.
Estimated # ext.(5) routes	Maximum number of ASE-5 routes that the MAX can maintain before it goes into an overload state.
OSPF packets rcvd	Total number of OSPF packets received by the MAX.
OSPF packets rcvd w/ errs	Total number of OSPF erroneous packets received by the MAX.
Transit nodes allocated	Allocated transit nodes, which are generated only by Router LSAs (Type 1) and Network LSAs (Type 2).
Transit nodes freed	Freed transit nodes, which are generated only by Router LSAs (Type 1) and Network LSAs (Type 2).
LS adv. allocated	Number of LSAs allocated.
LS adv. freed	Number of LSAs freed.
Queue headers alloc	Number of queue headers allocated. LSAs can reside in multiple queues. Queue headers are the elements of the queues that contain the pointer to the LSA.
Queue headers avail	Available memory for queue headers. To prevent memory fragmentation, the MAX allocates memory in blocks and allocates queue headers from the memory blocks. When the MAX frees all queue headers from a specific memory block, it returns the block to the pool of available memory blocks.
# Dijkstra runs	Number of times that the MAX has run the Dijkstra algorithm (short path computation).
Incremental summ. updates	Number of summary updates that the MAX runs when small changes occur that result in generation of Summary LSAs (Type 3) and Summary Router LSAs (Type 4).
Incremental VL updates	Number of incremental virtual link updates that the MAX performs.
Buffer alloc failures	Number of buffer allocation problems that the MAX has detected and from which it has recovered.
Multicast pkts sent	Number of Multicast packets sent by OSPF.
Unicast pkts sent	Number of unicast packets sent by OSPF.
LS adv. aged out	Number of LSAs that the MAX has aged and removed from its tables.

Field	Description
LS adv. flushed	Number of LSAs that the MAX has flushed.
Incremental ext.(5) updates	Number of incremental ASE-5 updates.
Incremental ext.(7) updates	Number of incremental ASE-7 updates.
Current state	State of the External (Type-5) LSA database, either Normal or Overload.
Number of LSAs	Number of LSAs in the External (Type-5) LSA database.
Number of over-flows	Number of ASE-5 that exceeded the limit of the database.

Displaying information about OSPF interfaces

Enter the Show OSPF Intf command to display either summarized information about all OSPF interfaces or specific information about a single interface.

To display summarized information on OSPF interfaces, enter the Show OSPF Intf command. For example:

```
ascend% show ospf intf

Ifc Address     Phys    Assoc. Area      Type    State    #nbrs #adjs DInt
194.194.194.2   phani   0.0.0.0          P-P     P-P        1     1   120
```

The output includes the following fields:

Field	Description
Ifc Address	Address assigned to the MAX unit's Ethernet interface. To identify WAN links, use the Type and Cost fields.
Phys	Name of the interface or the Connection profile for WAN links.
Assoc. Area	Area in which the interface resides.
Type	Point-to-Point (P-P) or Broadcast (Bcast). WAN links are P-P links.
State	State of the link according to RFC 1583. There are many possible states, and not all states apply to all interfaces.
#nbrs	Number of neighbors of the interface.
#adjs	Number of adjacencies on the interface.
DInt	Number of seconds that the MAX waits for a router update before removing the router's entry from its table. The interval is called the Dead Interval.

To display detailed information for a specific interface, enter the Show OSFP Intf command in the following format:

```
ascend% show ospf intf (ip address or physical name)
```

For example:

```
ascend% sh ospf intf 194.194.194.2
                Interface address:      194.194.194.2
                Attached area:          0.0.0.0
                Physical interface:     phani (wan1)
                Interface mask:         255.255.255.255
                Interface type:         P-P
                State:                  (0x8) P-P
                Designated Router:      0.0.0.0
                Backup DR:              0.0.0.0
                Remote Address:         194.194.194.3
DR Priority:        5  Hello interval:  30   Rxmt interval:  5
Dead interval:    120  TX delay:         1   Poll interval:  0
Max pkt size:    1500  TOS 0 cost:      10
# Neighbors:        1  # Adjacencies:    1   # Full adjs.:   1
# Mcast floods: 1856  # Mcast acks:   1855
```

The output includes the following fields:

Field	Description
Interface Address	The IP address specified for the MAX's Ethernet interface.
Attached Area	Area in which the interface resides.
Physical interface	Name of the interface or the Connection profile for WAN links.
Interface type	Point-to-Point (P-P) or Broadcast (Bcast). WAN links are P-P links.
State	State of the link according to RFC 1583. There are many possible states, and not all states apply to all interfaces.
Designated Router	IP address of the designated router for the interface.
Backup DR	IP address of the backup designated router for the interface.
Remote Address	IP address of the remote end of a Point-to-Point (WAN) link.
DR Priority	Priority of the designated router.
Hello interval	Interval in seconds that the MAX sends Hello packets as defined in RFC 1583.
Rxmt interval	Retransmission interval as described in RFC 1583.
Dead interval	Number of seconds that the MAX waits for a router update before removing the router's entry from its table.
TX delay	Interface transmission delay.
Poll interval	Poll interval of non-broadcast multi-access networks.
Max pkt size	Maximum packet size that the MAX can send to the interface.
TOS 0 Count	Type of Service normal (*0*) cost.
# neighbors	Number of neighbors.

Field	Description
# adjacencies	Number of adjacencies.
# Full adjs.	Number of fully formed adjacencies.
# Mcast floods	Number of multicast floods on the interface.
# Mcast acks	Number of multicast acknowledgments on the interface.

Displaying OSPF Link-State Advertisements (LSAs)

Enter Show OSPF commands to display a router's link state database and to expand the display of a particular LSA.

Displaying expanded OSPF link-state advertisements

To specify a link-state advertisement to be expanded, first display the database. To specify an LSA, enter a Show OSPF command in the following format, then specify the LSA to expand:

```
show ospf lsa area ls-type ls-id ls-orig
```

The Show OSPF LSA command requires that you include the first four fields of the LSA as listed in the database. Select the first four fields and paste them into the command line. For example, to display an expanded view of the last entry in the link-state database shown in the preceding section:

```
ascend% show ospf lsa 0.0.0.0 ase 10.5.2.160 10.5.2.162
```

```
LSA  type: ASE ls id: 10.5.2.160 adv rtr: 110.5.2.162 age: 568
        seq #: 80000037 cksum: 0xfffa
        Net mask: 255.255.255.255 Tos 0 metric: 10 E type: 1
        Forwarding Address: 0.0.0.0 Tag: c0000000
```

The output includes the following fields:

Field	Description
LSA type	Type of link as defined in RFC 1583 and identified by the type of LSA:
	• Type 1 (RTR)—Outer-LSAs that describe the collected states of the router's interfaces.
	• Type 2 (NET)—Network-LSAs that describe the set of routers attached to the network.
	• Types 3 and 4 (SUM)—Summary-LSAs that describe point-to-point routes to networks or AS boundary routers.
	• Type 7 (ASE)—Link advertisements that are flooded only within an NSSA.
ls id	Target address of the router.
adv rtr	Address of the advertising router.
age	Age of the route in seconds.
seq #	Number that begins with 80000000 and increments by one for each LSA received.

Field	Description
cksum	Checksum for the LSA.
Net mask	Subnet mask of the LSA.
Tos	Type Of Service for the LSA.
metric	Cost of the link, not of a route. The cost of a route is the sum of all intervening links, including the cost of the connected route.
E type	External type of the LSA indicating either 1 (Type 1) or 2 (Type 2).
Forwarding Address	Forwarding Address of the LSA, described in RFC 1583.
Tag	Tag of the LSA which is described in the OSFP RFC.

Displaying the OSPF link-state database

To display the router's link-state database, enter the Show OSPF LSDB command. For example:

```
ascend% show ospf lsdb
                        Area: 0.0.0.0
Type LS ID              LS originator    Seqno      Age     Xsum
RTR  192.192.192.2      192.192.192.2    0x800005f8  696    0x6f0b
RTR  192.192.192.3      192.192.192.3    0x800005f8  163    0x6f09
                # advertisements:       2
                Checksum total:         0xde14
```

The output includes the following fields:

Field	Description
Area	Area ID.
Type	Type of link as defined in RFC 1583: • Type 1 (RTR)—Outer-LSAs that describe the collected states of the router's interfaces. • Type 2 (NET)—Network-LSAs that describe the set of routers attached to the network. • Types 3 and 4 (SUM)—Summary-LSAs that describe point-to-point routes to networks or AS boundary routers. • Type 7 (ASE)—Link advertisements that are flooded only within an NSSA.
LS ID	Target address of the route.
LS originator	Address of the advertising router.
Seqno	Hexadecimal number that begins with 80000000 and increments by one for each LSA received.
Age	Age of the route in seconds.
Xsum	Checksum of the LSA.

Field	Description
# advertise-ments	Total number of entries in the link-state database.
Checksum total	Checksum of the link-state database.

Displaying OSPF neighbor information

To display information about OSPF neighbors to the MAX, enter the Show OSPF NBRS command. For example:

```
ascend% show ospf nbrs
Neighbor ID     Neighbor addr   State      LSrxl DBsum LSreq Prio Ifc
192.192.192.3   194.194.194.3   Full/-       0     0     0     5   phani
```

The output includes the following fields:

Field	Description
Neighbor ID	Address assigned to the interface. In the MAX, the IP address is always the address assigned to the Ethernet interface.
Neighbor addr	IP address of the router used to reach a neighbor. This is often the same address as the neighbor itself.
State	State of the link-state database exchange. Full indicates that the databases are fully aligned between the MAX and its neighbor.
LSrxl	Number of LSAs in the retransmission list.
DBsum	Number of LSAs in the database summary list.
LSreq	Number of LSAs in the request list.
Prio	Designated router election priority assigned to the MAX.
Ifc	Name for the Ethernet or Connection profile name for the WAN.

Displaying OSPF routers

To display OSPF routers, enter the Show OSPF Routers command. For example:

```
ascend% show ospf routers
DType  RType  Destination    Area      Cost        Next hop(s)    #
ASBR   OSPF   192.192.192.3  0.0.0.0   10          194.194.194.3  2
```

The output includes the following fields:

Field	Description
DType	Internal route type.
RType	Internal router type.
Destination	Router's IP address.
Area	Area in which the router resides.
Cost	Cost of the router.
Next hop(s)	Next hop in the route to the destination.

Field	Description
#	Number of the interface used to reach the destination.

Displaying OSPF External AS advertisements

To display OSPF External AS advertisements, enter the Show OSPF Ext command. For example:

```
ascend% show ospf ext
Type LS ID            LS originator    Seqno      Age   Xsum
ASE5 192.192.192.0    192.192.192.2    0x800005f6 751   0xc24d
# advertisements:     1
Checksum total:       0xc24d
```

The output includes the following fields:

Field	Description
Type	Displays ASE5.
LS ID	Target address of the route.
LS originator	Address of the advertising router.
Seqno	Hexadecimal number that begins with 80000000 and increments by one for each LSA received.
Age	Age of the route in seconds.
Xsum	Checksum of the LSA.
# advertise-ments	Total number of entries in the ASE5 database.
Checksum total	Checksum of the ASE5 database.

Displaying the OSPF routing table

To display the OSPF routing table, enter the Show OSPF Rtab command. For example:

```
ascend% show ospf rtab
```

The output includes the following fields:

Field	Description
DType	Internal route type. DType displays one of the following values: RTE (generic route), ASBR (AS border route), or BR (area border route).
RType	Internal router type. RType displays one of the following values: FIX (static route), NONE, DEL (deleted or bogus state), OSPF (OSPF-computed), OSE1 (type 1 external), or OSE2 (type 2 external).
Destination	Destination address and subnet mask of the route.
Area	Area ID of the route.
Cost	Cost of the route.
Flags	Hexadecimal number representing an internal flag.

Field	Description
Next hop(s)	Next hop in the route to the destination.
#	Number of the interface used to reach the destination.

Displaying summarized OSPF database information

To display summarized information about the OSPF database, enter the Show OSPF Database command. For example:

```
ascend% show ospf database
                     Router Link States (Area: 0.0.0.0)
Type LS ID            LS originator    Seqno      Age    Xsum
RTR  192.192.192.2    192.192.192.2    0x800005f8  783   0x6f0b
RTR  192.192.192.3    192.192.192.3    0x800005f8  250   0x6f09
                # advertisements:      2
                Checksum total:        0xde14

                     External ASE5 Link States
Type LS ID            LS originator    Seqno      Age    Xsum
ASE5 192.192.192.0    192.192.192.2    0x800005f6  783   0xc24d
                # advertisements:      1
                Checksum total:        0xc24d
```

The output includes the following fields:

Type	RTR (Router LSAs), NET (Network LSAs), ASE5 (External ASE5 link advertisements to destinations external to the autonomous system), or ASE7 (ASE-7 link advertisements that are flooded only within an NSSA).
LS ID	Target address of the route.
LS originator	Address of the advertising router.
Seqno	Hexadecimal number that begins with 80000000 and increments by one for each LSA received.
Age	Age of the route in seconds.
Xsum	Checksum of the LSA.
# advertisements	Total number of entries in the database.
Checksum total	Checksum of the database.

Displaying OSPF Translator information

The MAX that is configured to act as an Area Border Router (ABR) supports translation and summary Link State Advertisements (LSAs).The MAX can be a member of a multiple Areas and supports ABR features. The terminal-server includes a show command to display router IDs of the Not-So-Stubby-Area (NSSA) ABR. An NSSA is an Open Shortest Path First (OSPF) area that does not receive or originate Type-5 Link-State Advertisements (LSAs), and that imports Autonomous System (AS) external routes in a limited fashion. OSPF version 2 defines a new Type-7 LSA for NSSAs. For NSSAs, all routes imported to OSPF have the P-bit

set (P stands for propagate). When the P-bit is enabled, ABRs translate Type-7 LSAs to Type-5 LSAs, which can then be flooded to the backbone. These external routes are considered Type-7 LSAs.

The Show OSPF Translator command lists the Area ID that has to be a NSSA and the Router ID of the NSSA area border router performing the ASE7 to ASE5 translation:

```
admin > show ospf translators
Area ID Router ID
0.0.0.110.105.0.13
0.0.0.212.1.1.1
```

The output includes the following fields:

Area ID	Area number in dotted-decimal format.
Router ID	IP address assigned to the MAX, typically, the address specified for the Ethernet interface.

Verifying OSPF-related parameter settings

Verify the following OSPF-related parameter settings to assure proper OSPF performance on the MAX.

Parameter	Description
MAX # ASE LSA	Specifies the number of Link-State Advertisements (LSAs) the MAX unit stores before going into a state of database overload. When the unit reaches a database overload, it does not accept new entries and discards self-originated entries.
OSPF	Enables OSPF traps. With the Yes setting, the MAX unit generates traps that have been enabled in Ethernet > SNMP Traps > *any profile* > Enable traps. When you set OSPF to No, the MAX unit does not generate any OSPF traps regardless of any individual OSPF trap settings in Enable Traps.
OSPF If AuthFailure	Sends the OSPF If AuthFailure trap when the MAX unit receives a packet on a non-virtual interface from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type.
OSPF If ConfigError	Sends the OSPF If ConfigError trap when a nonvirtual interface receives a packet from a router whose configuration parameters conflicts with this router's configuration parameters.
OSPF If RxBadPacket	Sends the OSPF If RxBadPacket trap when the MAX unit receives an OSPF packet on a non-virtual interface that cannot be parsed.
OSPF If StateChange	Sends the OSPF If StateChange trap when there has been a change in the state of a nonvirtual OSPF interface.
OSPF LsdbApprchngOvrflw	Sends the OSPF LsdbApprchngOvrflw trap when the number of LSAs in the router's link-state database has exceeded ninety percent of ospfEx-tLsdbLimit.

Parameter	Description
`OSPF LsdbOverflow`	Sends the OSPF LsdbOverflow trap when the number of LSAs in the router's link-state database has exceeded `ospfExtLsdbLimit`.
`OSPF MaxAgeLsa`	Sends the OSPF MaxAgeLsa trap when the age of one of the LSAs in the router's link-state database reached the MaxAge value.
`OSPF Nbr StateChange`	Sends the OSPF Nbr StateChange trap when there has been a change in the state of a nonvirtual OSPF neighbor.
`OSPF OriginateLsa`	Indicates the number of new Link-State Advertisements (LSAs) that have been originated.
`OSPF TxRetrans`	Sends the OSPF TxRetransmit trap when the MAX unit retransmits an OSPF packet on a nonvirtual interface.
`OSPF VirtIf AuthFailure`	Sends the OSPF VirtIf AuthFailure trap when the MAX unit receives a packet on a virtual interface from a router whose authentication key or authentication type conflicts with the MAX unit's authentication key or authentication type.
`OSPF VirtIf ConfigError`	Sends the OSPF VirtIf ConfigError trap when the MAX unit receives a packet on a virtual interface from a router whose configuration parameters conflict with the MAX unit's configuration parameters.
`OSPF VirtIf StateChange`	Sends the OSPF VirtIf StateChange trap when there has been a change in the state of an OSPF virtual interface.
`OSPF VirtIf RxBadPacket`	Sends the OSPF VirtIf RxBadPacket trap when the MAX unit receives, on a virtual interface, an OSPF packet that cannot be parsed.
`OSPF VirtIf TxRetransmit`	Sends the OSPF VirtIf TxRetransmit trap when the MAX unit retransmits an OSPF packet on a virtual interface.
`OSPF VirtNbr StateChnge`	Sends the OSPF VirtNbr StateChnge trap when there has been a change in the state of an OSPF virtual neighbor.

Working with the OSPF routing table

The OSPF routing table includes routes built from the router's link-state database as well as those added by external routing protocols, such as RIP. Add routes statically (for example, to direct traffic destined for a remote site through one of several possible border routers). For details about adding static routes, see the *Network Configuration Guide* for your unit.

Only the main VRouter supports OSPF.

To display the IP routing table with added OSPF information, invoke the terminal server (System > Sys Diag > Term Serv) and enter the IProute Show command with the -l option:

```
ascend% iproute show -l
```

When you include the -l option, three columns of OSPF-specific fields appear at the routing table:

```
...     Cost        T       Tag
...     1           0       0xc0000000
...     9           1       0xc8000000
```

```
...      10           0            0xc0000000
...       9           1            0xc8000000
...       1           1            0xc0000000
...       3           1            0xc8000000
...       9           1            0xc8000000
...       4           1            0xc8000000
...       5           1            0xc8000000
...       3           1            0xc8000000
...       3           1            0xc8000000
...       3           1            0xc8000000
```

Table 7-11 describes the fields found in the OSPF routing table.

Table 7-11. OSPF routing table

Field	Description
Cost	Cost of an OSPF route. The interpretation of this cost depends on the type of external metric, which is displayed in the next column. If the MAX is advertising Type-1 metrics, OSPF can use the specified number as the cost of the route. Type-2 external metrics are an order of magnitude larger.
T	Link-state advertisement (LSA)-type of the metric to be advertised for an external route. A 0 (zero) in this column means that the metric is an external-Type-1 or an OSPF internal route. A 1 means that the route is an external-Type-2 route.
Tag	Specifies a 32-bit hexadecimal number attached to each external route to tag it as external to the AS. The number may be used by border routers to filter this record.

Displaying the size of the OSPF routing table

To display the size of the OSPF routing table, enter the Show OSPF Size command. For example:

```
ascend% show ospf size
             # Router-LSAs:                2
             # Network-LSAs:               0
             # Summary-LSAs:               0
             # Summary Router-LSAs:        0
             # AS External-LSAs (type-5):  1
             # AS External-LSAs (type-7):  0

             # Intra-area routes:     4
             # Inter-area routes:     0
             # Type 1 external routes: 0
             # Type 2 external routes: 0
```

The output includes the following fields:

Fields	Description
# Router-LSAs	Number of router link advertisements that are also Type-1 Link State Advertisements.
# Network-LSAs	Number of network link advertisements that are also Type-2 LSAs.
# Summary-LSAs	Number of summary link advertisements that are also Type-3 LSAs. Type-3 LSAs describe routes to networks.
# Summary Router-LSAs	Number of summary link advertisements that are also Type-4 LSAs. Type-4 LSAs describe routes to AS boundary routers.
# AS External-LSAs (type-5)	Number of AS external link advertisements which are also Type-5 LSAs.
# AS External-LSAs (type-7)	Number of ASE-7 link advertisements that are also Type-7 LSAs.
Intra-area routes	Number of routes with a destination within the area.
Inter-area routes	Number of routes with a destination outside the area.
Type 1 external routes	Number of external Type-1 routes that are typically in the scope of OSPF-IGP.
Type 2 external routes	Number of external Type-2 routes that are typically outside the scope of OSPF-IGP.

Multipath routing

A MAX unit running OSPF can alternate between two equal-cost gateways. When OSPF detects equally good gateways, in terms of routing costs, it puts each equal-cost gateway on an equal-cost list. The router alternates between the gateways on the list in what is called equal-cost multipath routing.

The M in the Flg column indicates an equal-cost multipath. A Traceroute from Router A to example.com would produce the following display:

```
ascend% traceroute -q 10 example.com

traceroute to example.com (10.174.88.1), 30 hops max, 0 byte packets

1  C.example.com (10.174.88.13)  20 ms B .example.com (10.174.88.12)
20 ms C.example.com (10.174.88.13)  20 ms B .example.com
(10.174.88.12)  20 ms  20 ms C.example.com (10.174.88.13)  60 ms  20 ms
B .example.com (10.174.88.12)  20 ms C.example.com (10.174.88.13)  20
ms B .example.com (10.174.88.12)  20 ms

2  example.com (10.174.88.1)  20 ms  20 ms  20 ms  20 ms  30 ms  20 ms
20 ms  30 ms  20 ms  30 ms
```

Notice the alternating replies. The replies are statistically dispatched to Router B and Router C, with roughly 50% of the packets sent through each gateway. (For background information about the routing table and about the Traceroute command, see the *Network Configuration Guide* for your unit.)

Third-party routing

A MAX running OSPF can advertise routes to external destinations on behalf of another gateway (a *third party*). This is commonly known as advertising a forwarding address. Depending on the exact topology of the network, other routers might be able to use this type of link-state advertisement (LSA) and route directly to the forwarding address without involving the advertising MAX, thereby increasing the total network throughput.

Third-party routing requires that all OSPF routers know how to route to the forwarding address. This usually means that either the forwarding address must be on an Ethernet that has an OSPF router acting as the forwarding router or the designated router is sending LSAs for that Ethernet to any area that sees the static route's forwarding-address LSAs. The following example shows how to configure a static route for OSPF to advertise a third-party gateway:

1 Open a static route in Ethernet > Static Rtes.

2 Set the Gateway to the forwarding address and set Third-Party to `Yes`.

```
Ethernet
  Static Rtes
    40-401 SRprofile1
      Name=SRprofile1
      Active=Yes
      Dest=10.212.65.0/24
      Gateway=101.2.3.4
      Metric=3
      Preference=100
      Private=No
```

3 Close the static route.

How OSPF adds RIP routes

When the MAX establishes an IP routing connection with a caller that does not support OSPF, it imports the AS-external route from the Connection profile and adds it to the routing table. The MAX does not have to run RIP to learn these routes. In fact, RIP should be turned off when the MAX is running OSPF.

To enable OSPF to add the RIP-v2 routes to its routing table, configure RIP-v2 normally in the Connection profile. OSPF will import all RIP routes as Type-2 Autonomous System Externals (ASEs). The reason that RIP routes are imported with Type-2 metrics by default is that RIP metrics are not directly comparable to OSPF metrics. To prevent OSPF from interpreting RIP metrics, the imported ASE route is assigned a Type-2 metric, which is so large compared to OSPF costs that the metric can be ignored.

Route preferences

Route preferences provide additional control over which types of routes take precedence over others. They are necessary in a router that supports multiple routing protocols, largely because RIP metrics are not comparable with OSPF metrics.

For each IP address and subnet mask pair, the routing table holds one route per protocol. The routes are assigned preferences as follows:

- Connected routes, such as Ethernet, have `Preference=0`.

- Routes learned from Internet Control Message Protocol (ICMP) redirects have `Preference=30`.

- Routes placed in the table by SNMP MIB II have `Preference=100`.

- Routes learned from OSPF have a default of `Preference=10`. Modify the default in Ethernet > Mod Config > Route Pref.

- Routes learned from RIP have a default of `Preference=100`. Modify the default in Ethernet > Mod Config > Route Pref.

- A statically configured IP Route or Connection profile has a default of `Preference=100`. Modify the default in the Connection or IP Route profile.

When choosing which routes should be put in the routing table, the router first compares the Preference values, preferring the lowest number. If the Preference values are equal, the router compares the Metric field and uses the route with the lowest Metric.

If multiple routes exist for a given address and subnet mask pair, the route with the lowest Preference is best. If two routes have the same Preference, then the lower Metric is better. The best route by these criteria is that actually used by the router. The others remain latent, or *hidden*, in case the best route is removed.

To assign a WAN link the same preference as a route learned from OSPF:

1 Open Connections > IP Options.

2 Specify a Preference value of 10 (the default value for OSPF routes). For example:

```
Ethernet
  Connections
    40-101 Cprofile1
      IP options…
        LAN Adrs=10.9.8.10/22
        WAN Alias=0.0.0.0
        IF Adrs=0.0.0.0
        Preference=10
        Metric=5
        DownPreference=
        DownMetric=
        ...
        ....
        ...
```

3 Close the Connection profile.

On Ethernet, the route preferences also include ASE-type and ASE-tag information for routes learned from RIP. These values affect all RIP information learned across the Ethernet. To change the route preferences on Ethernet:

1 Open Ethernet > Mod Config > Route Pref.

2 Modify the parameters to adjust Preference values. For example, the following profile assigns static routes the same Preference value as those learned from OSPF:

```
Ethernet
  Mod Config
    Route Pref...
      Static Preference=10
```

```
                       Rip Preference=100
                       Rip Queue Depth=50
```

3   Close the Ethernet profile.

MD5 cryptographic authentication

Support for OSPF on MAX 6000 and MAX 3000 units includes the MD5 cryptographic
authentication method. Verify the settings specified to support the MD5 authentication type.
The MAX can validate OSPF packet exchanges using MD5 encryption and an authentication
key of as many as 16 characters. The authentication key value in the KeyID field is a number
from 0 to 255. The authentication key in a MD5 Key field can have as many as 16 characters.
Table 7-12 summarizes the MD5 cryptographic parameters.

Table 7-12. MD5 Cryptographic parameters

Parameter	Description
MD5 Key	Specifies an authentication key (a password) used to allow OSPF routing. MD5 Key is a number from 0 to 255 inserted into the OSPF packet header. OSPF routers use MD5 Key to allow or exclude packets from an area. The default value is 0. The key can contain as many as 16 characters.
KeyID	Specifies an authentication key (a password) used to allow OSPF routing. KeyID is a number from 0 to 255 inserted into the OSPF packet header. OSPF routers use KeyId to allow or exclude packets from an area. The default value is 0.
AuthType	Specifies the type of authentication in use for validating OSPF packet exchanges: Simple (the default) or None. Simple authentication is designed to prevent configuration errors from affecting the OSPF routing database. It is not designed for firewall protection.

Enabling Finger support

Configure the MAX to respond to Finger requests, as specified in RFC 1288, *The Finger User Information Protocol*.

To enable the MAX to respond to Finger requests:

1   Open the Ethernet > Mod Config.

2   Set Finger to Yes.

3   Exit and save the changes.

Understanding the AppleTalk-routing environment

As another example, Smith Company adds AppleTalk devices to the network and sets up an AppleTalk-routed environment, illustrated in Figure 7-2. All sites support IP routing and AppleTalk routing or bridging. Twelve dial-in analog circuits are available for employees to dial in to 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 12 connections available for employees to dial into while traveling. The MAX dynamically assigns up to 10 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, Site A, SiteB, and SiteC. The units share Ethernet segments as follows:

- Devices that share the Ethernet segment with the MAX unit belongs to network 100-150.

- Devices that share the Ethernet segment with the Site A Pipeline belong to network 200-210.

- Devices that share the Ethernet segment with the Site B Pipeline belong to network 300-300.

- Devices that share the Ethernet segment with the Site C Pipeline belong to network 700-700.

Figure 7-2. Example AppleTalk-routed environment
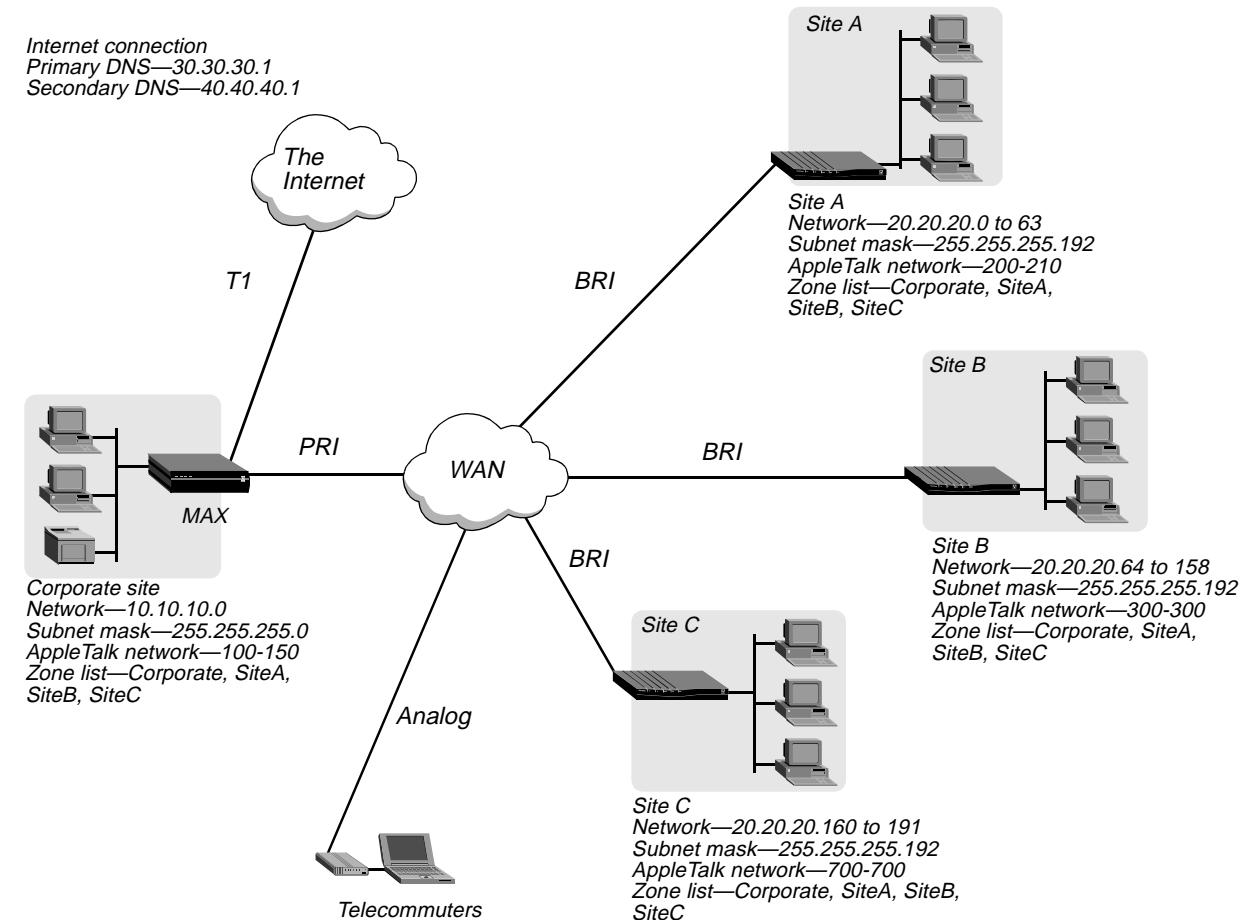
Administering PAD, X.25, and Frame Relay

8

You can manage the Packet Assembler/Disassembler (PAD), X.25 and Frame Relay functions
on the MAX unit through the unit's terminal-server CLI. You can verify the settings of support
PAD through the VT100 interface's Ethernet menu.

Administering X.25

X.25 is an international ITU-T protocol that enables users to transmit information over a
packet-switched network. It allows remote devices to communicate with one another across
high-speed digital links without the expense of individual nailed-up lines. The X.25 protocol
handles both high-volume data transfers and interactive use of host machines. As a full-duplex,
connection-oriented protocol, X.25 uses Virtual Circuits (VCs) and provides services such as
multiplexing, in-sequence delivery, transfer of addressing information, segmenting and
reassembly, flow control, transfer of expedited data, error control, reset, and restart. Allocation
of logical channels can be either static (using a Permanent Virtual Connection, or PVC) or
dynamic (using a Switched Virtual Connection, or SVC).

X.25 uses the first three layers of the OSI model. The Physical layer implements several
standards, such as V.35, RS-232 and X.21bis. The Data Link layer uses an implementation of
Link Access Procedure, Balanced (LAPB) and provides an error-free link between two
connected devices. The Network Layer uses the Packet Layer Protocol (PLP). PLP is primarily
concerned with network-routing functions and the multiplexing of simultaneous logical
connections over a single physical connection. X.25 exchanges packets between local Data
Terminal Equipment (DTE) and remote Data Circuit-Terminating Equipment (DCE).

Internet Protocol over X.25 is a method of transporting IP packets on X.25 facilities when the
circuit is established as an end-to-end X.25 connection. X.25/Transaction Processing Protocol
for Point-of-Service (X.25/T3POS) is a character-oriented, frame-formatted protocol designed
for an X.25 packet-switched network. The protocol provides reliable and efficient data
transactions between a host device and Data Terminal Equipment (DTE). The DTE is usually a
client device communicating through an asynchronous port, while the host is a mainframe
communicating by means of an X.25 packet network. The MAX converts data arriving from
the DTE to a format capable of being transmitted over a packet network. In addition,

X.25/T3POS enables you to send data over the ISDN D channel while continuing to send traffic over both B channels.

Displaying information about X.25

To display information about X.25 frame and packet layers, enter the Show X25 command. For example:

```
ascend% show x25


Frame       State           BytesIn         BytesOut
 1          LinkUp            15               45


Packet      State           BytesIn         BytesOut
 1          Ready             0                0
```

The output includes the following fields:

Field	Description
Frame	Frame layer.
Packet	Packet layer.
State	State of the connection at that layer.
	For the frame layer, the following states can occur:
	• SABMSent—The MAX has sent an Set Asynchronous Balanced Mode (SABM) message to establish the operating mode as Link Access Balanced Protocol (LABP), and the transmitter is waiting for a an Unnumbered Acknowledge response (UA).
	• DISCSent—The MAX sends a DISC message to disconnect the frame level, and the transmitter is waiting for a UA.
	• FRMRSent—The MAX sends an FRMR message, indicating that the MAX received a malformed frame, and the sender is waiting for a SABM message.
	• LinkUp—The link is up and sending I frames and S frames.
	• Disconnected—The MAX requests a disconnect, and the sender is waiting for a SABM message.
	For the packet layer, the following states can occur:
	• Ready—The packet layer is ready to send and receive data.
	• DTERestart—The DTE issues a Restart Request.
	• DCERestart—The DCE issues a Restart Request.
	• BothRestart—The MAX sends Restart Requests to both the DTE and the DCE.
	• InitState—Indicates the initial state of a call.
BytesIn	Number of bytes the MAX receives from the remote node.
BytesOut	Number of bytes the MAX transmits to the remote node.

X.25 clear cause codes

Table 8-1 shows hexadecimal X.25 clear cause codes.

Table 8-1. Clear cause codes

Hex value	Cause code
01	Number busy
03	Invalid facility request
05	Network congestion
09	Out of order
0B	Access barred
0D	Not obtainable
11	Remote procedure error
13	Local procedure error
15	RPOA out of order
19	Reverse charging acceptance not subscribed
21	Incompatible destination
29	Fast select acceptance not subscribed
39	Ship absent
C1	Gateway-detected procedure error
C3	Gateway congestion

X.25 diagnostic field values

Table 8-2 shows X.25 diagnostics.

Table 8-2. X.25 diagnostic field values

Hex value	Dec value	Diagnostic
0	0	No additional information
1	1	Invalid P(S)
2	2	Invalid P(R)

Table 8-2. X.25 diagnostic field values (continued)

Hex value	Dec value	Diagnostic
10	16	Packet type invalid
11	17	State r1
12	18	State r2
13	19	State r3
14	20	State p1
15	21	State p2
16	22	State p3
17	23	State p4
18	24	State p5
19	25	State p6
1A	26	State p7
1B	27	State d1
1C	28	State d2
1D	29	State d3
20	32	Packet not allowed
21	33	Unidentifiable packet
22	34	Call on one-way LC
23	35	Invalid packet type on a PVC
25	37	Reject not subscribed to
26	38	Packet too short
27	39	Packet too long
29	41	Restart packet with non-zero LC
2B	43	Unauthorized interrupt confirmation
2C	44	Unauthorized interrupt
2D	45	Unauthorized reject
30	48	Timer expired

Table 8-2. X.25 diagnostic field values (continued)

Hex value	Dec value	Diagnostic
31	49	Incoming call (or DTE timer expired for call request)
32	50	Clear indication (or DTE timer expired or retransmission count surpassed for clear request)
33	51	Reset indication (or DTE timer expired or retransmission count surpassed for reset request)
34	52	Rstart indication (or DTE timer expired or retransmission count surpassed for restart request)
40	64	Call setup, call clearing, or registration problem
41	65	Facility/registration code not allowed
42	66	Facility parameter not allowed
43	67	Invalid called address
44	68	Invalid calling address
45	69	Invalid facility/registration length
46	70	Incoming call barred
47	71	No logical channel available
48	72	Call collision
49	73	Duplicate facility requested
4A	74	Nonzero address length
4B	75	Nonzero facility length
4C	76	Facility not provided when expected

Administering PAD

A Packet Assembler/Disassembler (PAD) is an asynchronous terminal concentrator that enables several terminals (or other asynchronous devices) to share a single network line. In an X.25/PAD configuration, PAD-generated packets are transported using the X.25 protocol. The PAD assembles data from terminals into packets for transmission to an X.25 network and disassembles incoming packets from the network into a separate data stream for each terminal. In addition to this multiplexing function, the PAD also provides a nearly error-free connection.

The MAX unit's X.25/PAD implementation allows users to access a public or private packet-switched network over a nailed-up ISDN connection. When a user calls X.25/PAD

through a modem, the terminal server performs the authentication using a local Connection Profile or a RADIUS user profile.

Displaying information about PAD sessions

To display information about PAD sessions, enter the Show PAD commands. For example:

```
ascend% show pad

Port   State        LCN      BPS      User      Called Addr.
1      connected    0        9600     plato     419342855555
2      connected    0        9600     irma
```

The output includes the following fields:

Field	Description
Port	Port for the X.25 connection.
State	State of the connection, which can be one of the following:
	Idle—The PAD is open, but no call has been issued.
	Calling—A call has been issued and is awaiting acceptance.
	Connected—The call is connected and in session.
	Clearing—A Clear command has been issued and the transmitter is awaiting a clear confirmation.
LCN	Logical Channel Number for a PVC. An LCN of 0 means the circuit is not a PVC (but is a switched virtual circuit).
BPS	Data rate of the connection in bits per second.
User	Connection profile name of the caller.
Called Add	X.121 address of the remote node.

Verifying PAD-related settings

Verify PAD-specific settings in the Connection profile's Encaps Options or in the Ethernet menu's T3POS options in order to assure that the MAX performs PAD functions correctly. For more information, refer to the *Network Configuration Guide* for your unit. Table 8-3 summarizes PAD-specific parameters.

Table 8-3. PAD-specific parameters

Parameter	Description
T3POS T1	Specifies the Char-to-Char timer. This timer indicates the maximum amount of time permitted between characters sent from the DTE to the PAD.

Table 8-3. PAD-specific parameters (continued)

Parameter	Description
T3POS T2	Specifies the Syn-to-Syn timer. This timer applies to opening frames in Local or Bin-Local mode. Normally, the PAD sends Syn signals to the DTE at the interval specified by the T2 timer to indicate that an idle link is still alive. However, if the DTE sends a Syn signal to the PAD before the PAD sends one to the DTE, the T2 timer specifies the period of time the PAD expects Syn signals from the DTE. If the PAD does not receive two Syn signals with the interval specified by the T2 timer, it tries to restore the link. The T2 timer only applies to the opening frame and to Local or Bin-Local mode.
T3POS T3	Specifies the ENQ handling timer. This timer indicates the amount of time the PAD waits for an ENQ from the host. This is not applicable when you set the ENQ Handling parameter to Off.
T3POS T4	Specifies the Response Timer. This timer indicates the amount of time the PAD waits for a Syn from the DTE while the PAS is waiting for a response from the DTE. The Syn signal indicates that the response from the DTE is being delayed and also indicates that the link is still alive.
T3POS T5	Specifies the Data Link Escape (DLE), End of Transmission (EOT) timer. This timer indicates the maximum idle-time the PAD allows for a T3POS call (this is similar to the VC inactivity timer in the X25/PAD). The T5 timer applies only to transparent and blind mode only; it is disabled in both Local mode and Bin-Local mode. The T5 timer may apply even if the default modes for both the host- and DTE-initiated calls are Local or Bin-Local. This is because the mode can be changed through an opening frame, in which case this parameter applies. The T5 timer applies only to transparent and blind mode; it is disabled in both Local mode and Bin-Local mode.
T3POS T6	Specifies the Frame Arrival timeout. This timers indicates the maximum amount of time allowed between the time a dial-up connection is established and the first character of an opening frame is received.

Understanding PAD service signals

The PAD transmits PAD service signals to the terminal server to acknowledge PAD commands and to inform the user about the internal state of the PAD. The terminal-server user can

suppress the reception of PAD service signals by setting PAD parameter #6 to 0 (zero).
Table 8-4 lists the PAD service signal messages.

Table 8-4. PAD service signal messages

Service signal	Description
RESET DTE	The remote DTE has reset the virtual circuit.
RESET Err	A reset has occurred because of a local procedure error.
RESET NC	A reset has occurred because of network congestion.
COM	A call has been connected.
PAD ID	Precedes a string that identifies the PAD.
ERROR	The terminal-server user used faulty syntax when entering an X.25/PAD command.
CLR	A virtual circuit has been cleared.
ENGAGED	A response to the Stat command, indicates that a virtual call is up.
FREE	A response to the Stat command, indicates that a virtual call is cleared.
PAR	A response to the Set? command.

Administering Frame Relay

Frame Relay is a WAN architecture originally developed for ISDN lines. A Frame Relay network provides high throughput by handing monitoring functions to higher-level protocols. It is a very efficient standard, with a bandwidth of up to 2 Mbps. Frame Relay is ideal for situations in which periods of very high traffic are interspersed with idle periods. It is protocol independent, and performs routing over Virtual Circuits (VCs) called Data Link Connection Indicators (DLCIs). A datalink is the link interface to a Frame Relay device. The datalink refers to specific nailed-up bandwidth on the MAX unit and defines the operations and link-management functions that the unit performs on the interface.

A Frame Relay network is one in which every access point connects directly to a Frame Relay switch. Depending on how a device, such as the MAX, is integrated into the Frame Relay network, it can operate as a Frame Relay terminating unit (Customer Premises Equipment or CPE) or as a Frame Relay switch. A CPE is the source or destination of data using the Frame Relay service. For example, a MAX can be the source and destination of the data stream from its PPP callers. When a MAX is configured with a User-to-Network interface (UNI) to Frame Relay, it acts as the user side data terminal equipment (UNI-DTE) communicating with the network side data communications equipment (UNI-DCE) of a switch.

A network-side device connects the CPE device to a Frame Relay network. For example, a MAX can receive Frame Relay encapsulated frames from a CPE and forward them on to another Frame Relay switch. When it is configured with a UNI-DCE interface, the MAX acts as the network side (UNI-DCE) communicating with the user side (UNI-DTE) of a Frame Relay device.

A Frame Relay concentrator concentrates many low-speed, dial-in connections into one high-speed, nailed-up connection to a Frame Relay switch. As a Frame Relay concentrator, the MAX forwards many lower-speed PPP connections onto one or more high-speed Frame Relay interfaces.

A Frame Relay switch sends Frame Relay data out to the Frame Relay network. As a Frame Relay switch, the MAX receives frames on one interface and transmits them on another interface. The decision to forward frames onto the Frame Relay interface is made at OSI layer 2. The MAX router software is not involved. To use the MAX as a switch, you must configure a circuit that pairs two Frame Relay interfaces. Instead of going to the Layer 3 router for a decision on which interface to forward the frames, the MAX relies on the circuit configuration to relay the frames received on one interface to its paired interface. A circuit is defined in two Connection or RADIUS profiles.

Using the Set commands to configure Frame Relay

Use Set FR commands to dial and hang up the Frame Relay datalink and to remove the RADIUS Frame Relay datalink profile. With this command, you bring down the nailed connection specified in the named Frame Relay profile and the unit reestablishes the connection within a few seconds. The Set Circuit commands let you activate or deactivate a Frame Relay circuit.

Use the Set commands summarized in Table 8-5 to administer Frame Relay on the MAX unit.

Table 8-5. Set commands

Command	Description
set all	Displays current settings.
set term	Sets telnet/rlogin terminal type.
set password	Enables dynamic password serving (or password mode).
set fr do [name]	Do dial on the FR datalink.
set fr hangup [name]	Do hangup on the FR datalink.
set fr remove [name]	Remove the RADIUS FR datalink.
set circuit active [name]	Set the Frame Relay circuit to active.
set circuit inactive [name]	Set the Frame Relay circuit to inactive.

Using Traps to Monitor Performance

9

MAX unit 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.You can establish SNMP access security, use the SNMPv3 User-based Security Model (USM), set SNMP traps, use OSPF-related SNMP traps, and interpret Alarm/Error and Security events.

For complete information about each SNMP, SNMPv3, or OSPF-related parameter, see the *MAX Reference*.

Establishing SNMP access security

The MAX unit can support SNMPv1 and SNMPv3 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.

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=Lucent
      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
      Queue Depth=0
      Message Type=v1-and-v3
      Security Level=none
```

Enabling SNMP Set commands

The R/W Comm Enable parameter disables SNMP set commands by default. Before you 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

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, retrieve `sysAbsoluteStartupTime` and compare its value against the previous poll's value for Ascend Events Group variables.

Specifying User-based security

If the MAX unit has the Network Management option installed, specify whether the unit supports SNMPv1 (hereafter referred to as SNMP), SNMPv3, or both by using the Message Type parameter. In addition, the Security Level specifies whether or not the MAX unit verifies user's the Security Level settings. The unit compares the Security Level field in the incoming message to the one specified on the unit. If the Security Levels do not match, the unit sends a report message.

For more details regarding SNMPv3, see "Using the SNMPv3 User-based Security Model" on page 9-4.

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
```

```
Queue Depth=0
Message Type=v1-and-v3
Security Level=none
```

Using the SNMPv3 User-based Security Model

MAX units with the Network Management option enabled support security enhancements based on the SNMPv3 User-based Security Model (USM), which is compliant with RFC 2574.

Verifying Network Management is installed

Verify that the Network Management option is installed on your MAX unit, by checking the Sys Option status window. If the option is installed, the status window shows it, as in the following example:

```
00-100 Sys Option

   K56 Slot Card Only
   Not Installed
   Net Mgmt Installed
```

For complete information about using status windows, see the *Hardware Installation and Basic Configuration Guide* for your unit.

Required SNMP Options profile settings

The Message Type parameter Ethernet > Mod Config > SNMP Options > Message Type specifies the SNMP version(s) that the MAX unit's SNMP agent supports. Specify one of the following values:

- `V1-and-V3` (the default)—The SNMP agent supports both the SNMPv1 and SNMPv3 protocols.
- `V1-only`—The SNMP agent discards SNMPv3 messages.
- `V3-only`—The SNMP discards SNMPv1 messages.

The Security Level parameter specifies whether or not the MAX unit verifies user's the Security Level settings. The unit compares the Security Level field in the incoming message to the one specified on the unit. If the Security Levels do not match, the unit sends a report message. Specify one of the following settings:

- `None`—The MAX unit does not require a security level check for the incoming message. None is the default.
- `Auth-Nopriv`—The MAX unit requires a Security Level of `auth-nopriv` in the incoming message.
- `Auth-Priv`—The MAX unit requires a Security Level of `auth-priv` in the incoming message.

For the MAX unit to accept SNMPv3 USM messages, you must configure the Message Type and Security parameters (in the SNMP Options profile) to their default settings, `v1-and-v3` and `none`, respectively. For example:

```
90-B00 Mod Config

   SNMP Options...

   Read Comm=public
   R/W Comm Enable=Yes
   R/W Comm=write
   Security=No
   RDmgr1=0.0.0.0
   .
   RD Mgr5=0.0.0.0
   WR Mgr1=0.0.0.0
   .
   WR Mgr5=0.0.0.0
   Queue Depth=0
   Message Type=v1-andv3
   Security Level=none
```

Required SNMPv3 USM Users profile settings

To enable SNMPv3 USM security features, you must configure at least one SNMPv3 USM Users profile. Enable up to nine profiles on the MAX unit. For example:

```
90-B00 SNMPv3 USM Users

   90-B01
   90-B02
   90-B03
   90-B04
   90-B05
   90-B06
   90-B07
   90-B08
   90-B09
```

For each SNMPv3 USM Users profile, you must specify a profile name and set the Active parameter to `Yes`. You must also specify a password if the Auth Protocol parameter is set to any setting other than `none`. For example:

```
90-B01

   Name=Boston1
   Passwd=******
   Active=Yes
   R/W Access=No
   Auth Protocol=md5-auth
   Priv Protocol=N/A
```

In the preceding example, the user has specified Name and a Passwd values because the Auth Protocol setting is `md5-auth`. Specification of a Password is not required if the Auth Protocol

parameter specifies `none`. In most circumstances, accept the default settings for the other parameters in the SNMPv3USM Users profile.

Table 9-1 summarizes the SNMPv3 USM-related parameters in the SNMPv3 USM Users profile.

Table 9-1. SNMPv3-related parameters

Parameter	Description
Active (SNMPv3 USM Users)	Activates a SNMPv3 USM user profile and makes it available for use.
Auth Protocol	Specifies whether or not the MAX unit can authenticate messages sent to and from the SNMP engine, on behalf of the SNMPv3 USM user. Also, specifies the type of authentication protocol the unit uses.
Name (SNMPv3 USM Users)	Specifies the user (in the SNMPv3 USM Users profile) for whom the MAX unit exchanges an SNMPv3 USM message.
Passwd (SNMPv3 USM Users)	Specifies the user's password (in the SNMPv3 USM Users profile) which maps to a 16 or 20 octet key, in compliance with RFC 2574. Passwords are case sensitive.
Priv Protocol	Specifies whether or not messages that are sent to or from the SNMP engine can be protected by encryption and the type of privacy protocol to be used.
R/W Access	Specifies whether or not the MAX unit grants the SNMPv3 USM user read and write access to the unit's MIB settings.

Using 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
    40-901 SNMP Traps profile 1
      Name=
      Alarm=Yes
      Port=Yes
      Security=Yes
      Comm=
      Dest=10.2.3.4
      Enable traps...
```

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.

Configuration Change allows you to specify that the MAX unit sends an SNMP string of information containing the date, time, and information about the user who has made a change to the configuration of the unit. The unit also sends the security profile and security profile name of a user who modifies the configuration or loads a different software binary code to the MAX unit.

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, `Lucent`).

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
    40-901 SNMP Traps profile 1
      Name=security-traps
      Alarm=Yes
      Port=Yes
      Security=Yes
      Comm=Lucent
      Dest=10.2.3.4
      Enable traps...
```

Enable Traps profile settings

Following are the parameters related to Enable traps (shown with sample settings):

```
Enabletraps...
    Cold start=Yes
    Warm start=Yes
    Link Down=Yes
    Link Up=Yes
    Ascend=Yes
    Console=Yes
    Use exceeded=Yes
    Telnet password=Yes
    FR link up=Yes
    FR link down=Yes
    Event overwrite=Yes
    Radius change=Yes
    Multicast monitor=Yes
    Lan Modem=Yes
    Power supply=No
    SNMP authentication=Yes
    Configuration change=Yes
    Clock drifted=Yes
    Suspect access resource=Yes
    Call Log Dropped Pkt=Yes
    Call Log Server Change=Yes
    VOIP Gatekeeper Change=Yes
    WAN Line State Change=Yes
    Watchdog=No
```

Table 9-2 summarizes the parameters that ensure you can use SNMP traps.

Table 9-2. Trap-related parameters

Parameter	Description
Ascend	Specifies whether a trap is generated to indicate a change of state in a host interface. All port connections are monitored in a state machine and reported by this trap.
Cold Start and Warm Start	Cold Start specifies whether the system generates a trap when the MAX reinitializes itself so that the configuration of the SNMP manager or the system itself might be altered. Warm Start specifies whether the system generates a trap when the MAX reinitializes itself so that neither the configuration of the SNMP manager nor of the system itself is altered.
Configuration Change	Specifies whether the MAX unit can send a string of information containing the date and time of any change. It also sends the security profile and security profile name of a user who modifies the configuration or loads a new image to the unit.

Table 9-2. Trap-related parameters (continued)

Parameter	Description

Console	Specifies whether the MAX unit sends the console's IP address to the SNMP manager in the Console State Changed trap. The Console State Change trap carries the information displayed in the following example:
	
	`1999-07-02 12:07:26 eng-fast-4.ascend.com`
	`[192.168.25.4] enterprises.529:`
	`Enterprise Specific Trap (12)Uptime:0:16:43`
	`enterprises.529.8.2.1.1.2=2`
	`enterprises.529.12.2.1.4.2=IpAddress:10.40.40`
	`.133`

Event Overwrite	Specifies whether the system generates a trap when a new event has overwritten an unread event. This trap is sent only for systems that support the Ascend accounting MIB.
FR Link Up and FR Link Down	FR Link Down specifies whether a trap is sent whenever a DLCI ends. FR Link Up specifies whether a trap is sent whenever a DLCI is initiated.
LAN Modem	Specifies whether the system generates a trap when a digital modem is moved to the suspect list.
Link Up and Link Down	Link Up specifies whether the system generates a trap when the communication link between the unit and the SNMP manager is reestablished. Link Down specifies whether the system generates a trap when a failure occurs in a communication link between the unit and the SNMP manager.
Multicast Monitor	Specifies whether the system generates a trap when multicast heartbeat monitoring is configured and the system did not receive the specified number of heartbeat packets on a multicast interface.
Power Supply	Specifies whether or not the unit generates a trap when the power is introduced or interrupted.
RADIUS Change	Specifies whether the system generates a trap when a new RADIUS server is being accessed. The trap returns the objectID and IP address of the new server.
SNMP Authentication	Specifies whether the system generates a trap when an authentication failure occurs.
Suspect Access Resource	Specifies whether the system generates a trap when a slot card resource is moved to the suspect list.

Table 9-2. Trap-related parameters (continued)

Parameter	Description
Telnet Password	Specifies whether all failed Telnet login attempts generate a trap.
Use Exceeded	Specifies whether the system generates a trap when a specific port has exceeded the number of DS0 minutes allocated to it or when the system DS0 usage has been exceeded.

Using OSPF-related SNMP traps

MAX units support OSPF-related SNMP traps defined in RFC 1850 (rfc1850.mib), which replaces RFC 1253 (rfc1253.mb).

RFC 1850 defines MIB object `ospfSetTrap`, for enabling trap events, as follows:
```
iso.org.dod.internet.mgmt.mib-2.
ospf.ospfTrap.ospfTrapControl.ospfSetTrap
```

This object defaults initially to the octet string {'\0x0','0x0','0x0','0x0'} (or the hex value 00), which disables all trap events. NVRAM stores the value of this object.

SNMP Trap profile settings

The OSPF parameter, in the SNMP Trap profile, enables OSPF traps. Verify that OSPF is active (OSPF=Yes) in the SNMP trap profile, as it is in the following example:

```
90-801 trap-profile

   Name=trap-profile
   Alarm=No
   Port=No
   Security=No
   OSPF=Yes
   Comm=
   Dest=0.0.0.0
   Enable traps...
```

Note: With the Yes setting, the MAX unit generates traps that have been enabled in Ethernet > SNMP Traps > *any profile* > Enable Traps. When you set OSPF to No, the MAX unit does not generate any OSPF traps regardless of any individual OSPF trap settings in Enable Traps.

Mod Config settings

The MAX # ASE LSA parameter, in the Mod Config profile, specifies the number of Link-State Advertisements (LSAs) the MAX unit stores before going into a state of database overload. When the unit reaches a database overload, it does not accept new entries and discards self-originated entries. The default setting is 0, as in the following example:

```
90-900 Mod Config

   OSPF global options...
   >Enable ASBR=Yes
   MAX # ASE LSA=0
```

Enable Traps profile settings

Specify that the MAX unit generates up to 15 types of OPSF event-related traps. For example:

```
Enable traps...

   >OSPF If ConfigError=No
   OSPF If AuthFailure=No
   OSPF If RxBadPacket=No
   OSPF TxRetransmit=No
   OSPF Nbr StateChange=No
   OSPF VirtIf ConfigError=No
   OSPF VirtIf AuthFailure=No
   OSPF VirtIf StateChange=No
   OSPF VirtIf RxBadPacket=No
   OSPF VirtIf TxRetransmit=No
   OSPF VirtNbr StateChnge=No
   OSPF OriginateLsa=No
   OSPF MaxAgeLsa=No
   OSPF LsdbOverflow=No
   OSPF LsdbApprchngOvrflw=No
```

Keep in mind that the OSPF parameter, in the SNMP Traps profile, must be set to Yes if unit is to generate traps that have been enabled the Enable traps profile. If you set OSPF to No, the MAX unit does not generate any OSPF traps regardless of any individual OSPF trap settings in the Enable Traps profile.

Administering virtual interfaces

Use the OSPF Traps parameters summarized in Table 9-3 to monitor activity between the MAX unit's virtual interfaces and routers.

Table 9-3. Virtual interface-related OSPF traps

Trap	Description
OSPF VirtIf AuthFailure	Specifies whether the MAX unit generates an OSPF VirtIf AuthFailure trap when the unit receives a packet on a virtual interface from a router whose authentication key or authentication type conflicts with the MAX unit's authentication key or authentication type.
OSPF VirtIf ConfigError	Specifies whether the MAX unit generates an OSPF VirtIf ConfigError trap when the unit receives a packet on a virtual interface from a router whose configuration parameters conflict with the MAX unit's configuration parameters.

Table 9-3. Virtual interface-related OSPF traps (continued)

Trap	Description
OSPF VirtIf StateChange	Specifies whether the MAX unit generates an OSPF VirtIf StateChange trap when the unit detects a change in the state of an OSPF virtual interface.
OSPF VirtIf RxBadPacket	Specifies whether the MAX unit generates an OSPF VirtIf RxBadPacket trap when the unit receives, on a virtual interface, an OSPF packet that cannot be parsed.
OSPF VirtIf TxRetransmit	Specifies whether the MAX unit generates an OSPF VirtIf TxRetransmit trap when the unit retransmits an OSPF packet on a virtual interface.
OSPF VirtNbr StateChnge	Specifies whether the MAX unit generates an OSPF Virt-Nbr StateChnge trap when there has been a change in the state of an OSPF virtual neighbor.

Administering nonvirtual interfaces

Use the OSPF Trap parameters summarized in Table 9-4 to administer the MAX unit's nonvirtual interfaces.

Table 9-4. Nonvirtual interface-related OSPF traps

Parameter	Description
OSPF If AuthFailure	Sends the OSPF If AuthFailure trap when the MAX unit receives a packet on a nonvirtual interface from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type.
OSPF If ConfigError	Sends the OSPF If ConfigError trap when a nonvirtual interface receives a packet from a router whose configuration parameters conflicts with this router's configuration parameters.
OSPF If RxBadPacket	Sends the OSPF If RxBadPacket trap when the MAX unit receives an OSPF packet on a nonvirtual interface that cannot be parsed.
OSPF If StateChange	Sends the OSPF If StateChange trap when there has been a change in the state of a nonvirtual OSPF interface.
OSPF Nbr StateChange	Sends the OSPF Nbr StateChange trap when there has been a change in the state of a nonvirtual OSPF neighbor.
OSPF TxRetrans	Sends the OSPF TxRetransmit trap when the MAX unit retransmits an OSPF packet on a nonvirtual interface.

Administering Link-State Advertisements

Use the OSPF Traps parameters summarized in Table 9-5 to monitor Link-State Advertisement LSA activity.

Table 9-5. LSA-related OSPF Traps parameters

Parameter	Description
OSPF OriginateLsa	Specifies whether the MAX unit generates a trap that indicates the number of new LSAs that have been originated.
OSPF LsdbApprchngOvrflw	Specifies whether or not the MAX unit generates the OSPF LsdbApprchngOvrflw trap when the number of LSAs in the router's link-state database has exceeded ninety percent of `ospfExtLsdbLimit`.
OSPF LsdbOverflow	Specifies whether or not the MAX unit generates the OSPF LsdbOverflow trap when the number of LSAs in the router's link-state database has exceeded `ospfExtLsdbLimit`. You specify the number of LSAs the MAX unit stores before going into a state of database overload by using the MAX # ASE LSA parameter in the Mod Config profile.
OSPF MaxAgeLsa	Specifies whether or not the MAX unit generates the OSPF MaxAgeLsa trap when the age of one of the LSAs in the router's link-state database reaches the MaxAge value.

Matching an OSPF trap to an SNMP trap ID in RFC 1850

MAX units support OSPF traps defined in RFC 1850 (rfc1850.mib), which replaces RFC 1253 (rfc1253.mib). RFC 1850 defines MIB object `ospfSetTrap`, for enabling trap events, as follows: `iso.org.dod.internet.mgmt.mib-2.` `ospf.ospfTrap.ospfTrapControl.ospfSetTrap`

This object defaults initially to the octet string `{'\0x0','0x0','0x0','0x0'}` (or the hex value 00), which disables all trap events. NVRAM stores the value of this object.

The Enable Traps profile includes the following OSPF traps:

OSPF trap	SNMP Trap ID in RFC 1850
OSPF If ConfigError	ospfTraps 4
OSPF If AuthFailure	ospfTraps 6
OSPF If StateChange	ospfTraps 16
OSPF If RxBadPacket	ospfTraps 8
OSPF TxRetransmit	ospfTraps 10
OSPF Nbr StateChange	ospfTraps 2

OSPF trap *(continued)*	SNMP Trap ID in RFC 1850
OSPF VirtIf ConfigError	ospfTraps 5
OSPF VirtIf AuthFailure	ospfTraps 7
OSPF VirtIf StateChange	ospfTraps 11
OSPF VirtIf RxBadPacket	ospfTraps 9
OSPF VirtIf TxRetransmit	ospfTraps 11
OSPF VirtNbr StateChnge	ospfTraps 3
OSPF OriginateLsa	ospfTraps 12
OSPF MaxAgeLsa	ospfTraps 13
OSPF LsdbOverflow	ospfTraps 14
OSPF LsdbApprchngOvrflw	ospfTraps 15

Download the most recent version of these RFCs by logging in as `anonymous` to `ftp.ds.internic.net`. (no password is required).

Alarm/Error and Security events

The MAX unit generates traps that relate to alarm (error) and security events. Events are not logged on a per-VRouter basis. If you use VRouters, the servers and clients you specify in the SNMP Options and SNMP Traps profiles must be accessible to the main VRouter.

Alarm/Error 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 been either created or invalidated, or has toggled between the active and inactive states.
eventTableOverwrite (ascend trap-type 16)	Detects 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.

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 Lucent-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.

Understanding Syslog messages

A

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

Once you have verified that Syslog is enabled on the MAX unit, use syslog messages to understand the performance of the unit or to gather information tunneling information that is included in the End-of-Call Syslog message. When a call comes to an end, use the disconnect and progress codes to understand why a call may have disconnected unexpectedly and at what stage the call disconnected.

Refer to the UNIX man pages about logger(1), syslog(3), syslog.conf(5), and syslogd(8) for details of the syslog daemon.

Note: Stacked MAX units communicate with other members of the stack by using a directed-broadcast Ethernet packet on the specified UDP port. Because directed-broadcast packets are unlikely to cross a router, and because of the high traffic demands created by a multilink call that spans MAX units, all members of a stack must reside on the same physical LAN. The Syslog function requires UDP port 514.

Verifying Syslog support

Verify that a MAX unit is configured to report events to a syslog host on a local IP network. The MAX unit sends Syslog reports through the unit's Ethernet interface. Verify three parameter settings in the Mod Config menu's Log profile. Table A-1 summarizes the settings to verify and assure that the MAX supports Syslog.

Table A-1. Summary of Syslog settings

Parameter	Description
Log Host	Specifies the IP address of the Syslog host-a UNIX station to which the MAX sends system logs. This parameter applies only when `Syslog=Yes`. Verify that the MAX unit's configuration does not specify a Syslog host that can only be reached by a dial-up connection. This can cause the MAX to redial the log host for every logged action, including hang ups.
Log Facility	Specifies how the Syslog host sorts system logs. The Syslog host is the station to which the MAX sends system logs. All system logs using the same setting are grouped together in the host's file system. That is, all system logs using the Local0 facility are grouped together, all system logs using the Local1 facility are grouped together, and so on. This parameter applies only when `Syslog=Yes`.
Syslog	Specifies whether or not the MAX sends warning, notice, and Call Detail Reporting (CDR) records from the system logs to the Syslog host.

Understanding Message Log status window

The Message Log status window provides a log of up to 32 of the most recent system events since you last reset the MAX. As additional events occur, the earliest event information is overwritten. Maintain a permanent log of MAX system events and send CDR reports to a host that can record and process them.

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

Each message log displays up to 32 of the most recent system events the MAX has recorded. When you select the Message Log option, the most recent message appears.

The message logs update dynamically. Press the Up-Arrow key to display the previous entry. Press the Down Arrow key to display the next entry.

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

Use the arrow key to scroll up (previous messages) or down (later ones). 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` means an active call disconnected normally.

  `LAN session up` means that an incoming connection has been established.

  `No Connection` means 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.

Understanding Level 4 and Level 6 messages

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

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

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

The line represented by text-2 specifies the system name and IP address or MAC address of the remote end of a session for the LAN Session Up and LAN Session Down messages in the line represented by text-1. Table A-2 describes the fields of the in the Level 4 and Level syslog messages.

Table A-2. Level 4 and Level 6 syslog messages

Field	Description
`slot-n`	The module's slot number.
`port-n`	The serial port.
`channel-n`	The channel.
`text-1`	Line 3 of the Message Log (System) display.
`text-2`	Line 4 of the Message Log (System) display which specifies the system name and IP address or MAC address of the remote end of a session for the LAN Session Up and LAN Session Down messages in the line represented by text-1

Understanding Level 5 messages

The data for Level 5 (notice) Syslog messages is derived from the Call Detail Reporting (CDR) display, lines 3 and 4. The CDR database provides information about each call, including date, time, duration, called number, calling number, call direction, service type, and associated inverse multiplexing session and port. Because the network carrier charges for bandwidth on an as-used basis, and bills each connection in an inverse-multiplexed call as a separate charge, use CDR to understand and manage bandwidth usage and the cost of each inverse-multiplexed session. Because the date, type, and name of syslog messages are added by the Syslog host, the MAX does not include that data in its message format. Here are three examples of Syslog entries, including the entries sent by the Syslog host:

```
Feb 24 11:15:02 irmasmax ASCEND: slot 0 port 0, line 1, channel 1, \
No Connection

Feb 24 10:16:00 irmasmax ASCEND: slot 4 port 1, Call Terminated

Feb 24 10:16:55 irmasmax ASCEND: slot 4 port 1, Outgoing Call, 123
```

In the preceding example, the Syslog displays three messages regarding a unit named `irmasmax.` The backslash (\) indicates that the first log entry continues to the following line.

Level 5 messages are presented in the following format:

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

Table A-3 describes the output of Level 5 Syslog messages.

Table A-3. Level 5 Syslog messages

Field	Description
call-event-ID	Specifies the event ID in the CDR display.
event-description	Describes the Call Detail Reporting (CDR) event.
slot N-port-N	Indicates the (Ascend Inverse Multiplexing) AIM port, which is suppressed when it is not applicable or is unknown.
data-svcK	Indicates the data service in use.
phone-N	Indicates the phone number.

Gathering tunneling information

In an End-Of-Call Syslog message, the tunneling clause specified by `Tunn` provides tunnel information for Ascend Tunneling Management Protocol (ATMP), Layer2 Tunneling Protocol (L2TP), and Point-to-Point Tunneling Protocol (PPTP) calls. The message can include a combination of the following three items of information:

- Client endpoint
- Server endpoint
- Group ID

All tunneling protocols currently support the client and server endpoints, but only ATMP supports the group ID. For tunnel protocols other than TCP-Clear, the Tunn clause now has the following form:

```
Tunn=(#protocol# s=#server# c=#client# g=#groupID#)
```

The server, client and groupID values have meanings based on the different conditions outlined here:

Protocol	Mode	Type	s=#server#	c=#client#	g=#groupID#
ATMP	Foreign Agent	Gateway	Home Agent address	N/A**	Home Network
	Foreign Agent	Router	Home Agent address	N/A**	N/A**
	Home Agent	Gateway	N/A**	Foreign Agent address	Home Network
	Home Agent	Router	N/A**	Foreign Agent address	N/A**
	Foreign Agent + Home Agent	Gateway	Home Agent address *	N/A**	Home Network
	Foreign Agent + Home Agent	Router	Home Agent address *	N/A**	N/A
PPTP	PAC	N/A**	PNS address	N/A**	N/A**
L2TP	LAC	N/A**	LNS address	N/A**	N/A**
	LNS	N/A**	N/A**	LAC address	N/A**

* The address matches the local IP address of the unit, because it is acting as both the Foreign Agent and the Home Agent for the connection. The client and server endpoint items can be IP addresses or domain names.

** Items that are N/A do not appear in the message.

For TCP-Clear connections, the string s= appears in front of the server IP address in the Tunn clause. Following is a sample End-Of-Call message for TCP-Clear calls:

```
ASCEND: shelf 1 slot 2 port 1, LAN session info: Conn=(jimtest
1110965064->63230 ? 33600/33600 40/21) Auth=(320 0/0 85/0) Sess=(0
0/0 85/0) Chan=(1 1 1 1) Modem=(1 2 1) Tunn=(TCP s=204.253.164.11)
[MBID 1]
```

Call ID values

Syslog messages can include call *XX*. The call ID is the session ID of the call. Call ID is the same value that is displayed when you enter the Userstat command. SNMP and RADIUS accounting both refer to Call ID. The call ID is the same as the AN record for the same call, with one difference. On the MAX, the call ID has a range of 1 to 65,535.

ATMP-related disconnect codes

If an Ascend Tunneling Management Protocol (ATMP) client disconnects because of an ATMP error, ATMP disconnect codes can help you diagnose the exact cause of the problem.

Each code can appear in a Syslog record or as the value of Ascend-Disconnect-Cause (195) in a RADIUS accounting record.

The ATMP-related disconnect codes are as follows:

Number	Explanation
700	Authentication of the Foreign Agent failed.
701	Tunneling is not enabled on the Home Agent.
702	The system is out of resources because too many tunnels have been established.
703	One of the fields in the TUNNEL message contained an invalid value.
704	The tunnel number in the GRE packet is invalid or does not exist. This error usually indicates that one side was reset.
705	The peer agent did not respond.
706	The Connection profile for the home network in gateway mode is not active.
707	A DNS lookup of the Home Agent could not be resolved to an IP address.
708	This code denotes a general error, and has been superseded by codes 709 through 712. Code 708 appears only if you connect to a unit running software issued before the addition of codes 709 through 712.
709	The Home Agent is not in gateway mode.
710	The Home Agent failed to set up a route.
711	The Foreign Agent detected an idle tunnel and cleared it.
712	The Home Agent detected an idle tunnel and cleared it.

Understanding disconnect codes and progress codes

When a call disconnects, the MAX can send a message to the Syslog host that indicates why the call disconnected and how far the call had progressed before it disconnected. The Syslog displays the message in the following format:

```
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	Should not be applied to any completed call, although the MAX unit records Disconnect Code 1 in accounting checkpoint records. For details on checkpoint records, see the *TAOS RADIUS Guide and Reference*. In any other case, if the MAX unit displays a Disconnect code 1, contact technical support for further information.
2	Specifies an unknown disconnect, and is the default value that the MAX unit displays for disconnects that have not been explicitly defined.
3	Call disconnected.
4	CLID authentication failed.
5	RADIUS timeout during authentication.
6	Successful authentication. MAX unit is configured to call the user back.
7	Pre-T310 Send Disc timer triggered.
9	No modem is available to accept call.
10	Modem never detected Data Carrier Detect (DCD).
11	Modem detected DCD, but modem carrier was lost.
12	MAX failed to successfully detect modem result codes.
13	MAX failed to open a modem for outgoing call.
14	MAX failed to open a modem for outgoing call while `ModemDiag` diagnostic command is enabled.
15	MAX unit failed to receive an OK from the modem.
16	MAX unit modem is stuck in the CSMX message queue
17	MAX unit detected that the modem's data port failed.
18	MAX disconnected connection to modem after detecting a communication problem with modem.
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.

Disconnect code	Description *(continued)*
32	Establishment of rlogin session failed because of bad options.
33	MAX lacks resources to process terminal-server request.
35	MP+ session cleared because no null MP packets received. A MAX sends (and should receive) null MP packets throughout an MP+ session.
40	LCP timed out waiting for a response.
41	LCP negotiations failed, usually because user is configured to send passwords via PAP, and MAX is configured to only accept passwords via CHAP (or vice versa).
42	PAP authentication failed.
43	CHAP authentication failed.
44	Authentication failed from remote server.
45	MAX received Terminate Request packet while LCP was in open state.
46	MAX received Close Request from upper layer, indicating graceful LCP closure.
47	MAX cleared call because no PPP Network Core Protocols (NCPs) were successfully negotiated. Typically, there is no agreement on the type of routing or bridging that is supported for the session.
48	Disconnected MP session. The MAX accepted an added channel, but cannot determine the call to which to add the new channel.
49	Disconnected MP call because no more channels can be added.
50	Telnet or raw TCP session tables full.
51	MAX has exhausted Telnet or raw TCP resources.
52	For Telnet or raw TCP session, IP address is invalid.
53	For Telnet or raw TCP session, MAX cannot resolve hostname.
54	For Telnet or raw TCP session, MAX received bad or missing port number.
60	For Telnet or raw TCP session, host reset.
61	For Telnet or raw TCP session, connection was refused.
62	For Telnet or raw TCP session, connection timed out.
63	For Telnet or raw TCP session, connection closed by foreign host.
64	For Telnet or raw TCP session, network unreachable.
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.
90	For Telnet or raw TCP session, no port is available.
100	Session timed out.
101	Invalid user.
102	Callback enabled.

Disconnect code	Description *(continued)*
103	MAX disconnected call because of a validation failure on outgoing call-back call.
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	MAX disconnected V110 call because of it a timeout condition was triggered.
170	Timeout waiting to authenticate far end.
180	User disconnected by executing Do Hangup from VT100 interface.
171	MAX unit disconnected call when the PPP interface was released.
180	MAX unit disconnected call when user invoked the MAX unit DO Hangup command.
181	Call cleared by MAX.
185	Signal lost from far end, typically because the far end modem was turned off.
190	Resource has been quiesced.
195	Maximum duration time reached for call.
201	MAX has low memory.
210	MAX modem card stops working while it has calls outstanding.
220	MAX requires CBCP, but client does not support it.
230	MAX deleted Vrouter.
240	MAX disconnected call on the basis of LQM measurements.
241	MAX cleared backup call.
250	IP FAX call cleared normally.
251	IP FAX call cleared because of low available memory.
252	MAX detected an error for an incoming IP FAX call.
253	MAX detected an error for an outgoing IP FAX call.
254	MAX detected no available modem to support an IP FAX call.
255	MAX detected problem opening IP FAX session.
256	MAX detected a problem when performing a TCP function during an IP FAX call.
257	IP FAX session cleared abnormally.
258	MAX detected problem when parsing telephone number for IP FAX call.
260	MAX detected problem when decoding IP FAX variables.

Disconnect code	Description *(continued)*
261	MAX detected problem when decoding IP FAX variables.
262	MAX has no configured IP FAX server.
300	MAX detects X.25 error.
350	MAX unit detected that an MP Master Card has failed.
370	MAX unit disconnected call because DNIS was blocked.
400	MAX unit disconnected call because callback dialout failed.
420	MAX unit disconnected call because it could not find a private Route table.
425	MAX unit disconnected call because it could not find a filter profile.
450	Bidirectional authentication failed.

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.
7	Call still connecting.
10	MAX has detected and accepted call.
11	Dial Service blocked.
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 *(continued)*
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 is in Opened state.
92	V.110 call is in Carrier state.
93	V.110 call is in Reset state.
94	V.110 call is 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.

Code combinations and their possible meanings

A MAX unit applies a Disconnect code and Progress code to each call. Combinations of Disconnect and Progress codes might indicate similar causes. Following is a partial list of code combinations and their possible causes:

Disconnect code	Progress code	Possible cause
4	101	Before the call was answered, the call failed to provide a CLID phone number that is configured on the MAX unit.
10	31	During modem training, the MAX unit waited for the Data Carrier Detect) DCD signal from the user's modem, but never detected the signal. Typically, the modems had marginal line quality. Because the MAX unit's modem has a digital connection to its local CO, the poor line quality is between the user's modem and its local CO. This code combination could also be caused by a user testing the availability of the MAX unit by dialing into the MAX unit, then hanging up during modem training. Also, there might be an incompatibility between the modems. This causes of this combination are similar to calls with a Disconnect code 185 and a Progress code 31, but this code combination indicates that the MAX unit's modem detected a training failure before the phone line disconnected.
11	30	During modem training, the MAX unit's modem detected DCD but lost the modem carrier signal. Typically, the modems had marginal line quality. Because the MAX unit's modem has a digital connection to its local CO, the poor line quality is between the user's modem and its local CO. Also, there might be an incompatibility between the modems.
11	40	During an active terminal-server session, the MAX unit lost the carrier signal from the user's modem. The call could have ended normally, or the modems might have had marginal line quality. Because the MAX unit's modem has a digital connection to its local CO, the poor line quality is between the user's modem and its local CO. Also, there might be an incompatibility between the modems.
11	43	During an active raw TCP session, the MAX unit's modem lost the carrier signal which a modem connection requires. The call could have ended normally, or the modems had marginal line quality. Because the MAX unit's modem has a digital connection to its local CO, the poor line quality is between the user's modem and its local CO. Also, there might be an incompatibility between the modems.

Disconnect code	Progress code	Possible cause *(continued)*
11	60	While the session was active, the MAX unit's modem lost the carrier signal which a modem connection requires. Some client applications do not close PPP connections gracefully, so this combination might be a normal end to a customer call. Also, the modems might have had marginal line quality. Because the MAX unit's modem has a digital connection to its local CO, the poor line quality is between the user's modem and its local CO. Also, there might be an incompatibility between the modems.
11	65	Before the session was active (during PPP negotiation), the MAX unit's modem lost the carrier signal which a modem connection requires. Typically, the modems had marginal line quality. Because the MAX unit's modem has a digital connection to its local CO, the poor line quality is between the user's modem and its local CO. Also, there might be an incompatibility between the modems.
21	40	During a terminal-server session, the MAX unit disconnected the call because its terminal server timed out waiting for response from the dialin user.
24	43	During an active raw TCP session, the MAX unit's received a *forced disconnect* from the dialin client's terminal-server application. Typically, the call was a successful session.
25	40	During an active terminal-server session, the user failed to login successfully within the maximum number of attempts.
27	40	During an active terminal-server session, the user pressed `<ctrl>`, then the Enter key, manually ending the terminal-server session and connection. Typically, the call was a successful session.
35	60	During an active session, the MAX unit stopped receiving the MP+ management packets that indicate the line is active but idle. Typically, this code combination indicates that there was a problem with the MP+ connection.
40	75	During LCP negotiation, the MAX unit disconnected the call because the dialin client stopped sending LCP configuration frames. Some PPP applications require a user to press a key to continue LCP negotiation. If the user does not press a key to continue, the negotiation stops.
42	65	The dialin client and the MAX unit successfully negotiated LCP. The dialin client's PPP application (or the user) supplied an incorrect user name or password during Password Authentication Protocol (PAP) authentication.
42	200	Dialin client connected successfully to MAX unit, but the authentication server was not available to process the request from the MAX unit. The authentication server might be disabled or turned off.

Disconnect code	Progress code	Possible cause *(continued)*
43	65	The MAX unit and the dialin client had negotiated to use CHAP authentication. The MAX unit disconnected the call when the user (or the dialin client's PPP application) supplied an incorrect username or password.
45	60	While the session was active, the MAX unit received a *Terminate Request* from the user's PPP application. Typically, the call was a successful session., and the user has disconnected the session from the dialin client's PPP application.
45	63	After successfully completing LCP negotiation and authentication, the MAX unit received a Terminate Request message from the dialin client's PPP application. If this is an IP-routed connection, there might be an IP address assignment misconfiguration. If you configure the MAX unit to supply an IP address and the dialin client does not accept the assignment, the connection clears.
45	65	Before the initial connection was active (during PPP negotiation), the MAX unit received a *Terminate Request* from the user's PPP application. Typically, the user has manually disconnected the call from the dialin client before the PPP negotiation had completed between the dialin client and the MAX unit.
45	66	After successfully negotiating PPP Compression Control Protocol (CCP), the MAX unit received a *Terminate Request* from the user's PPP application. Typically, the user has disconnected the session from the dialin client's PPP application.
46	60	During an active PPP session, the MAX unit received a *Close Request* from the dialin client. This is also called a graceful disconnect. Typically, the call was a successful session.
47	60	Both the MAX unit and the dialin client successfully negotiated PPP, but no Network Control Protocols (NCPs) (IP routing, IPX routing, AppleTalk routing, or bridging), were successfully negotiated. Both the MAX unit and the dialin client must be configured to successfully negotiate at least one NCP.
47	63	The MAX unit successfully completed LCP negotiation and authentication. The configuration of the user's PPP application did not match the MAX unit's PPP configuration. The two devices could not successfully negotiate any Network Control Protocols (NCPs) (IP routing, IPX routing, AppleTalk routing, or bridging). Both the MAX unit and the dialin client must be configured to successfully negotiate at least one NCP.
100	60	While the session was active, the MAX unit disconnected the call because of a configured session timeout parameter. Typically, the call was a successful session.
100	65	During PPP negotiation, the MAX unit disconnected the call because of a configured session timeout parameter.

Disconnect code	Progress code	Possible cause *(continued)*
101	67	The MAX unit successfully negotiated LCP and authentication with the dialin client. The MAX unit disconnected the call during IP routing (IPCP) negotiation, which typically occurs because the computer's IP address (configured on the MAX unit) does not match the configuration of the IP address of the dialin client or because the MAX unit has no available IP address from its pool to assign to dialin client.
106	60	During an active session, the MAX unit disconnected the call because of a Multilink PPP (MP) session timeout.
120	30	The MAX unit received the call and allocated a modem to answer it. The dialin client requested to use a protocol that is either disabled or unsupported on the MAX unit or its modem.
181	10	The MAX unit received and answered the incoming call. Because of inferior line quality or modem incompatibilities, the MAX unit disconnected the call. Typically, the modems had marginal line quality. Because the MAX unit's modem has a digital connection to its local CO, the poor line quality is between the user's modem and its local CO.
185	10	Shortly after answering the call, the MAX unit could not detect any signal from the computer's modem. Typically, the modems had marginal line quality. Because the MAX unit's modem has a digital connection to its local CO, the poor line quality is between the user's modem and its local CO. Also, there might be an incompatibility between the modems.
185	30	The MAX unit received the user's modem call and allocated a MAX modem to answer the call. Before completing modem negotiation, the MAX unit could not detect any signal from the user's computer modem. Typically, the modems had marginal line quality. Because the MAX unit's modem has a digital connection to its local CO, the poor line quality is between the user's modem and its local CO. Also, there might be an incompatibility between the modems.
185	31	Before the modems had completed training, the connection disconnected. The MAX unit modem was waiting for a Data Carrier Detect (DCD) signal from the user's modem. Typically, the modems had marginal line quality. Because the MAX unit's modem has a digital connection to its local CO, the poor line quality is between the user's modem and its local CO. Also, there might be an incompatibility between the modems. This causes of this combination are similar to calls with a Disconnect code 10 and a Progress code 31. Rather than the MAX unit's modem detecting a training failure, this code combination indicates that the phone line disconnected before (presumably) the MAX unit's modem could detect the training failure.

Disconnect code	Progress code	Possible cause *(continued)*
185	40	Typically called an *ungraceful* disconnect. During an active terminal-server session, the user probably turned off the computer or manually disconnected the WAN line from the computer's modem. Typically, the call was a successful session. Also, there might be an incompatibility between the modems.
185	43	Typically called an *ungraceful* disconnect. During an active raw TCP session, the user probably turned off the computer or manually disconnected the WAN line from the computer's modem. Typically, the call was a successful session. Also, there might be an incompatibility between the modems.
185	60	Typically called an *ungraceful* disconnect. Instead of disconnecting the call from within the PPP application, the user probably turned off the computer or manually disconnected the WAN line from the computer. Typically, the call was a successful session. Also, there might be an incompatibility between the modems.
185	63	Typically caused when the MAX unit did not have an available IP address to assign to the dialin client.
185	65	Before the initial connection was active (during PPP negotiation), the MAX unit received an ungraceful disconnect from the user's computer. Typically, the user probably turned off the computer or manually disconnected the WAN line from the computer before the PPP negotiation had completed between the user's computer and the MAX unit. Also, there might be an incompatibility between the modems.
185	75	After having sent an LCP request (during LCP negotiation), the MAX unit could not detect any signal from the user's computer's modem. Typically, the modems had marginal line quality. Because the MAX unit's modem has a digital connection to its local CO, the poor line quality is between the user's modem and its local CO. Also, there might be an incompatibility between the modems.
185	77	The MAX unit has successfully completed LCP negotiation. Before beginning the authentication phase of PPP negotiation, the MAX unit could not detect any signal from the user's computer's modem. Typically, the modems had marginal line quality. Because the MAX unit's modem has a digital connection to its local CO, the poor line quality is between the user's modem and its local CO. Also, there might be an incompatibility between the modems.
185	203	The MAX unit could not detect any signal from the computer's modem during the authentication. Typically, the modems had marginal line quality. Because the MAX unit's modem has a digital connection to its local CO, the poor line quality is between the user's modem and its local CO. Also, there might be an incompatibility between the modems.
210	60	During an active session, the MAX unit modem slot card stopped working.

Diagnostic Parameters and Commands

B

Note: Every attempt has been made to confirm that this appendix correctly describes the functionality and output of the MAX diagnostic commands. But while diagnostic mode can be a valuable troubleshooting tool for anyone, its primary focus is on the requirements of Lucent Technologies development engineers. Therefore, Lucent Technologies does not guarantee the completeness of the list of commands or of the cataloging of functionality from release to release.

Under most circumstances, diagnostic commands are not required for correct operation of a MAX unit, and in some circumstances they might produce undesirable results. Please use the following information with caution. Contact Lucent Technologies Technical Support with any questions or concerns.

This appendix provides all available information about the MAX unit's diagnostic and commands. The information is organized for quick reference, and does not include tutorials. All commands are listed alphabetically. To use these commands, you must have sufficient permissions in the active Security profile.

Using diagnostics-related VT100 commands

A MAX unit's VT100 interface provides diagnostic commands you can use to troubleshoot the unit. Several are administrator-only commands. The interface also includes commands related to BRI/LT, E1, Host/Dual, modem and T1 performance.

Using administrator-only commands

To be allowed access to diagnostic mode, you must set the Field Service privilege to Yes in the active Security profile.

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:

>?

To display a complete listing, append `ascend` to the question mark:

>? 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 Diag Modemdrv (ModemDrvState in previous TAOS revisions), ModemDiag, and MDialout (if modem dial-out is supported on your MAX unit) 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.

MAX units provide system diagnostic commands 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 command, or transfers the profiles to another MAX unit. Because the Save Cfg command does not save passwords, the Restore Cfg command does not restore them.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 unit.

   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.

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

To save your configuration, proceed as follows:

1   Verify that the Download permission is enabled in the active Security profile.

2   Verify that the Term Rate parameter in the System profile is set to 9600.

3   Verify that your terminal-emulation program has a disk-capture feature and an autotype feature, and that its data rate is set to 9600 bps or lower.

4   Connect the backup device to the MAX unit's control port.

5   Turn on the autotype function on your emulator, and start the save process by pressing any key on the emulator.

6   Highlight Save Cfg and press Enter.

7   Verify that configuration data is being echoed to the terminal-emulation screen and that the captured data is being written to a file on your disk.

   The save process is complete when the message `Download complete--type any key to return to menu` appears on your emulator's display. The backup file is an ASCII file.

8   Turn off the autotype feature.

Use MIF

The Use MIF command opens the Machine Interface Format (MIF) interface. Enter `Use MIF` to switch to the MIF interface either on a local workstation or during a Telnet session.

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

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

Sys Reset

The Sys Reset command restarts the MAX unit and clears all calls without disconnecting the unit from its power source. The unit logs out all users and returns user security to its default state. In addition, the unit performs power-on self tests (POSTs) when it restarts. The POSTs are diagnostic tests. A system reset of a MAX unit 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 unit 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 screen 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 can 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 steadily illuminated, the MAX unit checks system memory, configuration, installed modules, and T1 connections. If the unit fails any of these tests, the Fault LED remains on 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 unit.

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 unit retrieves configuration from RADIUS at system startup or by use of this command.

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

When you select the Upd Rem Cfg command from the Sys Diag menu RADIUS adds the routes as follows:

- RADIUS looks for entries having the format route-*unit_name*-1, where *unit_name* is the system name.

- If at least one entry exists, RADIUS loads all existing entries having the format route-unit_*name*-*num* to initialize the IP routing table.
  The variable *num* is a number in a sequential series, starting with 1.

- The MAX unit queries route-*unit_name*-1, then route-*unit_name*-2, and so on, until it receives an authentication reject from RADIUS.

- Once the host-specific routes are loaded, RADIUS loads the global configuration entries; these configurations have the form route-*num*.

- The MAX unit queries route-1, then route-2, and so on, until it receives an authentication reject from RADIUS.

The routes remain in effect until the next restart or until overwritten by dynamic updates or routes specified in Connection profiles.

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

- The MAX unit 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.

Note: In some cases, you might wish to update the MAX unit's routing tables when connecting to a user whose profile includes Service-Type=Framed. In this case, set the Framed-Route attribute in an incoming user profile to specify the user's IP address and subnet mask in the host_ipaddr and subnet_mask arguments. The route you specify in this manner exists only during the time the call is on-line. When you enter a nonzero router address for router_ipaddr and it is different from the caller's address, the static route of a dial-in framed route persists even after the connection goes off-line.

Example: This example shows two RADIUS pseudo-user profiles defining global static IP routes:

```
route-1 Password=ascend Service-Type=Outbound

    Framed-Route=10.0.200.33/29 10.0.200.37 1 n lala-gw-out
    Framed-Route=10.0.200.50/29 10.0.200.37 1 n lala-gw-out
    Framed-Route=10.0.200.47/29 10.0.200.49 1 n nana-gw-out
    route-2 Password=ascend Service-Type=Outbound
    Framed-Route=11.0.200.33/29 11.0.200.37 1 n zzz-gw-out
    Framed-Route=12.0.200.47/29 11.0.200.49 1 n kk-gw-out
```

Using BRI/LT-related commands

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

```
BRI/LT
    Line Diag
        Line N...
            Line LoopBack
            Corrupt CRC
```

```
UnCorrupt CRC
Rq Corrupt CRC
UnRq Corrupt CRC
Clr NEBE
Clr FEBE
```

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

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

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

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

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

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

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

Line LoopBack

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

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

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

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

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

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

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

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

```
Line loopback terminated.
```

Corrupt CRC

The Corrupt CRC command causes the BRI-U interface to transmit inverted CRCs, until you cancel the command. When the command is issued, the Far-End Block Error counter should be viewed from the remote TA. The command is used to test the NEBE and FEBE counters, by simulating transmission errors with artificially corrupted CRCs.

Uncorrupt CRC

The Uncorrupt CRC command cancels a previous Corrupt CRC command.

Rq Corrupt CRC

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

Rq Uncorrupt CRC

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

UnRq Corrupt CRC

The UnRq Corrupt CRC command requests NT1 to return to normal.

Clr NEBE

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

Clr FEBE

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

Using E1-related commands

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

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

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

Line LB1

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

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

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

Line LB2

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

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

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

Using Host/Dual (Host/6) Port-related commands

MAX 6000 and MAX 3000 units provide the following port diagnostic parameters, which appear in the Host/Dual (or Host/AIM6) > Port Diag menu:

```
Host/Dual
  Port N
    Port Diag
      Local LB
        DSR
        RI
        CD
        DLO
        PND
        ACR
        Inc Ch Count
        Dec Ch Count
         Rate
```

The Local LB command in the Host/Dual (or Host/AIM6) > Port *N* Menu > Port Diag menu tests the Ascend Multiplexing (AIM) port. To execute the command, select it and press Enter.

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

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

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

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

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

- RI toggles the host port Ring Indicate (RI) V.25 output signal between active and inactive.

- CD toggles the host port Carrier Detect (CD) output signal between active and inactive.

- DLO toggles the host port Data Line Occupied (DLO) RS-366 output signal between active and inactive.

- PND toggles the host port Present Next Digit (PND) RS-366 output signal between active and inactive.

- ACR toggles the host port Abandon Call and Retry (ACR) output signal between active and inactive.

- Inc Ch Count simulates an increase in the number of channels in a call by increasing the clock rate to the host.

- Dec Ch Count simulates a decrease in the number of channels in a call by decreasing the clock rate to the host.

• Rate toggles the data rate of the simulated channels between 56 Kbps and 64 Kbps.

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

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

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

Using Modem-related commands

The MAX provides the following modem diagnostic commands, which appear in the V.90 K 56 II Modem > Modem Config menu:

```
V.90 K56 II Modem
  Modem Config
    Module Name=
    Ans 1#=
    Ans 2#=
    Ans 3#=
    Ans 4#=
    ModemSlot=enable slot
    Modem #1=enable modem
    Modem #2=enable modem
    Modem #3=enable modem
    Modem #4=enable modem
    Modem #5=enable modem
    Modem #6=enable modem
    Modem #7=enable modem
    ...
    ...
    Modem #24=enable modem
```

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

Ans N(N=1-4)

Specifies a phone number to be used for call-routing purposes. In a Modem Config profile, the answer number indicates that calls received on that number should be routed to an available digital modem in any digital modem slot card.

Specify the phone number for each Ans N# parameter. Enter up to 24 characters, which may include a subaddress. You must limit your specification to these characters:
1234567890()[]!z-*#|

ModemSlot

Set the ModemSlot parameter to quiesce a digital-modem slot card, that is, disable a digital-modem slot card in the MAX unit without disrupting existing connections. Active calls are not torn down. When an active call is dropped, that modem is added to the disabled modem

list and is not available for use. If all modems are on the disabled list, incoming callers receive a busy signal until the modems have been restored for service. When you re-enable the quiesced modem slot card, a delay of up to 20 seconds can occur before the modems become available for service.

Specify one of the following values:

- Enable Slot—The default value. Enables any modems on the disabled list for the selected slot card, making them available for service.

- Dis Slot—All modems that are not active appear in a disabled modem list, indicating that they are not available for use.

- Dis Slot+Chan—All modems on the selected slot card are disabled, along with an equal number of B channels. The B channels appear on a disabled-channel map. The MAX unit polls all channels on the map with Out-Of-Service messages until the modems on the associated slot card return to service.

To quiesce all the available modems on a slot card:

1 Open the Mod Config submenu from the Modem profile and select ModemSlot.

2 Press Enter, select `dis slot` and disable (quiesce) the slot card. Or, to disable the slot card and the channel, press Enter again to select `dis slot+chan`.

For example,

```
V.90 K56 II Modem
  Mod Config
    ModemSlot=dis slot
    Modem #1=NA
    Modem #2=NA
    ..
    ..
    ..
```

3 Close the Modem profile.

Note: Booting the MAX unit restores the queisced slot to service.

Modem #N

Set the Modem #*N* (where N=1–8, 1–12, 1-16, 1-24, 1-30) parameter to quiesce a digital-modem, that is, to disable a digital modem without disrupting existing connections. Active calls are not torn down. If you specify a modem that is currently inactive, the modem is added to the disabled list. If the modem has a call active, it is not added to the disabled list until it drops the call. If all modems are on the disabled list, incoming callers receive a busy signal until the modems have been restored for service. When you reenable the quiesced modem, a delay of up to 20 seconds can occur before the modem becomes available for service.

Specify one of the following values:

- Enable Modem—The default value. Enables any modems that were on the disabled list, entering them on the enabled modem list and making them available for service.

- Dis Modem—Places the modem on the disabled modem list, indicating that it is not available for use. When the last active connection is dropped, the card becomes available for maintenance.

- Dis Modem+Chan—An arbitrary B channel is taken out of service along with the disabled modem. The B channel appears on a disabled-channel map, and the MAX polls all channels on the map with Out-Of-Service messages until the associated modem is reenabled.

To quiesce a digital modem:

1   Open the Mod Config submenu from the Modem profile and select the modem (Modem #*N*) you want to disable. (The modem ports on a slot card are numbered starting with #1 for the leftmost port on the card.)

2   Press Enter to select `dismodem` and disable (quiesce) the modem. Or, press Enter again to select `dis modem+chan` and to disable the modem and the channel.

    For example,

```
V.90 K56 II Modem
  Mod Config
    ModemSlot=enable slot
    Modem #1=dis modem
```

Using T1-related commands

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

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

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

Line LB1

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

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

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

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

Line LB2

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

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

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

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

Switch D Chan

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

Clr Err1

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

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

Clr Perf1

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

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

Clr Err2

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

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

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

Clr Perf2

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

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

Using diagnostics-related DO commands

Chapter 2, "DO Commands and Administrative Tasks" describes how to use DO commands to activate administrative permissions. Is also reacquaints you with the basics of using the DO commands and introduces you to using DO commands to test and troubleshoot a MAX unit. In addition to the commands discussed in "DO Commands and Administrative Tasks," a MAX unit provides diagnostics-related DO commands. Following are diagnostics-related DO 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:

```
>?
? -> List all monitor commands
briDisplay -> briDisplay <n> [l]
cat -> usage: cat [socket]/pathName
cleval -> cleval
clr-history -> Clear history log
dtunnel -> Dump all/specific ATMP tunnels
dumpcachestat ->  dump cache stats
ether-display -> ether-display <port #> <n>
fatal-history -> List history log
```

```
fBackupImage -> copy code image from low half of PCMCIA flash to
high
fcat -> cat configuration from flash
fclear -> clear configuration from flash
fImageCopy -> copy code image from internal flash to PCMCIA (or
vice versa)
fload -> load file from tftp host to flash FAT/FTL filesystem
format ->  prepare a flash card for use
frestore -> restore configuration from flash, usage: frestore
[filename]
fsave -> save configuration to flash, usage: fsave [filename]
fVersionInfo -> Show code version stored on internal or PCMCIA
flash
FWALLdblog -> Inquire/change firewall debug logging
FWALLversion -> Display firewall software version number
fZLen -> Show image size stored on internal or PCMCIA flash
help -> List all monitor commands
if-admin -> debug command for snmp interface table.
IPsecSADump -> Display all active Security Associations
IPsecSchemeDump -> Display all active Security Schemes
l2tp -> display L2TP statistics and information
l2tpsessions -> Dump all/specific L2TP session
ls -> usage: ls [socket][/pathName]
mkdir -> usage: mkdir [socket]/pathName
mv -> usage: mv [socket]/pathName socket/pathName
nslookup -> Perform DNS lookup
pppif -> usage: pppif -option [ params ]
priDisplay -> priDisplay <n>
quit -> Exit from monitor to menus
reset -> Reset unit
rm -> usage: rm [socket]/pathName
snmpAuthPass -> usage: snmpAuthPass <username> <password>
snmpPrivPass -> usage: snmpPrivPass <username> <password>
sntp -> Usage: SNTP [options]
t1CoreDisplay -> t1CoreDisplay <n>
tempdisplay -> Display ambient temperature readings
tloadcode -> load code from tftp host
trestore -> restore configuration from tftp host
tsave -> save configuration to tftp host
vrouter -> VROUTER dump
wanDisplay -> wanDisplay <n>
wanDSess -> wandsess <sess <n>> (display per session)
wanNext -> wanNext <n>
wanOpening -> wanOpening <n> (displays packets during
opening/negotiation)
x25dl -> usage: x25dl -option
```

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:

```
> 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.

Clocksource

Description: Displays the source of clocking for the MAX. Clock slips can cause connectivity problems, particularly for analog users. If you use the Net/T1 > Line Config > Line # > Clock Source parameter to move the clock source, use this diagnostic command to validate your changes.

Note: You need to reboot the MAX to enable any changes to the Clock Source parameter. Also, if more than one line has Clock Source set to Yes, remember that the clock source will be derived from the first line that syncs. If you want to ensure that a particular line is the source, make sure it has Clock Source set to Yes and that all other lines have Clock Source set to No.

Usage: Enter clocksource at the command prompt.

Example: In the following example, the clock source is taken from the first T1/PRI line, designated dsl 0. Dsl# indicates the maximum number of possible sources for the clock. The source can be on Net/T1 slot cards. This MAX has three T1/PRI lines configured, so there are three possible external sources for the clock. LstSel is further validation that the clock is being derived from Dsl#0. After Now, a 2 indicates that layer 2 is up for that line and is available as the clock source.

```
> clocksource
Clock source is dsl 0
Dsl#    012345678901234567890123456789012345678901234567890123456789
LstSel  a?????????????????????????????????????????????????????????
Now     222-----------------------------------------------
```

Clr-History

Description: Clears the fatal-error log.

Usage: Enter `clr-history` at the command prompt. To display the log before clearing it, enter the `fatal-history` command.

Example:

```
> 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
> clr-history
```

The log is now empty:

```
> fatal-history
>
```

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 Lucent Technologies Technical Support.

The CoreDump command is a particularly useful tool for the Lucent Technologies development engineering, and Technical Support occasionally requests its use to help troubleshoot specific issues.

Include the `now` option to instruct the MAX to dump its core immediately. 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 unit to reboot after its memory (core) has been dumped. Do not use the command unless specifically requested to do so by a Lucent Technologies 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:

```
> coredump enable 1.1.1.1
coredump over UDP is enabled locally only with server 1.1.1.1
> coredump disable 1.1.1.1
coredump over UDP is disabled locally only with server 1.1.1.1
> coredump
coredump over UDP is disabled locally only with server 1.1.1.1
> 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
```

Diag

Description: Indicates the whether the modules installed in the MAX unit are currently running diagnostics.

Usage: Enter diag at the MAX prompt.

Example:

```
> diag
 Listing all modules with diag ON:
 callback debug is ON
>
```

Diag ?

Description: Displays a set of commands that use a common prefix, diag.

Usage: Enter diag ? at the prompt.

Example:

```
> diag ?
 Listing all available diag modules:
addrpool                  ( Internet Protocol )
 atmp                     ( Ascend Tunnel Mgmt Protocol )
 bacp                     ( PPP Bandwidth Allocation Control )
 bacpcm                   ( PPP Bandwidth Allocation Control )
 brouter                  ( Operating System )
 callback                 ( Operating System )
 callrout                 ( Call Control )
 chanstat                 ( Call Control )
 dnissnmp                 ( SNMP )
 flash                    ( PCMCIA Driver )
 fr1490                   ( Frame Relay )
```

```
frdirect                 ( Frame Relay )
frdlcall                 ( Frame Relay )
frlinkstate              ( Frame Relay )
frlmi                    ( Frame Relay )
frstate                  ( Frame Relay )
igmp                     ( Internet Group Mgmt Protocol )
igmphb                   ( IGMP Multi-Routing )
iproute <0x1fff>         ( Route Table Manager )
ipsec                    ( IPSEC )
ipx                      ( IPX Protocol )
ipxr                     ( IPX Protocol )
ipxrip                   ( IPX Protocol )
ipxsap                   ( IPX Protocol )
l2tunnel                 ( L2 Tunnel )
lannail                  ( Frame Relay )
lanval                   ( Call Control )
modemdrv                 ( Modem Driver )
mp                       ( MP Protocol )
mpcm                     ( MP Protocol )
mppcm                    ( MPP Protocol )
mppstack                 ( MPP Protocol )
networki                 ( Call Control )
ppp                      ( Point to Point Protocol )
pppfsm                   ( Point to Point Protocol )
pppif                    ( Point to Point Protocol )
pptp                     ( PPTP Protocol )
pptpdata <0xff>          ( PPTP Protocol )
radacct                  ( Radius )
radif                    ( Radius )
rip <0x1ff>              ( RIP Protocol )
rlogin                   ( Rlogin Protocol )
routmgr                  ( Call Control )
sntp                     ( Simple Network Time Protocol )
stacking                 ( MPP Protocol )
telnet                   ( Telnet Protocol )
tunnel                   ( Tunnel Mgmt Protocol )
vrouter <0xffff>         ( Virtual Router )
wan                      ( WAN Driver )
```

Diag AddrPool

Description: Displays messages related to dynamic address pooling. The command is a toggle that alternately enables and disables the debug display.

Usage: Enter `diag addrpool` at the MAX prompt.

Example: Following are several examples of output displayed from `diag 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 unit 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 show 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
```

Diag Callback

Description: Displays messages related to the callback functionality of the MAX unit. 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 unit hangs up after receiving an incoming call that matches the specifications in the Connection profile. The unit then uses the Dial # value specified in the Connection profile to call back the device at the remote end of the link.

Use the Diag 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 diag callback at the command prompt.

Example: Following are several examples of output displayed by the Diag Callback command.

```
> diag callback
CALLBACK debug is now ON
```

The following message appears as the MAX unit prepares to call back the remote end:

```
CALLBACK: processing entry topeka
```

The MAX unit 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:

```
> callback
CALLBACK debug is now OFF
```

Diag IPXrip

Description: Displays incoming and outgoing IPX RIP traffic. The command is a toggle that alternately enables and disables the debug display.

Usage: Enter diag ipxrip at the command prompt.

Example:

```
> diag ipxrip
```

```
IPX-RIP state display is ON
```

The following message appears as the MAX unit sends an IPX RIP packet announcing its route:

```
IPXRIP: 10000a17 announced 0 routes on interface 1000:
```

Next, a remote unit has dialed the MAX unit and sent a RIP route:

```
IPXRIP: received response from ac1b0001:00c07b5e04c0 (1 nets).
```

The following message indicates that the MAX unit is delaying sending a RIP packet in order to prevent the interpacket arrival time from being closer than busy or 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:
```

Diag Modemdrv

Description: Displays communication to and from the modem driver on the MAX. This command also displays which buffers are allocated and which AT command strings are being used to establish modem connections.

Use the command to 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. 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 `diag modemdrv` at the command prompt.

Example: The following series of messages shows that a modem call comes into the MAX, unit and a modem call is cleared from the unit:

```
> diag modemdrv
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,
parseState[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
```

Diag Networki

Description: Displays call control information related to incoming analog modem call processing.

Usage: Enter diag networki at the command prompt.

Example:

>**diag networki**
```
 networki debug is ON
NETWORKI: NetworkStateChanged: RINGING, callid 61
** 1495904.76: CALL 61  RINGING      globDsl  5, channel  2
NETWORKI: cached callID 61, routeID 255
NETWORKI: answering incoming call for routeID 255
NETWORKI: clearSessionData
NETWORKI: call block b0a9bcf0, service 1, phone
NETWORKI: alertingRequest( 61, 255 )
NETWORKI: answerCallRequest( 61, 255 )
NETWORKI: NetworkStateChanged: CONNECTED, callid 61
** 1495906.38: CALL 61  CONNECTED    globDsl  5, channel  2
NETWORKI: call state connected, callid: 61
NETWORKI: checking for pending completeness
checkForSessionCompleteness: sessionIx=3115 routeID=255
calls still pending == 0
NETWORKI: completeTransaction, route 255
NETWORKI: First call completed.  Got base profile, service 1,
type 2
NETWORKI: activateChannelList for route 255
NETWORKI: clearSessionData
```

Diag 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 diag pppfsm at the command prompt.

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

```
> diag 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
```

Diag 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 Diag PPPIF in conjunction with PPPDump.

Usage: Enter `diag pppif` at the command prompt.

Example:

```
> diag 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 unit 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.

Diag 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 diag pptpdata at the command prompt.

Example: The first of the following messages indicates that the MAX unit received a positive acknowledgment from the NT server:

```
PPTPDATA-[1.1.1.1]: Received GRE ACK
```

Also, the MAX unit received data from the NT server that needs to be forwarded out the WAN port:

```
PPTPDATA-[1.1.1.1]: _dataFromLan
```

The MAX unit 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
```

Diag RadAcct

Description: Displays RADIUS accounting information. The Diag 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 Diag RadIF command displays more detailed information.)

Usage: Enter diag radacct at the command prompt.

Example:

```
> diag 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
```

Diag RadIF

Description: Displays RADIUS-related messages. Diag RadIF is a powerful diagnostic command, because it displays RADIUS messages that the MAX unit receives and messages that it sends. Output from Diag 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 use this command to validate the IP port that you have configured (or think you have configured), and the username that is being sent by the client.

The command is a toggle that alternately enables and disables the diagnostic display.

Usage: Enter diag 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 Acknowledgment
    3 - Rejection
    4 - Accounting Request
    5 - Accounting Response
    7 - Password Change Request
    8 - Password Change Positive Acknowledgment
    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 unit. The unit creates the user's Connection profile from these attributes, and RadIF displays them. (For a complete list of attribute numbers, see the *TAOS RADIUS Guide and Reference*.)

```
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
```

Diag Routmgr

Description: Displays route manager information regarding incoming calls to the MAX unit.

Usage: Enter the diag routmgr at the command prompt.

Example:

```
> diag routmgr
routmgr debug is ON > ROUTMGR: route 260 reason 185
ROUTMGR: destroyRoute routeID = 260, cause = CLEAR
ROUTMGR-DNIS: Do not free new dnis# 5962165 (call unauthorized)
ROUTMGR-260: port is 246
ROUTMGR: deallocateCapability routeID=260, capability=ALL
ROUTMGR: route 260 destroyed
ROUTMGR: route 260 reason 185
```

Diag SNTP

Description: Displays messages related to Simple Network Time Protocol (SNTP). The command is a toggle that alternately enables and disables the diagnostics display.

Usage: Enter diag sntp at the command prompt.

Example: Following are sample messages displayed with SNTP enabled.

The MAX unit accepts time from a configured NTP server. The following message appears if the MAX does not accept a supplied time:

```
Reject:li= x stratum= y tx= z
```

The following message indicates that the MAX accepts the time from a specified NTP server:

```
Server= 0 Time is b6dd82ed d94128e
```

Because the stored time is off by more than one second, it is adjusted:

```
SNTP: x Diff1= y Diff2= z
```

Diag Telnet

Description: Displays messages as Telnet connections are attempted or established. The Telnet protocol negotiates several options as sessions are established, and Diag Telnet displays the Telnet option negotiations.

The command is a toggle that alternately enables and disables the diagnostic display.

Usage: Enter diag telnet at the command prompt.

Example: The following session shows the MAX terminal server establishing a successful Telnet connection with a UNIX host.

```
MAX> diag telnet
TELNET debug is now ON
```

The far-end UNIX host has been contacted:

```
TELNET-4: TCP connect
```

For this Telnet session, the MAX unit will support options 24 and 1:

```
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
```

Ether-Display

Description: Displays the contents of Ethernet packets.

If you enter the command while traffic through your MAX unit 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 unit reboots, it logs a fatal-error message to the fatal-error log. The fatal-error log also includes warnings, for which the MAX unit did not reset. Development engineers use Warnings for troubleshooting purposes. A warning indicates that the MAX unit detected an error condition but recovered from it. The number of entries in this log is limited by available flash memory space, and the errors rotate on a First-In, First-Out (FIFO) basis. Use the Clr-History command to clear the log.

Note: If your MAX unit experiences a fatal-error reset or warning, contact 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 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 unit 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 a MAX unit 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 unit goes down.

```
FATAL_SYSTEM_UP =            100
```

As a complement to entry 99, the preceding entry is logged as the MAX unit 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. A MAX unit 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 unit. When the unit boots, it loads the code and configuration from Flash memory into Dynamic Random Access Memory (DRAM). If you want to return your unit 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 unit 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 unit will load the configuration stored in flash memory rather than be reset to factory default settings.

Usage: Enter fsave at the command prompt.

Example:

```
MAX> fsave
```

See Also: FClear

Heartbeat

Description: Displays information related to multicast heartbeat functionality. The command is a toggle that alternately enables and disables the debug display.

Usage: Enter heartbeat at the command prompt.

Example: Following are several examples of output displayed by the Heartbeat command.

```
HB: Sending SNMP Alarm count
HB: Checking Number of HeartBeats received
HB: HeartBeats received x
HB: Changing to Alarm Mode, HeartBeats Received x Expected y
HB: HeartBeat group address changed
```

```
HB: Heart beat received with invalid UDP port
HB: Heart beat received from invalid source
HB: Received HeartBeat packet
```

Help

Description: Displays a list of the most commonly used diagnostic commands and a brief description of each command. Append the `ascend` modifier to display the complete list of commands.

Usage: `help` [`ascend`]

Syntax element	Description
ascend	List all commands.

Example:

```
> 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)
```

Lanport Modem

Description: Displays a report on the status of the availability of modems in the MAX unit. 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 can 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 unit. Poor line quality, software problems with the calling modem, wrong numbers, and forgotten passwords all can generate calls that appear as bad calls but have nothing to do with modems on the MAX unit.

Usage: Enter lanport modem at the command prompt.

Example: In the following display, an 8-mod modem card is located in slot 8 of the MAX unit. 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.

```
> lanport modem
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 = fffff00 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.

Lcstate

Description: Displays the LANCORE state of incoming traffic processed on the MAX unit.

Usage: Enter lcstate at the command prompt.

Example:

```
> lcstate
LANCORE state display is now ON
LANCORE state display is now ONLANCORE-257: incoming call
LANCORE-257: >> msg 'INCOMING' in state 'AVAILABLE:A'
LANCORE-257: _availableIncomingCall
LANCORE:_enterIncomingCallStateA: routeID:257
LANCORE-257: No profile found (optional).
LANCORE-257: << new state is 'INCOMING:A'
LANCORE-257: call complete, status=SUCCESS, 1 channels
LANCORE-257: >> msg 'COMPLETE' in state 'INCOMING:A'
LANCORE-257: _incomingCallComplete, success = SUCCESS
No coreInfo->miscInfo:route=257,mgmtType=0,wanProtocolType=255
LANCORE-257: wan complete
LANCORE-257: << new state is 'INCOMING:D'
LANCORE-257: _incomingWanOpenComplete, success = 1
LANCORE-257: >> msg 'WAN OPEN COMPLETE' in state 'INCOMING:D'
LANCORE-257: _incomingWanOpenComplete, success = 1
LANCORE-257: << new state is 'INCOMING:B'
LANCORE-257: wan detect
LANCORE-257: >> msg 'WAN DETECT' in state 'INCOMING:B'
LANCORE-257: _incomingWanUp
_incomingWanUp:userProtocol=0,mgmtType=2
LANCORE-257: << new state is 'IDLE:A'
```

MdbStr

Description: Modfies the default modem AT command strings used by the modems on a MAX unit for both incoming and for outgoing calls. WIth earlier software, you could not modify the AT command for modems on the unit. 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 a MAX unit 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. 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 unit:

- `AT&F0&C1V0W1X4`

- `AT%C3\N3S2=255S95=44S91=10+MS=11,1,300,33600A`

Usage: mdbstr [0] [1] [2] [*AT command string*]

Example: 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
```

MDialout

Description: Displays messages related to modem dialout. Use the command in conjunction with the diagnostic command Diag Modemdrv (ModemDrvState in previous TAOS revisions) 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 unit 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>
```

ModemDiag

Description: Displays diagnostic information about each modem as the modem's call is cleared. The command is a toggle that alternately enables and disables the diagnostic display.

With ModemDiag enabled, at the end of each modem call the command initiates an AT&V1 call and displays the following variables with their current values:

Usage: Enter `modemdiag` at the command prompt.

Variable	Description
TERMINATION REASON	LINK DISCONNECT—The remote side disconnected the call. LOCAL REQUEST—The MAX initiated a disconnect because of poor line quality. CARRIER LOSS GSTN CLEARDOWN—Global Switched telephone network (GSTN) initiated the disconnect. NO ERROR CORRECTION INCOMPATIBLE PROTOCOL EXCESSIVE RETRANSMISSIONS DTR LOSS INACTIVITY TIMEOUT INCOMPATIBLE SPEEDS BREAK DISCONNECT KEY ABORT
LAST TX data rate	Last data rate at which the modem on the MAX was transmitting.
HIGHEST TX data rate	Highest data rate at which the modem on the MAX was transmitting.
LAST RX data rate	Last data rate at which the modem on the MAX was receiving.
HIGHEST RX data rate	Highest data rate at which the modem on the MAX was receiving.
Error correction PROTOCOL	Negotiated error correction protocol.
Data COMPRESSION	Negotiated data compression protocol.
Line QUALITY	Probes are sent by each modem to determine the quality of the line and the connection. The range for this variable is 0 to 128. The lower the number, the better the perceived line quality.
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:

```
> 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
```

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 unit. 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]
```

NetRoute

Description:

Usage: Enter netroute at the command prompt.

Example:

```
> netroute
NETROUTE debug is now ON
netroute::Checking if incoming call on channel: 1, Dsl: 5 phone
number [59621
65] is net-to-net
NETROUTE:_ntMatch:dest in profile is: slot 0, slotDsl 0
```

NSLookup

Description: Similar to the UNIX nslookup command. When you specify a hostname, a Domain Name System (DNS) request is forwarded. If the host is found, the corresponding IP address is displayed.

Usage: Enter the following command at the command prompt:

nslookup [-v] [*-s dnsServerIpAddr*] [*-r vRouterName*] *hostname*

The optional elements of the NSLookup command are described below:

Optional Element	Specifies
-v	The MAX unit displays the details of packets received from the DNS server responding to the query.
-s dnsServer IPAddr	The MAX unit attempts to resolve the specified hostname into an IP address by using the specified dnsServerIpAddr as the DNS server. If you do not specify this optional element, the MAX unit uses the information specified for the Pri DNS and Sec DNS parameters to determine which server(s) provide the necessary DNS information.
-r vRouterName	An individual VRouter. If this option is not entered, the global VRouter will be used.
hostname	The host to which the MAX unit sends its DNS request.

Example:

```
> nslookup host1
Resolving host host1.
IP address for host drawbridge is 1.1.1.1.
```
```
> nslookup 198.4.92.1
Resolving host 198.4.92.1.
```
```
> nslookup
```
```
Missing host name.
```
```
> 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 *N*

Description: Very similar to the WANDisplay diagnostic command. But PPPDump *N* 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

PPPInfo

Description: Displays information about established PPP sessions. Has little practical use other than as a tool for developmental engineering.

Usage: `ppinfo index [all]`

Syntax element	Description
`index`	Selects a particular PPP information table.
`all`	Displays information about embedded structures.

Example:

```
> 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
```

PPTPEC

Description: Displays control link messages between the PPTP client and the PPTP server. The command is a toggle that alternately enables and disables the diagnostics display.

Usage: Enter `pptpec` at the command prompt.

Example: Following are messages from a successful connection and from an unsuccessful attempt.

Successful connection:

```
PPTPEC-[1.1.1.1]: pptpECSend called
PPTPEC-[1.1.1.1]: New state = Running
PPTPEC-[1.1.1.1]: Event = Send, current state = Running
PPTPEC-[1.1.1.1]: New state = Running
PPTPEC-[1.1.1.1]: Receive callback called
PPTPEC-[1.1.1.1]: Event = Receive, current state = Running
PPTPEC-[1.1.1.1]: New state = Running
```

Unsuccessful attempt:

```
PPTPEC-[2.2.2.2]: pptpECStart called-
PPTPEC-[2.2.2.2]: Event = Start, current state = Stopped
```

PPTPSend

Description: Sends an Echo Request to the specified NT PPTP server.

Usage: pptpsend *ip_address_of_PPTP_server*

Example:

```
> pptpsend 1.1.1.1
PPTPCM: Sending Echo Request to host [1.1.1.1]
```

PRIDisplay

Description: Displays the contents of WAN packets.

If you enter the command while traffic through your MAX is heavy, the resulting amount of output can make it tedious to find the information you are looking for. The screen might even display the message ----- data lost -----, which just means that not all the output can be displayed on the screen. You might prefer to use the PRIDisplay command during a period of low throughput.

Usage: pridisplay *n*

where *n* is the number of octets to display from each WAN packet.

Example: The output from the following PRIDisplay command shows the first 64 bytes from each packet sent to or received from the WAN:

```
> pridisplay 64
Display the first 64 bytes of PRI messages
PRI-RCV-0(task: B0479C00, time: 83251.39) 4 octets @ B0539620
[0000]: 02 01 01 61
PRI-XMIT-0(task: B04B3A40, time: 83251.39) 4 octets @ B050C340
[0000]: 02 01 01 49
PRI-RCV-0(task: B0479C00, time: 83261.64) 4 octets @ B052AF60
[0000]: 02 01 01 61
PRI-XMIT-0(task: B04B3A40, time: 83261.65) 4 octets @ B051EFA0
[0000]: 02 01 01 49
PRI-RCV-0(task: B0479C00, time: 83269.98) 27 octets @ B0539620
```

```
[0000]: 02 01 48 60 08 02 1A 7B 05 04 03 80 90 A2 18 04
[0010]: E9 82 83 88 70 05 C1 34 39 39 30
```
pridisplay 0
```
PRI message display terminated
```

Quit

Description: Exits diagnostic mode.

Usage: Enter quit at the command prompt.

RadStats

Description: Displays a compilation of RADIUS Authentication and Accounting statistics.

Usage: Enter radstats at the command prompt.

Example:

> **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 (zero) 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, 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:

> **reset**

See Also: NVRAM

Revision

Description: Displays a MAX unit's hardware revision level and serial number.

Usage: Enter the revision at the command prompt. The unit's response contains five elements:

[*HW_REV N NN SN*]

Element	Definition
HW_REV	The unit's hardware revision, represented a number 0 to 9.
	A value of 0 (zero) specifies that the hardware revision is unknown. This is not a cause for concern.
N NN	Information that Lucent Technologies uses internally.
SN	The serial number of the MAX unit.
	Note: For MAX 3000 units, this information determines whether you can downgrade from the current version of operating system software.

Example: In the following message, the MAX has a serial number of 6363077.

```
> revision
revision = 0 1 10 6363077
```

T1coredisplay

Description: Specifies the number of bytes to display from incoming T1 core messages.

Usage: Enter t1coredisplay [*n*] at the command prompt. [*n*] represents the number of bytes the unit displays. Specify 0 to turn off T1coredisplay.

Example:

```
> t1coredisplay 100
Display the first 100 bytes of T1Core messages
> t1coredisplay 0
T1Core message display terminated
```

Tempdisplay

Description: Displays the ambient temperature in Celsius from sensors located in the MAX 3000 unit to monitor the modems, the power supply, and the serial ports.

Usage: Type the tempdisplay command at the DO menu's Diagnostic prompt (>).

Example:

```
> tempdisplay

  Ambient temperatures:

    Location      Celcius

    Ethernet       28
    Modems         29
    Power supply   39
    Serial ports   32
>
```

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 unit needs to be reset to load the uploaded code, since the unit must load the code from Flash memory into DRAM.

Although the MAX unit 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 unit 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 a Lucent Technologies representative) that will enable the functionality in your MAX. After each string is entered, the word *complete* appears, indicating that the MAX accepted the hash code.

If you enter update without a text string modifier, the MAX displays a list of current configuration information.

Usage: update [*text_string*]

Example:

```
MAX> update
Host interfaces: 4
Net interfaces: 4
Port 1 channels: 255
Port 2 channels: 255
Port 3 channels: 255
Port 4 channels: 255
Field features 1: 182
Field features 2: 33
Field features 3: 54
Protocols: 1
MAX> update 5 1023 12321312312312321
```

The following two messages indicate that the text strings were entered incorrectly:

```
update command: invalid arg 3!
update command: disallowed
```

The following message indicates that the MAX accepted the update string:

```
update command: command complete.
```

WANDisplay

Description: Displays all packets received from or sent to any of the WAN interfaces. Because WANDisplay output shows the raw data the MAX is receiving from and sending to the remote device, the information can be very helpful in PPP negotiation problems.

If you enter the command while traffic through your MAX is heavy, the resulting amount of output can make it tedious to find the information you are looking for. The screen might even display the message `----- data lost -----`, which just means that not all the output can be displayed on the screen.

You might prefer to use the WANDisplay command during a period of low throughput. Alternatively, depending on the types of information you need to gather, you might use WANDSess, WANOpen, or WANNext to focus the display.

Usage: wandisplay *number_of_octets_to display_from_each_packet*

Enter `wandisplay 0` to disable the logging of this information.

Example: The bytes are displayed in hexadecimal format. Following are several examples of WANDisplay output.

```
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.

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. 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
MAX> wddialout
WANDATA dialout display is OFF
```

Using diagnostics-related DO commands for the MAX 6000 unit's PCMCIA card

This section describes the commands that manage the FAT file system on the MAX 6000 unit's PCMCIA card.

FImageCopy

Description: Copies a code image between a PCMCIA card and the MAX 6000 unit's internal flash memory.

Permission level: Requires Diagnostic mode permissions.

Usage: For an unformatted PCMCIA card:

fImageCopy (-i | -p)

For an FAT-formatted PCMCIA card:

fImageCopy (-i | -p *path*)

where:

- **-i** copies the code image from the internal flash memory to the PCMCIA card
- **-p** copies the code image from the PCMCIA card to internal flash memory
- ***path*** is the destination path and filename of the code image

Example: Examples are:

> **fImageCopy -i**	Copies the internal flash memory code image to the PCMCIA card.
> **fImageCopy -p**	Copies the code image from an unformatted PCMCIA card to the internal flash memory.
> **fImageCopy -p /current/TAOSfilem60.bin**	Copies TAOSfilem60.bin from a FAT-formatted PCMCIA card to internal flash memory.

Fload

Description: Uses TFTP to copy a file from the TFTP server to the MAX 6000 unit's PCMCIA card.

Permission level: Requires Diagnostic mode permissions.

Usage:

fload *tftp_server_IPadr path1* [*path2*]

where:

- ***tftp_server_IPadr*** is the IP address of the server on which you have stored the MAX executable files.
- ***path1*** is the pathname of the file you are copying to the PCMCIA card.
- ***path2*** is the pathname for the file on the PCMCIA card.

Example: The following command results in a TFTP transfer of the MAX 6000 load named m601t1bxkh.bin from the server with the IP address of 198.186.66.32 to the directory /current on the PCMCIA card. The file is renamed m60.bin when placed on the card.

> **fload 198.186.66.32 m601t1bxkh.bin /current/m60.bin**

The following command also results in a TFTP transfer of the MAX unit load named m60.bin from the server with the IP address of 198.186.66.32 to the /current directory on the PCMCIA card. The directory /current is the default.

> **fload 198.186.66.32 m60.bin**

Format

Description: Formats a PCMCIA card with a file system for storing the MAX 6000 unit's executable files and configuration files.

Permission level: Requires Diagnostic mode permissions.

Usage:

format [*options*] [*device*]

where:

options are one or more of the following:

-o	Formats the PCMCIA card with the old, version 2, format. This option is incompatible with the -b option.
-e	Erases the entire PCMCIA card.
-b	Formats the PCMCIA card and reserves the first 128 Kb for the handler software. This option is incompatible with the -o option.
-e -b	Erases the boot region of the PCMCIA card.

device —The PCMCIA card, which is specified as flash-card-1 or 1. Only one PCMCIA card exists on the MAX 6000, so the device name is optional.

Example:

> **format**
or
> **format 1**
or

> **format flash-card-1**	Formats the PCMCIA card and does not reserve space for the handler software.
> **format -b**	Formats the PCMCIA card and reserves the first 128 Kb for the handler software.
> **format -e**	Erases all contents from the PCMCIA card.
> **format -e -b**	Erases the handler portion of the file system only if you created the formatting by using the -b option.

FVersionInfo

Description: Displays the version of software stored on the PCMCIA card or in the internal flash memory.

Permission level: Requires Diagnostic mode permissions.

Usage:

fVersionInfo (-i | -p)

where:

- **-i** reports the version of the code image stored in internal flash memory.

- **-p** reports the version of the code image stored on the PCMCIA card.

Example: The following command displays the software version of an unformatted PCMCIA card:

> **fVersionInfo -p**

The following command displays the software version of a FAT-formatted PCMCIA card.

> **fVersionInfo -p /current/TAOSfilem60.bin**

Ls

Description: Lists the files and directories on the PCMCIA card's file system.

Permission level: Requires Diagnostic mode permissions.

Usage:

ls *path*

where *path* is the name of and path to the directory or file you want to list.

The following two commands list the contents of the all directories and the /current directory, respectively:

> **ls**
> **ls /current**

MkDir

Description: Creates a new directory on a PCMCIA card's file system.

Permission level: Requires Diagnostic mode permissions.

Usage:

mkdir *path*

where *path* is the path and name of the directory you want to create.

Example: The following two commands create directories named dump and testdir, respectively, in the current directory:

> **mkdir dump**   Creates the directory dump.
> **mkdir testdir**   Creates the directory testdir.

Mv

Description: Moves a file or directory on the PCMCIA card's file system.

Permission level: Requires Diagnostic mode permissions.

Usage:

mv *path1 path2*

where:

- *path1* is the path to and name of the file or directory you want to move.

- *path2* is the path to and name of the destination. When moving a file, you must include the destination filename.

Example: :

> **mv test.txt dump/test.txt**	Moves the test.txt file to the dump directory.
> **mv testdir dump**	Renames the testdir directory to dump.
> **mv graphics manual/graphics**	Moves the directory graphics to make it a subdirectory of the directory manual.

Rm

Description: Deletes a file or an empty directory.

Permission level: Requires Diagnostic mode permissions.

Usage:

rm *path*

where ***path*** is the path to and name of the directory or file you want to remove.

Example: Examples are:

> **rm dump/test.txt**	Removes the file test.txt from the directory dump.
> **rm dump**	Removes the directory dump. The directory must be empty.

TLoadCode

Description: Uses Trivial File Transfer Protocol (TFTP) to load software from a TFTP server into the MAX 6000 unit's flash memory or onto a PCMCIA card. The TFTP host can be accessed from the Ethernet interface or across the WAN.

You must reset the unit to load the new software.

The unit might experience performance degradation during the file transfer.

When you use the tloadcode command, the current configuration of the MAX unit is saved to flash memory. Manual reconfiguration, required when loading software through the serial connection, is unnecessary when using tloadcode for a TFTP transfer.

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 transfer is interrupted or the checksum of the uploaded file is incorrect, the new code does not load when the MAX 6000 unit is rebooted. The unit reloads its previous version of code. Also, if the new code *is* uploaded at boot time, the unit automatically performs an

FRestore and loads the configuration that is stored in flash memory. The unit reboots again to initialize the configuration properly.

Permission level: Requires Diagnostic mode permissions.

Usage: If no PCMCIA card is present, tloadcode loads the software to the unit's internal flash memory. If a PCMCIA card is present, tloadcode loads the software to the PCMCIA card. Options provide additional controls over how software is loaded.

Syntax is:

tloadcode [*options*] *tftp_server_IPadr filename*

where:

options include one or more of the following:

-f	Forces the load procedure. If you use -f, tloadcode does not return a warning message if you are loading an executable file not intended for the unit on which you are loading it.
-i	Loads the executable file to the MAX unit's internal flash memory, even though a PCMCIA card is present.
-b	Loads the executable file into the space reserved for the handler file on the PCMCIA card if the card was formatted using **-b**.

*   *tftp_server_IPadr* is the IP address of the server on which you have stored the MAX executable files.
*   *filename* is the name of the executable file.

Example:

The following command loads the handler file from the TFTP server 192.168.18.33 onto the PCMCIA card:

> **tloadcode -b 192.168.18.33 m60handler.bin**

The following command loads the m60.bin executable file into the boot directory of a FAT-formatted PCMCIA card:

> **tloadcode 192.168.18.33 current/m60.bin**

The following command loads the m60.bin executable file into internal flash memory of the MAX unit:

> **tloadcode -i 192.168.18.33 m60.bin**

Understanding Diagnostic command output

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 Lucent Technologies diagnostic traces:

Identifier	Description
C0 21	Link Control Protocol (LCP)
C0 23	Password Authentication Protocol (PAP)
C2 23	Challenge Handshake Authentication Protocol (CHAP)
80 21	Internet Protocol (IP)
80 29	Appletalk
80 2B	Novell's Internetwork Packet Exchange (IPX)
80 31	Bridging PDU
80 FD	Compression Control Protocol (CCP)

Following are the packet formats:

Packet Format ID	Description
01	Configure Request
02	Configure Acknowledgment
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 to 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 increased 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—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). Lucent Technologies 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—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. 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
```

Machine Interface Format (MIF)

<div style="text-align: right;">

C

</div>

Machine Interface Format (MIF) is a language specific to Lucent Technologies that provides an alternative configuration interface for MAX units. Use a command line or write a MIF program that sets the MAX unit's parameters, rather than use the configuration menus to change one parameter after another. MIF programs provide a batch-processing method of changing a configuration or performing a series of actions.

MIF is command-line driven. When you use MIF, the computer that controls the MAX does not have to process asynchronous events. However, the controlling computer can enable asynchronous event reporting.

Note: Every attempt has been made to confirm that this appendix correctly describes the functionality and output of the Machine Interface Format (MIF). However, Lucent Technologies does not guarantee the completeness of the list of commands or of the cataloging of functionality from release to release.

Accessing the interface

Access MIF with the Use MIF command, the MIF escape sequence, or a transfer command.

To start MIF from the VT100 configuration menus, select the Use MIF command in the Sys Diag menu:

```
00-200 Sys Diag
 00-201 Restore Cfg
 00-202 Save Cfg
>00-203 Use MIF
 00-204 Sys Reset
 00-205 Term Serv
 00-206 Upd Rem Cfg
```

After the MIF interface replaces the configuration menus, start entering MIF commands interactively, or download an ASCII file containing a series of MIF commands by using the appropriate transfer command (such as Send Text) in your VT100 emulation program.

The second way to start MIF from any location in the configuration menus by typing the following four-key sequence in rapid succession (press each key in the sequence shown, one after the other, as quickly as possible):

```
ESC [ ESC !
```

The third way to start MIF by using the appropriate transfer command (such as Send Text) in your VT100 emulation program, but that the first line in the emulation program must contain the MIF escape sequence `ESC [ ESC !`.

Using full and partial addresses

Each profile, parameter, DO menu item, or status window is called an *addressable entity.* Each of these entities has a unique address.

A *full address* specifies a specific entity and consists of the full syntax shown below. A *partial address* does not include the `name` attribute.

Addresses have the following syntax:

slot and port.type.entry.name

For example:

```
103.DIAL.1.Data Svc
```

Table C-1 summarizes the elements of the address.

Table C-1. Syntax element descriptions

Syntax element	Description
slot	One-digit slot number of the addressed entity (1 in the preceding example). For most addresses, the slot number of the addressed entity is identical to the first digit of the menu number in the standard user interface.
port	Two-digit port number of the addressed entity (03 in the preceding example). For most addresses, the port number of the addressed entity is identical to the second and third digits of the menu number of the standard user interface.

Table C-1. Syntax element descriptions (continued)

Syntax element	Description
type	This attribute contains the type of the addressed entity. The defined types are listed below, and are described in detail in "Using supported types" on page C-10. • ALARM—Line alarm indications • BRIDGE—Bridge Adrs profile • CONN—Answer and Connection profiles • DEST—Destination profiles • DIAG—System diagnostics • DIAGN—Line diagnostics • DIAL—Call profiles • DO—DO Command menu • ETHERNET—Ethernet profile • FILT—Filter profiles • FR—Frame Relay profiles • HOST2—Host-Interface profile for Host/Dual modules • HOST4—Host-Interface profile for Host/Quad modules • HOST6—Host-Interface profile for Host/6 modules • LINE—Line profiles • LMODEM—LAN Modem profiles • LOOP—Port diagnostics (loopback) • PORT—Port profile • ROUTE—Route profiles • SEC—Security profiles • STAT—Status menu • SWAN—Serial WAN profile (currently not supported) • SYS—System profile • TRAP—SNMP Traps profiles
entry	Identifies a specific entity, such as a profile. If there is only one entity of a particular type, as in the case of the Port profile of the DO menu, the entity's entry is a zero. When a type includes more than one entity, as in the case of Line N profiles, 0 (zero) is the current (default) entry, 1 is the first entry saved after the current entry, and so on. An address without an entry denotes the factor-default type profile.
name	Identifies the name of the addressed entity.

Using supported commands

Use the SET command to set the value attribute. Use the GET and NEXT commands to retrieve current information in the value attribute. Following are the supported MIF commands:

- LOAD <partial address>
- SAVE <partial address>
- GET <full or edit address>
- NEXT <address>
- SET <full or edit address>=<value>

For a definition of the edit address, see "Loading and saving entities" on page C-4.

Understanding responses

The LOAD and SAVE commands respond with a prompt (:) if the command is valid:

```
:
```

The GET and NEXT commands return a value in the following syntax:

```
+ <address>=<value>
```

For example,

```
: GET 201.DIAL.16.Call Type
+ 201.DIAL.16.Call Type=AIM
```

The plus-sign indicates a returned value or an error. Invalid commands return the following message:

```
+ ERROR
```

The SET command also responds with a prompt (:). When it is applied to a status or alarm entity, however, it creates a trap which is reported in the following syntax:

```
<address>=<value>
```

For example:

```
: SET 100.ALARM.0.alarm=20
100.ALARM.0.alarm=LA
:
```

The minus-sign indicates an asynchronous report. For more information, see "MIF traps and asynchronous reports" on page C-6.

Loading and saving entities

Only entities (such as profiles) that have been loaded into the edit area can be modified. Because there is only one edit area and it can have only one profile loaded into it at a time, commands that operate on entities in the edit area can use another version of the address called the *edit address*. The edit address has the following format:

```
<name>
```

The LOAD commands loads a profile into the edit area. It uses the following syntax:

```
LOAD <partial address>
```

For example,

```
: LOAD 201.PORT.0
```

When the profile has been loaded into the edit area, modify it, using only the SET command, for example:

```
: SET Port Name=Chicago #1
```

When you have finished modifying the profile, save it. The SAVE command copies the profile in the edit area to the specified address. It uses the following syntax:

```
SAVE <partial address>
```

For example,

```
: SAVE 201.PORT.0
```

Getting an entity's current value

If an entity (profile) has not already been loaded into the edit area by using the LOAD command, the GET command loads the profile and then extracts the requested value.

The GET command returns the value of the addressed attribute. When the addressed attribute is a parameter in the standard user interface, the value returned by GET is a parameter value. When the addressed attribute is a status window in the standard user interface, all lines in the status window are returned.

The GET command uses the following syntax:

```
GET <full or edit address>
```

For example, the following GET command uses a full address:

```
: GET 201.DIAL.16.Call Type
+ 201.DIAL.16.Call Type=AIM
```

Or, if the profile has already been LOADed into the edit area, use the following syntax:

```
: LOAD 201.DIAL.16
: GET Call Type
+ 201.DIAL.16.Call Type=AIM
```

Getting the address and value of the next entity

The NEXT command returns the address and value of the attribute with the next address. Addresses, though composed of both textual and numeric components, are ordered as if each component was a digit of a decimal number. The sequence is:

<name> within <entry>
<entry> within <type>

    <type> within <port>

    <port> within <slot>

The NEXT command uses the following syntax:

    NEXT <full address>

For example:

```
: NEXT 000.DIAL.1.Data Svc
+ 000.DIAL.1.Base Ch Count=1
```

Modifying parameter values

If an entity (profile) has not already been loaded into the edit area by using the LOAD command, the SET command loads the profile and then replaces the specified value.

The SET command replaces the current value of the entity with the <value> given in the command. In this context, it uses the following syntax:

    SET <edit address>=<value>

When the address refers to a parameter in a profile, the SET command accepts only an edit address. So, the profile must already be LOADed into the edit area. For example:

```
: LOAD 201.PORT.0
: SET Port Name=Chicago #1
: SAVE 201.PORT.0
:
```

Note: The SET command does not replace the parameter's value until you use the SAVE command.

To SET an enumerated parameter (such as Yes or No), the <value> must be identical to the enumerated value in the MAX unit's VT100 interface. However, the specified value is not case-sensitive. For example, use either one of these commands:

```
: SET 100.DIAGN.0.Clr Err1=Yes
: SET 100.DIAGN.0.Clr Err1=yes
```

Apply the SET command to status and alarm entities, as described in the next section.

MIF traps and asynchronous reports

When you apply the SET command to a status window or an alarm, it enables asynchronous reports (traps) of the requested status screen or alarms. In this context, the SET command uses the following syntax:

    SET <full address>=<value>

The <value> established in the SET command sets the time period in seconds between status checks. For example,

```
: SET 100.ALARM.0.alarm=20

– 100.ALARM.0.alarm=LA

:
```

Reports are generated only whenever a change is detected in the requested status window components or whenever an alarm occurs. If the <value> in the SET command is 0, asynchronous reports are not generated.

Understanding command-line basics

Begin using the MIF command line when you understand Command Line Length, Command Echo, Line Terminations, Prompt, and Output Indicators.

Table C-2 summarizes command-line processing in MIF.

Table C-2. Command-line processing

Command Line Length	The maximum command line is limited to 76 characters. Data entered after the 76th character is ignored and not echoed to the screen. The line is not terminated until a Line Termination is entered.
Command Echo	All data entered by the user except the line termination character will be echoed back to the user, character by character.
Line Terminations	Lines are terminated by either a Return (ASCII `<CR>`), or a Line Feed (ASCII `<LF>`), or both. When either is first received, the sequence `<CR>–<LF>` is echoed. An `<LF>` following a `<CR>` does not result in an additional `<CR>–<LF>` being echoed. The Line Termination character may be entered at any point on the line; the entire line is accepted.
Prompt	The display of a prompt is an explicit acknowledgment that the previous entry has been processed and that the system is now ready to process the next request. The default prompt is a colon (`:`).

Table C-2. Command-line processing (continued)

Output Indicators	To make it easier for a computer program to parse, all output lines are prefixed with either an output indicator, namely plus (+) or minus (–). There are two indicators used.
	The plus indicator (+) is used when the output is a response to a previous command. Multi-line responses start each line with the output indicator.
	The minus indicator (–) is used when the output is the result of an asynchronous event.

Modifying an entity in the edit area

Modify entities in the edit area by following line-editing conventions regarding Line History, Line Selection Characters, Cursor Movement, and Line Editing.

Table C-3 summarizes line-editing conventions are supported by the MAX unit's MIF.

Table C-3. Line-editing conventions

Convention	Usage
Line History	The last 10 lines entered are kept. Whenever a line is entered the oldest kept line is thrown away. The stack is initialized empty at power up. Previous lines can be selected using the line selection characters. When a previous line is selected, the newly edited line replaces the selected line. That line becomes the newest line.

Table C-3. Line-editing conventions (continued)

Convention	Usage
Line Selection Characters	There are two line selection characters, one to walk backwards through the Line History and another to walk forward through the Line History. When the oldest entry is selected while walking backwards through the line history, the next backward selection selects the newest line entered. When the newest entry is selected while walking forward through the line history, the next forward selection selects the oldest line.
	The backward line selection character is either a VT100 up arrow (the Escape sequence ESC-[-A) or the control character ^P. The P is mnemonic for Previous.
	The forward line selection character is either a VT100 down arrow (the escape sequence ESC-[-B) of the control character ^N. The N is mnemonic for Next.
	If you enter a Line selection character while editing a line, the current line is replaced by the current line -- any edits in progress are lost. The cursor is positioned at the end of the selected line.
Cursor movement	The cursor can be moved within a line by entering the Cursor Left character or the Cursor Right character. The Cursor Left character is ignored when the cursor is at the first character of a line. The Cursor Right character is ignored when the cursor is one position to the right of the last character of the line.
	The Cursor Left character is either a VT100 left arrow (the escape sequence ESC-[-D) or the control character ^B. The B is mnemonic for Backward.
	The Cursor Right character is either a VT100 right arrow (the escape sequence ESC-[-C) or the control character ^F. The F is mnemonic for Forward.
Line Editing	The current line can be edited until the Line Termination character is entered. Line editing is always in "insert" mode; the character typed will be entered before the cursor and any characters starting from the cursor to the end of the line will be shifted right one position. If the insertion causes the line to exceed the maximum line length the last (rightmost) character is dropped. Cursor movement and line selection commands are processed as described above. The backspace character deletes the character behind the cursor. When a backspace is received at the beginning of a line it is ignored.

Using supported types

This section lists each MIF type with its allowed values.

Types are listed alphabetically. The following format is used:

<address>=<value>

For example, the Remote Mgmt type can be set to Yes or No. It appears in the system profile (SYS) at the following MIF address:

```
000.SYS.0.Remote Mgmt
```

So, it is listed in this section like the following:

```
000.SYS.0.Remote Mgmt=Yes, No
```

Comments are set off by parentheses(), as shown below for the Clr Err1 type that can be SET but not read:

```
100.DIAGN.0.Clr Err1=Yes (write only)
```

If the type does not have enumerated values, the type of values it can take are given in *italics* as in the following two examples:

```
000.SYS.0.Name=text
```

```
000.SYS.0.Status 1=XN-n00
```

Note: The menu numbering shown in this section reflects the standard MAX unit whose base system slot 2 has a Host/Quad module.

The slot and port of most addresses are given explicitly; however, in some cases they are represented by *spp*, where *s* is the slot number and *pp* is the port number. For example, either one of the following two commands may be used:

```
000.SYS.0.Name=text
```

```
spp.SYS.0.Name=text
```

ALARM

For T1/PRI and E1/PRI units:

```
s00.ALARM.n.alarm= (write)
    DS,RA,YA,1S,DF,LA (read)
```

For BRI units:

```
100.ALARM.n.alarm= (write)
    -,X,.,P,M,D (read) (dash, X, period, P, M, D)
```

For Switched-56 units:

```
100.ALARM.n.alarm= (write)
    -,X,.,A (read) (dash, X, period, A)
```

Note:

•   Do not exceed 32,000 seconds when using SET to write to these addresses

- *s00*.ALARM.*n*...

    s = 1 or slot number of a T1/PRI or E1/PRI module

    n = the line number minus 1. Namely, *n*=0 is line #1, *n*=1 is line #=2, etc.

- Alarm definitions for T1/PRI lines are as follows:

    – DS (Line disabled)

    – RA (Red Alarm, loss of sync)

    – YA (Yellow Alarm)

    – 1S (AIS, Blue alarm)

    – DF (No D channel)

    – LA (Link Active)

- Alarm definitions for BRI/Switched 56 lines are as follows:

    – – (Line disabled)

    – X (No physical link)

    – P (Link active, BRI point-to-point)

    – M (Link active, BRI multipoint 1)

    – D (Line active, BRI multipoint 2)

    – A (Line active, switched 56)

For example:

Report status of the "100.ALARM.0.alarm" entity every 20 seconds if change occurs:

    : SET 100.ALARM.0.alarm=20

    - 100.ALARM.0.alarm=LA

    :

BRIDGE

*s*00.BRIDGE.*n*.Enet Adrs=*12-digit hexadecimal string*

    .Net Adrs=*dotted decimal format*

    .Connection #=*2-digit decimal string*

Note:

- *s00*.BRIDGE.*n*...

    s = slot into which the Ethernet card is installed

    n = 0 to 98

CONN

*s*00.CONN.*n*.Force 56=Yes,No (n=0)

    .Profile Reqd=Yes,No (n=0)

    .CLID Auth=Ignore,Prefer,Force (n=0)

    .Assign Adrs=Yes,No (n=0)

    .Encaps...MPP=Yes,No(n=0)

```
.Encaps...PPP=Yes,No(n=0)
.Encaps...COMB=Yes,No(n=0)
.Encaps...FR=Yes,No(n=0)
.Encaps...EU-RAW=Yes,No(n=0)
.Encaps...EU-UI=Yes,No(n=0)
.Encaps...TCP-CLEAR=Yes,No(n=0)
.Encaps...V.120=Yes,No(n=0)
.PPP options...Route IP=Yes,No (n=0)
.PPP options...Bridge=Yes,No (n=0)
.PPP options...Recv Auth=PAP,CHAP,Either,None (n=0)
.PPP options...MRU=number (n=0)
.PPP options...LQM=Yes,No (n=0)
.PPP options...LQM Min=number (n=0)
.PPP options...LQM Max=number (n=0)
.PPP options...Link Comp=Stac,None (n=0)
.PPP options...VJ Comp=Yes,No (n=0)
.PPP options...Dyn Alg=Constant,Linear,Quadratic (n=0)
.PPP options...Sec History=number (n=0)
.PPP options...Add Pers=number (n=0)
.PPP options...Sub Pers=number (n=0)
.PPP options...Min Ch Count=number (n=0)
.PPP options...Max Ch Count=number (n=0)
.PPP options...Target Util=number (n=0)
.PPP options...Idle Pct=number (n=0)
.COMB options...Password Reqd=Yes,No (n=0)
.COMB options...Interval=number (n=0)
.COMB options...Compression=Yes,No (n=0)

.Station=text (n=1 to 31)
.Active=Yes,No (n=1 to 31)
.Encaps=MPP,PPP,COMB,FR,EU-RAW,EU-UI,TCP-CLEAR (n=1 to 31)
.PRI # Type=Unknown,Intl,National,Local,Abbrev (n=1 to 31)
.Dial #=phone number (n=1 to 31)
.Calling #=phone number (n=1 to 31)
.Route IP=Yes,No (n=1 to 31)
.Route IPX=Yes,No (n=1 to 31)
.Bridge=Yes,No (n=1 to 31)
.Dial Brdcast=Yes,No (n=1 to 31)
.Encaps options...Send Auth=PAP,PAP-TOKEN,PAP-TOKEN-CHAP,
CACHE-TOKEN, CHAP,None (n=1 to 31)
.Encaps options...Send PW=text (n=1 to 31)
.Encaps options...Aux Send PW=text (n=1 to 31)
.Encaps options...Recv PW=text (n=1 to 31)
.Encaps options...Base Ch Count=number (n=1 to 31)
.Encaps options...Min Ch Count=number (n=1 to 31)
```

```
.Encaps options...Max Ch Count=number (n=1 to 31)
.Encaps options...Inc Ch Count=number (n=1 to 31)
.Encaps options...Dec Ch Count=number (n=1 to 31)
.Encaps options...MRU=number (n=1 to 31)
.Encaps options...LQM=Yes,No (n=1 to 31)
.Encaps options...LQM Min=number (n=1 to 31)
.Encaps options...LQM Max=number (n=1 to 31)
.Encaps options...Link Comp=Stac,None (n=1 to 31)
.Encaps options...VJ Comp=Yes,No (n=1 to 31)
.Encaps options...Dyn Alg=Constant,Linear,Quadratic(n=1 to 31)
.Encaps options...Sec History=number (n=1 to 31)
.Encaps options...Add Pers=number (n=1 to 31)
.Encaps options...Sub Pers=number (n=1 to 31)
.Encaps options...Target Util=number (n=1 to 31)
.Encaps options...Idle Pct=number (n=1 to 31)
.Encaps options...Password Reqd=Yes,No (n=1 to 31)
.Encaps options...Interval=number (n=1 to 31)
.Encaps options...Compression=Yes,No (n=1 to 31)
.Encaps options...FR Prof=text (n=1 to 31)
.Encaps options...DLCI=number (n=1 to 31)
.Encaps options...Login Host=text (n=1 to 31)
.Encaps options...Login Port=number or dotted decimal format (n=1 to
31)
.Ip options...LAN Adrs=dotted decimal format/subnet mask (n=1 to 31)
.Ip options...WAN Alias=dotted decimal format (n=1 to 31)
.Ip options...Metric=number (n=1 to 31)
.Ip options...Private=Yes,No (n=1 to 31)
.Ip options...RIP=Off,Send,Recv,Both (n=1 to 31)
.Ip options...Pool=number (n=1 to 31)
.Ipx options...Dial Query=Yes,No (n=1 to 31)
.Ipx options...IPX ENet#=number (n=1 to 31)
.Ipx options...IPX Alias=number (n=1 to 31)
.Ipx options...Handle IPX=None,Client,Server (n=1 to 31)
.Ipx options...Netware t/o=number (n=1 to 31)

.Session options...RIP=Off,Send,Recv,Both (n=0 to 31)
.Session options...Data Filter=number (n=0 to 31)
.Session options...Call Filter=number (n=0 to 31)
.Session options...Idle=number (n=0 to 31)
.Session options...Preempt=number (n=0 to 31)
.Session options...Backup=text (n=1 to 31)
.Session options...IP Direct=dotted decimal format
.Session options...FR Direct=Yes,No (n=1 to 31)
.Session options...FR Prof=text (n=1 to 31)
.Session options...FR DLCI=number (n=1 to 31)
```

```
                        .Telco options...AnsOrig=Both,Ans Only,Call Only (n=1 to 31)
                        .Telco options...Callback=Yes,No (n=1 to 31)
                        .Telco options...Call Type=Switched, Nailed, Nailed/MP+ (n=1
```
to 31)
```
                        .Telco options...Group=number (n=1 to 31)
```
.Telco options....FT1 Caller=Yes,No

.Telco options...Data Svc=Voice,56KR,56K,64K,384KR,

384K,1536K,1536KR,128K,192K,256K,320K,448K,

512K,576K,640K,704K,768K,832K,896K,960K,1024K,

1088K,1152K,1216K,1280K,1344K,1408K,1472K (n=1 to 31)
```
                        .Telco options...Force 56=Yes,No (n=1 to 31)
                        .Telco options...Bill #=number (n=1 to 31)
                        .Telco options...Call-by-Call=number (n=1 to 31)
                        .Telco options...Transit #=number (n=1 to 31)
```

Note:

- *s*00.CONN.*n*.PRI # Type is a T1/E1/PRI parameter only

- *s*00.CONN.*n*.Telco Options...Bill # is a BRI, T1/PRI parameter only

- *s*00.CONN.*n*.Telco Options...Call-by-Call is a T1/PRI parameter only

- *s*00.CONN.*n*.Telco Options...Transit # is a T1/PRI or E1/PRI parameter

- *s*00.CONN.*n*...

  s = slot into which the Ethernet card is installed

  n = 1 to 31

- *s*00.CONN.*n*.Data Svc for -SW56 units must = 56K.Data Svc for -BRI units can be Voice,56KR,56K,64K only

DEST

For T1/PRI units only:

```
000.DEST.n.Name=text
```
   .Option=1st Avail,1st Active,Any
```
   .Dial 1#=phone number
   .Call-by-Call 1=number
   .Dial 2#=phone number
   .Call-by-Call 2=number
   .Dial 3#=phone number
   .Call-by-Call 3=number
   .Dial 4#=phone number
   .Call-by-Call 4=number
   .Dial 5#=phone number
   .Call-by-Call 5=number
   .Dial 6#=phone number
   .Call-by-Call 6=number
```

Note:

- 000.DEST.*n*...

  n = 1 to 31

- 000.DEST .*n*.Call-by-Call are PRI parameters only

DIAG

`000.DIAG.0.Sys Reset=Yes` (write only)

`000.DIAG.0.UPD REM CFG=Yes` (write only)

For example:

: SET 000.DIAG.0.Sys Reset=No

+ ERROR

: SET 000.DIAG.0.Sys Reset=Yes

(unit resets!)

DIAGN

`s00.DIAGN.0.Line LB1=Yes,No`

`.Line LB2=Yes,No`

`.Clr Err1=Yes` (write only)

`.Clr Perf1=Yes` (write only)

`.Clr Err2=Yes` (write only)

`.Clr Perf2=Yes` (write only)

Note:

- This type applies to MAX-T1/PRI only. It does not apply to E1/PRI, BRI, or SW56 units.

- *s00*.DIAGN.*n*...

  s = 1 or slot number of a T1/PRI or E1/PRI module

For example:

: SET 100.DIAGN.0.LB1=No

:

DIAL

spp.DIAL.*n*.Name=*text*

`.Dial #=`*phone number*

`.Call Type=AIM,BONDING,1 Chnl,2 Chnl,FT1,Ft1-AIM,FT1-B&O`

`.Call Mgm=Manual,Static,Dynamic,Delta,Mode 1,Mode 2`

`.Data Svc=Voice,56KR,56K,64K,384KR,384K,1536K,1536KR,`
`128K,192K,256K,320K,448K,512K,576K,640K,704K,`
`768K,832K,896K,960K,1024K,1088K,1152K,1216K, 1280K,1344K,1408K,1472K`

`.Force 56K=Yes,No`

`.Base Ch Count=`*number*

`.Inc Ch Count=`*number*

`.Dec Ch Count=`*number*

`.Call-by-Call=`*number* (T1/PRI only)

```
.Bill #=number (T1/PRI only)
```
.Auto-BERT=Off,15 sec,30 sec,60 sec,90 sec,120 sec

.Bit Inversion=Yes,No

.Fail Action=Disc,Reduce,Retry
```
.PRI # Type=Unknown,Intl,National,Local,Abbrev (T1/PRI only)
```
```
.Transit #=number (T1/PRI only)
```
```
.Group=number
```
.FT1 Caller=Yes,No
```
.B&O Restore=number (n=30 to 30000)
```
.Flag Idle=Yes,No

.Dyn Alg=Constant,Linear,Quadratic
```
.Sec History=number
```
```
.Add Pers=number
```
```
.Sub Pers=number
```
.Time Period 1...Activ=Disabled,Enabled,Shutdown
```
.Time Period 1...Beg Time=hh:mm:ss
```
```
.Time Period 1...Min Ch Cnt=number
```
```
.Time Period 1...Max Ch Cnt=number
```
```
.Time Period 1...Target Util=number
```
.Time Period 2...Activ=Disabled,Enabled,Shutdown
```
.Time Period 2...Beg Time=hh:mm:ss
```
```
.Time Period 2...Min Ch Cnt=number
```
```
.Time Period 2...Max Ch Cnt=number
```
```
.Time Period 2...Target Util=number
```
.Time Period 3...Activ=Disabled,Enabled,Shutdown
```
.Time Period 3...Beg Time=hh:mm:ss
```
```
.Time Period 3...Min Ch Cnt=number
```
```
.Time Period 3...Max Ch Cnt=number
```
```
.Time Period 3...Target Util=number
```
.Time Period 4...Activ=Disabled,Enabled,Shutdown
```
.Time Period 4...Beg Time=hh:mm:ss
```
```
.Time Period 4...Min Ch Cnt=number
```
```
.Time Period 4...Max Ch Cnt=number
```
```
.Time Period 4...Target Util=number
```

Note:

- *spp*.DIAL.*n*...

  s = 0 or 2 or slot number of a Host/Dual or Host/6 module

  when s=0, *pp* = 00

  when *spp*=000, *n* = 0 through 15 (These shared Call Profiles 17 to 32)

  when s=2 or slot number, *pp* = 01 through last serial host port

  when *spp* is not 000, *n* = 0 through 16 (If *n*=0, this is the current Call Profile of serial host port *pp*. If *n* is not 0, these are stored Call Profiles 1 to 31.)

- *spp*.DIAL.*n*.Data Svc for -SW56 units must = 56K
  spp.DIAL.*n*.Data Svc for -BRI units can be Voice,56KR,56K,64K only

- s00.DIAL.*n*.PRI # Type is a T1/E1/PRI parameter only

- s00.DIAL.*n*.Bill # is a T1/PRI parameter only

- s00.DIAL.*n*.Call-by-Call is a T1/PRI parameter only

- s00.DIAL.*n*.Transit # is a T1/PRI only

For example:

    : NEXT 000.DIAL.1.Data Svc

    + 000.DIAL.1.Base Ch Count=1

    : GET 201.DIAL.16.Call Type

    + 201.DIAL.16.Call Type=AIM

    :

DO

spp`.DO.0.Dial=Yes,No` (read) `Yes` (write)

    `.Hang Up=Yes,No` (read) `Yes` (write)

    `.Answer=Yes,No` (read) `Yes` (write)

    `.Extend BW=Yes,No` (read) `Yes` (write)

    `.Contract BW=Yes,No` (read) `Yes` (write)

    `.Beg/End Rem LB=Yes,No` (read) `Toggle` (write)

    `.Beg/End BERT=Yes,No` (read) `Toggle` (write)

    `.Resynchronize=Yes,No` (read) `Yes` (write)

Note:

These commands apply only during certain conditions. For example, *spp*.DO.0.Hang Up applies only when the object specified has a call online, while *spp*.DO.0.Dial applies only to objects not having a call online. For details about each of the DO commands, see the *MAX Reference*.

- *spp*.DO...

    s = 2 or the slot number of a serial host or Ethernet module when s=2 or the slot number of a serial host module,

    pp = 01 through last serial host port when s= the slot number of the Ethernet module, *pp* = 00

- The <value> Toggle in a SET (write) command changes the state of the addressed entity from it current state to another state, i.e., from Yes to No or from No to Yes. The SET command applied to a DO <address> causes the DO action to be invoked if active.

- The GET (read) command returns the <value> YES or NO when applied to a DO <address>.YES is returned if the item can be invoked at the time of the request (is active) and NO is returned otherwise.

- DO P (password), DO S (save), and DO L (load) are not available.

For example:

    : NEXT 201.D0.0.Extend

    + 201.D0.0.Contract=Yes

    :

ETHERNET

*s*00.ETHERNET.0.Module Name=*text*

.Ether options...IP Adrs=*dotted decimal format/subnet mask*

.Ether options...2nd Adrs=*dotted decimal format/subnet mask*

.Ether options...RIP=Off,Send,Recv,Both

.Ether options...Ignore Def Rt=Yes,No

.Ether options...Proxy Mode=Off,Inactive,Active,Always

.Ether options...Filter=*number*

.Ether options...IPX Frame=802.3,802.2,SNAP,ENET II

.Ether options...IPX Net#=*number*

.WAN options...Dial Plan=Trunk Grp,Extended

.WAN options...Ans 1#=*Phone number*

.WAN options...Ans 2#=*Phone number*

.WAN options...Ans 3#=*Phone number*

.WAN options...Ans 4#=*Phone number*

.WAN options...Pool Start #1=*dotted decimal format*

.WAN options...Pool Count #1=*number*

.WAN options...Pool Start #2=*dotted decimal format*

.WAN options...Pool Count #2=*number*

.WAN options...Pool Only=Yes,No

.SNMP options...Read Comm=*text*

.SNMP options...R/W Comm=*text*

.Tserv options...TS Enabled=Yes,No

.Tserv options...Passwd=*text*

.Tserv options...Banner=*text*

.Tserv options...Prompt=*text*

.Tserv options...Term Type=*text*

.Tserv options...PPP=Yes,No

.Tserv options...SLIP=Yes,No

.Tserv options...SLIP BOOTP=Yes,No

.Tserv options...V42/MNP=Yes,No

.Tserv options...Telnet=Yes,No

.Tserv options...Def Telnet=Yes,No

.Tserv options...Clear Call=Yes,No

.Tserv options...Binary Mode=Yes,No

.Tserv options...Initial Scrn=Cmd,Menu

.Tserv options...Toggle Scrn=Yes,No

.Tserv options...Security=None,Partial,Full

.Tserv options...3rd Prompt=*text*

.Tserv options...Remote Conf=Yes,No

.Tserv options...Host #1 Addr=*dotted decimal format*

.Tserv options...Host #1 *Text=text*

.Tserv options...Host #2 Addr=*dotted decimal format*

.Tserv options...Host #2 *Text=text*

```
.Tserv options...Host #3 Addr=dotted decimal format
.Tserv options...Host #3 Text=text
.Tserv options...Host #4 Addr=dotted decimal format
.Tserv options...Host #4 Text=text
```
.Tserv options...Immed Telnet=Yes,No
.Tserv options...PPP Delay=Yes,No
.Tserv options...7-Even=Yes,No
.Tserv options...Login Case=L/P, l/p, L/p, l/P
.Tserv options...Ppp Info=Yes,No
.Tserv options...Clr Scrn=Yes,No
.Tserv options...Silent=Yes,No
.Bridging=Yes,No
.IPX Routing=Yes,No
.Shared Prof=Yes,No
```
.Telnet PW=text
```
.RIP Policy=Splt Hrzn,Poison Rvrs
.RIP Summary=Yes,No
.ICMP Redirects=Accept,Ignore
```
.DHCP Spoofing=Yes,No
.Spoof Adr=dotted decimal format/subnet mask
.Renewal Time=number
.DNS...Domain Name=text
.DNS...Pri DNS=dotted decimal format
.DNS...Sec DNS=dotted decimal format
.DNS...Pri WINS=dotted decimal format
.DNS...Sec WINS=dotted decimal format
```
.Acct...Acct= None,RADIUS
```
.Acct...Acct Host #1=dotted decimal format
.Acct...Acct Host #2=dotted decimal format
.Acct...Acct Host #3=dotted decimal format
.Acct...Acct Port=number
.Acct...Acct Timeout=number
.Acct...Acct Key=number
.Acct...Sess Timer=number
```
.Auth...Auth= None,TACACS,RADIUS,RADIUS/LOGOUT
```
.Auth...Auth Host #1=dotted decimal format
.Auth...Auth Host #2=dotted decimal format
.Auth...Auth Host #3=dotted decimal format
.Auth...Auth Port=number
.Auth...Auth Timeout=number
.Auth...Auth Key=number
```
.Auth...Auth Pool=Yes,No
.Auth...Auth Req=Yes,No
.Auth...APP Server=Yes,No
```
.Auth...APP Host=dotted decimal format
```

```
                           .Auth...APP Port=number
                           .Log...Syslog=Yes,No
                           .Log...Log Host=dotted decimal format
```
.Log...Log Facility=Local0,Local1,Local2,Local3,Local4,   Local5,Local6,Local 7
.Modem Ringback=Yes,No

Note:

• *s*00.ETHERNET...

 s = any slot into which the Ethernet expansion module is installed.

For example:

 : GET 200.ETHERNET.0.MODULE NAME

 ```
 200.ETHERNET.0.MODULE NAME=Tom's access device
 ```

:FILT=<type>

```
s00.FILT.n.Name=text
```
.In Filter 01...Valid=Yes,No
.In Filter 01...Type=Generic,Ip
.In Filter 01...Generic...Forward=Yes,No
```
    .In Filter 01...Generic...Offset=number
    .In Filter 01...Generic...Length=number
```
.In Filter 01...Generic...Mask= hexadecimal string
.In Filter 01...Generic...Value= hexadecimal string
.In Filter 01...Generic...Compare= ==, !=
.In Filter 01...Generic...More=Yes,No
.In Filter 01...Ip...Forward=Yes,No
```
    .In Filter 01...Ip...Src Mask=dotted decimal format
    .In Filter 01...Ip...Src Adrs=dotted decimal format
    .In Filter 01...Ip...Dst Mask=dotted decimal format
    .In Filter 01...Ip...Dst Adrs=dotted decimal format
    .In Filter 01...Ip...Protocol=number
```
.In Filter 01...Ip...Src Port Cmp=None,Less,Eql,Gtr,Neq
```
    .In Filter 01...Ip...Src Port #=number
```
.In Filter 01...Ip...Dst Port Cmp=None,Less,Eql,Gtr,Neq
```
    .In Filter 01...Ip...Dst Port #=number
```
.In Filter 01...Ip...TCP Estab=Yes,No
.Out Filter 01...Valid=Yes,No
.Out Filter 01...Valid=Yes,No
.Out Filter 01...Type=Generic,Ip
.Out Filter 01...Generic...Forward=Yes,No
```
    .Out Filter 01...Generic...Offset=number
    .Out Filter 01...Generic...Length=number
```
.Out Filter 01...Generic...Mask= hexadecimal string
.Out Filter 01...Generic...Value= hexadecimal string
.Out Filter 01...Generic...Compare= ==, !=

.Out Filter 01...Generic...More=Yes,No

.Out Filter 01...Ip...Forward=Yes,No

`.Out Filter 01...Ip...Src Mask=`*dotted decimal format*

`.Out Filter 01...Ip...Src Adrs=`*dotted decimal format*

`.Out Filter 01...Ip...Dst Mask=`*dotted decimal format*

`.Out Filter 01...Ip...Dst Adrs=`*dotted decimal format*

`.Out Filter 01...Ip...Protocol=`*number*

.Out Filter 01...Ip...Src Port Cmp=None,Less,Eql,Gtr,Neq

`.Out Filter 01...Ip...Src Port #=`*number*

.Out Filter 01...Ip...Dst Port Cmp=None,Less,Eql,Gtr,Neq

`.Out Filter 01...Ip...Dst Port #=`*number*

.Out Filter 01...Ip...TCP Estab=Yes,No

(.In/Out Filter 02 through 12... same as .In/Out Filter 01...)

Note:

- This type applies to the MAX equipped with an Ethernet module.

- *s*00.FILT.*n*...

  s = slot into which the Ethernet card is installed

  n = 0 to 15

FR

*s*00.FR.0.Name=*text*

.Active=Yes,No

.Call Type=Nailed,Switched

`.Nailed Grp=`*number*

.Data Svc=Voice,56KR,56K,64K,384KR,
384K,1536K,1536KR,128K,192K,256K,320K,448K,
512K,576K,640K,704K,768K,832K,896K,960K,1024K,
1088K,1152K,1216K,1280K,1344K,1408K,1472K

.PRI # Type=Unknown,Intl,National,Local,Abbrev

`.Dial #=`*number*

`.Bill #=`*number*

`.Call-by-Call=`*number*

`.Transit #=`*number*

.Link Mgmt=T1.617D,None

`.N391=`*number*

`.N392=`*number*

`.N393=`*number*

`.T391=`*number*

`.N392=`*number*

`.MRU=`*number*

Note:

- This type applies to the MAX equipped with the Ethernet module.

- HOSTN

`s00.HOST2.0.Module Name=`*text*
    .Dual Port=No Dual,1&2 Dual
    .Palmtop=Full,Restrict
    `.Palmtop Port #=`*number*
    .Palmtop Menus=Standard,Limited,MIF

`200.HOST4.0.Dual Port=No Dual,1&3 Dual,2&4 Dual,All Dual`
    .F Palmtop=Full,Restrict
    `.F Palmtop Port #=`*number*
    .F Palmtop Menus=Standard,Limited,MIF
    .L Palmtop=Full,Restrict
    `.L Palmtop Port #=`*number*
    .L Palmtop Menus=Standard,Limited,MIF
    .R Palmtop=Full,Restrict
    `.R Palmtop Port #=`*number*
    .R Palmtop Menus=Standard,Limited,MIF

`s00.HOST6.0.Module Name=`*text*
    .Port 1/2 Dual=Yes,No
    .Port 3/4 Dual=Yes,No
    .Port 5/6 Dual=Yes,No

Note:

- *s*00.HOST2...
  s = 2 or any slot in which a Host/Dual serial host expansion module is installed.
- *s*00.HOST6...
  s = any slot in which a Host/6 serial host expansion module is installed.

LINE

For units that interface to T1/PRI lines:

s`00.LINE.`*n*`.Name=`*text*
    .2nd Line=Disabled,D&I,Trunk
    `.2nd Line=Yes,No` (E1 units only)
    .Line 1...Sig Mode=Inband,ISDN,PBX T1,ISDN_NFAS
    `.Line 1...NFAS_ID num=`*number*
    .Line 1...Rob Ctl=Wink-Start,Idle-Start,Inc-W-200,Inc-W-400, Loop-Start
    .Line 1...Switch Type=AT&T,NTI,GloBanD,Japan,NI-2
    .Line 1...Framing Mode=D4,ESF
    .Line 1...Encoding=AMI,B8ZS,None
    `.Line 1...FDL=None,AT&T,ANSI,Sprint`
    .Line 1...Length=1-133,134-266,267-399,400-533,534-655
    .Line 1...Buildout=0 db,7.5 db,15 db,22.5 db
    .Line 1...Clock Source=Yes,No
    .Line 1...PBX Type=Voice,Data,Leased 1:1
    `.Line 1...Delete Digits=`*number*

```
.Line 1...Add Number=
```
.Line 1...Call-by-Call=number
```
.Line 1...Ans #=
```
phone number

.Line 1...Ans Service=Voice,56KR,56K,64K,384KR,384K,
1536K,1536KR,128K,192K,256K,320K,448K,512K,576K,
640K,704K,768K,832K,896K,960K,1024K,1088K,1152K,
1216K,1280K,1344K,1408K,1472K

.Line 1...Ch 1=Unused,Switched,D&I,Nailed,D-channel
```
.Line 1...Ch 1 #=number
.Line 1...Ch 1 Slot=number
.Line 1...Ch 1 Prt/Grp=number
.Line 1...Ch 1 TrnkGrp=number
```

(.Line 1...Ch 2 through Ch 23 same as Ch 1)

.Line 1...Ch 24=Unused,Switched,D&I,Nailed,D-channel, NFAS-Prime,NFAS-Second
```
.Line 1...Ch 24 #=number
.Line 1...Ch 24 Slot=number
.Line 1...Ch 24 Prt/Grp=number
.Line 1...Ch 24 TrnkGrp=number
```

(.Line 2... same as Line 1...)

For units that interface to BRI lines:
```
100.LINE.n.Name=text
```
.Switch Type=AT&T,NTI,NI1,FRANC,U.K.,JAPAN,BELGI,AUSTR,SWISS,
GERMAN,DUTCH, NET 3
.Line 1...Enabled=Yes,No
.Line 1...LinkType=P_T_P,Multi_P
.Line 1...B1 Usage=Unused,Switched,Nailed
```
.Line 1...B1 Prt/Grp=number
```
.Line 1...B2 Usage=Unused,Switched,Nailed
```
.Line 1...B2 Prt/Grp=number
.Line 1...Pri Num=phone number
.Line 1...Pri SPID=number
.Line 1...Sec Num=phone number
.Line 1...Sec SPID=number
```

(.Line 2... through .Line 8... same as Line 1...)

For units that interface to Switched-56 lines:
```
100.LINE.n.Name=text
```
.Line 1...Enabled=Yes,No
.Line 1...Ch Usage=Unused,Switched,Nailed
```
.Line 1...Phone Num=phone number
```

```
.Line 1...Port/Grp=number
```

(.Line 2... through .Line 7... same as Line 1...)

For units that interface to E1/PRI lines:

*s*00.LINE.*n*.Name=*text*

    .Line 1...Sig Mode=ISDN,None,DPNSS

    .Line 1...Switch Type=NTI,French,German,GloBanD,Net 5, Australian,DASS 2,ISDX,ISLX,MERCURY

    .Line 1...L2=A END,B END

    .Line 1...L3=X END,Y END

    `.Line 1...NL Value=`*number*

    `.Line 1...LoopAvoidance=`*number*

    .Line 1...Framing Mode=G.703,2DS

    .Line 1...Clock Source=Yes,No

    .Line 1...Ch 1=Unused,Switched,Nailed

    `.Line 1...Ch 1 #=`*number*

    `.Line 1...Ch 1 Slot=`*number*

    `.Line 1...Ch 1 Prt/Grp=`*number*

    `.Line 1...Ch 1 TrnkGrp=`*number*

(.Line 1...Ch 2 to Ch 15 and Ch 17 to Ch 31 same as Ch 1)

    .Line 1...Ch 16=D-channel

    . Line 1...Ch 16 #=N/A

    .Line 1...Ch 16 Slot=N/A

    .Line 1...Ch 16 Prt/Grp=N/A

    .Line 1...Ch 16 TrnkGrp=N/A

(.Line 2... same as Line 1...)

Note:

- *s*00.LINE.*n*...

  s = 1 or any slot in which a WAN (line) module is installed.

  n = 0 through 3, where 0 is the current Line Profile.

For example:

    : LOAD 100.LINE.1

    :

LMODEM

LMODEM applies MAX units with digital modems only.

*s*00.LMODEM.0.Module Name=*text*

    .Ans 1#=*phone number*

```
.Ans 2#=phone number
.Ans 3#=phone number
.Ans 4#=phone number
```

Note:

- *s*00.LMODEM...

  s = any slot in which a LAN modem (digital modem) module is installed.

LOOP

```
spp.LOOP.0.Local LB=Yes,No
    .DSR=Active,Inactive (read) Toggle (write)
    .RI=Active,Inactive (read) Toggle (write)
    .CD=Active,Inactive (read) Toggle (write)
    .DLO=Active,Inactive (read) Toggle (write)
    .PND=Active,Inactive (read) Toggle (write)
    .ACR=Active,Inactive (read) Toggle (write)
    .Inc Ch Count=Yes (write only)
    .Dec Ch Count=Yes (write only)
    .Rate=64K,56K (read) Toggle (write)
```

Note:

- *spp*.LOOP...

  s = 1 or any slot in which a serial host expansion module is installed.

  pp = 01 through last serial host port.

- Active/Inactive and 64K/56K are <value>s only for read commands such as GET.

- Toggle is a <value> only for write commands such as SET.

- SET `spp.LOOP.0.Local LB=Yes` must be commanded before any other LOOP commands, such as RI, CD, etc.

- The <value> Toggle in a SET command changes the state of the addressed entity from it current state to another state, i.e., from Active to Inactive or from Inactive to Active.

For example:

```
: SET 202.LOOP.0.DSR=Toggle
+ ERROR
: SET 202.LOOP.0.Local LB=Yes
: SET 202.LOOP.0.DSR=Toggle
:
```

PORT

```
spp.PORT.0.Port Name=text
    .Ans 1#=phone number
    .Ans 2#=phone number
    .Ans 3#=phone number
    .Ans 4#=phone number
```

.Idle=None,Call

.Dial=Terminal,DTR Active,RS-366 Ext1,RS-366 Ext2,V.25bis,

V.25bis-C,X.21 Ext1,X.21 Ext2,X.21 Ext1-P

.Answer=Auto,DTR Active,DTR+Ring,V.25bis,V.25bis-C,Terminal,

X.21,P-Tel Man,None

.Clear=DTR Inactive,DTR Active,RTS Inactive,RTS Active,

Terminal

.Term Timing=Yes,No

.RS-366 Esc=*,#,5,6,7,9,0,00

.Early CD=Answer,Originate,Both,No

.DS0 Min Rst=Monthly,Daily,Off

`.Max DS0 Mins=`*number*

`.Max Call Mins=`*number*

Note:

- *spp*.PORT...

   s = 1 or any slot in which a serial host expansion module is installed.

   pp = 01 through last serial host port.

For example:

   : LOAD 201.PORT.0

   : SET 201.PORT.0.Port Name=Chicago #1

   + ERROR

   : SET Port Name=Chicago #1

   : SAVE 200.PORT.0

   + ERROR

   : SAVE 201.PORT.0

   :

ROUTE

s`00.ROUTE.`*n*`.Name=`*text*

   .Active=Yes,No

   `.Dest=`*text in dotted decimal format/subnet mask*

   `.Gateway=`*text in dotted decimal format*

   `.Metric=`*number*

   .Private=Yes,No

Note:

- This type applies to the MAX equipped with the Ethernet module.

- *s*00.ROUTE.*n*...

   s = slot into which the Ethernet card is installed

   n = 0 to 63

- If n = 0, Name=Default and Dest=0.0.0.0/0

SEC

```
000.SEC.n.Name=text
    .Passwd=*SECURE*
    .Operations=Yes,No
    .Edit Security=Yes,No
    .Edit System=Yes,No
    .Edit Line=Yes,No
    .Edit All Port=Yes,No
    .Edit Own Port=Yes,No
    .Edit All Calls=Yes,No
    .Edit Com Call=Yes,No
    .Edit Own Call=Yes,No
    .Edit Cur Call=Yes,No
    .Sys Diag=Yes,No
    .All Port Diag=Yes,No
    .Own Port Diag=Yes,No
    .Download=Yes,No
    .Upload=Yes,No
    .Field Service=Yes,No
```

Note:

- 000.SEC.*n*...

  n = 0 through 8 (The default security profile is 0.)

- The command SAVE cannot be applied to a security profile address.

For example:

    : SAVE 000.SEC.8

    :

STAT

For all units:

```
000.STAT.0.Sys Options=
    n.Message Log= (n =0 through 31)
    0.Port Info=
    0.CDR=
```

For T1/PRI and E1/PRI units only:

```
s00.STAT.0.Line 1 Stat=
    0.Line 2 Stat=
    0.Line Errors=
    n.FDL1=(n=0 through 96) (not E1/PRI)
    n.FDL2=(n=0 through 96) (not E1/PRI)
    0.Net Options=
```

(*s*=1 or any other slot in which a T1/PRI module is installed in a MAX.

For BRI and Switched-56 units only:

```
100.STAT.0.Line 1 Stat=
    0.Line Errors=
    0.Net Options=
spp.STAT.0.Call Status=
    n.Message Log= (n=0 through 31)
    0.Statistics=
    0.Port Opts=
    0.Session Err=
    0.Port Leads=
```

s=2 or any other slot in which a serial host module is installed in a MAX. *pp*=01 through the last serial host port.

For units with Ethernet interface:

```
s00.STAT.0.Sessions=
    0.Routes=
    0.WAN Stat=
    0.Ether Stat=
    0.Ether Opt=
    0.Dyn Stat=
```

s=slot of a MAX in which the Ethernet module is installed.

Note:

- *n* can range from 0 through 96 for the FDL Status Screens. If *n* is 0, the last 24 hours are reported. 1 through 96 refer to the 15 minute time intervals occurring during the last 24 hours, with 1 being the most recent interval.

- Do not exceed 32,000 seconds when using SET to write to these addresses

- The GET command returns a multiple-line <value> when applied to a Status Screen <address>. Output from a status request is almost identical to the status display using the native mode user interface. The difference is that displays that would scroll (000.STAT.0.Sys Option, 100.STAT.0.Line Errors, etc.) have all lines listed. Each line of the multi-line response is separated by a <CR><LF> pair. Multi-line output is indicated by starting the value field of the response with a <CR><LF> pair.

- When you apply SET to CDR, all events that occurred during the time period are displayed. This is unlike other traps generated by SET. For example, SET 201.STAT.0.Port Leads=20 compares the Port Info screen at the beginning to the end of the 20 sec. time period; and if there is a difference, only the current Port Leads is displayed.

For example:

```
: GET 100.STAT.0.Line Errors
+ 100.STAT.0.Line Errors=
+ 01-005 Ln1 Ln2
+10 -
+2 10 -
:
```

: SET 000.STAT.0.CDR=1

For example:

: GET 600.STAT.0.Line 2 Stat

(Get status of line #2 in the module in slot 6.)

For example:

: GET 202.STAT.0.Call Status

(Get call status of serial host port #2.)

SYS

```
000.SYS.0.Name=text
```
.Location=*text* (Ethernet interface required)

.Contact=*text* (Ethernet interface required)

.Date=*mm/dd/yy*

.Time=*hh:mm:sec*

.Term Rate=300,1200,2400,4800,9600,19200,38400,57600

.Palmtop Rate=300,1200,2400,4800,9600,19200,38400,57600

.Console=Standard,Limited,MIF

.Remote Mgmt=Yes,No

.Parallel Dial=*number*

.Single Answer=Yes,No

.Sub-Adr=TermSel,Routing,None (T1/E1/BRI units only)

.DM=*number* (T1/E1/BRI units only)

.LAN=*number* (T1/E1/BRI units only)

.Serial=*number* (T1/E1/BRI units only)

.V110=*number*

.Use Trunk Grps=Yes,No (T1/PRI only)

.Excl Routing=Yes,No

.Auto Logout=Yes,No

.Idle Logout=*number*

.DS0 Min Rst=Monthly,Daily,Off

.Max DS0 Mins=*number*

.High BER=10 ** -3,10 ** -4,10 ** -5 (T1/PRI or E1/PRI only)

.High BER Alarm=Yes,No (T1/PRI or E1/PRI only)

.No Trunk Alarm=Yes,No (T1/PRI or E1/PRI only)

.Delay Dual=Yes,No

.Edit=*XN-n00* (menu number for an edit screen)

.Status 1=*XN-n00* (menu number for a status screen)

.Status 2=*XN-n00* " "

.Status 3=*XN-n00* " "

.Status 4=*XN-n00* " "

.Status 5=*XN-n00* " "

.Status 6=*XN-n00* " "

.Status 7=*XN-n00* " "

```
                              .Status 8=XN-n00 " "
```

For example:

```
    : GET 000.SYS.0.Name
    + =kansas BRI
```

TRAP

```
s00.TRAP.n.Name=text
    n.Alarm=Yes,No
    n.Port=Yes,No
    n.Security=Yes,No
    n.Comm=dotted decimal format
    n.Dest=dotted decimal format
```

Note:

• This type applies to the MAX equipped with the Ethernet module.

• *s*00.TRAP.*n*...

    s = slot into which the Ethernet card is installed

    n = 0 to 7

V110

V110 applies to MAX units with V.110 modules only.

```
s00.V110.0.Module Name=text
    .Ans 1#=phone number
    .Ans 2#=phone number
    .Ans 3#=phone number
    .Ans 4#=phone number
```

Note:

• *s*00.V110...

    s = any slot in which a V.110 module is installed.

Index