Lucent Technologies
Bell Labs Innovations

MAX™

Reference

Part Number: 7820-0647-004
For software version 9.0
January 2001

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of printing, but information is subject to change.

Safety, Compliance, and Warranty Information

Before handling any Lucent Access Networks hardware product, read the *Access Networks Safety and Compliance Guide* included in your product package. See that guide also to determine how products comply with the electromagnetic interference (EMI) and network compatibility requirements of your country. See the warranty card included in your product package for the limited warranty that Lucent Technologies provides for its products.

Security Statement

In rare instances, unauthorized individuals make connections to the telecommunications network through the use of access features.

Trademarks

Copyrights for Third-Party Software Included in Lucent Access Networks Software Products

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

Tables

About This Reference

This reference provides an alphabetical list of all the MAX profiles, parameters, and commands, and details the settings and options you can specify. For step-by-step instructions on setting up the MAX hardware, see the *Hardware Installation and Basic Configuration Guide* for your MAX 6000, MAX 3000, or MAX 800. For step-by-step instructions on configuring your network connections, see the network configuration guide for your MAX product.

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

Warning: Read the safety instructions in the *Edge Access Safety and Compliance Guide* before installing the product.

What you should know

This reference is intended for the person who will configure and maintain the MAX 6000, MAX 3000, or MAX 800 unit's data network environment. To use it effectively, you must have a basic understanding of local area network (LAN) and wide are network (WAN) concepts, and be familiar with authentication servers and networking operation.

What is in this reference

This guide is organized as follows:

- Chapter 1, "Status-Window Reference," describes in detail the contents of each status window that appears on the MAX VT100 interface.
- Chapter 2, "DO Menu Commands," describes the context-sensitive commands that appear when you press Ctrl-D.
- Chapter 3, "Terminal-server commands," describes the terminal-server command line interface (CLI) commands you use for monitoring networks, initiating sessions, and managing the system.
- Chapter 4, "VT100 Interface Parameters," describes all command parameters in alphabetical order.

This reference also includes an index.

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 bold type.
|	Separates command choices that are mutually exclusive.
>	Points to the next level in the path to a parameter or menu item. The item that follows the angle bracket is one of the options that 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.

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

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*
- 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* (this manual)
- The *MAX Security Supplement*
- The *TAOS Glossary*
- The *TAOS RADIUS Guide and Reference*

Status-Window Reference

1

The right side of the screen in the MAX VT100 interface displays eight status windows. The status windows display read-only information about what is currently happening in the MAX. This chapter describes in detail the contents of each status window that appears on the MAX VT100 interface. It lists the windows in alphabetic order.

Call Detail Reporting (CDR) window

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

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

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

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

Following is a sample four-line CDR display:

```
00-400 CDR
  3:05:28:10:33:52
  OR 025 384KR 02-01
  15105551212
```

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

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

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

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

Item	Description
CDR event description	Consists of one of the following abbreviations: • OR—Originated (outgoing call) • AN—Answered (incoming call) • AP—Assigned to Port or module (incoming call) • CL—Cleared • OF—Overflowed All events except OF are associated with calls. OF indicates that the CDR buffer overflowed because events occurred faster than the MAX could report them.
CDR event ID	The MAX creates a new event ID for every DS0 channel originating a connection. The event ID ranges from 0 to 255. Events after 255 start the count again at 0. In addition, CDR creates a new event ID for every change in a channel's status. Because a MAX call can consist of several channels, the MAX can generate multiple CDRs for every change in call status.
Data service in use	Indicates the data service, using values nearly identical to those available to the Data Svc parameter in the Call profile. The only difference is that the Data Svc values 384K/H0 and 1536K correspond to the CDR data service values 384K and 1536KR, respectively.

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

Dyn Stat window (dynamic status)

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

Following is the Dyn Stat display for an Ethernet module in slot 4:

```
40-500 Dyn Stat
  Qual Good 00:02:03
  56K     1 channels
  CLU  12%  ALU  23%
```

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

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

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

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

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

The fourth line displays the following values:

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

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

Ether Opt window (Ethernet options)

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

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

```
90-700 Ether Opt
 >I/F: UDP
  Adrs: 00c07b7aac5b
```

The interface type may be AUI, UTP, or COAX. The MAC address is a 6-byte hexadecimal address assigned to the Ethernet controller by the manufacturer.

Ether Stat window (Ethernet status)

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

For example, the following screen shows the Ether Stat display for an Ethernet module in slot 4:

```
40-400 Ether Stat
 >Rx Pkt:      106
  Tx Pkt:      118
  Col:        0
```

The screen shows the following fields:

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

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

Ethernet window

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

```
40-000 Ethernet
  40-100 Sessions
  40-200 Routes
  40-300 WAN Stat
  40-400 Ether Stat
  40-500 Dyn Stat
  40-600 FR Stat
  40-700 Ether Opt
```

FDL N Stats windows

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

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

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

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

```
10-000 Net/T1
  10-100 Line 1 Stat
  10-200 Line 2 Stat
  10-300 Line 3 Stat
  10-400 Line Errors
```

```
 >10-500 FDL1 Stats
  10-600 FDL2 Stats
  10-700 FDL3 Stats
  10-800 Net Options
```

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

```
10-600 FDL2 Stats
 >Error Events...
  Current Period...
  Last 24 Hours...
  00:00...
  01:00...
  ...
  ...
  23:00...
```

Note: Pressing the Down Arrow key displays additional statistics.

Error-register statistics

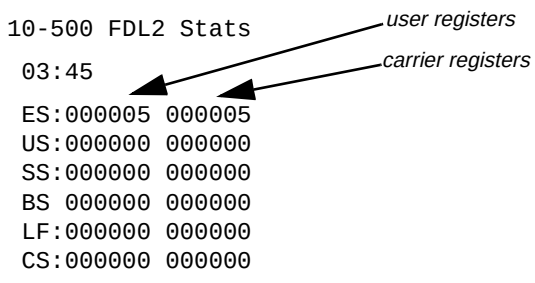
If you select Error Events, the MAX displays the accumulated error events in the user and carrier error events registers.

Performance register statistics

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

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

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



Use the Clr Perf1, Clr Perf2 and Clr Perf3 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 1-1 describes the FDL performance registers.

Table 1-1. FDL performance registers

Register name	Description
EE	Displays the number of error events accumulated since the last time this register was reset. An ESF error event is counted when the CRC-6 calculations at the receiving end of the T1 span do not match the CRC-6 calculations at the sending end. This mismatch indicates that the frame had at least one data error. Error events have no meaning for D4 lines. Only ESF lines carry the CRC-6 signature used to check the quality of the PRI line as a whole.
ES	Specifies errored seconds. For ESF lines, this register displays the number of seconds in the 15-minute period in which there was at least one error event, or in which two or more framing errors were detected within a 3 ms interval. For D4 lines, this register displays the number of seconds in which one or more framing bit errors (FE) were detected or in which a controlled slip (CS) occurred.
US	Indicates unavailable seconds—the number of seconds in the 15-minute period preceded by at least 10 consecutive severely errored seconds (SS).
SS	Displays severely errored seconds—the number of seconds, during the 15-minute period, in which there were at least 320 CRC-6 errors as detected by the MAX, or in which the T1 line was out of frame. For D4 lines, this register displays the number of one-second intervals containing eight or more framing bit errors (FEs) or one or more SEFs.
BS	Specifies bursty errored seconds—the number of seconds, during the 15-minute period, in which there were at least 2, but not more than 319, CRC-6 errors as detected by the MAX.
LF	Indicates loss of frame seconds— the number of seconds in the 15-minute period in which the T1 line was out of frame.
CS	Displays controlled slip seconds—the number of seconds in the 15-minute period in which a frame was either replicated or deleted.

FR Stat window

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

For example, the following screen shows an FR Stat profile display for a link using a serial WAN module is installed in slot 4:

```
40-600 FR Stat profile
  Rx Pxt:    2560
```

```
  Tx Pxt:    3000
    CRC:      003
CprofX         16
  Rx Pxt:    2560
  Tx Pxt:    3000
```

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

Line Errors window

The Line Errors status window shows errors recorded on all current channels, in a channel-by-channel, line-by-line list. 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 3 Stat
  10-400 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 the following columns. For example:

```
10-400 Ln1  Ln2   L3
  1:    0    -     0
  3:    33   -     0
  4:    0    -     0
```

The first column displays the T1 channel number followed by a colon (:).

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. The fourth column displays the number of byte errors the MAX has detected on the channel in Line 3 during the current call.

If a channel is not associated with a current call, a hyphen (-) appears instead of a number. The window does not display a channel that does not have an active call nor any byte errors to report.

Line Status windows

The Line Stat windows (Line 1 Stat, Line 2 Stat, Line 3 Stat) show the dynamic status of each WAN line, the condition of its electrical link to the carrier, and the status of its individual channels. To display the Line Status window, tab to a status window, then use the arrow keys to access the Net/T1 > Line *N* Stat (or Net/E1 >Line *N* Stat) window.

For example:

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

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

The second line begins with the line number, followed by the link status, which is indicated by one of the two-character abbreviations listed in Table 1-2. The link status is followed by a single character that indicates channel status. Table 1-3 lists the channel-status indicators. The third line has column headers for the remaining channels. The fourth line continues where the second line left off, showing the status of the remaining channels.

Table 1-2. T1/E1 link-status indicators

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

A single character represents the status of each channel in the line, as described in Table 1-3:

Table 1-3. T1 channel status indicators

Channel status	Mnemonic	Description
. (period)	Not available (Off-hook)	The channel is not available (or off-hook) because the line is disabled, has no physical link, or does not exist, or because the channel is set to Unused in the Ch *N* parameter of the Line *N* profile.
= (equals)	Connected	For Analog FXS only, indicates that the channel is connected in a current call.
* (asterisk)	Current	The channel is connected in a current call.
- (dash)	Idle	The channel is currently idle (but in service).
d	Dialing	The MAX is dialing from this channel for an outgoing call.
r	Ringing	The channel is ringing for an incoming call.
m	Maintenance	The channel is in maintenance/backup (ISDN only).
n	Nailed	The channel is marked Nailed in the Line *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).

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

Log messages

Table 1-4 shows the informational messages that can appear in the Message Log window:

Table 1-4. Informational log messages

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

Table 1-4. Informational log messages (continued)

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

Table 1-5 shows the warning messages that can appear in the Message Log windows.

Table 1-5. Warning log messages

Message	Description
`Busy`	The phone number was busy when the call was dialed.
`Call Disconnected`	The call has ended unexpectedly.
`Call Refused`	An incoming call could not be connected to the specified digital modem, packet-handling module, or terminal server because the resource was busy or otherwise unavailable.
`Dual Port req'd`	The call could not be placed because one or both ports of the dual-port pair were not available.
`Far End Hung Up`	The remote end terminated the call normally.
`Incoming Glare`	The MAX could not place a call because it saw an incoming *glare* signal from the switch. Glare occurs when you attempt to place an outgoing call and answer an incoming call simultaneously. If you receive this error message, you have probably selected incorrect settings in the Line *N* profile.
`Internal Error`	Call setup failed because of a lack of system resources. If this type of error occurs, notify Lucent Customer Service.

Table 1-5. Warning log messages (continued)

Message	Description
`LAN security error`	Appears after Incoming Call but before Call Terminated if a PPP, MP+, terminal-server, or Combinet session has failed authentication, another session by the same name already exists, or the timeout period for RADIUS/TACACS authentication has been exceeded. For details, see the Auth Timeout entry on page 4-39.
`Network Problem`	The call setup was faulty because of problems within the WAN or in the Line *N* profile configuration. The D channel might be getting an error message from the switch, or the telco might be experiencing a problem.
`No Chan Other End`	No channel was available on the remote end to establish the call.
`No Channel Avail`	No channel was available to dial the initial call.
`No Connection`	The remote end did not answer when the call was dialed.
`No Phone Number`	No phone number exists in the Call profile being dialed.
`No port DSO Mins`	No maximum has been specified for the MAX DS0 Mins or MAX Call Mins parameter in the Port profile.
`No System DSO Mins`	No maximum has been specified for the MAX DS0 Mins parameter in the System profile.
`Not Enough Chans`	A request to dial multiple channels or to increase bandwidth could not be completed because there were not enough channels available.
`Not FT1-B&O`	The local MAX attempted to connect an FT1-B&O call to the remote end, but the call failed because the call type at the remote end was not FT1-B&O.
`Request Ignored`	The MAX denied a request to manually change bandwidth during a call because the Call Mgm parameter in the Call profile is set to Dynamic. With this setting, the MAX allows only automatic bandwidth changes.
`Wrong Sys Version`	The remote-end product version was incompatible with the version of the local MAX. The software version appears on the Sys Option status window.

Table 1-6 shows connection messages that can appear on the fourth line of the Message Log windows.

Table 1-6. Message indicators

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

Net T1 and Net E1 windows

Net/T1 and Net/E1 windows are branches of the Main Status Menu window.

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

```
10-000  Net/T1
  10-100 Line 1 Stat
  10-200 Line 2 Stat
  10-300 Line 3 Stat
  10-400 Line Errors
  10-500 FDL1 Stats
  10-600 FDL2 Stats
  10-700 FDL3 Stats
  10-800 Net Options
```

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

```
10-000 Net/E1
  10-100 Line 1 Stat
 >10-200 Line 2 Stat
  10-300 Line Errors
  10-400 Net Options
```

Net Options window

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

The following screen shows the Net Options window:

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

The first line shows the type of physical interface to the WAN. The line can specify 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. Following are the values that can appear:

- Type—DSX/DSX
- Type—CSU/DSX
- Type—DSX/CSU
- Type—CSU/CSU

Routes window

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

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

```
40-200 Routes
 >D: 223.0.100.129
  G: 223.0.100.129
  LOOP Active
```

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

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

The third line shows the address of the router.

The fourth line can have one of the values listed in Table 1-7.

Table 1-7. Routes-window values

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

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

Serial WAN window

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

Session Err window

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

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

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

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

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

(For related information, see “Line Errors window” on page 1-7.)

Sessions window

The Sessions status window indicates the number of active bridging/routing links or remote terminal-server sessions. An online link, as configured in the Connection profile, constitutes a single active session. A session can be PPP or Combinet-encapsulated. The MAX treats each multichannel MP+ or MP link as a single session. The following screen shows the display when the Ethernet module is installed in slot 4:

```
40-100 Sessions
 >5 Active
  O Headquarters
```

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

status remote device

where *status* is a status indicator and *remote device* is the name, address, or CLID of the remote device. Table 1-8 lists the session-status characters that can appear.

Table 1-8. Session status characters

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

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

Syslog window

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

Level 4 and Level 6 Syslog messages

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

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

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

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

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

Level 5 Syslog messages

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

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

- *`call-event-ID`* specifies the event ID in the CDR display.
- *`event description`* is a description of the CDR event.
- *`data-svcK`* indicates the data service in use.
- *`phone-N`* is the phone number.

Example

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

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

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

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

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

Disconnect codes and Progress codes

If the Syslog option is set, a Call-Close (CL) message is sent to the `Syslog` daemon whenever a connection is closed. Additional information about the user name, Disconnect code, Progress code, and login host is appended to each CL message. The CL message uses the following format:

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

where:

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

Table 1-9 lists the Lucent Disconnect codes.

Table 1-9. Lucent Disconnect codes

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

Table 1-9. Lucent Disconnect codes (continued)

Disconnect code	Description
21	Terminal server timed out waiting for user input.
22	Forced disconnect when exiting Telnet session.
23	No IP address available when invoking PPP or SLIP command.
24	Forced disconnect when exiting raw TCP session.
25	Exceeded maximum login attempts.
26	Attempted to start a raw TCP session, but raw TCP is disabled on MAX.
27	Control-C characters received during login.
28	Terminal-server session cleared ungracefully.
29	User closed a terminal-server virtual connection normally.
30	Terminal-server virtual connect cleared ungracefully.
31	Exit from Rlogin session.
32	Establishment of rlogin session failed because of bad options.
33	MAX lacks resources to process terminal-server request.
35	MP+ session cleared because no null MP packets received. A MAX sends (and should receive) null MP packets throughout an MP+ session.
40	LCP timed out waiting for a response.
41	LCP negotiations failed, usually because user is configured to send passwords via PAP, and MAX is configured to only accept passwords via CHAP (or vice versa).
42	PAP authentication failed.
43	CHAP authentication failed.
44	Authentication failed from remote server.
45	MAX received Terminate Request packet while LCP was in open state.
46	MAX received Close Request from upper layer, indicating graceful LCP closure.

Table 1-9. Lucent Disconnect codes (continued)

Disconnect code	Description
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.
100	Session timed out.
101	Invalid user.
102	Callback enabled.
105	Session timeout on the basis of encapsulation negotiations.
106	MP session timeout.
115	Instigating call no longer active.
120	Requested protocol is disabled or unsupported.

Table 1-9. Lucent Disconnect codes (continued)

Disconnect code	Description
150	Disconnect requested by RADIUS server.
151	Call disconnected by local administrator.
152	Call disconnected via SNMP.

Table 1-10 lists the Lucent Progress codes.

Table 1-10. Lucent Progress codes

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

Table 1-10. Lucent Progress codes (continued)

Progress code	Description
63	Opening IPNCP.
64	Opening BNCP.
65	LCP opened.
66	CCP opened.
67	IPNCP opened.
68	BNCP opened.
69	LCP in Initial state.
70	LCP in Starting state.
71	LCP in Closed state.
72	LCP in Stopped state.
73	LCP in Closing state.
74	LCP in Stopping state.
75	LCP in Req-Sent state.
76	LCP in Ack-Rcvd state.
77	LCP in Ack-Sent state.
80	IPX NCP in Open state.
81	AT NCP in Open state.
82	BACP being opened.
83	BACP is now open.
84	CBCP being opened.

The backoff queue error message in the Syslog file

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

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

This error generally occurs for one of the following reasons:

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

Syslog messages initiated by a SecureConnect Manager firewall

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

`date time router name ASCEND: interface message`

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

The message fields appear in the following order:

`protocol local direction remote length frag log tag`

Table 1-11 describes the fields.

Table 1-11. Syslog message fields for SecureConnect firewalls

Field	Description
`protocol`	The four-character (hexadecimal) Ether Type or one of the following network protocol names: ARP, RARP, IPX, Appletalk. For IP protocols, the field contains either the IP protocol number (up to three decimal digits) or one of the following names: IP-IN-IP, TCP, ICMP, UDP, ESP, AH. In the special case of ICMP, the field also includes the ICMP Code and Type ([*`Code`*]/[*`Type`*]/`icmp`).
`local`	For non-IP packets, *`local`* is the source Ethernet MAC address of transmitted packets and the destination Ethernet MAC address of received packets. For a nonbridged WAN connection, the two MAC addresses are all zeros. For IP protocols, *`local`* is the IP source address of transmitted packets and the IP destination address of received packets. In the case of TCP or UDP, it also includes the TCP or UDP port number ([*`IP-address`*];[*`port`*]).
`direction`	An arrow (<- or ->) indicating the direction in which the packet was traveling (receive and send, respectively).

Table 1-11. Syslog message fields for SecureConnect firewalls (continued)

Field	Description
remote	For non-IP protocols, *remote* has the same format that *local* has for non-IP packets, but shows the destination Ethernet MAC address of transmitted packets and the source Ethernet MAC address of received packets. For IP protocols, *remote* has the same format as *local* but shows the IP destination address of transmitted packets and the IP source address of received packets.
length	The length of the packet in octets (8-bit bytes).
frag	Indicates that the packet has a nonzero IP offset or that the IP More-Fragments bit is set in the IP header.
log	Reports one or more messages based on the packet status or packet header flags. The packet status messages include: • corrupt—the packet is internally inconsistent • unreach—the packet was generated by an "unreach=" rule in the firewall • !pass—the packet was blocked by the data firewall • bringup—the packet matches the call firewall • !bringup—the packet did not match the call firewall • syn, fin, rst—TCP flag bits. The syn bit is only displayed for the initial packet, which has the syn flag set instead of the ack flag set.
tag	Any user-defined tags specified in the filter template used by SCM

Sys Option status window

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

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

Table 1-12 describes the information that the Sys Option status window can contain:

Table 1-12. Sys Option system status information

Option	Description
`Security Prof: 1`, `Security Prof: 2...`	Shows which of the nine Security profiles is active.
`Software`	Defines the version and revision of the system ROM code.
`S/N`	Displays the serial number of the MAX. The serial number of your MAX can also be found on the model number/serial number label on the MAX unit's bottom panel.
`Up:uptime`	Displays the system uptime in the following format: Up: *days*:*hours*:*minutes*:*seconds* For example: `Up: 13:12:18:26` The Days value *turns over* every 999 days. If the unit stays up continuously for 1000 days, the initial field resets to a 0 and begins incrementing again.
`MAX 6000` or `MAX 3000` or `MAX 800`	Identifies the MAX unit. **Note:** If you have a MAX running Multiband Simulation, the name that appears here is Multiband MAX 6000.
`Load`	Indicates the software load name. Lucent software releases are distributed in software loads, which vary according to the functionality and target platform for the binary.
`Switched Installed` or `Switched Not Inst`	Indicates whether the MAX can place calls over switched circuits.
`Frm Rel Installed` or `Frm Rel Not Inst`	Indicates whether the Frame Relay option is installed.
`Sec Acc Installed` or `Sec Acc Not Installed`	Indicates whether the Secure Connect Firewall option is installed.
`IPsec - Unlimited`	Indicates that IPsec is unlimited on the unit.
`MAX Link Installed` or `MAX Link Not Inst`	Indicates whether the MAX Link option is installed.

Table 1-12. Sys Option system status information (continued)

Option	Description
`PRI <-> T1 Installed` or `PRI <-> T1 Not Inst`	Indicates whether the PRI to T1 signaling option is installed. The option is used for PBX support.
`MAXDAX Installed` or `MAXDAX Not Installed`	Indicates whether the MAXDAX feature is installed on the unit.
`MEGAMAX Installed` or `MEGAMAX Not Inst`	Indicates whether the MegaMax MP+ feature is installed.
`MRate Installed` or `MRate Not Installed`	Indicates whether the unit supports MultiRate and GloBanD ISDN data services. Currently, T1 PRI providers in the U.S. do not support GloBanD.
`RS-366 Installed` or `RS-366 Not Inst`	Indicates whether the EIA RS-366 dialing protocol has been installed.
`Dyn Bnd Installed` or `Dyn Bnd Not Inst`	Indicates whether Dynamic Bandwidth Allocation functionality is available.
`ISDN Sig Installed` or `ISDN Sig Not Installed`	Indicates whether ISDN signaling is installed on the unit.
`AIM Nx56 Installed` or `AIM Nx56 Not Installed`	Indicates whether AIM Nx56 is installed on the unit.
`BONDING Installed` or `BONDING Not Inst`	Indicates whether BONDING functionality is available.
`V.25bis Installed` or `V.25bis Not Inst`	Indicates whether the CCITT V.25 bis dialing and answering protocol is installed.
`X.21 Installed` or `X.21 Not Inst`	Indicates whether the X.21 dialing and answering protocol is installed.
`MAX Dial Installed` or `MAX Dial Not Inst`	Indicates whether the MAX Dial client software option is installed.

Table 1-12. Sys Option system status information (continued)

Option	Description
`Selectools: Installed` or `Selectools Not Installed`	Indicates whether the unit supports Selectools services.
`AuthServer: a.b.c.d`	Shows the IP address of the current RADIUS authentication server for this unit.
`AcctServer: a.b.c.d`	Shows the IP address of the current RADIUS accounting server for this unit.
`Dual Slot T1`	Does not apply to this version of the MAX.
`Data Call`	Indicates whether the Hybrid Access option is installed.
`SerialPortT1-CSU`	Indicates whether the nailed T1 (or E1) line is installed. Does not apply to E1 units.
`K56 Slot Card Only Installed` or `K56 Slot Card Only Not Installed`	Indicates whether the unit supports only K56 slot cards.
`AO/DI Installed` or `AO/DI Not Inst`	Indicates whether Always On/Dynamic ISDN (AO/DI) is installed on the unit.
`PHS Installed` or `PHS Not Inst`	Indicates whether Personal Handy Phone services (PHS) are installed on the unit.
`PHS_2_1 Installed` or `PHS_2_1 Not Inst`	Indicates whether Personal Handy Phone services (PHS), version 2.1 is installed on the unit.
`Net Mgmt Installed` or `Net Mgmt Not Installed`	Indicates whether the Network Management option is installed on your MAX unit.
`Rte Ptls Avail` or `Rte Ptls Not Avail`	Indicates whether routing protocols are available.
`ATMP Avail` or `ATMP Not Avail`	Indicates whether Ascend Tunnel Management Protocol (ATMP) is available.
`PPTP Avail` or `PPTP Not Avail`	Indicates whether Point-to-Point Tunneling Protocol (PPTP) is available.

Table 1-12. Sys Option system status information (continued)

Option	Description
`L2TP Avail` or `L2TP Not Avail`	Indicates whether Layer 2 Tunneling Protocol (L2TP) is available.
`L2F Enabled` or `L2F Disabled`	Indicates whether Layer 2 Forwarding (L2F) is enabled.
`VRouter Enabled` or `VRouter Dis`	Indicates whether virtual router (VRouter) support is enabled.
`MAXTAP Enabled` or `Disabled`	Indicates whether the MAXTAP feature is enabled.

Note: Although GloBanD (Q.931W) does not appear in the Sys Option status window, its presence can be verified by checking the value of the Switch Type parameter.

System Status window

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

The System Status window contains the following selections:

```
00-000 System
  00-100 Sys Options
 >00-200 Message Log
  00-300 Port Info
  00-400 CDR
```

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

WAN Stat window

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

The following screen shows WAN statistics:

```
40-300 WAN Stat
 >Rx Pkt:  387112
  Tx Pkt:   22092
     CRC:  0
```

The first line displays the window number and name of the window. You can press the Down-Arrow key to get per-link statistics. The first line of a per-link display shows the name,

IP address, or MAC address of the remote device. The per-link count is updated every 30 seconds. The overall count is updated at the end of every active link.

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

DO Menu Commands

2

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

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

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

List of commands

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

Table 2-1. DO commands

Command	Description
Answer (DO 3)	Answer an incoming call.
Beg/End BERT (DO 7)	Begin/End a byte-error test.
Beg/End Rem LB (DO 6)	Begin/End a remote loopback.
Beg/End Rem Mgm (DO 8)	Begin/End remote management.
Close TELNET (DO C)	Close the current Telnet session.
Contract BW (DO 5)	Decrease bandwidth.
Diagnostics (DO D)	Access the diagnostic interface.
Dial (DO 1)	Dial the selected or current profile.
ESC (DO 0)	Abort and exit the DO menu.

Table 2-1. DO commands (continued)

Command	Description
Extend BW (DO 4)	Increase bandwidth.
Hang Up (DO 2)	Hang up from a call in progress.
Load (DO L)	Load parameter values into the current profile.
Menu Save (DO M) 8	Save the VT100 interface menu layout.
Resynchronize (DO R)	Resynchronize a call in progress.
Save (DO S)	Save parameter values in the specified profile.
Password (DO P) 9	Log into or out of the MAX.
Termmserv (DO E)	Access the terminal- server interface.
Toggle (DO T)	Toggle the palmtop controller.
View Call Routes (DO K)	Displays several fields of currently active call routes (in search order).

Example of using DO commands to place and clear a call

To manually place a call, the Connection profile for that call must be open or selected in the list of profiles. To clear a call, you can either open the Connection profile for the active connection or tab over to the status window in which that connection is listed.

To manually place a call:

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

   The DO menu appears:

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

3. Press 1 (or select 1=Dial) to invoke the Dial command.
4. Watch the information in the Sessions status window. You should see the number being called, followed by a message that the network session is up.

To manually clear a call:

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

2 Press Ctrl-D.

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

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

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

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

DO command reference in alphabetic order

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

Answer (DO 3)

Description: Answers an incoming call.

Usage: You can apply the command only from a menu specific to a serial host port. Select Answer.

You cannot answer a call if another call is currently using the port. The command applies when `Answer=Terminal` at the serial host port and an incoming call is ringing at that port. It is not available from the secondary serial host port of a dual-port pair.

Beg/End BERT (DO 7)

Description: Starts and stops a channel-by-channel Bit Error Rate Test (BERT). The command applies only to slot cards that support host ports. The test runs over the currently called circuits from end-to-end. It reports the total number of incorrect bytes errors found, and breaks the errors down according to DS0 channel. The results are displayed in the Session Err window.

Usage: Select DO Beg/End BERT. The following events occur:

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

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

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

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

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

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

Keep in mind the following additional information:

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

Beg/End Rem LB (DO 6)

Description: Begins and ends a loopback at the serial host port at the remote end of the call.

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

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

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

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

Keep in mind the following additional information:

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

switching Channel Service Units/Data Service Units (CSU/DSUs) recognize the remote loopback signal that the MAX sends, and remote loopbacks are usually possible with such equipment.

- The MAX uses the CCITT V.54 loopback pattern when no management subchannel is present (Call Type is set to 1 Chnl or 2 Chnl and `Call Mgm=Static` in a Call profile).
- If the MAX fails to set up a remote loopback, it establishes a loopback at the local host interface that tried to establish the call.
- The DO Beg/End LB command does not appear if you are not logged in with operational privileges.

Close Telnet (DO C)

Description: Closes the current Telnet session.

Usage: You must be running a Telnet session from the MAX unit's terminal-server interface. Select Close Telnet.

Contract BW (DO 5)

Description: Decreases the bandwidth by the amount specified in the Dec Ch Count parameter of the current Call profile.

Usage: Select Contract BW. If the specified amount in Dec Ch Count is not available, the MAX removes the maximum number of channels possible without clearing the call.

Keep in mind the following additional information:

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

Diagnostics (DO D)

Description: Invokes diagnostics mode. The user must have sufficient privileges in the active Security profile.

Usage: Select Diagnostics. In diagnostics mode, the VT100 interface displays a command-line prompt:

```
>
```

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

```
> help ascend
```

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

```
> quit
```

Dial (DO 1)

Description: Dials a selected Call or Connection profile.

Usage: Before you dial a Call profile, the selector (>) must be in one of the following positions:

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

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

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

Keep in mind the following additional information:

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

Esc (DO 0)

Description: Exits the DO menu.

Usage: Select ESC.

Extend BW (DO 4)

Description: Increases the bandwidth by the amount specified in the Inc Ch Count parameter of the current Call profile.

Usage: Select Extend BW. If the amount specified in Inc Ch Count is not available, the MAX adds the maximum number of channels available to the call.

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

Keep in mind that the DO Extend BW command does not appear if you are not logged in with operational privileges.

Hang Up (DO 2)

Description: Ends an online call.

Usage: Select Hang up. Either the caller or the receiver can terminate at any time.

Keep in mind the following additional information:

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

Load (DO L)

Description: Loads a saved or edited profile and overwrites the values of the current profile.

Usage: Select Load. The MAX unit offers you two options.

- 0 (zero)—Aborts the load.
- 1 (one)— The profile loads and the MAX unit uses it as the current profile.

Dependencies: The DO Load command is not available if you are not logged in with operational privileges.

Menu Save (DO M)

Description: Saves the entire current VT100 interface layout. The current layout replaces the default layout.

Usage: Select Menu Save. Keep in mind the following additional information:

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

Password (DO P)

Description: Enables you to log into the MAX.

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

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

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

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

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

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

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

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

Resynchronize (DO R)

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

Usage: Select Resynchronize. Keep in mind the following additional information:

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

Save (DO S)

Description: Saves the current parameter values in a specified profile.

Usage: Select Save. Keep in mind the following additional information:

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

Termserv (DO E)

Description: Invokes the terminal-server command-line interface.

Usage: Select Termserv. In terminal-server mode, the VT100 interface displays a command-line prompt. By default the prompt is:

```
ascend%
```

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

```
ascend% help
```

To exit terminal-server mode and return to the VT100 interface, enter the Quit command:

```
ascend% quit
```

Dependencies: The user must have sufficient privileges in the active Security profile.

View Call Routes (DO K)

Description: Displays several fields of currently active call routes (in search order). This display also shows the specific Call Route profile (in System > Call Routes) that was used to generate the call route.

Usage: Select K in the DO command menu. The unit responds with the following:

Column Head	Description
#	Call route profile number in System > Call Routes.
phone #	Phone # filter in the call route profile. Note that if the phone # is > 11 digits, then the first 10 digits are displayed followed by the abbreviation indicator.
SSP	Source slot and port filter.
T	Call route type filter (T=trunk-any, D=trunk-digital, V=trunk-voice).
Dest	Destination of call route (C12=Channel Group 12, T5=Trunk Group 5, T#=Trunk Group from dialed number, 3:1=Dest slot/port 3:1, FA=first available).

Dependencies: View Call Routes applies to a MAX unit that supports the MAXDAX™.

Terminal-server commands

3

The terminal-server command line interface (CLI) includes commands for monitoring networks, initiating sessions, and managing the system. This chapter includes an alphabetic listing of the commands with a summary of purpose and usage.

For information about accessing and using the terminal server, see the *Hardware Installation and Basic Configuration Guide* for your MAX.

Close

Description: Terminates a connection through the terminal server to a digital modem on a MAX unit.

Usage: Enter the command at the terminal-server prompt.

Example: `ascend%` **`close`**

Dependencies: The MAX must have digital modems installed and Modem Dialout must be enabled in the TServ Options subprofile.

See Also: Open and Resume terminal-server commands and TServ Options subprofile.

CSLIP

Description: CSLIP direct dial-in is not currently supported on the MAX. When the terminal server is in terminal mode, the CSLIP command enables a user to initiate a Compressed Serial Line Internet Protocol (CSLIP) session to transmit IP packets over a serial connection.

Usage: Enter the command at the terminal-server prompt.

Example: `ascend%` **`cslip`**

Dependencies: The terminal server must be configured for terminal mode and SLIP mode. See the *Hardware Installation and Basic Configuration Guide* for configuration information. If the terminal is not configured properly for terminal and SLIP mode, the following error message results:

```
SLIP mode not available from the console.
```

fBackupImage

Description: Copies the existing primary image on the PCMCIA flash card into the backup position on that card.

Usage: Enter `fBackupImage` at the command prompt.

To create the redundant backup image, proceed as follows:

Note: The order of these two steps is not important, but the MAX is unable to recover from a failure in the primary code image until they have both 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 to successfully.
 >
```

2 Load the `lvs.m60` image into internal flash with 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.
```

`fBackupImage` must be used with the `tload -i` command.

Hangup

Description: Closes terminal-server session and returns to the Main Edit Menu in the VT100 interface.

Usage: Enter the command at the terminal-server prompt.

Example: `ascend%` **hangup**

IProute

Description: Performs IP route management by displaying the routing table and enabling you to add or delete routes. Changes you make to the routing table by using IProute remain in effect until the MAX unit is reset.

Usage: To add a static route to the routing table, enter the command in the following format:

iproute add *destination gateway* [***metric***]

The elements of the syntax are as follows:

Syntax element	Description
destination	The destination network address.
gateway	The IP address of the router that can forward packets to that network.
metric	The virtual hop count to the destination network. The default is 8.

To remove a route from the routing table, enter the command in the following format:

iproute delete *destination gateway*

The elements of the syntax are as follows:

Syntax element	Description
destination	The destination network address.
gateway	The IP address of the router that can forward packets to that network.

Note: RIP updates can restore any route you remove with IProute Delete. After a system reset, the MAX restores all routes listed in the Static Rtes profile.

To display the routing table, enter the command in the following format:

iproute show

The output includes the following information fields:

Field	Destination
`Destination`	Target address of a route. To send a packet to this address, the MAX uses this route. Note that the router uses the most specific route (having the longest mask) that matches a given destination.

Field	Destination
`Gateway`	Address of the next hop router that can forward packets to the given destination. Direct routes (without a gateway) do not show a gateway address in the gateway column.
`IF`	Name of the interface through which a packet addressed to this destination is sent. • `ie0`—Ethernet interface • `lo0`— Loopback interface • `wanN`—Each of the active WAN interfaces • `wanidle0`— Inactive interface (the special interface for any route whose WAN connection is down)
`Flg`	Flag values, including the following: • `C`— A directly connected route, such as Ethernet • `I`—ICMP Redirect dynamic route • `N`—Placed in the table via SNMP MIB II • `O`—Route learned from OSPF (Open Shortest Path First) • `R`—Route learned from RIP • `r`—RADIUS route • `S`—Static route • `?`—Route of unknown origin, which indicates an error • `G`—Indirect route via a gateway • `P`—Private route • `T`—Temporary route • `*`—Hidden route that will not be used unless another better route to the same destination goes down
`Pref`	Preference value of the route. Note that all routes that come from RIP have a preference value of 100, but 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. Open Shortest Path First (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.

Example: Following are examples of IProute commands and resulting output:

```
ascend% iproute ?

iproute ?       Display help information
iproute add     iproute add <destination/size> <gateway> [ pref ] [
metric
```

```
iproute delete  iproute delete <destination/size> <gateway> [ proto ]
iproute show    displays IP routes (same as "show ip routes" command)
```

```
ascend% iproute show
Destination        Gateway        IF       Flg Pref  Met   Use   Age
0.0.0.0/0          10.0.0.100     wan0     SG   1     1     0     20887
10.207.76.0/24     10.207.76.1    wanidle0 SG   100   7     0     20887
10.207.77.0/24     10.207.76.1    wanidle0 SG   100   8     0     20887
127.0.0.1/32       -              lo0      CP   0     0     0     20887
10.0.0.0/24        10.0.0.100     wan0     SG   100   1     21387 20887
10.1.2.0/24        -              ie0      C    0     0     19775 20887
10.1.2.1/32        -              lo0      CP   0     0     389   20887
255.255.255.255/32 -              ie0      CP   0     0     0     20887
```

```
ascend% iproute add 10.1.2.0 10.0.0.3/24 1
ascend% iproute delete 10.1.2.0 10.0.0.3/24
```

IPXping

Description: Performs network-layer verification of the transmission path to NetWare stations across the LAN on which the MAX unit is located or across a WAN connection for which IPX Routing has been enabled.

In a vrouter application, the `ipxping` command also helps to check the connectivity with another IPX host.

Usage: Enter the command in the following format:

`ixping [-c count]|[-i delay]|[-s packetsize] hostname`

or in a vrouter application

`ipxping [-r vRoutername] server-name`

The elements of the syntax are as follows:

Option	Description
?	Display help information.
`stats`	Display NetWare IPX statistics
`servers`	Display NetWare IPX servers
`pings`	Display NetWare IPX Ping stats

Example: `ascend%` **`ipxping CFFF1234:000000000001`**

Kill

Description: Disconnects a user who established a Telnet connection to the MAX by specifying the session ID. The resulting disconnect code is identical to the RADIUS disconnect code, allowing you to track all administrative disconnects.

Usage: To terminate a Telnet session, enter the command in the following format:

`kill session ID`

where ***session ID*** is the session ID as displayed by the Show Users command. The reported disconnect cause is DIS_LOCAL_ADMIN. 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.
```

Dependencies: 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.
```

L2TPStop *N*

Description: Captures a log of disconnect and progress codes that enables you to troubleshoot the configuration of your unit's tunneling systems. These progress and disconnect codes are logged by Syslog, RADIUS accounting, and Call Logging.

Usage: The L2TPStop *N* command limits the length of such optional message to be less than or equal to 100 characters. The L2TPStop *N* accepts (or *echoes*) an optional message of any length.

Example:

```
admin> l2tpstop 2
LAC: c=736 p=244 (DIS_L2TUNNEL_ADMIN_DISCONNECT, PR_TUNNEL_UP)
   Syslog :
      May  9 16:21:52 max ASCEND: call 2 CL 0K u=test c=736
p=244
       s=14400 r=14400
    Radacct:
       Ascend-Disconnect-Cause = 736
(DIS_L2TUNNEL_ADMIN_DISCONNECT)
       Ascend-Connect-Progress = 244 (PR_TUNNEL_UP)
LNS: c=736 p=60 (DIS_L2TUNNEL_ADMIN_DISCONNECT,
PR_LAN_SESSION_UP)
   Syslog :
      May  9 16:21:51 maxlns ASCEND: call 3 CL 0K u=test c=736
p=60
       s=14400 r=14400
Radacct:
   Ascend-Disconnect-Cause = 736
(DIS_L2TUNNEL_ADMIN_DISCONNECT)
   Ascend-Connect-Progress = 60 (PR_LAN_SESSION_UP)
```

Local

Description: When entered by a dial-in user, establishes a direct Telnet connection to the local MAX unit, displaying the VT100 interface.

Usage: Enter the command at the terminal-server prompt.

Example: `ascend% local`

Menu

Description: Invokes the terminal server's menu mode, which lists up to four hosts from which the user selects to begin a session. The four hosts can be either Telnet hosts, raw TCP hosts, or a mixture of the two types. The hosts must be configured in the Ethernet > Mod Config > TServ Options subprofile.

Usage: To invoke menu mode, enter the command at the prompt. To return to the command line from the menu, press 0. Terminal-server security must be set up through the Security parameter to allow the operator to toggle between the command line and menu mode, or the Menu command has no effect.

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

See Also: TAOS Host #*N* Addr, Host #*N* Text, ToggleScrn.

NSlookup

Description: Resolves the IP address of a specified hostname or Vrouter by performing a Domain Name System (DNS) lookup.

Permission level: Diagnostic

Usage: nslookup [**-r** ***Vroutername***][**-s** ***DNS_server***] [**-v**] ***hostname***

Syntax element	Description
-r ***Vroutername***	The VRouter for which you want to obtain an IP address.
-s ***DNS_server***	New option specifies the IP address of the DNS server that the unit uses to resolve the hostname or VRouter name. If you do not specify the `-s` option, the system uses the local DNS server.
`-v`	New options specifies that the unit prints the details of the packet received from the DNS server.
hostname	The hostname for which you want to obtain an IP address.

Example: To look up the IP address of `host-231` by means of the DNS server at 10.65.12.10:

```
admin> nslookup -s 10.65.12.10 host-231
Resolving host host-231.
IP address for host host-231 is 10.65.12.231.
```

Dependencies: Unless you use the `-s` option, your unit must be configured with the address of at least one DNS server.

Open

Description: Sets up a virtual connection to a digital modem installed in the MAX unit, enabling a local user to issue AT commands to the modem as if connected locally to the modem's asynchronous port.

Usage: To set up a virtual connection to a modem, enter the Open command. Enter the command in the following format:

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

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

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

Example:

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

Dependencies: The MAX must have digital modems installed and Modem Dialout must be enabled in the TServ Options submenu.

See Also: Close and Resume terminal-server commands and TServ Options submenu.

Ping

Description: Verifies that the transmission path is open between the MAX and another station. It sends an ICMP echo-request packet to the specified station. If the station receives the packet, it returns an ICMP echo-response packet.

Usage: Enter the command in the following format:

ping [**-q**] [**-v**] [**-c** ***count***] [**-i** ***sec*** | **-I** ***msec***] [**-s** ***packetsize***] [**-x src_address**] ***host***

The only required argument is the destination hostname or IP address. The elements of the syntax are as follows:

Syntax element	Description
-q	Quiet mode. The MAX displays a summary of all Ping responses it has received.
-v	Verbose output. The MAX displays information from each Ping response that it receives as well as the summary of all Ping responses. This is the default.
-c ***count***	Specifies the number of Ping requests that the MAX sends to the host. By default, the MAX sends continual Ping requests until you press Ctrl-C.
-i ***sec***	Specifies the length of time, in seconds, between Ping requests. You can specify seconds, using the `-i` option, or milliseconds, using the `-I` option, but not both. The default is one second.

-I *msec*	Specifies the length of time, in milliseconds, between Ping requests. You can specify milliseconds, using the `-I` option, or seconds, using the `-i` option, but not both.
-s *packetsize*	Specifies the size of each Ping request packet that the MAX sends to the host. The default is 64 bytes.
-x *srcaddress*	Specifies a source IP address that overwrites the default source address.
host	The destination host by name or IP address.

You can terminate the Ping exchange at any time by pressing Ctrl-C. When you press Ctrl-C, the command reports the number of packets sent and received, the percentage of packet loss, any duplicate or damaged echo-response packets, and round-trip statistics. In some cases, round-trip times cannot be calculated.

During the Ping exchange, the MAX displays information about the packet exchange, including the Time-To-Live (TTL) of each ICMP echo-response packet.

Note: The maximum TTL for ICMP Ping is 255, and the maximum TTL for TCP is often 60 or lower, so you might be able to Ping a host but not be able to run a TCP application (such as Telnet or FTP) to that station. If you Ping a host running a version of Berkeley UNIX earlier than 4.3BSD-Tahoe, the TTL report is 255 minus the number of routers in the round-trip path. If you Ping a host running the current version of Berkeley UNIX, the TTL report is 255 minus the number of routers in the path from the remote system to the station performing the Ping.

The Ping command sends an ICMP Mandatory echo-request datagram, which asks the remote station "Are you there?" If the echo-request reaches the remote station, the station sends back an ICMP echo-response datagram, which tells the sender "Yes, I am alive." This exchange verifies that the transmission path is open between the MAX and a remote station.

Example:

```
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
```

PPP

Description: When the terminal server is in terminal mode, initiates a Point-to-Point Protocol (PPP) session to transmit IP packets over a serial connection. Useful for dial-in users with software that does not support direct PPP dial-in.

Usage: Enter the command at the terminal-server prompt.

Example: `ascend%` **`ppp`**

Dependencies: The terminal server must be configured for terminal mode and PPP mode. See the *Hardware Installation and Basic Configuration Guide* for configuration information. If the

terminal is not configured properly for terminal and SLIP mode, the following error message appears when you enter the command:

```
PPP mode not available from the console.
```

Remote

Description: After an MP+ connection has been established with a remote station (for example, by using the DO Dial command), starts a remote management session with that station.

Usage: Enter the command in the following format:

`remote` ***`station`***

During the remote management session, the user interface of the remote device replaces your local user interface, as if you had opened a Telnet connection to the device. You can enter Ctrl-\ at any time to terminate the Remote session. Note that either end of an MP+ link can terminate the session by hanging up all channels of the connection.

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

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

At the beginning of a remote management session, you have privileges set by the default Security profile at the remote end of the connection. To activate administrative privileges on the remote station, activate the appropriate remote Security profile by using the DO Password command.

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

Message	Explanation
`not authorized`	Your current security privileges are insufficient for beginning a remote management session. To assign yourself the required privileges, log in, with the DO Password command, to a Security profile in which the 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.

Message	Explanation
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 > Sys Config profile.

Example:

```
ascend% remote lab17gw
```

Resume

Description: You can temporarily suspend a virtual connection to a digital modem by pressing Ctrl-C three times. This control sequence causes the MAX to display the terminal-server interface. To resume a virtual connection suspended with Ctrl-C, you can use the Resume command.

Usage: Enter the command at the terminal-server prompt.

Example: `ascend% resume`

Dependencies: The MAX must have digital modems installed and Modem Dialout must be enabled in the TServ Options submenu.

See Also: Open and Close terminal-server commands and TServ Options submenu.

Rlogin

Description: Initiates a login session to a remote host.

Usage: Enter the command in the following format:

rlogin [-***echar***] ***hostname*** [**-l*username***]

The elements of the syntax are as follows:

Syntax element	Description
-***echar***	Sets the escape character to ***char***. For example: `rlogin -e$ 10.2.3.4` The default escape character is a tilde (~).
hostname	The remote system's DNS name if you have configured DNS. If you have not, you must specify the IP address of the remote system.

-l*username*	Specifies that you log into the remote host as ***username***, rather than as the name with which you logged into the terminal server. If you can specify this option on the command line, you can enter it either before or after the ***hostname*** argument. For example, the following two lines perform identical functions:
	`rlogin -l jim 10.2.3.4`
	`rlogin 10.2.3.4 -l jim`
	If you logged in through RADIUS or TACACS, you are prompted for a username if you do not use the attribute User Name (1) to specify a login identification in the user profile.

To terminate the remote login, choose the Exit command at the remote system's prompt. Or, you can press the Enter key, then type the escape character followed by a period. For example, to terminate a remote login that was initiated with the default escape character (a tilde), press the Enter key, then the ~ key, then the . key.

Set

Description: Sets terminal type, enables dynamic password serving, sets Frame Relay datalink control and circuit control, sets and stores session identification, clears the ARP cache, and clears statistics. Also accesses a list of set arguments and displays current settings.

Usage: Enter the command in the following format:

`set [all]|[term]|[password]|[fr]|[circuit]|[sessid [val]]|[arp clear]|[stat]|[?]`

The elements of the syntax are as follows:

Syntax element	Description
`all`	Displays the current settings.
`term`	Sets the Telnet/Rlogin terminal type.
`password`	Enables dynamic password service.
`fr`	Enables Frame Relay datalink control.
`circuit`	Enables Frame Relay circuit control.
`sessid [val]`	Sets and stores ***val*** representing a session identification, or the current session identification.
`arp clear`	Clears the Address Resolution Protocol (ARP) cache.
`stat`	Clears the current statistics.
`?`	Displays a list of Set command arguments with a short explanation of each.

Enter the Set All command to display current settings.

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

You can enter the Set Password command to put the terminal server in password mode when using security card authentication. Password mode enables a third-party ACE or SAFEWORD

server at a secure site to display password challenges dynamically in the terminal-server interface. When the terminal server is in password mode, it passively waits for password challenges from a remote Security Dynamics ACE/Server or Enigma Logic SafeWord ACS network authentication server. For more information about ACE/Server or SafeWord ACS, see the *TAOS Glossary.*

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

The Set FR command enables you to bring down the nailed connection specified in the named Frame Relay profile. The connection is reestablished within a few seconds. The Set Circuit command enables you to activate or deactivate a Frame Relay circuit.

Example:

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

Show

Description: Displays a variety of MAX statistics. Used with an argument, as described in the following sections.

Show ?

Description: Lists each Show command argument available with the software load and version and summarizes the command function.

Usage: Enter the command in the following format:

```
show ?
```

Example:

```
ascend% show ?
show ?          Display help information
show arp        Display the Arp Cache
show icmp       Display ICMP information
show if         Display Interface info. Type 'show if ?' for
help.
show igmp       Display IGMP information. Type 'show igmp ?' for
help.
show mrouting   Display MROUTING info. Type 'show mrouting ?'
for help.
show ospf       Display OSPF information. Type 'show ospf ?' for
help.
show pad        Display status of all pads.
show tcp        Display TCP information. Type 'show tcp ?' for
help.
show dnstab     Display local DNS table. Type 'show dnstab ?'
```

```
for help.
show netware   Display NetWare IPX info. Type 'show netware ?'
for help.
show isdn      Display ISDN events.  Type 'show isdn <line
number>'
show fr        Display Frame relay info. Type 'show fr ?' for
help.
show pools     Display the assign address pools.
show modems    Display status of all modems.
show uptime    Display system uptime.
show revision  Display system revision.
show v.110s    Display status of all v.110 cards.
show x25       Display status of X.25 stack.
show users     Display concise list of active users
show filters   Display filters of active users. Type 'show
show sessid    Display current and base session id
show dnis      Display DNIS informations
```

Show ARP

Description: Displays the content of the ARP cache.

Usage: Enter the command in the following format:

```
show arp
```

The output includes the following information:

Field	Description
IP Address	The address contained in ARP requests.
Hardware Address	The MAC address of the host with that IP address.
Type	How the address was learned, dynamically (Dynamic) or statically (Static).
Interface	The interface on which the MAX received the ARP request.
RefCount	Number of times the entry has been referenced.

Example:

```
ascend% show arp
IP Address      Hardware Address    Type     Interface  RefCount
10.101.0.10     08:00:20:a5:0c:86   Dynamic  ie0              5
```

Show Calls

Description: Displays information about active calls on an E1 line with a German 1TR6 or Japanese NTT switch type.

Usage: Enter the command in the following format:

`show calls`

The output includes the following fields:

Field	Description
CallID	An identifier for the call.
CalledPartyID	The telephone number of the answering device (that is, this unit). This ID is obtained from Layer 3 protocol messages during Layer 3 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.

Example:

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

Show DNIS

Description: Displays statistics related to Dialed Number Information Service (DNIS) usage.

Usage: Enter the command in the following format:

`show dnis [session]|[stats]|[?]`

The Show DNIS Session command displays the active and maximum sessions per DNIS. The output includes the following fields:

Field	Description
`DNIS#`	Displays the last 11 digits of the DNIS number.
`Used`	Specifies the number of active sessions to the specified DNIS number.
`Max`	Specifies the value specified in the Ethernet > Mod Config > DNIS Options subprofile.

The Show DNIS Stats command displays DNIS session statistics. The output includes the following fields:

Field	Description
`DNIS#`	Displays the last 11 digits of the DNIS number.
`Tot`	Specifies the total number of calls *received* to the specified DNIS number.
`Accept`	Specifies the total number of calls *accepted* to the specified DNSI number.

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

Dependencies: If Ethernet > Mod Config > DNIS Options > DNIS Limitation = No, and you enter the Show DNIS commands, the MAX displays the following message:

```
DNIS Inactive
```

Example:

```
ascend% show dnis session
```

DNIS#	GLOBAL Used/Max	MODEM Used/Max	HDLC Used/Max	V110 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

```
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

Show DNStab

Description: Displays the contents of the local DNS table on the MAX unit.

Usage: Enter the command in the following format:

```
show dnstab
```

The output includes the following information:

Field	Description
`Name`	The hostname.
`IP Address`	The IP address for the named host.
`# Reads`	The number of reads since the entry was created. This field is updated each time a local name query match is found in the local DNS table.
`Time of last read`	The date and time of the last read.

Example: Following are examples of the Show DNIStab commands and the resulting output:

```
ascend% show dnstab
Local DNS Table
Name                IP Address  # Reads    Time of last read
1: ""               ------      -------     - ---
2: "server.corp.com" 200.0.0.0  2          Nov 11 10:40:44 3: ""
3: “boomerang”      221.0.0     2          Nov 11 9.13.33
4: “”               ------      ------
5: “”               ------      ------
6: “”               ------      ------
```

Show Filters

Description: Displays the filters active for each active session on the MAX unit, including filters downloaded from an external authentication server, such as a RADIUS server.

Usage: Enter the command in the following format:

`show filters` [***`ID#`***]

where ***`ID#`*** is a number identifying a specific session.

When you enter the command without the ***`ID#`*** argument, the output summarizes the active sessions. The output does not display the names of filters from externally authenticated sessions. Instead, if a filter is present, displays *`filters present`*. You can use the Show Filters command with the ***`ID#`*** argument to find the names of the filters.

The output includes the following fields:

Field	Description
ID	The ID number for the session, for use as an argument to the Show Filter command for displaying complete details about a specific session.
Username	The active user.
Src	Whether the profile was downloaded from a local Connection profile (loc) or from an external server (ext).
Data-Filter	The name of the active data filter or a zero to indicate no filter.
Call-Filter	The name of the active call filter or a zero to indicate no filter.
Ipx-Filter	The name of the active route filter or a zero to indicate no filter.
TOS-Filter	The name of the active type-of-service filter or a zero to indicate no filter.

When you use the *ID#* argument to identify a specific session, the Show Filters command displays additional information about all filters in use for the session.

Example:

```
ascend% show filters
ID   Username    Src    Data-Filter   Call-Filter   TOS-Filter
-----------------------------------------------------------------
000  tnt2max1    loc         0             0             0
001  tnt2max2    loc         1             5             3
002  edmax       ext         -             -             -
003  tnt2max4    loc         0             0             0
ascend% show filters 0

Hostname:    tnt2max1
No associated filters
ascend% show filters 1

Hostname:    tnt2max2
*******************************************
Data 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
*******************************************
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:
*******************************************
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:    932
Server Name:    abcde
*******************************************
Ipx Sap Filter
Direction: Out
----------------------------
Type-filter:    include
Server Type:    1112
Server Name:    nowhere
*******************************************
Tos 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
*******************************************
Tos 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
00:00:00:00:00
```

Show FR

Description: Displays statistics used to monitor Frame Relay usage in the MAX.

Usage: Enter the command in the following format:

`show fr [stats]|[lmi]|[dlci ]|[circuits]|[?]`

The Show FR Stats command displays Frame Relay statistics. The output includes the following fields:

Field	Description
`Name`	Name of the Frame Relay profile associated with the interface.
`Type`	Type of interface.
`Status`	Status of the interface. Up means the interface is functional, but is not necessarily handling an active call. Down means the interface is not functional.
`Speed`	Data rate in bits per second.
`MTU`	Maximum packet size allowed on the interface.
`InFrame`	Number of frames the interface has received.
`OutFrame`	Number of frames transmitted.

The Show FR LMI command displays Link Management Information for each link activated by a Frame Relay profile.

The Show FR DLCI command displays the status of each Data Link Connection Indicator (DLCI). The output includes the following fields:

Field	Description
DLCI	DLCI number.
Status	ACTIVE if the connection is up or INACTIVE if not.
input pkts	Number of frames the interface has received.
output pkts	Number of frames the interface has transmitted.
input octets	Number of bytes the interface has received.
output octets	Number of bytes the interface has transmitted.
in FECN pkts	Number of packets received with the Forward Explicit Congestion Notification (FECN) bit set. This field always contains a 0 (zero), because congestion management is not currently supported.
in BECN pkts	Number of packets received with the Backward Explicit Congestion Notification (BECN) bit set. This field always contains a 0 (zero), because congestion management is not currently supported.
in DE pkts	Number of packets received with the Discard Eligibility (DE) indicator bit set.
last time status changed	Time at which the DLCI state last changed.

The Show FR Circuits command displays the Frame Relay profile name, the DLCI, and the status of configured circuits.

The Show FR ? command lists the available arguments to Show FR.

Example: Following are examples of Show FR commands and the resulting output:

```
ascend% show fr stats
Name     Type  Status  Speed   MTU   InFrame  OutFrame
frswan   DTE   Down    64000   1532     0        0
ascend% show fr lmi
T1_617D LMI for frswan
Invalid Unnumbered Info      0   Invalid Protocol Disc   0
Invalid Dummy Call Ref       0   Invalid Msg Type        0
Invalid Status Message       0   Invalid Lock Shift      0
Invalid Information ID       0   Invalid Report Type     0
Num Status Enqs Sent         0   Num Status Msgs Rcvd    0
Num Update Status Rcvd       0   Num Status Timeouts     0

ascend% show fr circuits
cir-9 User Setting Up
fr1-temp-916  Up
fr1-temp17    Up
```

Show If

Description: Displays information used to monitor the activity on the MAX unit's interfaces.

Usage: Enter the command in the following format:

```
show if [stats]|[totals]|[?]
```

The Show If Stats command displays statistics about each WAN interface. The output includes the following fields:

Field	Description
Interface	Interface name.
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.
OutPacket	The number of packets the interface has transmitted.

The Show If Totals command displays the packet count at each interface, broken down by type of packet. The output includes the following fields:

Field	Description
Name	Interface name.
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.

Example: Examples of Show If commands and the resulting output follow:

```
ascend% show if stats
Interface   Name      Status   Type  Speed     MTU   InPackets  OutPacket

ie0         ethernet  Up       6    10000000  1500      784        3266
wan0                  Down     1    0         1500      0          0
wan1                  Down     1    0         1500      0          0
wan2                  Down     1    0         1500      0          0
wan3                  Down     1    0         1500      0          0
wan4        ppp       Up      23    56000     1524      13450      13438
wan5                  Down     1    0         1500      0          0
wan6        ppp       Up      23    56000     1524      13431      13416


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
```

Show ICMP

Description: Displays the number of ICMP packets received intact, received with errors, and transmitted.

Usage: Enter the command in the following format:

```
show icmp
```

Input and output histograms show the number of ICMP packets received and transmitted.

Example:

```
ascend% show icmp

3857661 packet received.
20 packets received with errors.
   Input histogram: 15070
2758129 packets transmitted.
0 packets transmitted due to lack of resources.
   Output histogram: 15218
```

Show ISDN

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

Usage: Enter the command in the following format:

show isdn *line-number*

where ***line-number*** is the number of the ISDN line. (For details about how lines are numbered, see the *Network Configuration Guide* for your MAX unit.)

Example: To display information about the leftmost built-in WAN port:

```
ascend% show isdn 0

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 MAX response includes a phone number (prefixed by #), a data service (suffixed by K for Kbps), a channel number, TEI assignment, and cause code. For example, the following information might appear:

```
PH: ACTIVATED
NL: CALL REQUEST: 64K, #442
NL: CALL CONNECTED: B2, #442
NL: CLEAR REQUEST: B1
NL: CALL CLEARED WITH CAUSE 16 B1 #442
```

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

Show Modems

Description: Displays the status of the MAX unit's digital modems.

Usage: Enter the command in the following format:

show modems

The output contains these fields:

Field	Description
`slot:item`	The slot and port number of the modem. For example, 8:1 indicates the first port on the digital modem card installed in slot 8.
`modem`	The SNMP interface number of each modem.
`status`	Modem status, which can be one of the following strings: • `idle`—The modem is not in use. • `awaiting DCD`—The call is up and waiting for DCD. • `awaiting codes`—DCD is up, and the call 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.

Example: Examples of Show Modems commands and the resulting output follow.

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

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

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

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

Show Mrouting

Description: Displays the number of multicast packets received and forwarded.

Usage: Enter the command in the following format:

```
show mrouting stats
```

Often the number of packets forwarded exceed the number of packets received because packets can be duplicated and forwarded across multiple links.

Example:

```
ascend% show mrouting stats
34988 packets received.
    57040 packets forwarded.
        0 packets in error.
       91 packets dropped.
        0 packets transmitted.
```

Show Netware

Description: Displays statistics for monitoring IPX activities.

Usage: Enter the command in the following format:

```
show netw [stats]|[servers]|[networks]|[pings]|[?]
```

The Show Netw Stats command displays IPX packet statistics, listing packets received, forwarded, dropped because they have passed through too many routers, and outbound packets with no route.

The Show Netw Servers command displays the IPX service table. The output includes the following fields:

Field	Description
IPX address	IPX address of the server. The address uses this format: *network number*:*node number*:*socket number*

Field	Description
type	Type of service available (in hexadecimal format). For example, 0451 designates a file server
server name	The first 35 characters of the server name.

The Show Netw Networks command displays the IPX routing table. 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. 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.

The Show Netw Pings command displays 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 request and replies).

Example: Examples of Show Netw commands and the resulting output follow:

```
ascend% show netw stats

27162 packets received.
25392 packets forwarded.
0 packets dropped exceeding maximum hop count.
0 outbound packets with no route.

ascend% show netw servers

IPX address                    type            server name
ee000001:000000000001:0040     0451            server-1

ascend% show netw networks

networknext routerhopsticksorigin
CFFF000100000000000001EthernetS

ascend% show netw pings

InPing Requests/OutPing Replies OutPing Requests/InPing Replies
      10           10                 18           18
```

Show OSPF

Description: Displays information used for monitoring OSPF in the MAX.

Usage: Enter the command in the following format:

```
show ospf [size]|[areas]|[stats]|[intf]|[lsa]|[lsdb]|
```

[nbrs]|[routers]|[ext]|[rtab]|[database]|[internal]|[trans]

The Show OSPF Size command displays the size of the OSPF routing table. 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.
# DoNotAge-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.
# Routes Alloc/ Inuse	
# I/O Buffers Inuse	

The Show OSPF Areas command displays information about OSPF areas. 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.

The Show OSPF Stats command displays general information about OSPF. 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.

Field	Description
`LS adv. aged out`	Number of LSAs that the MAX has aged and removed from its tables.
`LS adv. flushed`	Number of LSAs that the MAX has flushed.
`Incremental ext.(5) updates`	Number of incremental ASE-5 updates.
`Incremental ext.(7) updates`	Number of incremental ASE-7 updates.
`Current state`	State of the External (Type-5) LSA database, either Normal or Overload.
`Number of LSAs`	Number of LSAs in the External (Type-5) LSA database.
`Number of overflows`	Number of ASE-5 that exceeded the limit of the database.
`Number of internal routes`	Number of internal routes. Internal (no assigned Type) routes provide the configuration with alternatives to the External (Type-7) routes.

The Show OSPF Intf command displays 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. The output includes the following fields:

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

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

`show ospf intf` ***`interface`***

where ***`interface`*** is the IP address or physical address of the interface.

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.
`# 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.

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

```
ascend% show ospf lsa 0.0.0.0 ase 10.5.2.160 10.5.2.162
LSA  type: ASE ls id: 10.5.2.160 adv rtr: 110.5.2.162 age: 568
          seq #: 80000037 cksum: 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.
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.

The Show OSPF LSDB command displays the router's link-state database. 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.

Field	Description *(continued)*
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 link-state database.
Checksum total	Checksum of the link-state database.

The Show OSPF Nbrs command displays information about OSPF neighbors to the MAX. 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.

The Show OSPF Routers command displays OSPF routers. 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.
#	Number of the interface used to reach the destination.

The Show OSPF Ext command displays OSPF External AS advertisements. 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.

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 Rtab command displays the OSPF routing table. The output includes the following fields:

Field	Description
`DType`	Internal route type. DType displays one of the following values: RTE (generic route), ASBR (AS border route), or BR (area border route).
`RType`	Internal router type. RType displays one of the following values: FIX (static route), NONE, DEL (deleted or bogus state), OSPF (OSPF-computed), OSE1 (type 1 external), or OSE2 (type 2 external).
`Destination`	Destination address and subnet mask of the route.
`Area`	Area ID of the route.
`Cost`	Cost of the route.
`Flags`	Hexadecimal number representing an internal flag.
`Next hop(s)`	Next hop in the route to the destination.
`#`	Number of the interface used to reach the destination.

The Show OSPF Database command displays summarized information about the OSPF database. 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.

`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).
`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 database.
`Checksum total`	Checksum of the database.

The Show OSPF Internal command displays the currently active internal routes. The output includes the following fields:

Field	**Description**
`Area`	Area in which the router resides.
`Destination`	Route's target address. To send a packet to this address, the MAX uses this route. If the target address appears more than once in the routing table, the MAX uses the most specific route (having the largest subnet mask) that matches the address.
`Mask`	The subnet mask of the route.
`Cost`	The cost of the route.

The Show OSPF Trans command is not implemented.

Example: Examples of Show OSPF commands and the resulting output follow:

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

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
```

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
```

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
```

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
```

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
```

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
ascend% show ospf rtab

DTyp    RType   Destination           Area      Cost  Flags   Next hop(s)    #

RTE     FIX     192.192.192.0/24          -     1     0x82    0.0.0.170      170
RTE     OSPF    194.194.194.2/32      0.0.0.0   20    0x1     194.194.194.3  2
ASBR    NONE    192.192.192.2/32          -     0     0x0     None           -1
RTE     OSPF    192.192.192.2/32      0.0.0.0   0     0x1     0.0.0.170      170
RTE     OSPF    194.194.194.3/32      0.0.0.0   10    0x101   194.194.194.3  2
RTE     NONE    194.194.194.0/24          -     0     0x2     None           -1
ASBR    OSPF    192.192.192.3/32      0.0.0.0   10    0x100   194.194.194.3  2
RTE     OSPF    192.192.192.3/32      0.0.0.0   10    0x1     194.194.194.3  2
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
ascend% show ospf internal
                           Area: 0.0.0.1
Destination    Mask              Cost
33.240.0.0     255.255.255.224   1
103.240.0.0    255.255.255.192   1
113.240.0.0    255.255.255.128   1
183.240.0.0    255.255.255.128   1
193.240.0.0    255.255.255.128   1

ascend% show ospf trans
Not Applicable
```

Show Pad

Description: Displays information about Packet Assembler/Disassembler (PAD) sessions.

Usage: Enter the command in the following format:

```
show pad
```

The output includes the following fields:

Field	Description
Port	Port for the X.25 connection.

Field	Description
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.

Example:

```
ascend% show pad

Port   State        LCN        BPS       User     Called Addr.
1     connected      0         9600      rchan     419342855555
2     connected      0         9600      landie
```

Show Pools

Description: Displays the status of the MAX unit's IP address pool.

Usage: Enter the command in the following format:

```
show pools
```

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).

Example:

```
ascend% show pools
Pool#                Base          Count      InUse
   1                11.101.0.1      126          0
   2               111.101.0.1       62          0
   3               211.101.0.1       30          0
   4               191.101.0.1       30          0
 Number of remaining allocated addresses:    0
```

Show Revision

Description: Displays the software load and version number running on the MAX.

Usage: Enter the command in the following format:

show revision

Example:

```
ascend% show revision
lab-22 system revision:  tbaxkh.m60 8.0b2c2
```

Show Sessid

Description: Displays the current session's identification number.

Usage: Enter the command in the following format:

show sessid

Example:

```
ascend% show sessid
Session ID current 311106294, saved base 0
```

Show TCP

Description: Displays statistics used for monitoring TCP activity.

Usage: Enter the command in the following format:

show tcp [**stats**]|[**connection**]

The Show TCP Stats command displays the number of active open, passive open, and currently active connections and the segments received and transmitted. An active open is a TCP session that the MAX initiated, and a passive open is a TCP session that the MAX did not initiate.

The Show TCP Connection command displays current TCP connections.

Example: Examples of Show TCP commands and the resulting output follow:

```
ascend% show tcp ?
show tcp ?          Display help information
show tcp stats      Display TCP Statistics
show tcp connection Display TCP Connection Table
ascend% show tcp stats
        0 active opens.
       11 passive opens.
        1 connections currently established.
     6614 segments received.
     6256 segments transmitted.
ascend% show tcp connection
Socket  Local                  Remote                 State
0       *.23                   *.*                    LISTEN
2      10.101.0.2.23         10.101.0.10.32796     ESTABLISHED
```

Show Uptime

Description: Reports how long the MAX has been running.

Usage: Enter the command in the following format:

`show uptime`

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

Example:

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

Show Users

Description: Displays the number of active sessions.

Usage: Enter the command in the following format:

`show users`

The output includes the following fields:

Field	Content
`IO`	I for an incoming call or O for an outgoing call.
`Session ID`	Unique session-ID. This is the same as Acct-Session-ID in RADIUS.
`Line:Chan`	Line and channel on which the session is established.
`Slot: Port`	Slot and port of the service being used by the session. Can indicate the number of a slot containing a modem card, and the modem on that card. Or can indicate the virtual slot of the MAX unit's bridge/router, with the port indicator showing the virtual interfaces to bridge/router starting with 1 for the first session of a multichannel session.
`Tx Data`	Transmit data rate in bits per second.
`Rx Rate`	Receive data rate in bits per second.
`Service Type`	Type of session, which can be Termsrv or a protocol name. For MP and MP+ (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 Termsrv sessions during the login process.
`Host Address`	Network address of the host originating the session. For some sessions this field is N/A. For outgoing MP+ 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.`

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 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.

Show V.110s

Description: Displays the status of the MAX unit's V.110 cards.

Usage: Enter the command in the following format:

`show v.110s`

The output includes the following fields:

Field	Content
`slot:item`	The slot and port number of the port. For example, 8:1 indicates the first port on the V.110 card installed in slot 8.
`v.110s`	The SNMP interface number of each V.110 card.
`status`	V.110 port status, which can be one of the following: • `Idle`—The V.110 port is not in use. • `Open issued`—An open was issued, but the MAX unit has not synced up with the far end. • `Carrier detected`—A carrier was detected from the remote end. • `In use`—A V.110 session is up. • `Session closed`—A session has been closed.

Example:

```
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
```

Sh X25

Description: Displays only the status and statistics of the dedicated X.25 connection's packet level and link level information. When you add the on-demand X.25 connections to a MAX

6000, this command displays the existing status and statistics, as well as the X.25 profile name, for all the permanent and on-demand X.25 connections.

Usage: Enter the command in the following format:
`sh x25`

Example: A MAX unit responds as follows:

```
Frame    State     BytesIn  BytesOut
25       LinkUp    83       111

Packet   State     BytesIn  BytesOut
25       Ready     20       20
```

A MAX 6000 unit that is configured to support on-demand X.25 connections responds as follows:

```
X.25 profile name: Nailed X25B DTE

Frame    State     BytesIn  BytesOut
25       LinkUp    296      530

Packet   State     BytesIn  BytesOut
25       Ready     30       33

X.25 profile name: X.32 X25B DTE A

Frame    State     BytesIn  BytesOut
26       LinkUp    296      530

Packet   State     BytesIn  BytesOut
26       Ready     30       33

X.25 profile name: X.32 X25B DTE B

Frame    State     BytesIn  BytesOut
27       LinkUp    296      530

Packet   State     BytesIn  BytesOut
27       Ready     30       33
```

```
X.25 profile name: X.32 X25B DTE C

Frame    State     BytesIn  BytesOut
28       LinkUp    296      530

Packet   State     BytesIn  BytesOut
28       Ready     30       33
```

SLIP

Description: When the terminal server is in terminal mode, enables a user to initiate a Serial Line Internet Protocol (SLIP) session to transmit IP packets over a serial connection. SLIP direct dial-in is not supported on the MAX.

Usage: Enter the command at the terminal-server prompt. After beginning a SLIP session, the user can use an application such as File Transfer Protocol (FTP).

Example: `ascend%` **`slip`**

Dependencies: The terminal server must be configured for terminal mode and SLIP mode. See the *Hardware Installation and Basic Configuration Guide* for configuration information. If the terminal is not configured properly for terminal and SLIP mode, the following error message results:

```
SLIP mode not available from the console.
```

snmpAuthPass

Description: Generates the authentication key of an SNMPv3 USM user.

Usage: **`snmpAuthPass`** ***`username password`***

Argument	Description
`username`	SNMPv3 USM user for whom an authentication key is generated.
`password`	Password for generating the authentication key.

The snmpAuthPass command can accept a username in escape sequence format.

Example: To generate the authentication key of the user `robin` with the password `abc123`:

```
admin> snmpAuthPass robin abc123
```

Dependencies: The password you specify is not stored in the system. It is used to generate an authentication key when the user is authenticated. The key is stored in the system.

See Also: snmpPrivPass

snmpPrivPass

Description: Generates the privacy key of an SNMPv3 USM user.

Usage: **snmpPrivPass *username password***

Argument	Description
username	SNMPv3 USM user for whom a privacy key is generated.
password	Password for generating the privacy key.

The snmpPrivPass command can accept a username in escape sequence format.

Example: To generate the privacy key of the user `robin` with the password `abc123`:

```
admin> snmpPrivPass robin abc123
```

Dependencies: The password you specify is not stored in the system. It is used to generate a privacy key when the user is authenticated. The key is stored in the system.

See Also: snmpAuthPass

TCP

Description: Initiates a login session to a remote host.

Usage: Enter the command in the following format:

tcp *hostname* [***port-number***]

The elements of the syntax are as follows:

Syntax element	Description
hostname	The remote system's DNS name if you have configured DNS. If you have not, you must specify the IP address of the remote system.
port-number	The port to use for the session. The port number typically indicates a custom application that runs on top of the TCP session. For example, port number 23 starts a Telnet session. However, terminating the Telnet session does not terminate the raw TCP session. When the raw TCP session starts running, the MAX displays the word `connected`. You can then use the TCP session to transport data by running an application on top of TCP. You can hang up the device at either end to terminate the raw TCP session. If you are using a remote terminal-server session, ending the connection also terminates raw TCP.

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

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

Telnet

Description: Initiates a login session to a remote host.

Usage: Enter the command in the following format:

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

The elements of the syntax are as follows:

Syntax element	Description
`–a` **`|–b`** **`|`** **`–t`**	Optional arguments specifying ASCII, Binary, or Transparent mode, respectively. If one of the arguments is entered, it overrides the setting of the Telnet Mode parameter. In ASCII mode, the MAX uses standard 7-bit mode. In Binary mode, the MAX tries to negotiate 8-bit mode with the server at the remote end of the connection, so that the user can send and receive binary files by means of 8-bit file transfer protocols. In transparent mode, either of the other modes can be used without specifying the mode.
`hostname`	The remote system's DNS name if you have configured DNS. If you have not, you must specify the IP address of the remote system.
`port-number`	An optional argument specifying the port to use for the session. The default is 23, which is the port number of the well-known port for Telnet.

When your screen displays the `telnet>` prompt, you can enter any of the Telnet commands described later in this section. You can quit the Telnet session at any time by entering the Quit command at the Telnet prompt:

```
telnet> quit
```

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

Enter the following commands at the Telnet prompt during an open session:

Command	Action
Ctrl-]	Display the Telnet prompt while logged into a host.
`Help` or **`?`**	Display information about Telnet session commands.
`open`	Open a Telnet connection.
`send`	Send standard Telnet commands such as Are You There or Suspend Process.
`send ?`	Displays a list of Send commands and their syntax.
`set`	Specify special characters for use during the Telnet session.
`set all`	Display current settings.
`set ?`	Display a list of Set commands.
`close` or **`quit`**	Quit the Telnet session and close the connection.

Example: Examples of Telnet commands and the resulting output follow:

```
ascend% telnet myhost
```

If you do not configure DNS, you must specify the host's IP address instead of a symbolic name such as **myhost**.

Several options in the Ethernet > Mod Config > TServ Options subprofile affect Telnet. For example, if you set Def Telnet to Yes, you can just type a hostname to open a Telnet session with that host:

```
ascend% myhost
```

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

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

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

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

Test

Description: The MAX can use two open channels to run a self-test in which it calls itself by placing the call on one channel and receiving it on the other channel.

Usage: To run the test, execute the Test command:

test *phonenumber* [***frame-count***] [**data-svc=*data-svc* **] [**call-by-call=*T1-PRI-service***] [**primary-number-type=*AT&T-switch***] [**transit-number=*IEC***]

The elements of the syntax are as follows:

Syntax element	Description
phonenumber	The phone number of the channel receiving the test call. This can include the numbers 0 through 9 and the characters ()[]-, but cannot include spaces.
frame-count	The optional frame-count argument is a number from 1 to 65535 specifying the number of frames to send during the test. The default is 100.
data-svc	A data service identical to any of the values available for the Data Svc parameter of the Connection profile. If you do not specify a value, the default value is the one specified for the Data Svc parameter.

T1-PRI-service	Any value available to the Call-by-Call parameter of the Connection profile. The Call-by-Call parameter specifies the PRI service that the MAX uses when placing a PPP call. If you do not specify a value, the default is as specified for the Call-by-Call parameter.
AT&T-switch	Any value available to the PRI # Type parameter of the Connection profile. The PRI # Type parameter specifies an AT&T switch. If you do not specify a value, the default value is the one specified for the PRI # Type parameter.
IEC	Any value available to the Transit # parameter of the Connection profile. The Transit # parameter specifies the U.S. Interexchange Carrier (IEC) you use for long distance calls over a PRI line. If you do not specify a value, the default is as specified for the Transit # parameter.

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

If you enable trunk groups on the MAX, you can specify the outgoing lines to be used in the self-test. If you do not, the MAX uses the first available T1 (or E1) line.

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

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

Message	Explanation
`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 phone number you specified was incorrect.

Example:

```
ascend% test 555-1212
calling...answering...testing...end
200 packets sent, 200 packets received
```

Traceroute

Description: Traces the route an IP packet follows by launching UDP probe packets with a low time-to-live value and listening for an ICMP time exceeded reply from a router. This command is used to locate slow routers or diagnose IP routing problems.

Usage: Enter the command in the following format:

`traceroute` [**`-n`**] [**`-v`**] [**`-m`** ***`max_ttl`***][**`-p`** ***`port`***] [**`-q`** ***`nqueries`***] [**`-w`** ***`waittime`***] ***`host`*** [***`datasize`***]

All flags are optional. The only required argument is ***`host`***, the destination hostname or IP address. The elements of the syntax are as follows:

Syntax element	Description
`-n`	Print hop addresses numerically rather than symbolically and numerically. This eliminates a name server address-to-name lookup for each gateway found on the path.
`-v`	Verbose output. Lists all received ICMP packets other than Time Exceeded and ICMP Port Unreachable.
`-m` ***`max_ttl`***	Set the maximum time-to-live (maximum number of hops) for outgoing probe packets. The default is 30 hops.
`-p` ***`port`***	Set the base UDP port number used in probes. Traceroute depends on having nothing listening on any of the UDP ports from the source to the destination host (so that an ICMP Port Unreachable message is returned to terminate the route tracing). If something is listening on a port in the default range, you can set the `-p` option to specify an unused port range. The default is 33434.
`-q` ***`nqueries`***	Set the maximum number of queries for each hop. The default is 3.
`-w` ***`waittime`***	Set the time to wait for a response to a query. The default is 3 seconds.
`host`	The destination host by name or IP address.
`datasize`	Set 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: For example, to trace the route to the host `techpubs`:

```
ascend% traceroute techpubs

traceroute to techpubs (10.65.212.19), 30 hops MAX, 0 byte packets
 1  techpubs.eng.ascend.com (10.65.212.19)  0 ms  0 ms  0 ms
```

Trunk-Quiesce-Enable

Description: Enables automatic trunk quiescing whenever a MultiVoice gateway is unable to register with either a primary or secondary MultiVoice Access Manager, or forces a MultiVoice gateway to unregister whenever the trunk connection to the PSTN is unavailable.

Usage: Assigning the value `yes` to the Trunk-Quiesce-Enable parameter will cause the MultiVoice gateway to make itself unavailable to accept calls whenever it becomes unregistered or it looses the connection to the PSTN. Assigning the value `no`, the default, will allow it to continue processing call requests when unregistered or its PSTN connection goes down.

Example: The following commands enable trunk deactivation for T1 PRI lines configured for VoIP:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read

admin> set trunk-quiesce-enable = yes

admin> write
VOIP/{ 0 0 } written
```

Location: Voip { 0 0 }, Voip { x x }

Quit

Description: Closes terminal server session and returns to the Main Edit Menu in the VT100 interface.

Usage: Enter the command at the terminal-server prompt.

Example: `ascend% quit`

VT100 Interface Parameters

4

Note: MAX 6000, MAX 3000, and MAX 800 units support a variety of software loads and hardware features, which are customized for particular purposes. Your unit might not support all of the parameters described in this guide.

Numeric

Complete

Description: Enables detection and collection of up to 15 digits for inbound dialed telephone numbers on MultiVoice gateways using E1 trunks supporting inband CMF R2.

Usage: Press [Enter] to toggle through the list of valid values for the # Complete parameter, from `0 digits` through `15 digits`, to select the desired value. Press [Esc] to exit this menu; then press [Enter] to save the change.

Example: `# Complete=15 digits`

Dependencies: The following dependencies apply when `Sig Mode=DTMF_R2`:

- Once selected, DTMF R2 detection is enabled with the next VoIP call
- This parameter defaults to `N/A` when the Sig Mode parameter is assigned the following values:
  - `Kuwait`
  - `ISDN`
  - `P7`
  - `DPNSS`
  - `NONE`

Location: Net/E1 > Line Config > <*Line number*>

Complete (E1 MFC-R2)

Description: Sets the condition the MultiVoice gateway uses to determine the length of the dial string. For E1 MFC-R2, the MultiVoice gateway continues to collect digits until the on/off pulsing used to transmit the dial string is complete.

Usage: The Number Complete parameter now accepts the following value:

Parameter value	Usage
`Timeout`	Assigning this value configures the MultiVoice gateway to reset the network idle timer after the initial digit is received and then wait for silence. Once silence is detected, wait the interval specified by the InterDigit Timeout parameter for the next digit. The MultiVoice gateway continues to collect digits, while waiting for the network idle timer to expire before continuing with call processing.

Example: The following illustrates how to configure a MultiVoice gateway to determine the length of a dial string using time-out processing.

1. From the MAX administration menu, select the Net/E1 > Line Config > Line profile.
2. Scroll down to the appropriate Line, then select the Line Config > Line # profile. Press [Enter] to open this profile.
3. Scroll down to the # Complete parameter, then press [Enter] to toggle the value of this parameter, as illustrated.

   ```
   # Complete=Timeout
   ```

4. Press [Esc] until the option to `Exit and accept` your changes appears, then save your changes.

Dependencies: E1 MFC-R2 signaling is country specific. The Sig Mode parameter, and the Country parameter in the System profile, must be set for the country-appropriate signaling in order for the MultiVoice gateway to properly detect dialed digits.

Location: Net/E1 > Line Config > Line *xx* > Line *x*

1st Line

Description: Enables or disables the first T1 or E1 line. If the line is disabled, the MAX drops existing connections and brings down the line.

Usage: Specify one of the following values:

- Quiesced—Set all inactive channels on that line to the out_of_service state, as soon as the user saves the changes to the profile. When current calls on that line are ended, the associated channels will be put out of service. When the MAX unit has been quiesced, setting the 1st Line parameter to any other setting restores all channels to the in_service state as soon as the user saves the profile.
- Disabled—Disable the line.
- Trunk (the default)—Enable line 1 to exchange signaling information over the interface.
- T-Online-USER —Specify that the line connects to the switch, allowing the user to dial in.
- T-Online-ZGR—Specify that the line connects to the ZGR server.

Example: `1st Line=Trunk`

Dependencies: If you specify Quiesced, 2nd Line cannot specify D&I.

Location: Net/T1 > Line Config, Net/E1 > Line Config

See Also: Sig Mode

2nd Adrs

Description: Assigns a second IP address to the Ethernet interface. This parameter gives the MAX a logical interface on a second network or on a different subnet on the same backbone. This feature is called *dual IP.*

Usage: Specify a valid IP address on the remote subnet. The default value is 0.0.0.0/0.

Example: `2nd Adrs=10.65.212.56/24`

Location: Ethernet > Mod Config > Ether Options

See Also: IP Adrs

2nd Line

Description: Enables or disables the second T1 or E1 line and specifies the type of service it supports. Drop-and-Insert applications are used to accept calls on line 1 and drop them through to line 2. Drop-and-Insert is typically used to drop voice calls through from line 1 to a PBX on line 2.

Usage: Specify one of the following values:

- Quiesced—Set all inactive channels on that line to the out_of_service state as soon as the user saves the changes to the profile. When current calls on that line are ended, the associated channels will be put out of service. When the MAX unit has been quiesced, setting the 2nd Line parameter to any other setting restores all channels to the in_service state as soon as the user saves the profile.
- Disabled—Disable the line.
- Trunk (the default)—Enable line 2 to exchange signaling information over the interface.
- D&I—Use the second line for Drop-and-Insert applications only.
- T-Online-USER—Specify that the line connects to the switch, allowing the user to dial in.
- T-Online-ZGR—Specify that the line connects to the ZGR server.

Note: For the MAX 3000, this parameter does not have a D&I value. D&I is an option for the 3rd Line parameter.

Example: `2nd Line=Trunk`

Dependencies: If you specify D&I, some channels on line 1 must also be set up for Drop-and-Insert, and 1st Line cannot be set to Quiesced. To support a PBX, the signaling mode must specify PBX.

Location: Net/T1 > Line Config, Net/E1 > Line Config

See Also: Sig Mode, Ch *N* (*N*=1–24, 1–32)

2nd RIP

Description: Specifies how the MAX unit handles RIP update packets on a second Ethernet interface.

Note: Lucent recommends that all routers and hosts run RIP-v2 instead of RIP-v1. The IETF has voted to move RIP version 1 into the historic category and its use is no longer recommended.

Usage: Specify one of the following values:

- Off (the default)—Do not transmit or receive RIP updates on the interface.
- Recv-v2—Receive RIP-v2 updates on the interface but do not send RIP updates.
- Send-v2—Send RIP-v2 updates on the interface but do not receive RIP updates.
- Both-v2—Send and receive RIP-v2 updates on the interface.

- Recv-v1—Receive RIP-v1 updates on the interface but do not send RIP updates.
- Send-v1— Send RIP-v1 updates on the interface but do not receive RIP updates.
- Both-v1—Send and receive RIP-v1 updates on the interface.

Example: `2nd RIP=Send-v2`

Dependencies: 2nd RIP does not apply if the MAX does not route IP.

Location: Ethernet > Mod Config > Ether Options

See Also: 2nd Adrs, RIP, Route IP

3rd Line

Description: Enables or disables the third T1 or E1 line and specifies the type of service it supports. Drop-and-Insert is typically used to drop voice calls through from line 1 to a PBX on line 3.

Note: This parameter applies to the MAX 3000 only.

Usage: Specify one of the following values:

- Quiesced—Set all inactive channels on that line to the out_of_service state, as soon as the user saves the changes to the profile. When current calls on that line are ended, the associated channels will be put out of service. When the MAX unit has been quiesced, setting the 3rd Line parameter to any other setting restores all channels to the in_service state as soon as the user saves the profile.
- Disabled—Disable the line.
- D&I—Accept calls on line 1 and drop them to line 3.

Location: Net T1 > Line Config > *any profile*

3rd Prompt

Description: Specifies an optional third prompt for a terminal-server login. If this value is null, no third prompt is displayed. If the connection is RADIUS-authenticated, the information entered by the user at the third prompt (up to 80 characters) is passed to the server as the value of the Ascend-Third-Prompt attribute. What the RADIUS server does with this information depends upon how the server is configured.

Usage: Specify up to 20 characters. The default is null.

Example: `3rd Prompt=Password2  > >`

With the setting shown in the example, the terminal server displays the following prompts:

```
Login:
Password:
Password2 > >
```

Dependencies: This parameter is not applicable if terminal services are disabled or if the Auth parameter is set to a value other than RADIUS or RADIUS/LOGOUT.

Location: Ethernet > Mod Config > TServ Options

See Also: TS Enabled, Auth

3rd Prompt Seq

Description: Specifies whether the third prompt appears before or after the login and password prompts.

Usage: Specify one of the following values:

- Last (the default)—If terminal-server security is set to Partial or Full and 3rd Prompt Seq=Last, the MAX unit sends the user's input to the additional prompt to RADIUS as a part of the authentication request. The user's response for this prompt is not echoed, since it is treated like an extra password.
- First—If terminal-server security is set to Partial or Full and 3rd Prompt Seq=First, the string specified for 3rd Prompt parameter appears as soon as the user connects. In this case, the user's input is echoed. It is passed to RADIUS, as part of the authentication request, after the user enters a login name and password.

Example: `3rd Prompt Seq=Last`

Dependencies: This parameter is not applicable if terminal services are disabled or if the Auth parameter is set to a value other than RADIUS or RADIUS/LOGOUT.

Location: Ethernet > Mod Config > TServ Options

See Also: TS Enabled, Auth

7-Even

Description: Specifies whether the MAX uses 7-bit even parity on data it sends toward a dial-in terminal-server user.

In 7-bit communication, each device sends only the first 128 characters in the ASCII character set, because each of these characters can be represented by seven bits or fewer. Parity is a way for a device to determine whether it has received data exactly as the sending device transmitted it. Each device must determine whether it will use even parity, odd parity, or no parity.

The sending device adds the 1s in each string it sends and determines whether the sum is even or odd. Then, it adds an extra bit, called a parity bit, to the string. If even parity is in use, the parity bit makes the sum of the bits even. If odd parity is in use, the parity bit makes the sum of the bits odd. For example, if a device sends the binary number 1010101 under even parity, it adds a 0 (zero) to the end of the byte, because the sum of the 1s is already even. However, if it sends the same number under odd parity, it adds a 1 to the end of the byte in order to make the sum of the 1s an odd number.

The receiving device checks whether the sum of the 1s in a character is even or odd. If the device is using even parity, the sum of the 1s in a character should be even. If the device is using odd parity, the sums of the 1s in a character should be odd. If the sum of the 1s does not equal the parity setting, the receiving device knows that an error has occurred during the transmission of the data.

For special ASCII characters (128–256), eight bits are necessary to represent the data. In 8-bit communication, no parity bit is used.

Usage: Specify Yes or No. No is the default and should be used for most applications.

Yes turns on the use of 7-bit even parity on data sent to dial-in terminal-server users.

No turns off 7-bit even parity.

Example: `7-Even=No`

Dependencies: This parameter is not applicable if terminal services are disabled.

Location: Ethernet > Mod Config > TServ Options

See Also: TS Enabled

A

Acct

Description: Specifies the type of accounting service to use for incoming and outgoing bridging/routing calls, and for incoming terminal-server calls. When you enable accounting using RADIUS or TACACS+, you must use the Acct Host parameter to specify the address of the server.

Usage: Specify one of the following values:

- None (the default)—No accounting takes place.
- RADIUS—Enable RADIUS accounting.
- TACACS+—Enable TACACS+ accounting.

Example: `Acct=RADIUS`

Dependencies: RADIUS accounting is disabled if you set Auth to RADIUS/LOGOUT.

Location: Ethernet > Mod Config > Accounting

See Also: Acct Host #*N*, Auth

Acct Checkpoint

Description: Specifies the interval, in minutes, at which RADIUS accounting checkpoint records should be sent for all users. The Checkpoint message contains the same attributes as the Stop message, except that the value for Acct-Status-Type is 3 (Checkpoint).

Usage: Press Enter to open the text field. Type a number from 0 to 60. The default setting is 0, which disables this feature.

Dependencies: The Acct Checkpoint parameter does not apply (`Acct Checkpoint=N/A`) if RADIUS accounting is not used.

Location: Ethernet > Mod Config > Accounting

Acct Compat Mode

Description: Enables or disables Vendor-Specific attribute (VSA) compatibility mode when the unit is using Remote Authentication Dial-In User Service (RADIUS) for accounting purposes.

Usage: Specify one of the following settings:

- Old (the default)—The unit does not send the Vendor-Specific attribute to the RADIUS server and does not recognize the Vendor-Specific attribute if the server sends it. All attributes are sent in standard RFC format.
- VSA—Specifies 8-bit VSA support. All standard attributes are sent in standard RFC format and all VSAs are sent in 8-bit VSA format. The unit ignores all VSAs in received packets that do not have Vendor-Id set to Ascend-Vendor-Id.
- 16Bit VSA—Specifies 16-bit VSA support. All standard attributes are sent in standard RFC format and all VSAs are sent in the 16-bit VSA format as Lucent VSAs. The system ignores all VSAs in received packets that do not have Vendor-Id set to Lucent-Vendor-Id. In this format, the first 256 Lucent VSAs are mapped to the 256 Ascend VSAs.

Example: `Acct Compat Mode=VSA`

Location: Ethernet > Mod Config > Accounting

See Also: Auth Compat Mode, Compat Mode

Acct Host

Description: Specifies the IP address of a connection-specific accounting server to use for information related to this link.

Usage: Specify the IP address of an accounting server.

Example: `Acct Host=10.2.3.4/24`

Dependencies: This parameter does not apply unless the Acct Type parameter specifies that a connection-specific server will be used.

Location: Ethernet > Connections > *Connection profile* > Accounting

See Also: Acct Type

Acct Host #*N* (*N*=1–3)

Description: Specifies the IP address of an external accounting server. The MAX first tries to connect to server #1. If it receives no response, it tries to connect to server #2. If it receives no response, it tries server #3. If the MAX unit connects to a server other than server #1, the unit continues to use that server until it fails to service requests, even if the first server has come online again.

Note: The addresses must all point to servers of the same type, as specified by the Acct parameter (either TACACS+ or RADIUS).

Usage: Specify an IP address in dotted-decimal format, separating the optional netmask with a slash character. The default value is 0.0.0.0. This setting specifies that no authentication server exists.

Dependencies: The Acct Host #*N* parameter does not apply if Acct is set to None.

Location: Ethernet > Mod Config > Accounting

See Also: Acct

Acct-ID Base

Description: Specifies whether the numeric base of the RADIUS Acct-Session-ID attribute is 10 or 16. It controls how the Acct-Session-ID attribute is presented to the accounting server. For example, a base-10 session ID is presented as 1234567890, and a base-16 ID as 499602D2. You can set this parameter globally and for each connection.

The Acct-Session-ID attribute is defined in section 5.5 of the RADIUS accounting specification. For more information, see the *TAOS RADIUS Guide and Reference*.

Note: Changing the value of this parameter while accounting sessions are active results in inconsistent reporting between the Start and Stop records.

Usage: Specify one of the following values:

- 10 (decimal)—The numeric base is 10. This is the default.
- 16 (hexadecimal)—The numeric base is 16.

Example: `Acct-ID Base=10`

Dependencies: This parameter applies only to RADIUS accounting. (It does not apply to TACACS+.) Also, this parameter applies in a Connection profile only if the Acct Type parameter specifies that connection-specific accounting information will be used.

Location: Ethernet > Mod Config > Accounting, Ethernet > Connections > *Connection profile* > Accounting

See Also: Acct, Acct Type

Acct Key

Description: Specifies a RADIUS or TACACS+ shared secret. A shared secret acts like a password between the MAX and the accounting server.

Usage: Specify the text of the shared secret. The value you specify must match the value assigned in the RADIUS clients file or the TACACS+ configuration file.

Example: `Acct Key=Lucent`

Dependencies: This parameter applies in a Connection profile only if the Acct Type parameter specifies that connection-specific accounting information will be used.

Location: Ethernet > Mod Config > Accounting, Ethernet > Connections > *Connection profile* > Accounting

See Also: Acct, Acct Host #*N*, Acct Type

Acct Max Retry

Description: Addresses the situation in which the RADIUS accounting server is not responding to the MAX unit's Accounting Request packets. The parameter specifies the number of times the unit sends an Accounting Request packet before giving up. If the RADIUS accounting backoff queue overflows, the unit discards Accounting Requests packets whether or not they have reached the maximum number of attempts.

Usage: Enter an integer to specify the maximum number of retries allowed. Enter 0 to disable this feature and remove the retry limit.

Dependencies: This parameter applies only if the Acct parameter is set to RADIUS and the other required RADIUS accounting parameters have been set.

Location: Ethernet > Mod Config > Accounting

See Also: Acct Checkpoint, Acct Timeout, Acct, Acct Host, Acct Port, Acct Src Port, Acct Key, Sess Timer, Acct Reset Terminal, Allow Stop Only

Acct Port

Description: Specifies the UDP port number that the MAX unit uses in accounting requests.

Usage: Specify a UDP port number that matches the port number the accounting daemon uses. For RADIUS, the default value is 1646. For TACACS+, the default value is 49.

Example: `Acct Port=1545`

Dependencies: This parameter applies in a Connection profile only if the Acct Type parameter specifies that connection-specific accounting information will be used.

Location: Ethernet > Mod Config > Accounting, Ethernet > Connections > *Connection profile* > Accounting

See Also: Acct, Acct Host #*N*, Acct Type

Acct Reset Timeout

Description: Forces the MAX to try to return to the primary RADIUS accounting server, specifically, the server specified by the Acct Host #1 parameter.

If a timeout occurs while the MAX unit is waiting for a reply to an accounting request to the primary RADIUS server, the unit sends the accounting request to the secondary RADIUS server specified by Acct Host #2, and if that fails, to the secondary RADIUS server specified by Acct Host #3. If either of the secondary servers acknowledges the request, the MAX unit continues to use that server instead of the primary server. The Acct Reset Timeout parameter specifies the period of time for which the unit uses the secondary RADIUS server. At the end of this time period, the unit sends the next accounting request to Acct Host #1.

Usage: Enter the time period in seconds. Any value from 0 to 86400 is allowed. To disable this feature enter 0, which is equivalent to an infinite number of seconds. That is, the MAX does not return to the primary server as long as the secondary server is replying to requests.

Location: Ethernet > Mod Config > Acct

See Also: Acct Host #*N*

Acct Src Port

Description: Specifies the source port used to send a RADIUS or TACACS+ accounting request. You can specify the same source port for authentication and accounting requests.

Usage: Specify a port number from 0 to 65535. The default value is 0 (zero). If you accept this value, the MAX can use any port number from 1024 to 2000.

Location: Ethernet > Mod Config > Accounting

See Also: Auth Src Port

Acct Timeout

Description: Specifies the amount of time the MAX waits for a response to a RADIUS accounting request. You can set this parameter globally and for each connection.

If the MAX unit does not receive a response within the specified amount of time, the unit sends the accounting request to the next server's address (for example, server #2). If all RADIUS accounting servers are busy, the unit stores the accounting request and tries again at a later time. It can queue up to 154 requests.

Usage: Specify a number from 1 to 10. The default global value is 0. The default in a Connection profile is 1.

Example: `Acct Timeout=3`

Dependencies: This parameter applies only to RADIUS accounting. Because TACACS+ uses TCP, it has its own timeout method. Also, this parameter applies in a Connection profile only if the Acct Type parameter specifies that connection-specific accounting information will be used.

Location: Ethernet > Mod Config > Accounting, Ethernet > Connections > *Connection profile* > Accounting

See Also: Acct, Acct Type

Acct Type

Description: Specifies whether to use a connection-specific accounting server for accounting related to this link.

Usage: Specify one of the following values:

- None (the default)—The MAX logs information to the accounting server specified in the Ethernet profile.
- User—The MAX logs information to the accounting server specified elsewhere in the same Connection profile.
- User+Default—The MAX logs accounting information to both servers.

Example: `Acct Type=User`

Dependencies: Connection-specific accounting options rely on the setup in the Accounting subprofile of the Ethernet profile.

Location: Ethernet > Connections > *Connection profile* > Accounting

ACK Suppression

Description: For DTE-initiated calls, specifies whether the PAD sends an acknowledgment when it receives an opening frame from the DTE and also when it establishes a virtual call with the host.

Usage: Specify one of the following values:

- Off (the default)—The PAD acknowledges the DTE's opening frame and the establishment of a call with the host.
- On—The PAD acknowledges neither the DTE's opening frame nor the establishment of a call with the host.

Dependencies: This parameter applies only to DTE-initiated calls using Transparent or Blind mode.

Location: Ethernet > Connections > *Connection profile* > Encaps Options,
Ethernet > Answer > T3POS Options

Activ

Description: Activates a call management time period for an AIM call. You can divide an AIM call that specifies dynamic call management into time periods, each characterized by separate Activ, Beg Time, Max Ch Cnt, Min Ch Cnt, and Target Util parameters.

Usage: Specify one of the following values:

- Enabled—Activate the time period. This is the default for Time Period 1.
- Disabled—Ignore the time period. This is the default for Time Periods 2, 3, and 4.
- Shutdown—Clear the dynamic call during the time period and redial it at the end of the time period. The MAX unit can use a shutdown port for answering and dialing calls, but the unit clears these calls when the shutdown period ends.

Example: `Activ=Enabled`

Dependencies: This parameter is not applicable unless Call Mgm is set to Dynamic.

Location: Host/Dual (Host/AIM6) > Port*N* > Directory > Time Period *N*

See Also: Beg Time, Call Mgm, Target Util, Time Period *N*

Activation

Description: Selects the signals at the serial WAN port that indicate that the Data Circuit-Terminating Equipment (DCE) is ready to connect. Flow control is always handled by the Clear To Send (CTS) signal.

Usage: Specify one of the following values:

- Static—The MAX does not use flow control signals because the DCE is always connected.
- DSR Active—The DCE raises the DSR signal when it is ready.
- DSR+DCD—The DCE raises the DSR and DCD signals when it is ready.

Example: `Activation=Static`

Location: Serial WAN > Mod Config

Active (Numbering Plan)

Description: Activates a profile or feature (making it available for use).

Usage: Specify Yes or No. The default is No.

- Yes—Activates the profile or feature.
- No—Disables the profile or feature.

Location: System > Numbering Plan > *Numbering Plan profile;* System > Call Routes > *Call Routes profile*

Active (SNMPv3)

Description: In an SNMPv3 Notifications or SNMPv3 Target Params submenu, specifies whether the profile is used to generate notification messages (traps). In an SNMP Traps submenu, specifies whether traps are sent to the host specified by the profile.

Usage: Specify Yes or No.

- Yes specifies that the profile is used to generate notifications or that traps are sent.
- No (the default) specifies that the profile is not used to generate notifications or that traps are not sent.

Example: `Active=yes`

Location: Ethernet > SNMPv3 Notifications, Ethernet > SNMPv3 Target Params, Ethernet > SNMP Traps

See Also: Dest Port, Message Proc Model, Notify Tag List, Security Level, Security Model, Security Name, Tag, Target Param Name

Active (SNMPv3 USM Users)

Description: Activates an SNMPv3 USM user profile and makes it available for use.

Usage: Specify Yes or No. No is the default.

Example: `Active=Yes`

Location: Ethernet > SNMPv3 USM Users > *SNMPv3 USM Users profile*

See Also: Auth Protocol, Message Type, Name (SNMPv3 USM Users), Passwd (SNMPv3 USM Users), Priv Protocol, R/W Access, Security Level

Add Number

Description: 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.

Usage: Specify the digits you want the MAX to add to the beginning of the telephone number. You can specify any digit string that the PRI switch requires. The default is null.

Example: `Add Number=923`

Dependencies: This parameter applies only to T1 lines using PBX-T1 conversion.

Location: Net/T1 > Line Config > Line *N*

See Also: Dial #, Delete Digits, Sig Mode

Add Pers

Description: Specifies the number of seconds that average line utilization (ALU) must persist beyond the target utilization threshold before the MAX adds bandwidth from available channels. When adding bandwidth, the MAX adds the number of channels specified by the Inc Ch Count parameter.

Usage: Specify a number from 1 to 300. The factory default value is 5 for MP+ calls and 20 for AIM calls with dynamic call management.

Example: `Add Pers=10`

Dependencies: This parameter is not applicable in a call profile unless Call Mgm=Dynamic. It is not applicable in a Connection profile unless Encaps=MPP. (Call profiles are in Host/Dual (Host/AIM6) > Port *N* > Directory menu.)

Location: Ethernet > Answer > PPP Options, Host/Dual (Host/AIM6) > Port*N* Menu > Directory, Ethernet > Connections > *Connection profile* > Encaps Options

See Also: Call Mgm, Encaps

Adv Dialout Routes

Description: Specifies whether the MAX should stop advertising (*poison*) its IP dialout routes if no trunks are available.

Note: This parameter is intended for use when two or more MAX units on the same network are configured with redundant profiles and routes. It solves a problem that occurred when two or more MAX units on the same network were configured with redundant profiles and routes. If one of the redundant MAX units lost its trunks temporarily, it continued to receive outbound packets that should have been forwarded to the redundant MAX.

Usage: Specify one of the following values:

- Always (the default)—Always advertise IP routes. Use this setting unless you have redundant MAX units or do not use dial-out routes.
- Trunks Up—Stop advertising (poison) the unit's IP dialout routes if it temporarily loses the ability to dial out.

Example: `Adv Dialout Routes=Always`

Dependencies: This parameter is not applicable unless the MAX is being used in a redundant configuration.

Location: Ethernet > Mod Config

Alarm

Description: Specifies whether the MAX traps alarm events and sends a traps Protocol Data Units (PDU) to the SNMP manager. The following alarm events are defined in the Ascend Enterprise MIB. (For the most up-to-date information, see the Ascend Enterprise MIB.)

Alarm event	Signifies
coldStart (RFC-1215 trap-type 0)	Is reinitializing itself and the configuration of the SNMP manager or the unit might be altered.
warmStart (RFC-1215 trap-type 1)	Is reinitializing itself but neither the configuration of the SNMP manager nor that of the unit will be altered.
linkDown (RFC-1215 trap-type 2)	Recognizes a failure in one of the communication links represented in the SNMP manager's configuration.
linkUp (RFC-1215 trap-type 3)	Recognizes that one of the communication links represented in the SNMP manager's configuration has come up.
frDLCIStatusChange (RFC-1315 trap-type 1)	Recognizes that one of the virtual circuits (to which a DLCI number has been assigned) has changed state. That is, the link has either been created or invalidated, or it has toggled between the active and inactive states
eventTableOverwrite (ascend trap-type 16)	Detected that a new event has overwritten an unread event. This trap is sent only for systems that support the Ascend 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.

Usage: Specify Yes or No. Yes is the default.

Yes causes the MAX to generate alarm-event traps and send the trap PDUs to the SNMP host.

No specifies alarm-events traps are not generated.

Example: `Alarm=Yes`

Location: Ethernet > SNMP Traps

Alarm Threshold

Description: Specifies a number to use as a threshold for generating an SNMP alarm trap as part of the heartbeat monitoring feature. If the number of monitored packets falls below this number, the following SNMP alarm trap is sent:

```
Trap type: TRAP_ENTERPRISE
Code: TRAP_MULTICAST_TREE_BROKEN (19)
Arguments:
1) Multicast group address being monitored (4 bytes),
2) Source address of last heartbeat packet received (4 bytes),
3) Slot time interval configured in seconds (4 bytes),
4) Number of slots configured (4 bytes),
5) Total number of heartbeat packets received before the MAX
started sending SNMP Alarms (4bytes).
```

When it is running as a multicast forwarder, the MAX is continually receiving multicast traffic. The heartbeat-monitoring feature enables you to monitor possible connectivity problems by continuously polling for this traffic and generating an SNMP alarm trap if there is a traffic breakdown.

Note: Heartbeat monitoring is optional. It is not required for multicast forwarding.

Usage: Specify a number.

Example: `Alarm Threshold=3`

Dependencies: To set up heartbeat monitoring, you must configure several parameters that define what packets will be monitored, how often and for how long to poll for multicast packets, and the threshold for generating an alarm. These parameters do not apply if multicast forwarding is not in use.

Location: Ethernet > Mod Config > Multicast

See Also: HeartBeat Addr, HeartBeat Udp Port, Source Addr, Source Mask, HeartBeat Slot Time, HeartBeat Slot Count

AlertProgInd

Description: The AlertProgInd parameter configures the type of call progress events which are captured and reported in the Q.931 Alert message progress indicator information element by the MultiVoice gateway. Once configured, MultiVoice gateways report when specific call routing events occur for VoIP calls passing from the packet network and the switched telephone network.

Usage: The AlertProgInd parameter may be assigned the following values:

Parameter value	Usage
`No Indicator`	Assigning this value, the default, disables alert reporting of call routing events on the egress switched telephone network.

Parameter value	Usage
`Non End2End ISDN`	Assigning this value, the egress MultiVoice gateway reports when calls are connected to a egress switched telephone network which does not use ISDN signaling. The egress switched telephone network may support robbed-bit or detectable DTMF.
`Non ISDN Dest`	Assigning this value, the egress MultiVoice gateway reports when calls are connected to an egress switched telephone network which does not use ISDN signaling, such as a transit network or private network, which does not return call progress signals to the MultiVoice gateway.
`Non ISDN Orig`	Assigning this value, the ingress MultiVoice gateway reports when calls are received from a local switched telephone network which does not use ISDN signaling, such as a transit network or private network, which does not provide call progress signals to the MultiVoice gateway.
`Return to ISDN`	Assigning this value, the egress MultiVoice gateway reports when calls connected across a transit network are routed back on to trunk supporting ISDN signaling.
`Interworking`	Assigning this value, the egress MultiVoice gateway reports if interworking occurs upon connecting a call to the switched telephone network. Such events occur when the selected bearer capability is not supported or when a resource or route with the preferred capability is not available.
`Inband Info`	Assigning this value, the egress MultiVoice gateway reports if inband call progress signaling or other supported non-ISDN signaling is available from the switched telephone network for the connected call.

Example: The following example illustrates how to report when calls are connected to a far-end switched telephone network which does not use ISDN signaling:

1 From the MAX administration menu, select the `Ethernet` > `Mod Config` profile.

2 Scroll down to the PSTN Options, then press [Enter] to open this profile. The following menu appears on your screen:

```
90-C00 Mod Config            x
x PSTN Options...            x
x >Cause Code Enabled=No     x
x  AlertProgInd=No Indicator x
x  ProcProgInd=No Indicator  x
x  Bearer Info=Speech        x
```

3 Scroll down to the AlertProgInd parameter, then press [Enter] to toggle the value of this parameter, as illustrated.

```
AlertProgInd=Non ISDN Dest
```

4 Press [Esc]; then, when prompted, select the option to `Exit and Save` your changes.

Dependencies: Changes to the AlertProgInd parameter take effect with the next VoIP call.

Location: Ethernet > Mod Config > PSTN Options

All Calls Are Fax

Description: Specifies whether all calls should be treated as fax calls or whether the MAX unit needs to authenticate an incoming call on the basis of DNIS or DID.

Note: This parameter applies only to MAX 6000 units.

Usage: Specify one of the following values:

- `yes`—The MAX unit receives all calls as fax calls.
- no—The MAX unit authenticates calls on the basis of DID numbers or DNIS numbers, depending on what is specified in the `InCall Type` parameter.

Dependencies: A MAX unit authenticates a call on the basis of the values specified by the `All Calls Are Fax` and `InCall Type` parameters as follows:

If `All Calls Are Fax` is set to:	**And `InCall Type` is set to:**	**The MAX unit:**
`yes`	`redialer`	Receives any incoming call as a redialer type of fax call
`yes`	`did`	Treats any incoming call as a DID type of fax call
`no`	`did`	Authenticates calls against the (up to four) DID numbers specified by the `DID #N` parameters
`no`	`redialer`	Authenticates calls against the DNIS numbers specified by the `DNIS #N` parameters

Location: Ethernet > Mod Config > IP Fax Options

See Also: Dialer Type, DID #N, DNIS #*N*, InCall Type

Allow as Client DNS

Description: Specifies whether the local DNS servers should be made accessible to PPP connections if the client DNS servers are unavailable.

Client DNS configurations define DNS server addresses that will be presented to WAN connections during IPCP negotiation. They provide a way to protect your local DNS information from WAN users. Client DNS has two levels: a global configuration that applies to

all PPP connections, and a connection-specific configuration that applies to that connection only. The global client addresses are used only if none are specified in the Connection profile.

This parameter acts as a flag to enable the MAX to present the local DNS servers to the WAN connection when not all client DNS servers are defined and available.

Usage: Specify Yes or No. Yes is the default.

- Yes allows clients to use the local DNS servers.
- No prevents clients from using the local DNS servers.

Example: `Allow as Client DNS=No`

Location: Ethernet > Mod Config > DNS

See Also: Client Assign DNS, Client Pri DNS, Client Sec DNS

Allow Coder Fallback

Description: Disallows fall back to alternate audio codecs for VoIP calls. When coder fall back is disabled, the default codec, set using the Pkt Audio Mode parameter, is the only available codec reported by a MultiVoice gateway during call capabilities negotiation. This setting affects VoIP, fax, and transparent modem calls.

Usage: Pressing [Enter] toggles between the following values for the Allow G.711 Fallback parameter:

Value	Description
`Yes`	Using this value, the default, allows a MultiVoice gateway to enable any supported audio codecs for call processing, when that codec is reported as supported on both gateways during call capabilities negotiation.
`No`	Using this value, a MultiVoice gateway overrides the default system behavior and rejects the call if it is unable to select its preferred codec.

Example: The following procedure disables fall back to any audio codecs, except the default codec, following call capabilities negotiation by a MultiVoice gateway.

1. From the MAX Main Edit menu, select: `Ethernet` > `Mod Config` > `VOIP Options`.
2. Scroll down to the Allow Coder Fallback parameter:

   ```
   Allow Coder Fallback=Yes
   ```

3. Press [Enter], changing the value to `No`:

   ```
   Allow Coder Fallback=No
   ```

4. Continue by pressing [Esc] until you are prompted to exit and save your changes, then save this change.

   Only the default audio codec is available for processing the next VoIP call.

Dependencies: The Allow Coder Fallback parameter has the following dependencies:

- If this parameter is set to `no`, the Allow G711 Fallback parameter has no effect.
- If Allow Coder Fallback parameter is set to `Yes`, you can set the Allow G711 Fallback parameter to `No` to prevent the system from selecting the G.711 codec when selecting an

alternate codec. In this case, the system terminates the call if G.711 is the only available choice and it is not the preferred codec. This setting affects VoIP, fax, and transparent modem calls.

Location: Ethernet > Mod Config > VOIP Options

Allow Extern Cfg Rqsts

Description: Limits excess RADIUS traffic by enabling or disabling the MAX to request pseudouser profiles from the RADIUS database. Pseudouser profiles, stored on the MAX, contain information that the MAX can query, including static route configurations, and Frame Relay profile information.

Usage: Specify Yes or No. Yes is the default.

Yes enables the MAX to send external configuration requests to the Radius Auth server.

No disables the MAX so that it does not send any external configuration requests.

Location: Ethernet > Mod Config > Auth

Allow G.711 Fallback

Description: Disallows fall back to the G.711 audio codecs for VoIP calls. Both G.711 a-law and u-law can be removed from the available codecs reported by a MultiVoice gateway during call capabilities negotiation. This setting affects VoIP, fax, and transparent modem calls.

Usage: Pressing [Enter] toggles between the following values for the Allow G.711 Fallback parameter:

Value	Description
`Yes`	Using this value, the default, allows a MultiVoice gateway to enable either of the G.711 audio codecs for call processing, when that codec is reported as supported on both gateways during call capabilities negotiation.
`No`	Using this value prevents a MultiVoice gateway from selecting either of the G.711 audio codecs for call processing, and will not report either of these codecs as supported during call capabilities negotiation.

Example: The following procedure disables fall back to either of the G.711 codecs following call capabilities negotiation by a MultiVoice gateway.

1. From the MAX Main Edit menu, select: `Ethernet` > `Mod Config` > `VOIP Options`.
2. Scroll down to the Allow G.711 Fallback parameter:

   ```
   Allow G.711 Fallback=Yes
   ```

3. Press [Enter], changing the value to `No`:

   ```
   Allow G.711 Fallback=No
   ```

4. Continue by pressing [Esc] until you are prompted to exit and save your changes, then save this change.

   Neither G.711 audio codec is available for the next VoIP call.

Location: Ethernet > Mod Config > VOIP Options

Allow Stop Only

Description: Specifies whether the MAX can send accounting Stop packets that do not contain a username to the RADIUS server. Typically, when RADIUS is turned on, the MAX sends both a Start and a Stop packet to the RADIUS accounting server to record a connection. User authentication is required before a Start packet is sent, so when the connection is terminated before authentication occurs, or when the name and password supplied by the user is rejected, the Start packet is not sent and the Stop packet contains no username.

Usage: Specify Yes or No. No is the default.

Yes specifies that the MAX can send Stop Accounting Packets that do not contain a username to the RADIUS server.

No specifies that there are no restrictions on the type of Account Request packet the MAX can send. This is the default.

Dependencies: Allow Stop Only applies only when the Acct parameter is set to RADIUS and the other required RADIUS accounting parameters have been set.

Location: Ethernet > Mod Config > Accounting

See Also: Acct Checkpoint, Acct Timeout, Acct, Acct Host, Acct Port, Acct Src Port, Acct Key, Sess Timer, Acct Reset Terminal, Allow Stop Only

All Port Diag

Description: Enables or disables a permission that allows a user to perform all port diagnostic commands listed in the Port Diag profile.

Usage: Specify Yes or No. Yes is the default.

Yes specifies that the user can perform all diagnostic commands in the Port Diag profile.

No specifies that the user cannot use those commands.

Example: `All Port Diag=Yes`

Dependencies: This parameter is not applicable if the Operations parameter disables the Operations permission.

Location: System > Security

See Also: Own Port Diag

Analog Encoding

Description: Specifies the encoding standard for digitized analog data. This setting is used for all codecs on the MAX.

If an encoding standard other than the default is selected, modem dial-out does not work; choosing a nondefault encoding method works only for incoming analog data. To arrive at the

proper default, you must clear NVRAM. If a System > Sys Config profile already exists on the MAX and NVRAM is not cleared, the value of Analog Encoding always defaults to u-Law, even if you are using E1.

Usage: Specify one of the following values:

- u-Law—MU-Law encoding. This setting is the default for T1.
- a-Law—A-Law encoding. This setting is the default for E1.

Example: `Analog Encoding=u-Law`

Location: System > Sys Config

Ans

Description: Specifies a telephone number to be used for routing incoming calls from the first T1 line to the second line. This can be an add-on number.

Usage: Specify a telephone number. The default is null. You can enter up to 18 characters, and you must limit your specification to the following characters: `1234567890()[]!z-*#|`

Example: `Ans #=555`

Dependencies: This parameter applies only to T1 lines using PBX-T1 conversion.

Location: Net/T1 > Line Config > Line *N*

See Also: Sig Mode

Ans *N*(*N*=1–4)

Description: Specifies a telephone number to be used for call-routing. This parameter appears in a number of profiles. In each case, it indicates “route calls received on this number to me.” For example, answer numbers specified in the Ethernet profile indicate that calls received on that number should be routed to the Ethernet module (bridge/router). In a modem 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.

Note: Only two answer numbers appear in the Host/BRI line profile.

Usage: Specify the telephone number for each Ans *N*# parameter. You can enter up to 24 characters, which can include a subaddress. You must limit your specification to these characters: `1234567890()[]!z-*#|`

Example: `Ans 1#=1212`

Dependencies: Call routing using the answer number works only when the network conveys the number dialed to the answering device. This service is commonly called Dialed Number Information Service (DNIS). Under most circumstances, the Ans *N*# number setting specifies the number of the device being called (the MAX). However, if the switch type is GloBanD, it specifies the number of the calling device. Routing calls by Ans *N*# number with EAZ service in Europe requires that you include the EAZ subaddress in the Ans *N*# setting.

Location: Ethernet > Mod Config > WAN Options, V.34 Modem > Mod Config, Host/BRI > Line Config > Line *N*, BRI/LT > Line Config > Line *N*, Host/Dual (Host/AIM6) > Port*N* Menu > Port Config, V.110 > Mod Config

See Also: Switch Type, Sub-Adr

AnsOrig

Description: Specifies whether the MAX will enable incoming calls, outgoing calls, or both, for this connection.

Usage: Specify one of the following values:

- Both—The MAX can both initiate calls to and receive calls from the destination specified in the Connection profile. Both is the default.
- Call Only—The MAX can dial out to the destination specified in the Connection profile, but cannot answer calls from that destination.
- Ans Only—The MAX can receive calls from the destination specified in the Connection profile, but cannot initiate calls to that destination.

Example: `AnsOrig=Both`

Dependencies: This parameter is not applicable for leased connections.

Location: Ethernet > Connections > *Connection profile* > Telco Options

See Also: LAN Adrs, Station

Ans Service

Description: Causes the MAX to route 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. This parameter 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 does not route incoming calls to line 2.

Usage: Specify one of the following values:

- 56K—56K data calls
- 56KR—56K calls whose data meets the density restrictions of D4-framed lines
- 64K—64K data calls
- Voice—Voice calls
- 384K/H0—Switched-384K data calls
- 384KR—Switched-384K calls whose data is restricted and which connect to MultiRate or GloBanD data services
- 1536K—Switched-1536 calls that are supported only with ISDN NFAS signaling
- 1536KR—Switched-1536 calls that are supported only with ISDN NFAS signaling, and whose data is restricted
- 128K, 192K, 256K and other multiples of 64K

  These values are available on a line with MultiRate or GloBanD data services. If the MAX has the MultiRate option, these data services appear.

Example: `Ans Service=Voice`

Dependencies: This parameter applies only to T1 lines using PBX-T1 conversion.

Location: Net/T1 > Line Config > Line *N*

See Also: Ans #, PBX Type, Sig Mode

Answer

Description: Specifies how the control-line state determines the way that the MAX answers a call at the port associated with the Port Config profile.

Note: The Answer parameter setting does not prevent you from answering manually.

Usage: Specify one of the following values:

- Auto—Answer every call automatically, regardless of the control-line state. This is the default.
- Terminal—Answer manually by using DO 3.
- DTR Active—Answer only if DTR is asserted at the port, indicating that the codec is ready to receive data. This setting operates with most codecs configured to answer manually.
- DTR+Ring—Answer after one ring if DTR is asserted at the port, for codecs configured to answer manually.
- P-Tel Man—Same as DTR+Ring, but used for a Picture Tel codec configured to answer calls manually. The P-Tel Man setting causes the MAX to wait until all channels of the call are synchronized before it asserts Ring Indicate (RI) to inform the codec of the incoming call. When the codec asserts DTR, it tells the MAX that it is ready.
- V.25bis—Answer according to V.25 bis hardware handshaking. The port must support AIM functionality for this value to have any effect. Note that the MAX does not process the data that go to its AIM ports. The codec processes the data.
- V.25bis-C—Same as V.25bis, but the CTS signal cannot change state during a call.
- X.21—Answer according to X.21 hardware handshaking, as described in CCITT Blue Book Rec. X.21. The X.21 dialing interface on the MAX is often used for direct dialing and answering from an attached codec, router, or other codec.
- None—Use the port for outgoing calls only.

Example: `Answer=Auto`

Location: Host/Dual (Host/AIM6) > Port*N* Menu > Port Config

See Also: Answer-Delay

Answer Delay

Description: Specifies the number of milliseconds the MAX waits before answering an incoming R2 call.

Usage: Specify a number from 100 to 3000. The default is 200. Change the value if the MAX answers calls too quickly.

Example: `set answer-delay=500`

Location: Net/E1 > Line Config > *Line Config profile* > Line *N*

Answer Enabled

Description: Enables or disables answering of calls.

Usage: Specify Yes or No. The default is Yes.

- Yes—Enables the answering of calls.
- No—Disables the answering of calls.

Location: Analog FXS > FXS Config > *FXS Configuration profile* > Line *N*

Answer X.121 Addr

Description: Specifies the X.121 address of the remote X.25 host to which this profile connects. The remote host is assumed to also support RFC1356 encapsulation of IP packets.

Usage: Specify the X.121 address of the remote X.25 host. An X.121 address contains from 1 to 15 decimal digits, such as 031344159782738.

Example: `Answer X.121 Addr=031344159782111`

Dependencies: This parameter applies only to X.25/IP connections. Also, this field cannot be left empty if Call Mode is set to Both or Incoming.

Location: Ethernet > Connections > *Connection profile* > Encaps Options

See Also: Call Mode

APP Host

Description: Specifies the IP address of the host that runs the Ascend Password Protocol (APP) Server Utility. Enigma Logic SafeWord AS and Security Dynamics ACE authentication servers are examples of APP servers.

Usage: Specify the IP address of the authentication server.

The address consists of four numbers from 0 to 255, separated by periods. Use a slash to separate the optional netmask from the address. The default value is 0.0.0.0/0, which specifies that no APP server is available.

Example: `APP Host=200.65.207.63/29`

Dependencies: This parameter applies only to outgoing calls using security card authentication. You must set Send Auth to PAP-Token and APP Server to Yes for the APP Host parameter to have any effect.The APP Server utility must be running on a UNIX or Windows workstation on the local net work.

Location: Ethernet > Mod Config > Auth

See Also: APP Server, Send Auth

Appl Mode

Description: Specifies the application mode for an on-demand X.25 switched connection. A MAX unit supports two X.32 connections, and AO/DI over the switched X.25 connections. This parameter also enables you to route incoming calls to a dedicated X.25 connection.

Note: The X.25 Node Type parameter specifies the X.25 application and how the MAX unit uses the switched-B channel(s) to support that application.

Usage: Specify one of the following values:

- `Net2Net`—The default. This net-to-net X.25 application requires one dedicated X.25 connection for routing incoming X.25 switched virtual calls received from switched B-channel X.25 connections. The switched B-channel
  - Can be set up only by an inbound ISDN circuit-mode call.
  - Requires that X.25 Node Type parameter be set to `DCE`.
  - Can be set up for any 56K/64K bearer capability supported by the MAX unit for one X.25 connection, with X.25 addresses known only to the calling X.25 DTE and the MAX unit.

  The MAX unit can match either the calling number or the called number of the X.32 Connection profile. By setting the `Net2Net` value, you can have a dedicated connection coexisting with the switched connection as long as they each have a unique X.25 address.
- `ISDN Pkt Mode`—Enables the MAX unit to accept ISDN packet-mode calls and bring up on-demand packet-mode X.25 connections. On-demand X.25 implementation is based on X.31, case B, of the 1988 CCITT/ITU blue book. The switched B-channel
  - Can be set up only by an inbound ISDN packet-mode call.
  - Requires that X.25 Node Type be set to `DTE`, because the X.25 connection is connected to the Packet Handler.
  - Must be set up for 64K unrestricted digital transfer mode for one X.25 connection with a unique X.25 address.

  Although you can still set the Answer > Id Auth parameter to have the MAX unit attempt to match a profile to the calling number (which reflects only the X.25 calling address of one of the many X.25 callers), the unit first attempts to match an X.32 Connection profile with the called-party number (which is the X.25 address of the packet-mode call).

Location: Ethernet > Connections > X.32 > *Connection profile* > Encaps Options

Apply To

Description: Specifies how the type of service applies to data flow for each connection.

Usage: Specify one of the following values:

- Incoming—The MAX applies the type of service filter to incoming traffic for this connection.
- Outgoing—The MAX applies the type of service filter to outgoing traffic for this connection.
- Both—The MAX applies the type of service filter to incoming and outgoing traffic for this connection.

Dependencies: If TOS Enabled=No, the Apply To setting is not applicable.

Location: Ethernet > Connections > *Connection profile* > IP Options

See Also: Precedence, Source IP Check, TOS, TOS Enabled, TOS Filter

APP Port

Description: Specifies the UDP port number monitored by the APP server identified by the APP Host parameter.

Usage: Specify a UDP port number. Valid port numbers range from 0 to 65535. The default value is 0, which indicates that no UDP port is being monitored by the APP server.

Example: `APP Port=35`

Dependencies: This parameter applies only to outgoing calls using security card authentication. You must set Send Auth to PAP-Token and APP Server to Yes for the APP Port parameter to have any effect. The APP Server utility must be running on a UNIX or Windows workstation on the local network.

Location: Ethernet > Mod Config > Auth

See Also: APP Server, Send Auth

APP Server

Description: Enables responses to security card password challenges by using the APP Server utility on a UNIX or Windows workstation.

Usage: Specify Yes or No. No is the default.

Yes enables the MAX to respond to password challenges via the APP Server utility running on a local host.

No disables the use of the APP Server utility

Example: `APP Server=Yes`

Dependencies: This parameter applies only to outgoing calls using security card authentication. You must set Send Auth to PAP-Token and APP Server to Yes for the APP Port parameter to have any effect. The APP Server utility must be running on a UNIX or Windows workstation on the local network.

Location: Ethernet > Mod Config > Auth

See Also: Send Auth

AppleTalk

Description: Specifies whether the MAX enables an AppleTalk stack to support AppleTalk routing and AppleTalk Remote Access (ARA) connections.

Usage: Specify Yes or No. No is the default.

Yes enables AppleTalk to support AppleTalk routing and ARA connections.

No disables AppleTalk.

Example: `AppleTalk=Yes`

Location: Ethernet > Mod Config

See Also: ARA, Encaps, Route AppleTalk, AppleTalk Router

AppleTalk Router

Description: Determines whether the MAX is a seed or nonseed router. A routed AppleTalk network must include at least one seed router. Other routers on the network can have a network range of 0, which means that they acquire the network-number range from RTMP packets sent by the seed router. If you specify Non-Seed, the router learns network number and zone information from other routers. You can set up more than one router on a network to be a seed router, but all seed routers must have the same value for both the start and end of the network number range.

Usage: Specify one of the following:

- Seed—The router is an AppleTalk seed router. If you select `AppleTalk Router=Seed`, enter the network-number range in its port description. To prevent conflicts, all seed routers on the same network must have the same value for the start and end of the network-number range.

  The value 0 (zero) does not cause a conflict. Nonseed routers and other seed routers can have a value of 0 for the network-number range. A router with a value of 0 for a network-number range does not send this value to other routers, which means it does not seed the other routers in the network with this range. A router with the 0 value will not acquire a value for that network-number range.

  You must also specify the Default Zone name for the seed router, and the names of any zones that the seed router can seed.
- Non-Seed—The router is not an AppleTalk seed router. It will acquire a network-number range value from a seed router on the network.

Location: Ethernet > Mod Config > AppleTalk Options

See Also: Route AppleTalk, AppleTalk, Net Start, Net End, Peer (Appletalk Options), Default Zone, Zone Name #*N*.

ARA

Description: Specifies whether the MAX allows incoming AppleTalk Remote Access (ARA) calls.

Usage: Specify Yes or No. Yes is the default.

Yes allows the MAX to answer incoming ARA calls, provided they meet all other connection criteria.

No specifies the MAX will not answer incoming ARA calls.

Example: `ARA=Yes`

Dependencies: This parameter is not applicable if AppleTalk is not enabled.

Location: Ethernet > Answer > Encaps

See Also: AppleTalk, Encaps

Area

Description: Specifies the OSPF area that this interface belongs to.

Usage: Specify an area ID in dotted-decimal format. The default 0.0.0.0 represents the backbone network.

Example: `Area=0.0.0.1`

Dependencies: Lucent currently recommends that you configure the local and WAN interfaces in the same area.

Location: Ethernet > Connections > *Connection profile* > OSPF Options, Ethernet > Mod Config > OSPF Options

AreaType

Description: Specifies the type of OSPF area this interface belongs to. If a network is large, the size of the database, time required for route computation, and related network traffic become excessive. You can partition an AS into areas to provide hierarchical routing connected by a backbone.

The backbone area is special and always has the area number 0.0.0.0. Other areas are assigned area numbers that are unique within the autonomous system.

Note: You must set the AreaType parameter consistently on all OSPF routers within the area.

Usage: Specify one of the following values:

- Normal (the default)—In a normal OSPF area, the router maintains information about external routes.
- Stub—For areas that are connected only to the backbone by one ABR (that is, the area has one exit point), there is no need to maintain information about external routes. To reduce the cost of routing, OSPF supports stub areas, in which all external routes are summarized by a default route. Stub areas are similar to regular areas except that the routers do not enter external routes in the area's databases.

Example: `AreaType=Normal`

Location: Ethernet > Connections > *Connection profile* > OSPF Options, Ethernet > Mod Config > OSPF Options

ASE-Tag

Description: Specifies the OSPF ASE tag of this link. The tag is a 32-bit hexadecimal number attached to each external route. This field is not used by the OSPF protocol itself. It can be used by border routers to filter this record.

Usage: Specify a 32-bit hexadecimal number. The factory default is c0:00:00:00.

Example: `ASE-tag=c8:ff:00:00`

Location: Ethernet > Connections > *Connection profile* > OSPF Options, Ethernet > Mod Config > OSPF Options, Ethernet > Static Rtes

ASE-Type

Description: Specifies the OSPF ASE type of the Link-State Advertisement (LSA).

Usage: Specify one of the following settings:

- Type-1 (the default)—A Type-1 external metric. This metric is expressed in the same units as the link-state metric.
- Type-2—A Type-2 external metric. This metric is considered larger than any link-state path. Using a Type-2 external metric assumes that routing between autonomous systems is the major cost of routing a packet. A Type-2 metric eliminates the need for conversion of external costs to internal link-state metrics.

Example: `ASE-type=type1`

Dependencies: RunOSPF must be set to No and Private must be set to No.

Location: Ethernet > Mod Config > OSPF Options

See Also: Area, Area-Type, ASE-Tag, IP-Options, OSPF, OSPF-ASE-Pref, OSPF-Options, OSPF-Pref, Third-Party

Assign Adrs

Description: Enables or disables dynamic IP address assignment for incoming calls.

Usage: Specify Yes or No. No is the default.

Yes enables the MAX to assign an IP address to an incoming PPP call that requests dynamic assignment, provided it has access to a pool of designated IP address.

No disables dynamic IP address assignment.

Example: `Assign Adrs=Yes`

Dependencies: The MAX must have at least one configured pool of IP addresses, either locally or on a RADIUS server.

Location: Ethernet > Answer

See Also: Encaps, LAN Adrs, Pool # Count, Pool # Start, Recv Auth, WAN Alias

AT Answer String

Description: Enables you to add customized AT commands in the answer string of the system's modem configuration.

Usage: Specify one or more valid AT commands, up to a limit of 36 characters. The default is null.

Dependencies: Consider the following:

- Do not begin the string with the characters *AT*. These two characters are automatically added to the beginning of the string, before the MAX sends the commands to the modem.
- Do not include an `A` (answer) or a `D` (dial) command anywhere in the string. An `A` command is automatically added to the end of the string. A `D` command in the answer string causes the call to fail.
- The answer string is the last of four strings sent to the modem when the MAX answers a call. Therefore, the commands you enter can overwrite settings specified elsewhere.
- Be very careful when entering AT commands for AT Answer String. The system does not prevent you from entering incorrect strings.

Location: System > Sys Config

ATMP HA RIP

Description: Enables or disables the sending of Routing Information Protocol (RIP) updates to a mobile client.

Usage: Specify one of the following values:

- Off (the default)—Disabled.
- Send v2—Enabled.

Example: `ATMP HA RIP=Off`

Dependencies: This parameter is not applicable (N/A) if any of the following conditions apply:

- Profile Type parameter is set to disabled.
- Tunnel Protocol parameter is set to PPTP, L2F, or L2TP.
- ATMP Gateway parameter is set to No.

Location: Ethernet > Mod Config > *any Connection profile* > Tunnel Options

See Also: Client ID, Home Network Name, Max Tunnels, Password, Pri. Tunnel Server, Profile Type, Sec. Tunnel Server, Tunnel Protocol, Tunnel VRouter, UDP Port

ATMP Gateway

Description: Instructs the MAX to send data it receives back from the home network on this connection to the mobile node.

Usage: Specify Yes or No. No is the default.

Yes enables the MAX to send data it receives back from the home network on this connection to the mobile node.

No disables this function.

Example: `ATMP Gateway=Yes`

Dependencies: This parameter is not applicable unless the MAX is configured as an ATMP Home Agent in gateway mode.

Location: Ethernet > Connections > *Connection profile* > Session Options

See Also: ATMP Mode, Password, Type, UDP Port

ATMP Mode

Description: Specifies whether Ascend Tunnel Management Protocol (ATMP) is enabled and, if so, whether this MAX unit is a Home Agent, a Foreign Agent, or both.

Usage: Specify one of the following values:

- Disabled (the default)—ATMP is not enabled.
- Home—This unit is a Home Agent.
- Foreign—This unit is a Foreign Agent.
- Both—The MAX will function as both a Home Agent and Foreign Agent on a tunnel-by-tunnel basis.

Example: `ATMP Mode=Home`

Dependencies: If you set ATMP Mode to Disabled, all other fields in the ATMP Options profile become not applicable.

Location: Ethernet > Mod Config > ATMP Options

See Also: ATMP Gateway, Password, Type, UDP Port

Attributes

Description: Specifies which RADIUS attributes will be required to identify a session when Session Key is enabled.

Usage: Specify one of the following values:

- Any (the default)—Any Attribute can be used to identify the session. If multiple attributes are sent, the order in which they are checked is (1) session key, (2) session id, (3) user name, (4) IP address.
- Session—Only the session key attribute is checked for identification.
- All—All Attributes that are applicable must be present and pass validation before any operation is performed on the connection. For example, if a session has a user name, IP address, session id, and session key, all four attributes must be sent. As another example, if a session has a user name, session id, and session key, these attributes must be sent. The IP address is not required.

Example: `Attributes=Any`

Dependencies: This parameter does not apply if Session Key is disabled.

Location: Ethernet > Mod Config > RADIUS Server

See Also: Session Key

Auth

Description: Specifies the type of external authentication server to access for incoming connections. For details about RADIUS, see the *TAOS RADIUS Guide and Reference*. For details about other authentication servers, see the *MAX Security Supplement*.

Usage: Specify one of the following values:

- None (the default)—Disable the use of an authentication server.
- TACACS—Access a TACACS server. TACACS supports PAP, but not CHAP authentication.
- TACACS+—Access a TACACS+ server. TACACS+ supports PAP, but not CHAP authentication, and provides more extensive accounting statistics and a higher degree of control than TACACS authentication.
- RADIUS—Access a RADIUS server. In a RADIUS query, the MAX provides a user ID and password to the server. If the validation succeeds, the server sends back a complete profile. This profile specifies routing, packet filtering, destination-specific static routes, and usage restrictions for the user. RADIUS supports PAP, CHAP, and terminal server validation.
- RADIUS/LOGOUT—Identical to RADIUS, except that when you select RADIUS/LOGOUT, the MAX sends a request to the RADIUS server to initiate logout when the session ends.

  Use this setting to set up an AppleTalk Remote Access connection to a SecurID server using RADIUS.
- Defender—Access a Digital Pathways Defender authentication server.
- SECURID—Access a SecurID ACE server.

Note: If the MAX is configured to use SecurID ACE authentication, all authenticated users are given service only according to the settings in the Ethernet > TServ Options profile. Currently, using RADIUS is the only way to get user-specific configuration information from the SecurID ACE server.

Example: `Auth=RADIUS` (for authentication using RADIUS), `Auth=RADIUS/LOGOUT` (for authentication using RADIUS and a SecurID server).

Dependencies: You must set an Auth Host # parameter to specify a server address.

Location: Ethernet > Mod Config > Auth

See Also: Auth Host*N*, Auth Key, Auth Port, Auth Timeout, Encaps

Auth Boot Host #1

Description: Specifies the IP address of the first RADIUS server from which to request pseudouser configuration information. The MAX requests the information from the specified server rather than from the RADIUS server used for authentication.

Usage: Specify an IP address.

Dependencies: You must also set the Auth Boot Port parameter to specify a port number.

Location: Ethernet > Mod Config > Auth

See Also: Auth Boot Host #2, Auth Boot Port

Auth Boot Host #2

Description: Specifies the IP address of a backup RADIUS server from which to request pseudouser configuration information if the server specified by Auth Boot Host #1 fails to respond. Also applies if no IP address has been specified for Auth Boot Host #1.

Usage: Specify an IP address.

Location: Ethernet > Mod Config > Auth

See Also: Auth Boot Host #1, Auth Boot Port

Auth Boot Port

Description: Specifies the port number the MAX uses when it contacts the server specified by Auth Boot Host #1 or Auth Boot Host #2.

When communicating with either of the Auth Boot Host servers, the MAX uses the Key and, if available, the Src Port setting specified for the RADIUS main authentication server.

Usage: Specify a value from 1 to 65535.

Location: Ethernet > Mod Config > Auth

See Also: Auth Boot Host #1, Auth Boot Host #2

Auth Compat Mode

Description: Enables or disables Vendor-Specific Attribute (VSA) compatibility mode when the unit is using Remote Authentication Dial-In User Service (RADIUS) for authentication and authorization purposes.

Usage: Specify one of the following settings:

- Old (the default)—Specifies that the unit does not send the Vendor-Specific attribute to the RADIUS server and does not recognize the Vendor-Specific attribute if the server sends it. All attributes are sent in standard request for comment (RFC) format.
- VSA—Specifies 8-bit VSA support. All standard attributes are sent in standard RFC format and all VSAs are sent in 8-bit VSA format. The unit ignores all VSAs in received packets that do not have the Vendor-Id parameter set to Ascend-Vendor-Id.
- 16Bit VSA—Specifies 16-bit VSA support. All standard attributes are sent in standard RFC format and all VSAs are sent in the 16-bit VSA format as Lucent VSAs. The system ignores all VSAs in received packets that do not have the Vendor-Id parameter set to Lucent-Vendor-Id. In this format, the first 256 Lucent VSAs are mapped to the 256 Ascend VSAs.

Example: `Auth Compat Mode=VSA`

Location: Ethernet > Mod Config > Auth

See Also: Acct Compat Mode, Compat Mode

Auth Host #*N* (*N*=1–3)

Description: Each of these parameters specifies the IP address of an external authentication server. The MAX unit first tries to connect to server #1. If the unit receives no response, it tries to connect to server #2. If it receives no response, it tries server #3. If the MAX unit connects to a server other than server #1, the unit continues to use that server until it fails to service requests, even if the first server has come online again.

Note: The addresses must all point to servers of the same type, as specified by the Auth parameter (RADIUS, TACACS, or TACACS+). If you are using Defender or SecurID authentication, only Auth Host #1 is applicable, because the MAX can access only one of those servers.

Usage: Specify an IP address in dotted-decimal format, separating the optional netmask with a slash character. The default value is 0.0.0.0, which indicates that no authentication server exists.

Example: `Auth Host #1=10.207.23.6`

Dependencies: This parameter does not apply if authentication services are disabled.

Location: Ethernet > Mod Config > Auth

See Also: Auth, Auth Key, Auth Port, Auth Timeout

Auth Key

Description: Specifies an authentication key for SNMPv3 USM users.

Usage: In most cases, you do not set the authentication key directly. Instead, use the snmpAuthPass command to generate the value. If you have permission to view passwords, the authentication key appears as a hexadecimal value on your screen for save-and-restore purposes. Otherwise, the authentication key appears as a row of asterisks. The default is null.

If you change the value of Auth Key directly, keep in mind that the first byte indicates the length of the field. This value must be 10 (16d in hexadecimal) if Message Digest 5 (MD5) is in use and 14 (20d in hexadecimal) if the Secure Hash Algorithm (SHA) is in use. If you specify an invalid value, the unit uses the previous key, if any, to communicate with the SNMP manager. If no previous key exists, this USM user cannot communicate with the network until a valid key is generated by means of the snmpAuthPass command.

Example: Suppose you use the snmpAuthPass command to generate the following 16-byte string:

```
27 0a dc 75 f8 98 e5 7c 4c 03 22 7d dd ac 0d ef
```

The system displays it as the following Auth Key value:

```
10270adc75f898e57c4c03227dddac0def00000000
```

Dependencies: Consider the following:

- You must generate the authentication key by means of the snmpAuthPass command before the SNMPv3 USM Users profile can be used for communication with the SNMP manager.

- If you change the authentication protocol from MD5 to SHA (or vice versa), you must change the authentication key by means of the snmpAuthPass command. The previous protocol-and-key combination is used until you specify a new one.
- If Auth Protocol is No-Auth, Auth Key does not apply.

Location: Ethernet > SNMPv3 USM Users

See Also: Priv Key

Auth Max Retry Time

Description: Specifies the maximum length of time that the MAX attempts to authenticate a caller by means of an external authentication server, or servers, before disconnecting the call.

Whereas Auth Timeout specifies the number of seconds between retries to each external authentication server, Auth Max Retry Time specifies the total length of time that the MAX stays in retry mode. For example, suppose you have set:

- Auth Timeout to 2
- Auth Max Retry Time to 5

A caller dials in. The MAX sends an authentication request and waits two seconds for a response. If it does not receive a response, the MAX sends a second request and waits two more seconds. If it does not receive a response, the MAX sends a third request and waits one second. If it receives no response from the authentication server, the MAX disconnects the call.

Usage: Specify the number of seconds that the MAX attempts to authenticate a user by means of an external authentication server, or servers, before the MAX disconnects the call. Specify any number of from 0 to 255. The default is zero (0).

The 0 value directs the MAX to send three requests to each configured external authentication server. You set the Auth Timeout parameter to specify the time that the MAX waits before sending each retry.

Example: `Auth Max Retry Time=5`

Dependencies: Auth Max Retry Time only applies if you set Ethernet > Mod Config > Auth > Auth parameter to TACACS+, RADIUS, or RADIUS/LOGOUT.

Location: Ethernet > Mod Config > Auth

See Also: Auth Timeout

Auth Pool

Description: Enables or disables dynamic address assignment for RADIUS-authenticated IP routing connections. The RADIUS server must be configured with at least one pool of addresses for assignment, and must be running the Lucent INS daemon. For details, see the *TAOS RADIUS Guide and Reference*.

Usage: Specify Yes or No. No is the default.

Yes specifies dial-in callers can obtain an IP address dynamically from the RADIUS server.

No disables dynamic IP address assignment for RADIUS-authenticated connections.

Example: `Auth Pool=Yes`

Location: Ethernet > Mod Config > Auth

See Also: Auth

Auth Port

Description: Specifies the UDP or TCP port to use to communicate with the external authentication server. The setting must match the port specified for use in the server's configuration.

If the MAX is acting as a RADIUS client, this parameter specifies the UDP destination port to use for authentication. The UDP port used by RADIUS daemons is specified in the `/etc/services` file (UNIX).

If the MAX is acting as a TACACS or TACACS+ client, this parameter specifies the UDP destination port to use for authentication (49 by default).

If the MAX is acting as a RADIUS server, this parameter specifies the UDP port to use for the on-board RADIUS server. (The on-board server is a mechanism that enables the MAX to respond to messages from the RADIUS daemon, as described in the *TAOS RADIUS Guide and Reference*.) It is set to 1700 by default.

If the MAX is acting as a Defender client, this parameter specifies the TCP port to use to communicate with the server. It is set to 2626 by default.

If the MAX is acting as a SecurID client, this parameter specifies the TCP port to use to communicate with the server. It is set to 5500 by default.

Note: Make sure that the number you specify matches the number that is actually used by the authentication server daemon.

Usage: Specify the port number used by the server.

Example: `Auth Port=1565`

Location: Ethernet > Mod Config > Auth

See Also: Auth, Auth Host*N*, Auth Key, Auth Timeout

Auth Protocol

Description: 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.

Usage: Specify one of the following settings:

- None—No authentication.
- MD5-Auth (the default)—The MAX unit uses the MD5 protocol to authenticate incoming and outgoing messages.

- SHA-Auth—The MAX unit uses the SHA protocol to authenticate incoming and outgoing messages.

Example: `Auth Protocol= md5-auth`

Location: Ethernet > SNMPv3 USM Users> *any SNMPv3 USM Users profile*

See Also: Auth Protocol, Message Type, Name (SNMPv3 USM Users), Passwd (SNMPv3 USM Users), Priv Protocol, R/W Access, Security Level

Auth Req

Description: Specifies how the MAX unit acts if an authentication request times out after a call has been CLID-authenticated.

Usage: Specify Yes or No. Yes is the default.

Yes specifies that the MAX unit drops a call if the authentication request times out after the call has been CLID-authenticated.

No specifies that if the MAX unit attempts external authentication but the request times out, the unit allows the session to be established solely on the basis of CLID authentication.

Example: `Auth Req=Yes`

Dependencies: This parameter is not applicable unless CLID authentication is required.

Location: Ethernet > Mod Config > Auth

See Also: Auth, Auth Host #, Auth Key, Auth Pool, Auth Port, Auth Timeout

Auth Reset Timeout

Description: Forces the MAX unit to try to return to the primary RADIUS authentication server, specifically the server specified by the Auth Host #1 parameter.

If a timeout occurs while the MAX unit is waiting for a reply to an authentication request sent to the primary RADIUS server, the unit sends the authentication request to the secondary RADIUS server specified by Auth Host #2, and if that fails, to the secondary RADIUS server specified by Auth Host #3. If either of the secondary servers acknowledges the request, the MAX unit continues to use that server instead of the primary server. The Auth Reset Timeout parameter specifies the period of time for which the unit uses the secondary RADIUS server. At the end of this time period, the unit sends the next authentication request to the server specified by Auth Host #1.

Usage: Enter the time period in seconds. Any value from 0 to 86400 is allowed. To disable this feature enter 0, which is equivalent to an infinite number of seconds. That is, with the 0 setting, the MAX does not return to the primary server as long as the secondary server is replying to requests.

Dependencies: This parameter is not applicable if `Auth=None` or `Auth=TACACS+` in this profile.

Location: Ethernet > Mod Config > Auth

See Also: Auth Host #*N*

Auth Send Attr 6,7

Description: Specifies whether the MAX unit sends values for RADIUS attributes 6 and 7. Typically, the unit generates appropriate values for RADIUS attribute 6 (user-service) and 7 (framed-protocol) and includes them in authentication requests for incoming calls. To support RADIUS servers that should not receive that information, you can disable this behavior.

Note: When this parameter is set to No, the system cannot differentiate between terminal server users, asynchronous PPP users that authenticate through the terminal server, and SLIP users that authenticate via the terminal server.

Usage: Specify Yes or No. Yes is the default.

Yes causes attributes 6 and 7 to be sent to the RADIUS server in the authentication request. Use this setting if you want to control terminal-server access to PPP and SLIP explicitly by the RADIUS response, or if you use a MERIT RADIUS server.

No excludes attributes 6 and 7 from authentication requests.

Example: `Auth Send Attr 6,7=Yes`

Dependencies: This parameter applies only to RADIUS authentication.

Location: Ethernet > Mod Config > Auth

Auth Src Port

Description: Specifies the source port used to send remote authentication requests. You can specify a source port for all the external authentication services the MAX supports. You can specify the same source port for authentication and accounting requests.

Usage: Specify a port number from 0 to 65535. The default value is 0 (zero). If you accept this value, the MAX can use any port number from 1024 to 2000.

Example: `Auth Src Port=0`

Dependencies: This parameter does not apply if external authentication is not in use.

Location: Ethernet > Mod Config > Auth

See Also: Acct Src Port

Auth Timeout

Description: Specifies the number of seconds between retries to the external authentication server.

If the MAX is acting as a RADIUS, TACACS, or TACACS+ client, the MAX waits the specified number of seconds for a response to an authentication request. If it does not receive a response within that time, it times out and sends the authentication request to the next authentication server (for example, Auth Host #2).

If the MAX is acting as a client of Defender or SecurID client (which do not support more than one server address), the MAX waits the specified number of seconds before assuming that the server has become nonfunctional. For more information about SecurID timeouts, see SecurID Host Retries.

Note: Because remote authentication is tried first if the Local Profiles First parameter is set to No, the MAX waits for the remote authentication to time out before attempting to authenticate locally. This timeout could take longer than the timeout specified for the connection and could cause all connection attempts to fail. To prevent this, set the authentication timeout value low enough to not cause the line to be dropped, but still high enough to permit the server to respond if it is able to. The recommended time is 3 seconds.

Usage: Specify a number from 1 to 10. The default is 1.

Example: `Auth Timeout=10`

Dependencies: This parameter applies only when using an external authentication server.

Location: Ethernet > Mod Config > Auth

See Also: Auth, Auth Host*N*, Auth Key, Auth Port, SecurID Host Retires.

Auth TS Secure

Description: Specifies whether remote dial-in users will be dropped if the immediate login service is TCP-Clear or Telnet and a host is not specified in the RADIUS user profile.

Usage: Specify Yes or No. Yes is the default.

Yes specifies that the connection is dropped if no login host is specified for a terminal-server connection whose immediate service is set to TCP or Telnet.

No specifies that the caller will have access to the terminal-server interface instead.

Example: `Auth TS Secure=Yes`

Dependencies: This parameter does not apply if terminal services are disabled or if RADIUS authentication is not in use.

Location: Ethernet > Mod Config > Auth

See Also: Auth, TS Enabled

AuthKey

Description: Specifies an authentication key (a password) for OSPF routing. The value of this parameter is a 64-bit clear password inserted into the OSPF packet header. The value is used by OSPF routers to allow or exclude packets from an area. The default value for OSPF is *ascend0*.

Usage: Specify a string of up to nine characters for an OSPF auth-key.

Example: `AuthKey=Ascend`

Dependencies: This parameter is not used if AuthType is None.

Location: Ethernet > Connections > *Connection profile* > OSPF Options, Ethernet > Mod Config > OSPF Options

See Also: AuthType

AuthType

Description: Specifies the type of authentication in use for validating OSPF packet exchanges. Note that Simple authentication (the default) is designed to prevent configuration errors from affecting the OSPF routing database. It is not designed for firewall protection.

Usage: Specify one of the following values:

- None—Routing exchanges are not authenticated. The 64-bit authentication field in the OSPF header can contain data, but it is not examined on packet reception. When you use this setting, the MAX performs a checksum on the entire contents of each OSPF packet (other than the 64-bit authentication field) to ensure against data corruption.
- Simple—This setting requires that you specify a 64-bit value for the Auth Key parameter. Each packet sent on a particular network must have the configured value in its OSPF header 64-bit authentication field. Simple is the default.
- MD5—This setting requires that you specify a key identifier for the KeyID parameter or MD5 Key parameter. Each packet sent on a particular network must have the configured value in its OSPF header Key ID or MD5 Key field.

Example: `AuthType=Simple`

Location: Ethernet > Connections > *Connection profile* > OSPF Options, Ethernet > Mod Config > OSPF Options

See Also: KeyID, MD5 Key

Auto-BERT

Description: Specifies that an automatic Bit-Error Rate Test (Auto-BERT) begins as soon as a call connects and runs for the number of seconds you specify for Auto-BERT.

During the test, the MAX unit monitors the entire data stream between codecs. At the end of the time period, if any channels have failed, the unit clears them, redials, and repeats the test. The Call Status window displays BERT MAST at the dialing end of the call, and BERT SLAVE at the answering end of the call. The following status windows display the results of the Auto-BERT:

- The Line Errors window displays errors recorded on all current channels.
- The Session Errors window for a specific AIM port displays the cumulative error count for all channels connected to the port.
- The Port Info window displays the quality of all active calls.
- The Statistics window displays the quality of a call on a specific AIM port.

The maximum number of errors that can accumulate per channel is approximately 65,000. Note that the MAX unit reports the total number of errors for each channel during the current call, not the error rate.

The unit resets the error display for the current call to 0 (zero) when the call disconnects, or if the unit disconnects a channel during the Auto-BERT or during the call itself. You can abort the Auto-BERT at any time by displaying the DO commands and choosing Beg/End BERT.

Usage: Specify 15, 30, 60, 90, or 120 seconds, or Off. The default setting is Off, which disables the Auto-BERT.

Example: `Auto-BERT=Off`

Dependencies: You increase call setup time by at least the amount of time you specify for the Auto-BERT parameter.

Location: Host/Dual (Host/AIM6) > Port*N* Menu > Directory

Auto-Call X.121 Addr

Description: Specifies the X.25 host to call immediately when an X.25/PAD session is established by means of this Connection profile. If Auto-Call X.121 Addr specifies an address, the PAD session can begin automatically. Otherwise, the MAX displays the terminal-server prompt, at which the user can issue the `pad` command to begin a session.

Usage: Specify the information needed to call the X.25 host, up to 48 characters. Use the following format:

address [*P|*D|*F *data*]

where: address is the X.121 address (up to 15 characters) to which the call is made.

- `*P` means do not echo what is entered at the keyboard after the `*P` command, even if you set X.3 parameter number 2 to Echo. (This is to protect passwords that are carried with the call user data.)
- `*D` means echo what is entered at the keyboard after the `*D` command.
- `*F` means that what follows the `*F` command is fast-select data.
- *data* is inserted into the last 12 bytes of the user data field.

Example: `Auto-Call X.121 Addr=031344159782111 *Dpassword`

Dependencies: This parameter applies only to X.25/PAD connections.

Location: Ethernet > Connections > *Connection profile* > Encaps Options

See Also: Immed Service

Auto Logout

Description: Specifies whether the MAX unit automatically logs a user out when a device disconnects from the unit's control port or when the unit loses power.

Usage: Specify Yes or No. No is the default.

Yes causes the MAX unit to log out the current user and go back to default privileges when a device disconnects from the unit's control port or when the unit loses power.

No disables automatic-logout.

Example: `Auto Logout=Yes`

Location: System > Sys Config

Aux Send PW

Description: Specifies the password the MAX sends when it adds channels to a multichannel PPP call that uses PAP-TOKEN-CHAP authentication. The MAX obtains authentication of the first channel of this call from the user's hand-held security card.

Usage: Specify a password. This password must match the one set up for your MAX in the RADIUS users file on the network authentication server (NAS).

Example: `Aux Send PW=Ascend`

Dependencies: This parameter applies only to multichannel PPP calls.

Location: Ethernet > Connections > *Connection profile* > Encaps Options

See Also: Send Auth

B

B&O Restore

Description: Specifies how many seconds the MAX waits before restoring a nailed-up channel to an FT1-B&O call—that is, a call for which Call Type=FT1-B&O.

When the quality of a nailed-up channel falls to Marginal or Poor in an FT1-B&O call, the MAX drops all the nailed-up channels. It then attempts to replace dropped nailed-up channels with switched channels. It also monitors dropped nailed-up channels. When the quality of all dropped channels changes to Fair or Good, the MAX reinstates them.

Usage: Specify the number of seconds you want the MAX to wait before restoring a nailed-up channel. You can enter a number from 30 to 30000. The default is 300.

Example: `B&O Restore=50`

Location: Host/Dual (Host/AIM6) > Port*N* Menu > Directory

See Also: Call Mgm, Call Type

Bi-Dir Auth

Description: Specifies whether CHAP authentication must be bidirectional.

Usage: Specify one of the following values:

- None (the default)—Authentication is unidirectional. The called device identifies the calling device. The MAX unit prevents the authentication in which the calling device identifies the called device.
- Allowed—Authentication can be bidirectional. When the MAX unit is the called device, the MAX unit identifies the calling device. The system also allows the calling device to

authenticate the MAX unit, but this authentication is not mandatory. Therefore, if the calling device does not authenticate the MAX unit, the unit can still accept the call.

When the MAX unit is the calling device, the unit answers the authentication initiated by the called device. The MAX unit tries to negotiate authentication in the opposite direction as well, but if the called device refuses this second authentication option, the call is still established.

- Required—Authentication must be bidirectional. The MAX unit requires that both the calling and called devices authenticate each other. If authentication is not performed in both directions, the MAX unit rejects the call (in the case of an incoming call) or tears down the call (in the case of an outgoing call).

Dependencies: Consider the following:

- If you specify Allowed or Required, and the second authentication is attempted, it must be successful. Otherwise, the MAX unit rejects the call (in the case of an incoming call) or tears down the call (in the case of an outgoing call).
- Bidirectional authentication is applicable only if the authentication mode is CHAP, MS-CHAP, or CACHE-TOKEN.
- When Receive Auth is set to Either, and PAP authentication is negotiated, bidirectional authentication is automatically disabled, even if the Bi-Dir Auth parameter is set to Required. For example, suppose you set Receive Auth to Either and Bi-Dir Auth to Required. If an incoming call occurs and the authentication negotiated is PAP, the authentication will be performed in one direction only.
- Bi-Dir Auth is not applicable if PPP is not enabled, or if Receive Auth is set to None, PAP, PAP-Token, or PAP-Token-CHAP.

Location: Encaps > Answer > PPP Options, Ethernet > Connection > PPP Options

See Also: Receive Auth, Recv Name

B*N* Prt/Grp (*N*=1–2)

Description: B*N* Prt/Grp has two functions, depending on a channel's configured usage. For switched channels, it specifies a port number to be used with the B*N* Slot parameter for call routing purposes. In effect, it reserves the channel for calls to and from that port. For nailed channels, it assigns a group number, which will be referenced from call or Connection profile to use the nailed channels for a connection.

Usage: Specify a number.

Dependencies: When specifying a port number for call-routing purposes, you must also set the B*N* Slot parameter specify the slot number.

Example: `B1 Prt/Grp=5`

Location: Net/BRI > Line Config > Line *N*, BRI/LT > Line Config > Line *N*

See Also: B*N* Slot, Group

B*N* Slot (*N*=1–2)

Description: Specifies a slot number to be used for call routing. In effect, the parameter reserves the channel for calls to and from that slot. Note that there is no way to tell whether a call will come in on the first or second B channel of a BRI line, so both B1 Slot and B2 Slot should specify the same slot number.

Usage: Specify one of the following values:

- 0 (zero), the default—This parameter is not used to route incoming calls.
- 1 and 2 are invalid settings, because they represent the built-in slots containing T1 or E1 lines.
- 3–8—Expansion slots. When looking at the back panel of the MAX 6000 unit, slot #3 is the bottom slot in the left bank of slots, followed by #4 and #5 in ascending order. Slot #6 is the bottom right slot, followed by #7 and #8 in ascending order.

  Note: A MAX 3000 unit has only two expansion slots.
- 9—the LAN. Calls are routed to the bridge/router module.

Dependencies: This parameter is applicable only for switched channels.

Example: `B1 Slot=7`

Location: Net/BRI > Line Config > Line *N*

See Also: B*N* Prt/Grp

B*N* Trnk Grp (*N*=1–2)

Description: Assigns a B channel to a trunk group, making the channel available for outbound calls. Note that you cannot specify the same trunk-group number for channels that belong to a BRI line and for channels that belong to a PRI line.

Usage: Specify a number from 4 to 9 for each trunk group. The default is 9.

Example: `B1 Trnk Grp=8`

Dependencies: This parameter applies only if trunk groups are enabled in the System > Sys Config profile.

Location: Net/BRI > Line Config > Line *N*, BRI/LT > Line Config > Line *N*

See Also: B2 Trnk Grp, Ch *N* Trnk Grp, Dial #

B*N* Usage (N=1–2)

Description: Specifies the B channel's usage.

Usage: Specify one of the following values:

- Switched (the default)—The channel supports switched connectivity.
- Nailed—The channel is used for a leased connection.
- Unused—The MAX does not use the channel.

Example: `B1 Usage=Switched`

Location: Net/BRI > Line Config > Line *N*, BRI/LT > Line Config > Line *N*

See Also: B2 Usage

Back-to-back

Description: 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 to an E1 port of another MAX. No switch is required, and the connection is entirely local. One MAX should be set up for DTE operation, and the other for DCE operation.

Usage: Specify Yes or No. No is the default.

Yes specifies that the MAX is set up for DTE operation.

No specifies that the MAX is set up for DCE operation.

Dependencies: This parameter applies only to E1 lines with signaling mode set to DPNSS.

Location: Net/E1 > Line Config

See Also: Sig Mode

Backup

Description: Specifies the name of a backup Connection profile for a nailed connection. The profile is intended as a backup if the far-end device goes out of service, in which case the backup call is made. The profile is not intended to provide alternative lines for getting to a single destination.

Usage: Specify the Connection profile name. The default value is null.

Example: `Backup=CORP-SITE`

Dependencies: Backup applies only to nailed connections.

Location: Ethernet > Connections > *Connection profile* > Session Options

See Also: Name

BACP

Description: Enables or disables the Bandwidth Allocation Control Protocol (BACP). If BACP is enabled, connections encapsulated in MP (RFC 1990) use BACP to manage dynamic bandwidth on demand. Both sides of the connection must support BACP.

Note: BACP uses the same criteria as MP+ connections for managing bandwidth dynamically.

Usage: Specify Yes to enable BACP. No is the default.

Example: `BACP=Yes`

Dependencies: This parameter applies only to connections encapsulated in MP.

Location: Ethernet > Answer > PPP Options, Ethernet > Connections > *Connection profile* > Encaps Options

See Also: Encaps, Dyn Alg, Sec History, Target Util, Add Pers, Sub Pers, Base Ch Count, Min Ch Count, Max Ch Count, Inc Ch Count, Dec Ch Count

Banner

Description: Specifies the text to be used as the terminal server login banner.

Usage: Specify the banner text. You can enter up to 84 alphanumeric characters. The default is ** Ascend MAX Terminal Server **.

Example: `Banner="Welcome to ABC Corporation"`

Dependencies: This parameter is not applicable if terminal services are disabled or if the terminal server obtains its login setup from RADIUS.

Location: Ethernet > Mod Config

See Also: Remote Conf, TS Enabled

Base Ch Count

Description: Specifies the initial number of channels to use to set up a session. For a fixed session using MP, Base Ch Count specifies the total number of channels to be used for the call. For an AIM, BONDING, or multichannel PPP call, the channel count can be augmented.

A BONDING Mode 1 call cannot exceed 12 channels. For an MP+ call, the number is limited by the number of available channels. For a Combinet link, you can specify up to two channels. No matter what type of link you use, the number you specify cannot exceed the maximum channel count specified by the Max Ch Count parameter.

If the data service is MultiRate or GloBanD, and the data service you select is a multiple of 64 Kbps, specify a value for Base Ch Count that is a multiple of 6. If the data service is 384K/H0, 384KR, or GloBanD, the value you specify for Base Ch Count should be divisible by 6. In this case, specify a value of 6, 12, 18, 24, or 30.

Usage: Specify a number from 1 to 32. The default is 1.

Example: `Base Ch Count=2`

Dependencies: This parameter does not apply for leased connections.

Location: Host/Dual (Host/AIM6) > Port*N* Menu > Directory, Ethernet > Connections > *Connection profile* > Encaps Options

See Also: Call Mgm, Data Svc, Max Ch Count, Parallel Dialing

Bearer Info

Description: The Bearer Info parameter configures the request for a specific bearer service from the egress switched circuit network for outbound VoIP calls. This request is transmitted to the switched telephone network in the bearer service information element of the call setup message sent by the MultiVoice gateway.

Usage: The Bearer Info parameter may be assigned the following values:

Parameter value	Usage
`Speech`	Assigning this value, the default, requests a switched network routing over a channel that supports speech bearer capability.
`UnresDigital Info`	Assigning this value requests a switched network routing over a channel that supports unrestricted digital information (UDI) bearer capability.
`ResDigital Info`	Assigning this value requests a switched network routing over a channel that supports restricted digital information (RDI) bearer capability.
`3.1KHZ Audio`	Assigning this value requests a switched network routing over a channel that supports digital audio bearer capability up to 3.1KHZ.
`video`	Assigning this value requests a switched network routing over a channel that supports video signaling bearer capability.

Example: The following example illustrates how to request digital audio bearer capability for VoIP calls:

1. From the MAX administration menu, select the `Ethernet` > `Mod Config` profile.
2. Scroll down to the PSTN Options, then press [Enter] to open this profile. The following menu appears on your screen:

```
90-C00 Mod Config            x
x PSTN Options...            x
x >Cause Code Enabled=No     x
x  AlertProgInd=No Indicator x
x  ProcProgInd=No Indicator  x
x  Bearer Info=Speech        x
```

3. Scroll down to the Bearer Info parameter, then press [Enter] to toggle the value of this parameter, as illustrated.

```
Bearer Info=3.1KHZ Audio
```

4. Press [Esc]; then, when prompted, select the option to `Exit and Save` your changes.

Dependencies: Changes to the Bearer Info parameter take effect with the next VoIP call.

Location: Ethernet > Mod Config > PSTN Options

Beg Time

Description: Specifies the starting time of a dynamic AIM call's time period. You do not need to specify an ending time. The implicit ending time is the starting time of the next time period.

Usage: Specify the time of day you want the time period to begin. The setting you specify must have the format *hour* : *minutes* : *seconds*. The default is 00:00:00.

Example: `Beg Time=13:59:59`

Dependencies: This parameter applies only when Call Mgm=Dynamic.

Location: Host/Dual (Host/AIM6) > Port*N* Menu > Directory > Time Period *N*

See Also: Time Period

Bill

Description: Specifies a telephone number to be used for billing purposes. If a number is specified, it is used either as a billing suffix or the calling party number. For robbed-bit lines, the MAX uses the billing number as a suffix that is appended to each telephone number it dials for the connection.

For PRI lines, the MAX uses the value of the Bill # parameter rather than the telephone number ID to identify itself to the answering party.

If the calling party uses the value of the Bill # parameter instead of its telephone number as its ID, the CLID used by the answering side is not the true telephone number of the caller. This situation presents a security breach if you use CLID authentication. Further, be aware that if you specify a value for the Bill # parameter, there is no guarantee that the telephone company will send it to the answering device.

Note: For outgoing calls on a PRI line, the value of the Bill # parameter in the Dial Plan profile overrides the value of the Bill # parameter in the call profile or Connection profile.

Usage: Specify the billing number provided by the carrier. You can enter up to 24 characters. The default value is null.

Example: `Bill #=666`

Location: Host/Dual (Host/AIM6) > Port*N* Menu > Directory, Ethernet > Connections > *Connection profile* > Telco Options, System > Dial Plan, Ethernet > Frame Relay, Ethernet > X.25

See Also: Calling #, Clid Auth

Bit Inversion

Description: Specifies whether the MAX performs bit inversion when it sends or receives data over the WAN. Bit Inversion applies only to calls between codecs. It turns data 1s into 0s and data 0s into 1s. In some connections, you need to invert the data to avoid transmitting a pattern that the connection cannot handle. If you apply bit inversion, you should do so on both sides of the connection.

Note: If you are not certain about the requirements of bit inversion, contact your carrier.

Usage: Specify Yes or No. No is the default.

- Yes causes the MAX to perform bit inversion between two codecs.
- No does not modify the bit stream.

Example: `Bit Inversion=No`

Dependencies: You must set Bit Inversion to the same value on the calling unit and the answering unit.

Location: Host/Dual (Host/AIM6) > Port*N* Menu > Directory

Block Calls After

Description: Specifies how many unsuccessful attempts the MAX unit will make before beginning to block outgoing calls.

Usage: Enter the number of connection attempts permitted before the MAX unit blocks calls for the connection. The maximum number you can enter is 65535 (65535 attempts). The default is 0, which disables outward call blocking.

Location: Ethernet > Connections > *Connection profile* > Session Options

See Also: Blocked Duration

Blocked Duration

Description: Specifies the length of time, in seconds, during which the MAX unit will block outgoing calls.

Usage: Enter the number of seconds for the MAX unit to block all calls made to the connection. When this period has elapsed, the unit again allows calls to this connection. The default is 0.

Location: Ethernet > Connections > *Connection profile* > Session Options

See Also: Block Calls After

BOOTP Relay Enable

Description: Specifies whether Boot Protocol (BOOTP) requests are relayed to other networks. If you enable BOOTP relay, you must also set the Server parameter to specify the address of at least one BOOTP server.

Usage: Specify Yes or No. No is the default.

Yes enables the MAX to relay BOOTP requests to a server on another network.

No disables BOOTP relay.

Example: `BOOTP Relay Enable=Yes`

Dependencies: For the BOOTP relay feature to work, DHCP Spoofing and SLIP BOOTP must be disabled.

Location: Ethernet > Mod Config > BOOTP Relay

See Also: Server

BRI Analog Encode

Description: In previous software versions, the system chose the type of analog encoding for modem calls on the basis of the Switch Type setting. This was the default. In the current software version, you can override this Switch Type default by specifying Mu-Law or A-Law for the BRI Analog Encode parameter.

Usage: Specify one of the following values:

SwitchType (the default)—The system determines analog encoding for modem calls on the basis of the Switch Type setting.

Mu-Law—The system uses mu-law analog encoding (T1).

A-Law—The system uses a-law analog encoding (E1).

Example: `BRI Analog Encode=Mu-Law`

Location: Net/BRI > Line Config > BRI Analog Encode

Bridge

Description: Enables or disables link-level packet bridging for this connection. If you disable bridging, you must enable routing. Enabling bridging in the Answer profile enables the MAX to answer a call that contains packets other than the routed protocols (IP or IPX).

Usage: Specify Yes or No. No is the default.

Yes enables the MAX to bridge packets across this connection on the basis of the packet's destination MAC address (if specified in a Connection profile) or to answer incoming bridged connections (if specified in the Answer profile).

No disables link-level bridging.

Example: `Bridge=Yes`

Dependencies: This parameter does not apply unless Bridging is enabled in the Ethernet > Mod Config profile. If you have a MAX running Multiband Simulation, Bridge is disabled.

Location: Ethernet > Answer > PPP Options, Ethernet > Connections > *Connection profile*

See Also: Bridging, Encaps, Route IP, Route IPX

Bridging

Description: Enables or disables packet-bridging systemwide. With bridging enabled, the MAX unit's Ethernet controller runs in promiscuous mode. In promiscuous mode, the Ethernet

driver accepts all packets regardless of address or packet type and passes them up the protocol stack for a higher-layer decision on whether to route, bridge, or reject the packets.

Note: Running in promiscuous mode incurs greater processor and memory overhead than the standard mode of operation for the Ethernet controller. On heavily loaded networks, this increased overhead can result in slower performance, even if no packets are actually bridged.

Usage: Specify Yes or No. No is the default.

Yes enables the MAX to bridge packets on the basis of MAC addresses by running its Ethernet controller in promiscuous mode, which causes it to accept all packets regardless of packet type or address.

No disables packet bridging and turns off promiscuous mode in the Ethernet controller.

Example: `Bridging=Yes`

Dependencies: If you have a MAX running Multiband Simulation, Bridging is disabled.

Location: Ethernet > Mod Config

See Also: Bridge

Buffer Chars

Description: Specifies whether to buffer characters in a terminal-server session or to process each character as it is received. If enabled, this feature causes the MAX to buffer input characters for 100 milliseconds.

Usage: Specify Yes or No. Yes is the default.

Yes causes the MAX to buffer characters for 100 milliseconds in terminal-server sessions.

No causes the MAX to process each character as it is received.

Example: `Buffer Chars=Yes`

Dependencies: This parameter is not applicable when terminal services are disabled.

Location: Ethernet > Mod Config > TServ Options

See Also: Immed Telnet, TS Enabled

Buildout

Description: Specifies the line buildout value for a T1 line connected to an internal Channel Service Unit (CSU). The buildout value is the amount of attenuation the MAX should apply to the line's network interface if it is too close to a repeater.

Usage: Check with your carrier to determine the correct value for this parameter. Specify one of the following values (dB stands for decibels):

- 0–dB (the default)
- 7.5–dB
- 15–dB

- 22.5–dB

Example: `Buildout=0`

Dependencies: This parameter is not applicable if the T1 line does not have an internal CSU to connect to the local digital telephone system.

Location: Net/T1 > Line Config > Line *N*

C

Callback

Description: Enables or disables the callback feature. When you enable the callback feature, the MAX hangs up after receiving an incoming call that matches the one specified in the Connection profile. The MAX then uses the Dial # setting specified in the Connection profile to call back the device at the remote end of the link.

The Callback parameter enables you to tighten security, as it ensures that the MAX always makes a connection with a known destination.

Usage: Specify Yes or No. No is the default.

Yes enables the callback feature, causing the MAX to hang up and dial out to the caller when it receives an incoming call that matches the Connection profile.

No disables callback.

Example: `Callback=Yes`

Dependencies: This parameter does not apply to leased connections. If it is enabled on a switched connection, the Connection profile must be configured for both answering the call and calling back the device requesting access. By the same token, any device calling into a Connection profile set for callback must be configured to both dial calls and answer them.

Location: Ethernet > Connections > *Connection profile* > Telco Options

See Also: AnsOrig, Call Type, Dial #, Calling #

Call-by-Call

Description: In a T1 Line *N* profile, specifies the call-by-call signaling value for routing calls from a local device through the MAX to the network. When the parameter is set in another profile, it specifies the PRI service to use when using that profile to place a call.

Note: The Call-by-Call setting in the Dial Plan profile overrides the Call-by-Call setting in either a call or Connection profile.

If the service provider is AT&T, the following call-by-call services are available:

- 0 (Disable call-by-call service)
- 1 (SDN, including GSDN)
- 2 (Megacom 800)

- 3 (Megacom)
- 6 (ACCUNET Switched Digital Services)
- 7 (Long Distance Service, including AT&T World Connect)
- 8 (International 800–I800)
- 16 (AT&T MultiQuest)

If the service provider is Sprint, the following VPN and GVPN call-by-call services are available:

- 0 (Reserved)
- 1 (Private)
- 2 (Inwatts)
- 3 (Outwatts)
- 4 (FX)
- 5 (Tie Trunk)

If the service provider is MCI, the following call-by-call services are available:

- 1 (VNET/Vision)
- 2 (800)
- 3 (PRISM1, PRISM II, WATS)
- 4 (900)
- 5 (DAL)

Usage: Specify a number from 0 to 65535, corresponding to the type of call-by-call service in use. The factory default is 0, which disables call-by-call service.

Example: `Call-by-Call=6`

Location: Ethernet > Connections > *Connection profile* > Telco Options, System > Dial Plan, Ethernet > Frame Relay, Net/T1 > Line Config > Line *N*, Ethernet > X.25, Host/Dual (Host/AIM6) > Port*N* Menu > Directory > *any call profile*

See Also: Call-by-Call *N*

Call-by-Call *N* (*N*=1–6)

Description: In a Destination profile, specifies the PRI service to use when using the associated Dial # parameter to place a call. For example, when the MAX dials the number specified by Dial 5#, the MAX uses the services specified by Call-by-Call 5.

Note: The setting of the Call-by-Call *N* parameter in the Destination profile overrides the setting of the Call-by-Call parameter in a call profile or Connection profile.

If the service provider is AT&T, the following call-by-call services are available:

- 0 (Disable call-by-call service)
- 1 (SDN, including GSDN)
- 2 (Megacom 800)
- 3 (Megacom)

- 6 (ACCUNET Switched Digital Services)
- 7 (Long Distance Service, including AT&T World Connect)
- 8 (International 800–I800)
- 16 (AT&T MultiQuest)

If the service provider is Sprint, the following VPN and GVPN call-by-call services are available:

- 0 (Reserved)
- 1 (Private)
- 2 (Inwatts)
- 3 (Outwatts)
- 4 (FX)
- 5 (Tie Trunk)

If the service provider is MCI, the following call-by-call services are available:

- 1 (VNET/Vision)
- 2 (800)
- 3 (PRISM1, PRISM II, WATS)
- 4 (900)
- 5 (DAL)

Usage: Specify a number from 0 to 65535, corresponding to the type of call-by-call service in use. The factory default is 0, which disables call-by-call service.

Example: `Call-By-Call 1=4`

Location: System > Destinations

See Also: Call-by-Call, Option

Call Distrib Type

Description: Specifies the routing method for POTS calls.

Usage: Specify one of the following values:

- First Avail—Routes the call to the first available port on the basis of slot and port number. This is the default.
- Fair Share—Routes the call to the available port that has been idle the longest.

Dependencies: This parameter applies only to POTS ports.

Location: System > Sys Config

Call Filter

Description: Specifies the number of a filter used to determine if a packet should cause the idle timer to be reset or a call to be placed. If both a call filter and data filter are applied to a

connection, the MAX applies a call filter after applying a data filter. (Only those packets that the data filter forwards can reach the call filter.)

Usage: Specify a number from 0 to 199. The number you enter depends on whether you are applying a filter you created through the VT100 interface, or a firewall you created with SecureConnect Manager (SCM).

If you are applying a filter created through the VT100 interface, enter the last 2 digits of the filter number as it appears in the Filters menu.

If you are applying a firewall created through SCM, add 100 to the last 2 digits of the firewall number as it appears in the Firewalls menu. For example, if the number of your firewall is 90-601, specify 101. (For information about downloading firewalls to the MAX, see your SCM documentation.) The numbering scheme for filters and firewalls is:

- 0 (the default) indicates that no filtering is being used.
- 1-99 indicates that a filter created through the VT100 interface is being used.
- 100-199 indicates that a filter created with SCM is being used.

Example: `Call Filter=7`

Location: Ethernet > Answer > Session Options, Ethernet > Connections > *Connection profile* > Session Options

See Also: Data Filter, Filter

Call Mode

Description: Specifies whether the MAX can initiate a call request on the X.25 IP connection.

Usage: Specify one of the following values:

- Incoming —The MAX does not issue a call request when data shows up for forwarding. If there is no virtual circuit established, the IP packet is dropped. If an incoming call is received from a host whose address matches the Answer X.121 Addr setting, the call is accepted.
- Outgoing—The MAX issues a call request to the remote X.121 address when data shows up for forwarding. If there is no virtual circuit established and an incoming call request is received, the call is rejected.
- Both—The MAX accepts both incoming and outgoing call requests if the CUD indicates encapsulation that is supported. The called address must match the Answer X.121 Addr setting. If no virtual circuit is established and IP packets arrive, a call request is issued to the remote X.121 address.

Example: `Call Mode=Both`

Dependencies: This parameter applies only to X.25/IP connections. The setting relies on matching an address specified by the Answer X.121 Addr or Remote X.121 Addr parameter.

Location: Ethernet > Connections > *Connection profile* > Encaps Options

See Also: Encaps, Answer X.121 Addr, Remote X.121 Addr

Call Mgm

Description: Specifies the way that the MAX manages calls at an AIM port when AIM, FT1-AIM, FT1-B&O, or BONDING is the value for the Call Type parameter.

Depending upon the type of call in use, different call management features are available. For AIM, FT1-B&O, and FT1-AIM calls, call management consists of remote management, online error monitoring, remote loopbacks, and online bandwidth control between codecs. For BONDING calls, call management consists of the remote loopback and online bandwidth control features only.

A remote loopback tests the entire connection from host interface to host interface. The MAX places a call to itself over the WAN and sends a user-specified number of packets over the connection. At the AIM port interface of the remote MAX, the data loops back to the local MAX. The loopback tests the MAX unit's ability to initiate and receive calls, and shows whether the connection over the digital access line and the WAN is sound.

For the call management features available by command, see the *MAX Administration Guide*.

Usage: Specify one of the following values:

- Manual (the default)—Enables you to add or remove bandwidth manually during an AIM, FT1-B&O, or FT1-AIM call. When you choose Manual, the codec receives 99.8% of the bandwidth allocated for the T1 PRI line. The MAX uses the remaining 0.2% of bandwidth for AIM's management subchannel. For example, in a Manual call between codecs with a Base Ch Count value of 5 and the Switched-56 data service, the host device receives approximately 279 Kbps, or 99.8% of 280 Kbps (5x56 Kbps).

  If you have an FT1-B&O call online with manual call management, and the MAX has replaced the nailed-up channels with switched channels, the MAX does not automatically drop the switched channels when it restores the nailed-up channels.

- Delta—Differs from Manual in that you cannot add or subtract bandwidth while the call is online, and the MAX provides the host with a different clock.

  When you set up AIM, FT1-B&O, and FT1-AIM calls, the AIM ports are synchronous and the WAN lines are synchronous. The AIM ports receives its clock signal from the clock provided by the WAN. When you choose Delta, the MAX provides a clock that is an exact multiple of 64 Kbps. The following table lists the host bandwidths available and the bandwidth that the network provides. The network values listed do not include the D channel when the signaling mode is ISDN.

Host bandwidth (in Kbps)	Base Ch Count	Network bandwidth (in Kbps) for 56Kaccess	Network bandwidth (in Kbps) for 64K access
1536	24	1568	1600
1344	21	1400	1408
1024	16	1064	1088
768	12	784	832
512	8	560	576
384	6	392	448
256	4	280	320

The *Host bandwidth* is the bandwidth delivered to the codec. The *Base Ch Count* column specifies the Base Ch Count value needed to achieve this host bandwidth. However, the actual number of channels required for the host bandwidth is greater than the setting for Base Ch Count. Divide the value in the *Network bandwidth* columns by the data rate of the access line to arrive at the required number of channels.

- Dynamic—Uses dynamic bandwidth allocation algorithms to automatically add or remove bandwidth during an AIM, FT1-B&O, or FT1-AIM call.

  The codec receives 99.8% of the bandwidth allocated for the T1 PRI line. The MAX uses the remaining 0.2% of the bandwidth for AIM's management subchannel. For example, in a Dynamic call between codecs with a Base Ch Count value of 5 and the Switched-56 data service, the host device receives approximately 279 Kbps, or 99.8% of 280 Kbps (5x56 Kbps).

  If you choose Dynamic and the MAX receives an incoming call set to Manual mode, the resulting connection is Dynamic for the answering device and Manual for the calling device. In all other cases, the incoming call determines call management in both directions. If you choose Dynamic, you must also set the Add Pers, Dyn Alg, Sec History, and Sub Pers parameters in the call profile.

- Static—Does not provide the ability to change bandwidth or resynchronize channels during an AIM, FT1-B&O, or FT1-AIM call. Once the call is established, you cannot add or remove channels. When you choose Static, the host device uses a clock that is an exact multiple of 56 Kbps or 64 Kbps, and receives 100% of the bandwidth allocated from the network. For example, in a Static call with a Base Ch Count value of 5 and the Switched-56 data service, the host device receives 280 Kbps (5x56Kbps).

- Mode 0—Required when the remote device uses the BONDING inverse-multiplexing protocol and is connected in dual-port mode to a videoconferencing codec.

  Inverse multiplexing is a method of combining individually dialed channels into a single, higher-speed data stream. A codec (COder/DECoder) is a device that encodes analog data into a digital signal for transmission over a digital medium. Typically, the MAX uses a videoconferencing codec that encodes and decodes video and audio information.

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

  In Mode 0, the user enters only the telephone number of the primary host port associated with the remote codec. The remote BONDING device must have the secondary host port's telephone number. No management subchannel exists, and the codec (not the MAX) performs the inverse multiplexing.

- Mode 1—Uses the BONDING inverse-multiplexing protocol, provides the host device with a clock that is an exact multiple of 56 Kbps or 64 Kbps, and gives the host 100% of the bandwidth allocated from the network. For example, in a Mode 1 call with a Base Ch Count value of 5 and the Switched-56 data service, the host device receives 280 Kbps (5x56Kbps). Mode 1 does not provide a management subchannel. This setting provides a subset of Static features.

- Mode 2—Uses the BONDING inverse-multiplexing protocol. Specify this setting when the codec does not require exact clocking. When you choose Mode 2, the codec receives 98.4% of the bandwidth allocated from the T1 PRI line, and uses a clock that is 98.4% of a multiple of 56 Kbps or 64 Kbps. The MAX constructs the BONDING management subchannel by using the remaining 1.6% of the bandwidth specified for the call with the Base Ch Count parameter. Mode 2 provides a subset of Manual features.

- Mode 3—Uses the BONDING inverse-multiplexing protocol, provides the host device with a clock that is an exact multiple of 64 Kbps, and uses a management subchannel. This setting provides a subset of Delta features.

Dependencies: This parameter is not applicable if the call type is single channel or two-channel. The Dynamic setting is not applicable for Host/AIM6 cards.

Location: Host/Dual (Host/AIM6) > Port*N* Menu > Directory

See Also: Add Pers, Base Ch Count, Call Type, Dyn Alg, Sec History, Sub Pers

Call Password

Description: Specifies the password for outgoing AIM or BONDING calls. Authentication is used only if the receiving unit has a password defined in the Host/Dual (or Host/AIM6) > Port*N* Menu > Directory > any directory profile. If the Port profile in the receiving unit does not have a password defined, the units connect without authentication even though the originating unit might have sent parameters. Note that the MAX only authenticates AIM and BONDING calls. Dual-port calls are not authenticated.

Usage: Enter a password of nine characters or less.

Example: `Call Password=Ascend`

Location: Host/Dual (or Host/AIM6) > Port*N* Menu > Directory

See Also: Port Password

Call Rte Type

Description: Specifies the type of call to which the specified route applies.

Usage: Specify one of the following values:

- Trunk-Any—The unit can use this call route for any trunk call.
- Trunk-Voice—The unit can use this call route for voice trunk calls.
- Trunk-Digital—The unit can use this call route for digital trunk calls.

Location: System > Call Routes > *Call Routes profile*

Call Type

Description: Specifies a type of connection, or in the case of codecs, the architecture of the connection. These two different usages for the parameter are described in the following two Usage sections.

Usage: To specify the type of connection in a Frame Relay, Connection, or X.25 profile, specify one of the following values:

- Nailed—A link that consists of nailed-up channels. This is the default for Frame Relay and X.25 profiles. You must set the Group or Nailed Grp parameter to specify which nailed channels to use.
- Switched—A link that consists of switched channels. This is the default in a Connection profile.

- Nailed/MPP—Nailed channels that can be augmented with switched channels if bandwidth is needed during an MP+ call. A Nailed/MP+ connection is established when its nailed OR switched channels are connected end-to-end. The switched channels are dialed when the MAX receives an outbound packet for the far end and cannot forward it across the nailed connection, either because those channels are down or because they are being fully utilized.

  If both the nailed and switched channels in a Nailed/MP+ connection are down, the connection does not reestablish itself until the nailed channels are brought back up or the switched channels are dialed. The maximum number of channels for the Nailed/MP+ connection is either the Max Ch Count value or the number of nailed channels in the specified group, whichever is greater. If a nailed channel fails, the MAX replaces that channel with a switched channel, even if the call is online with more than the minimum number of channels.

  Note: If the nailed connection is the serial WAN line, the MAX does not add switched channels on the basis of maximum usage on the nailed connection. The MAX currently does not calculate Current Line Utilization (CLU) or Average Line Utilization (ALU) for nailed connections through the serial WAN interface.

  The MAX must be the originator of the switched call. If you modify a Nailed/MPP Connection profile, most changes become active only after the call is brought down and then back up. However, if you add a group number (for example, changing Group=1,2 to Group=1,2,5) and save the modified profile, the additional channels are added to the connection without having to bring it down and back up.
- Perm/Switched (Connection profile only)—A permanent switched connection is an outbound switched call that attempts to remain up at all times. If the unit or central switch resets or if the link is terminated, the MAX attempts to restore the link at 10-second intervals, which is similar to the way a nailed connection is maintained. A permanent switched connection results in a long connection time but conserves connection attempts, which might be cost-effective for some customers. For the answering device at the remote end of the permanent switched connection, Lucent recommends that the Connection profile be configured to answer calls but not originate them. If the remote device initiates a call, the MAX simply does not answer it. This situation could result in repeated charges for calls that have no purpose. To keep the remote device from originating calls, set AnsOrig to Ans Only for that device.
- D-channel (X.25 profile only)—Specifies that the MAX supports X.25 over the D channel.
- MegaMAX—Enables you to set up a MP+ session using a mix of data services. Each connection in a MegaMax MP+ session can use a data service (H0, H11, or H12 (E1)) independent of the data service used by other connections in that session. That is, one connection might be established as a 24 channel (64k) H11 call, while another was established as a 30 channel H12 call. This software option is available only when the MegaMAX option is installed.

Usage: To specify the architecture of an end-to-end connection between codecs (call profiles), specify one of these values:

- AIM (Ascend Inverse Multiplexing)—Inverse multiplexing is a method of combining individually dialed channels into a single, higher-speed data stream. The AIM setting is the default for units with the AIM option, and is not available on host ports not equipped with AIM functionality. Both ends of the call must have AIM-compatible equipment.
- 1 Chnl (single channel)—The MAX uses a single channel to achieve the required bandwidth. The 1 Chnl setting is the default for units that do not have the AIM option. Use

it to set up calls to terminal adapters, CSUs, or DSUs that do not have inverse multiplexing capability.

- 2 Chnl (dual-port)—In a dual-port call, a codec performs inverse multiplexing on two channels so that a call can achieve twice the bandwidth of a single channel. The codec provides two ports, one for each channel. Two AIM ports on the MAX connect a dual-port call to the codec. These ports are the primary port and the secondary port. Because the MAX places the two calls in tandem and clears the calls in tandem, it considers them a single call.

  Use the 2 Chnl setting to set up calls to a codec that has a dual-port interface. The remote end of the link can be equipped with a terminal adapter (TA) or a data service unit (DSU) that does not have inverse multiplexing capability.

- FT1-AIM—The MAX combines nailed-up channels with switched channels to achieve the required bandwidth. This setting uses the AIM protocol, and is not available on host ports not equipped with AIM functionality. Both ends of the call must have AIM-compatible equipment. When the quality of a nailed-up channel falls to Marginal or Poor in an FT1-AIM call, the MAX drops the channel and does not replace it. The MAX cannot monitor these channels or restore them to an online call.

- FT1-B&O—Provides automatic backup and overflow protection of nailed-up circuits. For this setting to appear in the profile of a Host/AIM6 module, the current host port must be the primary port of a dual-port pair.

  In providing backup bandwidth, the MAX unit drops all the nailed-up channels when the quality of a nailed-up channel falls to Marginal or Poor in an FT1-B&O call. The unit then attempts to replace dropped nailed-up channels with switched channels.

  The MAX unit also monitors dropped nailed-up channels. When the quality of all dropped channels changes to Fair or Good, the unit reinstates them. You must specify Call Mgm=Dynamic in order for the unit to drop switched channels after restoring the nailed-up channels.

  In providing overflow protection, the MAX supplies supplemental dial-up bandwidth during times of peak demand in order to prevent saturation of a nailed-up line. The circuit remains in place until the traffic subsides, and then it is removed.

  The FT1-B&O setting uses the AIM protocol, and is not available on host ports not equipped with AIM functionality. Both ends of the call must have AIM-compatible equipment. You must limit calls of this type to 28 channels.

- FT1—Specifies a call consisting entirely of nailed-up channels. Use the FT1 setting to connect to terminal adapters, CSUs, or DSUs over fractional T1 or other nailed-up circuits. A fractional T1 circuit is a nailed-up connection to a T1 line with a bandwidth that might be only a fraction of the full T1 bandwidth. Contact your T1 line provider if you plan to use this call type with more than one line.

- BONDING—The MAX combines 56-Kbps or 64-Kbps channels to achieve the required bandwidth. It can combine a maximum of 12 channels. This setting uses the BONDING (Bandwidth On Demand Interoperability Group) September 1992 1.0 specification. This setting is not available on host ports not equipped with AIM functionality. Calls using BONDING require BONDING-compatible equipment at both ends of the call.

Dependencies: A call type of Nailed makes parameters related to switched connections (for example, the Callback parameter) inapplicable, and a call type of Switched makes parameters related to nailed connections (for example, the Group parameter) inapplicable. Because a call type of Perm/Switched is always outbound, the following parameters are inapplicable for permanent switched connections: AnsOrig, Callback, Idle, and Backup.

The following parameters in the X.25 profile are not applicable when you set Call Type to D-Channel: Nailed Grp, Data Svc, PRI # Type, Dial #, Bill #, Call-by-Call, Transit #, LAPB T1, LAPB T2, LAPB N2, LAPB K, X.25 Seq Number Mode, X.25 Link Setup Mode, X.25 Node Type, X.25 Pkt Size, X.25 Min Pkt Size, and X.25 Max Pkt Size

Location: Host/Dual (Host/AIM6) > Port*N* Menu > Directory, Ethernet > Connections > *Connection profile* > Telco Options, Ethernet > Frame Relay, Ethernet > X.25

See Also: AnsOrig, Backup, Callback, Call Mgm, Data Svc, DLCI, FR DLCI, Group, Idle, Max Ch Count, Min Ch Count, Nailed Grp

Call Type (MultiVoice gateway)

Description: The Call Type parameter specifies which call-type the MultiVoice gateway should expect for incoming calls on this trunk, for purposes of call routing and detecting call progress signaling. This enhancement applies to both inband and PRI signaling for VoIP calls.

Usage: The Call Type parameter may be assigned the following values:

Parameter value	Usage
`Digital Call`	Assigning this value configures the MultiVoice gateway to treat incoming calls on this line as digital calls, for call routing purposes.
`Modem Call`	Assigning this value configures the MultiVoice gateway to treat incoming calls as analog calls. Used for routing modem calls from the switched telephone network.
`VoIP Call`	Assigning this value configures the MultiVoice gateway to treat incoming calls as VoIP calls, for call routing purposes.

Example: The following example illustrates how to configure routing and detecting call progress signaling received from the switched telephone network for VoIP calls, received on a MultiVoice gateway using T1 trunks:

1 From the MAX administration menu, select the Net/T1 > Line Config > Line profile.

2 Scroll down to the appropriate Line, then select the Line Config > Line # profile. Press [Enter] to open this profile. The following menu appears on your screen:

```
10-1** Factory              ??x
x Line 1...                    x
x >Sig Mode=Inband            ^x
x  NFAS ID num=N/A             x
x  Rob Ctl=Inc-W-200           x
x  Switch Type=N/A             x
x  .......
x  Clock Source=Yes            x
x  Call Type=VoIP Call         x
x  Collect DNIS/ANI=Yes        x
X  ......
```

3 Scroll down to the Call Type parameter, then press [Enter] to toggle the value of this parameter, as illustrated.

```
Call Type=VoIP Call
```

4 Press [Esc] until the option to `Exit and accept` your changes appears; then save your changes.

Dependencies: Changes to the Call Type parameter take effect with the next VoIP call.

Location: Net/T1 > Line Config > Line *xx* > Line *x*, Net/E1 > Line Config > Line *xx* > Line *x*

Called

Description: Specifies the number called to establish this connection, which is typically the number dialed by the far end. It is presented in an ISDN message as part of the call when Dial Number Information Service (DNIS) is in use. In some cases, the telephone company might present a modified called number for DNIS. This number is used for authentication and to direct inbound calls to a particular device from a central rotary switch or PBX. For details, see the *MAX Security Supplement.*

Usage: Specify the number to be used for Called Number authentication.

Example: `Called #=5551234`

Location: Ethernet > Connections > *Connection profile* > Ethernet > Answer

See Also: Id Auth

CallerID

Description: Specifies whether any caller-ID information supplied by the Central Office is forwarded to the POTS port.

Note: MAXPOTS slot cards only support the Bellcore Type I caller ID format, which might not be supported in all countries.

Usage: Specify Yes or No. The default is No.

- Yes—Enables the MAX to forward caller-ID information (if provided by the inbound trunk) to the phone.
- No—Disables this feature.

Location: Analog FXS > FXS Config > *FXS Configuration profile* > Line *N*

Calling

Description: Specifies the calling number (the far-end device's number). Many carriers include the calling number in each call. Calling # is the caller ID number displayed on some telephones and used by the MAX for Calling Line ID (CLID) authentication.

CLID authentication enables you to prevent the MAX from answering a connection unless it originates at the specified telephone number. The number you specify for this parameter can also be used for callback security if you configure callback in the per-connection Telco Options profile.

Usage: Specify the calling number to be used for authentication.

Example: `Calling #=555-6787`

Location: Ethernet > Connections > *Connection profile* > Ethernet > Answer

See Also: Id Auth, Callback

Cause Code Enable

Description: The Cause Code Enable parameter is used to enable transparent delivery of the Q.931 disconnect cause codes generated by the far-end switched network—passed across the packet network from the far-end MultiVoice gateway to the near-end MultiVoice gateway—to the local telephone company. The local telephone company switch then plays the appropriate tone or disconnect message for the caller.

Usage: The Cause-Code-Transparency parameter may be assigned the following values:

Parameter value	Usage
`yes`	Assigning this value enables transparent delivery of the Q.931 disconnect cause codes generated by the far-end switched network to a local telephone company switch, across a MultiVoice network. The local telephone company switch responds to these messages by playing the appropriate tones or messages for the caller.
`no`	Assigning this value, the default, disables transparent delivery of the Q.931 disconnect cause codes generated by the far-end switched network to a local telephone company switch, configuring the near-end MultiVoice gateway to play the appropriate tones or messages for the caller.

Example: The procedure illustrates how to enable transparent delivery of disconnect cause codes:

1 From the MAX administration menu, select the `Ethernet` > `Mod Config` profile.

2 Scroll down to the PSTN Options, then press [Enter] to open this profile. The following menu appears on your screen:

```
90-C00 Mod Config            x
x PSTN Options...            x
x >Cause Code Enabled=No     x
x  AlertProgInd=No Indicator x
x  ProcProgInd=No Indicator  x
x  Bearer Info=Speech        x
```

3 Scroll down to the Cause Code Enabled parameter, then press [Enter] to toggle the value of this parameter, as illustrated.

```
Cause Code Enabled=Yes
```

4 Press [Esc]; then, when prompted, select the option to `Exit and Save` your changes.

Dependencies: The Cause Code Enabled parameter has the following dependencies:

- This feature should be enabled (`Cause Code Enabled=yes`) whenever voice announcement reporting is enabled (`Voice Ann Enbl=yes`), in order for callers to hear both a busy signal and the call failure message. When voice announcements are enabled, if transparent delivery of disconnect codes is disabled (`Cause Code Enabled=no`),

callers will not hear the busy tone. Instead, the near-end MultiVoice gateway plays the call failure message.

- Changes to the Cause Code Enabled parameter take effect with the next VoIP call.

Location: Ethernet > Mod Config > PSTN Options

CBCP Enable

Description: Specifies how the MAX responds to caller requests to support CBCP.

Usage: Press Enter to cycle through the choices. You can select Yes or No.

Yes specifies that the MAX will positively acknowledge, during LCP negotiations, support for CBCP.

No (the default) specifies that the MAX will reject any request to support CBCP.

Location: Ethernet > Answer > PPP Options

See Also: CBCP Mode, CBCP Trunk Group

CBCP Mode

Description: Specifies what method of callback the MAX offers the incoming caller.

Usage: Press Enter to cycle through the choices. You can specify one of the following settings:

Setting	Description
No Cback	Applies for Windows NT or Windows 95 clients who must not be called back. Because CBCP has been negotiated initially, the Windows clients must have validation from the MAX that no callback is used for this connection.
User Num	Specifies that the caller will supply the number the MAX uses for the callback.
Prof Num	Specifies that the MAX will use the number specified for Ethernet > Connections > *Connection profile* > Dial # for the callback.
User Num or No Cback	Specifies that the caller has the option of either supplying the number to dial or specifying that no callback is used for the call. If no callback is chosen, the call will not be disconnected by the MAX.

Dependencies: CBCP Mode applies only if CBCP is successfully negotiated for a connection. Encaps must be set to PPP, MPP or MP.

Location: Ethernet > Connections > *Connection profile* > Encaps Options

See Also: CBCP Enable, CBCP Trunk Group

CBCP Trunk Group

Description: Assigns the callback to a MAX trunk group. This parameter is used only when the caller is specifying the telephone number the MAX uses for the callback. The value specified for CBCP Trunk Group is prepended to the caller-supplied number when the MAX calls back.

Usage: Press Enter to open a text field. Then type a number from 4 to 9. The default is 9.

Dependencies: CPCP Trunk Group applies only if CBCP is negotiated for a connection. Encaps must be set to PPP, MPP or MP.

Location: Ethernet > Connections > *Connection profile* > Encaps Options

See Also: CBCP Enable, CBCP Mode

CC Establish Timer

Description: Specifies the maximum number of seconds the MAX unit allows for establishment of an L2TP tunnel with another unit. Any change you make to the setting of this parameter is reflected as soon as the previous timer expires.

Usage: Enter a decimal number from 0 to 600. 60 is the default.

Example: `CC Establish Timer=60`

Dependencies: This parameter applies only if you have set L2TP Mode to LAC, LNS, or Both.

Location: Ethernet > Mod Config > L2 Tunneling Options

See Also: First Retry Timer, Hello Timer, L2TP Mode, LAC In Call Timer, LNS In Call Timer, Retry Count

Cell First

Description: Determines whether the MAX attempts a cellular connection before a land connection. When an incoming call is routed by the MAX to one of its digital modems, the modem answers the call by issuing an AT command string to the selected modem. This answer string contains the following command for support of cellular modems:

`sec=`*`X`*`,`*`Y`*

where *X* is the value that specifies whether the modem negotiates land-based or cellular first, and *Y* is the modem gain used for cellular communication. For example, if Cell First is set to No and Cell Level is set to 18 in the TServ Options profile, the command would be:

`sec=0,18`

Usage: Specify Yes or No. No is the default.

Yes specifies that a cellular connection is attempted first, followed by a land-based connection.

No specifies that a land-based connection is attempted first, followed by an attempt at a cellular connection.

Example: `Cell First=No`

Dependencies: This parameter is not applicable if terminal services are disabled.

Location: Ethernet > Mod Config > TServ Options

See Also: Cell Level

Cell Level

Description: Specifies the modem cellular communications transmit and receive level. Valid values are -10 dB through -18 dB.

Usage: Specify one of the following values:

- 18 (the default)
- 17
- 16
- 15
- 14
- 13
- 12
- 11
- 10

Example: `Cell Level=18`

Dependencies: This parameter is not applicable if terminal services are disabled.

Location: Ethernet > Mod Config > TServ Options

See Also: Cell First

Ch *N* (*N*=1–24, 1–32)

Description: Specifies the usage for this channel. Channel usage can be different from the usage specified for the line itself. For example, you might have specified switched usage for the line, while you could specify nailed usage for individual channels within that line.

Usage: Specify one of the following values for T1 channels:

- Switched (the default)—Supports switched connections. Can be robbed-bit or a B channel, depending on the line's signal mode.
- Nailed—A clear-channel 64K circuit.
- D channel—Channel used for ISDN D channel signaling. Assigned automatically to channel number 24 on T1 lines when ISDN signaling is in use.
- Unused—Unavailable for use.
- D&I (Drop-and-Insert)—Passes the calls through to the second T1 line, which typically supports a PBX.
- NFAS-Prime—Primary D channel for two NFAS lines.

- NFAS-Second—Secondary D channel for two NFAS lines. Is inactive unless the user activates it, or unless a failure of the primary D channel causes it to go online. This setting is optional.

Specify one of the following values for E1 channels:

- Switched (the default)—Supports switched connections. Can be robbed-bit or a B channel, depending on the line's signal mode.
- Nailed—A clear-channel 64K circuit.
- D channel—Channel used for ISDN D channel signaling. Assigned automatically to channel number 16 on E1 lines when ISDN signaling is in use.
- Unused—Unavailable for use.

Example: `Ch 1=Switched`

Location: Net/T1 > Line Config > Line *N*, Net/E1 > Line Config > Line *N*

See Also: Sig Mode

Ch *N* # (*N*=1–24, 1–32)

Description: Specifies an add-on number for a call on a T1 or E1 line. You build multichannel calls (MP, MP+, AIM, or BONDING) by specifying add-on numbers. A multichannel call begins as a single-channel connection to one telephone number. The calling unit can then request and store additional numbers that it dials to connect additional channels. To add channels to the call, the calling unit must integrate the add-on numbers with the number it dialed initially.

Note: Do not enter telephone numbers of the MAX you are calling in the Line *N* profile. The numbers you are calling belong in the call and Connection profiles.

The group of channels used for a multichannel call is called a bundle. A 10-channel bundle, in which each channel is 64Kbps, provides a 640-Kbps connection.Typically, the telephone numbers assigned to the channels share a group of leading (leftmost) digits. Enter only the unique digits identifying each number, as follows:

- If the add-on number in the called unit is shorter than the number dialed by the calling unit, the MAX unit replaces only the rightmost digits. For example, suppose you dial 777-3330 to reach channel 1 of line 1, and dial 777-3331 through 777-3348 to reach other channels. In this case, set Ch1# to 30 and set the Ch *N* parameter for the other channels to 31, 32, and so on.
- If the add-on number is longer than the number dialed, the unit discards the extra digits. For example:
  - Ch1#=510-655-1212
  - Dial#=655-1212
  - Derived number for channel 1=655-1212
- If there is no add-on number, the derived number equals the dialed number. For example:
  - Ch1#=(null)
  - Dial#=555-1213
  - Derived number for channel 1=555-1213

The most common reason multichannel calls fail to connect beyond the initial connection is that the answering unit sends the calling unit add-on numbers it cannot use to dial the other channels.

AIM and BONDING call bundles should not span dial plans. If you are receiving AIM or BONDING calls and have multiple dial plans, set up each dial plan as a separate trunk group. This also prevents MP and MP+ call bundles from spanning dial plans.

For example, if you have two PRI lines from different service providers, you might set the Ch*N* Trnk Grp parameters for the first line to 9 and for the second line to 8. Also, enabling trunk groups on your MAX unit separates the two dial plans, and prevents the formation of bundles with channels from both PRI lines.

The telephone numbers that you specify are the ones used to call this unit. There is a one-to-one correspondence between a telephone number and a channel, except when you are using GloBanD lines. (When the switch type is GloBanD, the MAX pools the numbers and can apply them to any channel of the PRI line.)

Usage: Specify a telephone number with a limit of 24 characters, which can include the following:

1234567890()[]!z-*#|

The default is null.

Example: `Ch 1 #=1212`

Dependencies: This parameter is applicable only for switched channels.

Location: Net/T1 > Line Config > Line *N*, Net/E1 > Line Config > Line *N*

See Also: Pri Num, Sec Num, Sub-Adr

Ch *N* Prt/Grp (*N*=1–24, 1–32)

Description: Ch *N* Prt/Grp has two functions, depending on a channel's configured usage. For switched channels, it specifies a port number to be used with the Ch *N* Slot parameter for call-routing purposes. In effect, it reserves the channel for calls to and from that port. For nailed channels, it assigns a group number, which will be referenced from a call or Connection profile to use the nailed channels for a connection.

Usage: Specify a number.

Dependencies: When specifying a port number for call routing purposes, you must also set the Ch *N* Slot parameter to specify the slot number.

Example: `Ch 1 Prt/Grp=5`

Location: Net/T1 > Line Config > Line *N*, Net/E1 > Line Config > Line *N*

See Also: Ch *N* Slot, Group

Ch *N* Slot (*N*=1–24, 1–32)

Description: Specifies a slot number to be used for call-routing purposes. In effect, it reserves the channel for calls to and from that slot.

Usage: Specify one of the following values:

- 0 (zero, the default)—This parameter is not used to route incoming calls.
- 3–8—Expansion slots. When looking at the back panel of the MAX unit, slot #3 is the bottom slot in the left bank of slots, followed by #4 and #5 in ascending order. Slot #6 is the bottom right slot, followed by #7 and #8 in ascending order.
- 9—The LAN. Calls are routed to the bridge/router module.

  Values 1 and 2 are invalid settings, because they represent the built-in slots containing T1 or E1 lines.

Dependencies: This parameter is applicable only for switched channels.

Example: `Ch 1 Slot=7`

Location: Net/T1 > Line Config > Line *N*, Net/E1 > Line Config > Line *N*

See Also: Ch *N* Prt/Grp

Ch *N* Trnk Grp (*N*=1–24, 1–32)

Description: Assigns a channel to a trunk group, making it available for outbound calls. Dial numbers for connections can then be directed to specific channels by specifying the trunk group as a single-digit dialing prefix to the far-end telephone number.

Usage: Specify a number from 4 to 9 for each trunk group. The default is 9.

Dependencies: This parameter applies only when trunk groups have been enabled in the System Sys Config profile.

Location: Net/T1 > Line Config > Line *N*, Net/E1 > Line Config > Line *N*

See Also: Use Trunk Grps

Circuit

Description: Specifies an alphanumeric name for a DLCI end point. When combined as a circuit, the two DLCI end points act as a tunnel. Data received on one DLCI bypasses the MAX router and is sent out on the other DLCI.

A circuit is a permanent virtual circuit (PVC) segment that consists of two DLCI end points and possibly two Frame Relay profiles. It requires two and only two DLCI numbers. Data is dropped if the circuit has only one DLCI, and if more than two are defined, only two are used. Circuits are defined in two Connection profiles. Data coming in on the DLCI configured in the first Connection profile is switched to the DLCI configured in the second one.

Usage: Specify a name of up to 16 characters for the circuit. The other end point of the PVC must specify the same name for its Circuit setting.

Example: `Circuit=circuit-1`

Dependencies: This parameter applies only to FR_CIR-encapsulated calls.

Location: Ethernet > Connections > *Connection profile* > Encaps options

See Also: Encaps

Clear

Description: Specifies the protocol that applies when the port receives a request to clear a call.

Usage: Specify one of the following values:

- Terminal—Clear the call manually by using DO 2. This setting is the default.
- DTR Active—Clear the call only if DTR is asserted at the port, indicating that the codec is ready to receive data.
- DTR Inactive—Clear the call when DTR becomes inactive, indicating that the codec is not ready to receive data.
- RTS Inactive—Clear the call when RTS becomes inactive, indicating that the codec does not have data to send.
- RTS Active—Clear the call when RTS is asserted, indicating that the codec is ready to send data.

Dependencies: If the Answer or Dial parameter is set to RS-366, V.25 bis, or X.21, set Clear to DTR Inactive unless your application requires otherwise. This setting is compatible with the CCITT recommendation for the V.25 bis and X.21 protocols and with most implementations of RS-366 dialing.

Location: Host/Dual (Host/AIM6) > Port*N* Menu > Port Config

See Also: Answer, Dial

Clear Call

Description: Specifies whether the dial-in connection is cleared when an interactive Telnet, Rlogin, or TCP session terminates. If the parameter is set to No, the user is returned to the terminal-server menu when the Telnet, Rlogin, or TCP session terminates.

Usage: Specify Yes or No. The default is No.

Yes specifies that the MAX clears the call when a Telnet, Rlogin, or TCP session terminates.

No specifies that the MAX returns the user to the terminal server menu when a Telnet, Rlogin, or TCP session terminates.

Example: `Clear Call=Yes`

Dependencies: This parameter is not applicable when terminal services are disabled.

Location: Ethernet > Mod Config > TServ Options

Clid Number

Description: Specifies the telephone number of the caller.

Usage: Enter up to 24 characters. By default, this parameter has a null value.

Location: Analog FXS > FXS Config > *FXS Configuration profile* > Line *N*

CLID PW

Description: Specifies the CLID authentication password the MAX unit requires to grant access to the calling device or dial-in user.

Usage: Specify up to 21 bytes of hidden text. The default is Ascend-CLID.

Location: Ethernet > Mod Config > Auth

Auth, Auth Host #, Auth Key, Auth Pool, Auth Port, Auth Timeout, Auth Req, Id Auth, Login Prompt

Client

Description: Enables the MAX to respond to multicast clients on the local Ethernet network. Clients cannot be supported on the MBONE interface, which means that the multicast router resides across a WAN link.

Usage: Specify Yes or No. No is the default.

Yes specifies that the MAX unit begins handling IGMP client requests and responses on the interface. It does not begin forwarding multicast traffic until the rate limit is set. The Rate Limit parameter specifies the rate at which the MAX accepts multicast packets from its clients. It does not affect the MBONE interface.

No specifies that the MAX does not handle IGMP client requests and responses on the interface.

Example: `Client=Yes`

Dependencies: This parameter is not applicable if Forwarding is disabled or if the local Ethernet interface is the MBONE interface (supporting a multicast router).

Location: Ethernet > Mod Config > Multicast

See Also: Forwarding, Mbone Profile

Client #*N* (*N*=1–9)

Description: Specifies up to nine IP address of clients permitted to make RADIUS requests. Each client address can support a range of addresses instead of a single client IP address. For example:

- Client #1=125.65.5.0/24
  This setting enables RADIUS requests from any hosts on the 125.65.5 subnet.
- Client #2=125.5.0.0/16

This setting enables RADIUS requests from any hosts on the 125.5 subnet.

- Client #3=135.50.248.76/32
  This setting enables requests from the host whose address is 138.50.248.76.

Note: If an address does not include a slash followed by the number of the mask bits, the software supplies a default mask based on the *class* of the address.

Usage: Specify an IP address. The default is 0.0.0.0, which disables the associated client field. At least one of the fields must contain an IP address other than 0.0.0.0 for the server to be active.

Dependencies: This parameter does not apply if the on-board RADIUS server is disabled.

Location: Ethernet > Mod Config > RADIUS Server

See Also: Server, Server Key, Server Port, *TAOS RADIUS Guide and Reference.*

Client Assign DNS

Description: Specifies whether client DNS server addresses will be presented while this connection is being negotiated.

Usage: Specify Yes (to use client DNS servers) or No. No is the default.

Example: `Client Assign DNS=No`

Location: Ethernet > Connections > *Connection profile* > IP Options

See Also: Client Pri DNS, Client Sec DNS

Client ID

Description: Specifies the system name used by a tunnel initiator during tunnel establishment.

Note: The value you specify does not affect user authentication.

Usage: Specify a value of up to 21 case-sensitive characters.

Example: `Client ID=1234567890Abcdefgklm1`

Location: Ethernet > Mod Config > *any Connection profile* > Tunnel Options

See Also: ATMP HA RIP, Home Network Name, Max Tunnels, Password, Pri. Tunnel Server, Profile Type, Sec. Tunnel Server, Tunnel Protocol, Tunnel VRouter, UDP Port

Client Gateway

Description: Specifies a connection-specific default route to be used for forwarding packets received on this connection. The MAX uses this default route instead of the system wide default route in its routing table. This route is connection-specific, so it is not added to the routing table.

Note: The MAX must have a direct route to the address you specify.

Usage: Specify the IP address of a next-hop router. The default value is 0.0.0.0. If you accept this value, the MAX unit routes packets as specified in the routing table, using the system wide default route if it cannot find a more specific route.

Example: `Client Gateway=10.1.2.3`

Location: Ethernet > Connections > *Connection profile* > IP Options

Client Pri DNS

Description: Specifies a primary DNS server address to be sent to any client connecting to the MAX. Client DNS has two levels: a global configuration that applies to all PPP connections and a connection-specific configuration that applies to that connection only. The global client addresses are used only if none are specified in the Connection profile. You can also choose to present your local DNS servers if no client servers are defined or available.

Usage: Specify the IP address of a DNS server to be used for all connections that do not have a DNS server defined. The default value is 0.0.0.0.

Example: `Client Pri DNS=10.9.8.7/24`

Location: Ethernet > Mod Config > DNS, Ethernet > Connections > *Connection profile* > IP Options

Client Sec DNS

Description: Specifies a secondary DNS server address to be sent to any client connecting to the MAX. Client DNS has two levels: a global configuration that applies to all PPP connections and a connection-specific configuration that applies to that connection only. The global client addresses are used only if none are specified in the Connection profile. You can also choose to present your local DNS servers if no client servers are defined or available.

Usage: Specify the IP address of a secondary DNS server to be used for all connections that do not have a DNS server defined. The default value is 0.0.0.0.

Example: `Client Sec DNS=10.9.8.7/24`

Location: Ethernet > Mod Config > DNS, Ethernet > Connections > *Connection profile* > IP Options

Client WINS Addr Assign

Description: Specifies whether the MAX presents the WINS server addresses to the dial-in client.

Usage: Specify Yes or No. Yes is the default.

Dependencies: This parameter applies if the PC dialing into the MAX supports DHCP.

Location: Ethernet > Connections > *Connection profile* > IP Options

See Also: Client WINS Primary Addr, Client WINS Secondary Addr

Client WINS Primary Addr

Description: Specifies the primary WINS server address.

Usage: Specify a valid IP address. The default value is 0.0.0.0/0.

Dependencies: This parameter applies if the PC dialing into the MAX supports DHCP.

Location: Ethernet > Connections > *Connection profile* > IP Options

See Also: Client WINS Addr Assign, Client WINS Secondary Addr

Client WINS Secondary Addr

Description: Specifies the secondary WINS server address.

Usage: Specify a valid IP address. The default value is 0.0.0.0/0.

Dependencies: This parameter applies if the PC dialing into the MAX supports DHCP.

Location: Ethernet > Connections > *Connection profile* > IP Options

See Also: Client WINS Addr Assign, Client WINS Primary Addr

Clock Source

Description: Specifies whether the T1 or E1 line can be used as the clock source for timing synchronous transmissions. With the Yes setting, the line provides timing as long as it is active and not in Red Alarm mode, and the MAX runs in recovered loop timing mode. If the MAX connects to more than one line, specifying Yes for each one gives the MAX the option of using any of the lines as a source of synchronous timing.

Usage: Specify Yes or No. Yes is the default, and is the proper setting for normal operations.

- Yes specifies that the line can be used as the clock source for timing synchronous transmissions.
- No specifies that the line cannot be used as the clock source. With this setting, the MAX uses another line for timing or uses its internal clock. This setting is recommended only when two MAX units connect to each other by a crossover cable (with optional T1 repeaters) between their network ports.

Example: `Clock Source=Yes`

Location: Net/T1 > Line Config > Line *N*, Net/E1 > Line Config > Line *N*, Net/BRI > Line Config > Line *N*

Clr Scrn

Description: Specifies whether the screen is cleared when a terminal-server session begins.

Usage: Specify Yes or No. Yes is the default.

Yes specifies that the MAX clears the screen when a terminal server session begins.

No specifies that the MAX does not clear the screen.

Example: `Clr Scrn=Yes`

Dependencies: This parameter is not applicable when terminal services are disabled.

Location: Ethernet > Mod Config > TServ Options

See Also: TS Enabled

Collect DNIS/ANI

Description: Specifies whether the Digital Signal Processor (DSP) decodes the calling and called DTMF digits on a T1 line that uses inband signaling, making DNIS and CLID information presented by the switch available for authentication and accounting.

Usage: Specify Yes or No. The default is No.

Yes specifies that the DSP decodes the DTMF digits.

No specifies that the DSP does not decode the DTMF digits.

Dependencies: This parameter is N/A if Sig Mode is not Inband *and* Rob Ctl is either Loop-Start, Ground-Start, Wink-Start or Idle-Start.

Location: Net T1 >Line Config > *any Line Config profile* > Line x

See Also: Sig Mode, Rob Ctl

COMB

Description: Specifies whether the MAX accepts or rejects incoming calls that use Combinet encapsulation and meet all other Answer profile criteria. Combinet requires authentication by password and MAC address.

Usage: Specify Yes or No. Yes is the default.

Yes specifies that the MAX will answer inbound Combinet calls, provided that they meet all other connection criteria.

No specifies that the MAX will not answer inbound calls from a Combinet bridge.

Dependencies: This parameter is not applicable unless bridging is enabled system wide in the Ethernet Mod Config profile.

Location: Ethernet > Answer > Encaps

See Also: Bridge, Bridging, Encaps

Comm

Description: Specifies the SNMP community name associated with the SNMP Protocol Data Units (PDU). The string you specify becomes a password that the MAX sends to the SNMP manager when an SNMP trap event occurs. The password authenticates the sender identified by the host address.

Usage: Specify the community name, up to 31 characters. The default is *public*.

Example: `Comm=Ascend`

Dependencies: If this parameter and the Dest parameter are null, the MAX does not generate SNMP traps.

Location: Ethernet > SNMP Traps

See Also: Dest

Command Spoof

Description: The Command Spoof parameter enables a MultiVoice gateway to spoof certain fax commands. Command spoofing allows two faxes connected across a low-latency network to better maintain a connection by having the MAX 6000 mimic certain fax commands and signals.

Usage: Pressing [Enter] toggles the value of the Command Spoof parameter between the following:

Value	Description
Yes	Enable spoofing of certain fax commands. Command spoofing is a method of improving performance and reducing fax errors on low latency networks.
No	Command spoofing is disabled (default).

Dependencies: The Command Spoof parameter has the following dependencies:

- This parameter defaults to `N/A` when a MultiVoice gateway is not hashed for real-time fax or T.38 fax processing is disabled (`T.38 Fax Enabled=No`).
- Changes to this parameter are effective with the next VoIP call.

Compare

Description: Specifies the type of comparison to make between the specified value in a filter and the specified location in the contents of a packet.

Usage: Specify one of the following values:

- Equals—The filter matches the packet when the specified value and the packet contents are equal. This is the default setting.
- NotEquals—The filter matches the packet when the specified value and the packet contents are not equal.

Dependencies: This parameter does not apply if the filter's Valid parameter is set to no or if the filter type is IP.

Location: Ethernet > Filters > Input Filters > In Filter *N* > Generic, Ethernet > Filters > Output Filters > Out Filter *N* > Generic

See Also: Length, Mask, Offset, Value, Valid

Compat Mode

Description: Enables or disables Vendor-Specific attribute (VSA) compatibility mode when the unit is either using Remote Authentication Dial-In User Service (RADIUS) for call logging to NavisAccess™ or acting as a RADIUS server that is able to accept requests for certain limited purposes, such as changing a filter or disconnecting a user.

Usage: Specify one of the following settings:

- Old specifies that the unit does not send the Vendor-Specific attribute to the RADIUS server and does not recognize the Vendor-Specific attribute if the server sends it. All attributes are sent in standard RFC format.

  Note: The Old setting applies only when the unit is acting as a RADIUS server and is the default value for this configuration.
- VSA specifies 8-bit VSA support. All standard attributes are sent in standard RFC format and all VSAs are sent in 8-bit VSA format. The unit ignores all VSAs in received packets that do not have the Vendor-Id parameter set to Ascend-Vendor-Id. VSA is the default for call logging to NavisAccess.
- 16Bit VSA specifies 16-bit VSA support. All standard attributes are sent in standard RFC format and all VSAs are sent in the 16-bit VSA format as Lucent VSAs. The system ignores all VSAs in received packets that do not have the Vendor-Id parameter set to Lucent-Vendor-Id. In this format, the first 256 Lucent VSAs are mapped to the 256 Ascend VSAs.

Example: `Compat Mode=16Bit VSA`

Location: Ethernet > Mod Config > Call Logging, Ethernet > Mod Config > RADIUS Server

See Also: Acct Compat Mode, Auth Compat Mode

Complete

Description: Specifies the criteria for having received enough digits on an incoming call that uses R2 signaling.

Usage: Specify 1-Digits, 2-Digits, and so on, up to 10-Digits, to specify up to ten digits of a telephone number. Or, to indicate that the full number has been received, accept the default End-Of-Pulsing setting. For call-routing purposes, the digits received before the call is answered are considered the called number.

Example: `# Complete=End-Of-Pulsing`

Location: Net/E1 > Line Config > *any Line Config profile* > Line *N*

Compression

Description: Enables or disables data compression for a Combinet link. Both sides of the link must enable compression for the algorithm to have any effect.

Usage: Specify one of the following values:

- None—The default in the Answer profile.
- Stac—Use a Lucent-modified version of draft 0 of the CCP protocol.

- Stac-9—Use draft 9 of the Stac LZS Compression protocol.
- MS-Stac—Use Microsoft/Stac compression (the same method as Windows95). If the caller does not acknowledge Microsoft/Stac compression, the MAX attempts to use standard Stac compression. If that does not work, it uses no compression.

Dependencies: This parameter is applicable only for Combinet connections. Both sides of the link must enable compression for the algorithm to have any effect.

Location: Ethernet > Answer > COMB Options, Ethernet > Connections > *Connection profile* > Encaps Options

See Also: Link Comp

Configuration Change

Description: Specifies whether the MAX unit sends an SNMP string whenever a user changes the configuration of the MAX or loads a different software binary. The string includes:

- Date and time of the change
- Security profile of the user who made the change
- Name of the user's Security profile

Usage: Specify Yes or No.

Yes specifies that the MAX sends an SNMP string each time a user modifies the configuration or loads a different software binary.

No specifies that modifications do not cause the MAX to send the SNMP string.

Example: `Configuration change=Yes`

Location: Ethernet > SNMP Traps > Enable Traps

Connection

Description: Specifies the number of a Connection profile needed to bring up a bridged or routed connection. The MAX unit uses this number to locate the profile and bring up the connection needed to forward packets whose destination address is not on the local network.

If the unit receives a packet whose destination MAC address is not on the local Ethernet network, it looks in the bridging table for a matching MAC address and uses the specified Connection profile to bring up a bridged connection.

If the unit receives an IPX packet whose destination address is not on the NetWare LAN, it checks its IPX routing table and uses the specified Connection profile to bring up an IPX connection.

Note: The number of a Connection profile is the unique portion of the number preceding the profile's name in the Connections menu.

Usage: Specify a Connection profile number.

Dependencies: Bridge Adrs profiles are not used for connections that enable dial-on-broadcast.

Location: Ethernet > Bridge Adrs, Ethernet > IPX Routes

See Also: Dial Brdcast, Route IPX

Console

Description: Specifies the interface established at the VT100 Control port on the MAX back panel.

Usage: Specify one of the following values:

- Standard—The standard set of edit menus comes up in the VT100 window at system startup. This setting is the default.
- MIF—Machine Interface Format (MIF) is accessible at system startup. From the MIF interface you can display the edit menus by pressing Ctrl-C. You can return to MIF again by using the Use MIF command.
- Limited—A set of simplified menus comes up. The menus are useful for operating AIM ports (but not for bridging or routing). To enter or exit the simplified menus, press Ctrl-T.

Dependencies: You cannot operate MIF through a hand-held terminal. Only a VT100 terminal or emulator can operate MIF.

Location: System > Sys Config

Console Security

Description: Protects the console port by using Security profile authentication or RADIUS server authentication.

Usage: Specify one of the following values:

- None—The default. Serial console password protection is disabled.
- Profile—Requires Security profile authentication. The terminal prompts for login and password. The MAX authenticates these values through the Security profiles.
- Auth Setting—Requires external authentication. Currently, the only types of external authentication available for the console port are RADIUS and RADIUS/LOGOUT.

Dependencies: The Ascend-Telnet-Profile attribute must be set to Full Access or to the name of a valid Security profile. In either case, the MAX searches all the Security profiles to find the login name and password.

Location: System > Sys Config

Contact

Description: Specifies the person or department to contact to report error conditions. This field is SNMP readable and settable.

Usage: Specify the name of the contact person or department. You can enter up to 80 characters.

Example: `Contact=rchu`

Location: System > Sys Config

See Also: Location

Cost

Description: Specifies the cost of an OSPF link. The cost is a configurable metric that must take into account the speed of the link and other issues. The lower the cost, the more likely the interface will be used to forward data traffic.

With the exception of links to stub networks, the output cost must always be nonzero. A link with a cost of 0xFFFFFF (16777215) is considered nonoperational.

In a static route, the interpretation of this cost depends on the type of external metrics specified by the ASE-Type parameter. 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. Any Type-2 metric is considered greater than the cost of any path internal to the autonomous system (AS).

Usage: Specify a number greater than 0 and less than 16777215. The default is 1 on the Ethernet interface and 10 on the WAN links.

Example: `Cost=50`

Location: Ethernet > Connections > *Connection profile* > OSPF Options, Ethernet > Mod Config > OSPF Options

Country

Description: Specifies country-specific port settings.

Usage: Specify a name.

For the T1 unit: Specify U.S. or Japan. The default is U.S.

For the E1 unit: Specify Australia, Brazil, France, Germany, or U.K. The default is U.K.

For the BRI unit: Specify U.S. or Japan. The default is U.S.

Note: MAXPOTS slot cards only support the Bellcore Type I caller ID format which might not be supported in all countries.

Location: System > Sys Config

CUG Index

Description: Specifies the closed user group (CUG) index/selection facility to use in the next call request. The closed user group selection/index facility is used to indicate to the called switch the closed user group selected for a virtual call.

Usage: Specify the CUG index to use in the next call request. You can specify up to two digits. The default is null.

Dependencies: Encaps must be set to X25/PAD for CUG Index to be applicable.

Location: Ethernet > Connections > *Connection profile* > Encaps Options, Ethernet > Answer > PAD Options, Ethernet > Answer > T3POS Options

D

Data Filter

Description: Specifies the number of a filter used to determine if packets should be forwarded or dropped. If both a call filter and data filter are applied to a connection, the MAX applies a call filter after applying a data filter. (Only those packets that the data filter forwards can reach the call filter.)

Usage: Specify a number from 0 to 199. The number you enter depends on whether you are applying a filter you created through the VT100 interface or a firewall you created with Secure Connect Manager (SCM).

If you are applying a filter created through the VT100 interface, enter the last 2 digits of the filter number as it appears in the Filters menu.

If you are applying a firewall created with SCM, add 100 to the last 2 digits of the firewall number as it appears in the Firewalls menu. For example, if the number of your firewall is 90-601, specify 101. For information about downloading firewalls to the MAX, see your SCM documentation. The numbering scheme for filters and firewalls is:

- 0 (the default) indicates that no filtering is being used.
- 1-99 indicates that a filter created through the VT100 interface is being used.
- 100-199 indicates that a filter created through SCM is being used.

When you set Data Filter to 0 (zero), the MAX forwards all data packets.

Example: `Data Filter=7`

Location: Ethernet > Answer > Session Options, Ethernet > Connections > *Connection profile* > Session Options

See Also: Call Filter, Filter

Data Format

Description: Specifies the data format and parity checking/generation behavior of the Packet Assembler/Disassembler (PAD) when it validates opening frames and during Local mode data transfer.

Usage: Specify one of the following values:

- 7-E-1 (the default)—The PAD uses 7 data bits, even parity, and 1 stop bit during opening frame validation and local mode data transfer.
- 7-O-1—The PAD uses 7 data bits, odd parity, and 1 stop bit during opening frame validation and local mode data transfer.
- 7-M-1—The PAD uses 7 data bits, mark parity, and 1 stop bit during opening frame validation and local mode data transfer.

- 7-S-1—The PAD uses 7 data bits, space parity, and 1 stop bit during opening frame validation and local mode data transfer.
- 8-N-1—The PAD uses 8 data bits, no parity, and 1 stop bit during opening frame validation and local mode data transfer.

Dependencies: None. This parameter is always applicable.

Location: Ethernet > Connections > *Connection profile* > Encaps Options, Ethernet > Answer > T3POS Options

Data Svc

Description: 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 call profile, Connection profile, X.25 profile, or Frame Relay profile, Data Svc specifies the type of data service the link uses. In a Dial Plan profile, Data Svc specifies the data service associated with the number the MAX dials under the extended dial plan.

Note: Either party can request a data service that is unavailable. In this case, the MAX cannot connect the call.

Usage: Specify one of the following values:

- 56K—The call contains any type of data and connects to the Switched-56 data service. The only services available to lines using inband signaling (T1 or E1 lines containing one or more switched channels, and Switched-56 lines) are 56K and 56KR.
- 56KR—The call contains restricted data, guaranteeing that the data the MAX transmits meets the density restrictions of D4-framed TI lines, and connects to the Switched-56 data service. The only services available to lines using inband signaling (T1 or E1 lines containing one or more switched channels, and Switched-56 lines) are 56K and 56KR.
- 64K—The call contains any type of data and connects to the Switched-64 data service. Data services above 64 Kbps are not valid for a BONDING call.
- Voice—The call is an end-to-end digital voice call for transporting data when a switched data service is not available. If you choose this setting, the data can become unusable unless you meet the following technical requirements:
  - Use only digital end-to-end connectivity. No analog signals should be present anywhere in the link.
  - Make sure that the telephone company is not using any intervening loss plans to economize on voice calls.
  - Do not use echo cancellation. Analog lines can echo, and the technology used to take out the echoes can also scramble data in the link.
  - Do not make any modifications that can change the data in the link.
- Modem —The call uses a digital modem. If no digital modems are available, the call is not placed. The data rate depends upon the quality of the connections between modems and the types of modems used. This setting requires that your MAX have digital modems installed. Modem applies only when Encaps=MPP, PPP, or X.25/PAD. Currently, multichannel modem calls are not supported even if Encaps=MPP.
- V.110 Bit-Rate Data-Service —The call uses a V.110 terminal adapter, using the PPP protocol at the specified bit rate over the specified data service line. The bit rate can be one of the following values:

  - v110 2.4
  - v110 4.8
  - v110 9.6
  - v110 19.2
  - v110 38.4

  The data-service can be one of the following values:

  - 56K (switched-56)
  - 56KR (restricted switched-56)
  - 64K (switched-64)

  If the MAX cannot establish communication with the remote terminal adapter at the specified bit rate, it attempts to use one of the other four bit rates.

- Inherit—The call connects with the data service as requested by the caller on the local Host/BRI line. This setting is available only in Dial Plan profiles. If Data Svc is not set to Inherit in the Dial Plan profile, the setting in the Dial Plan profile overrides the settings in the call profile and Connection profile.
- 384K/H0—The call contains any type of data and connects to the Switched-384 data service. This setting is available only in call profiles. This AT&T data service does not require MultiRate or GloBanD. A Host/AIM6 expansion module supports a maximum of four 384K/H0 calls.
- 384KR—The call contains restricted data and connects to MultiRate or GloBanD data services at 384 Kbps. This setting is available only in call profiles.
- 1536K—The call contains any type of data and connects to the Switched-1536 data service at 1536 Kbps. This setting is available only in call profiles, and is valid only for lines using NFAS signaling.
- 1536KR —The call contains restricted data and connects to the Switched-1536 data service at 1536 Kbps. This setting is valid only for lines using NFAS signaling, and is available only in call profiles.
- 128K, 192K, 256K, and other multiples of 64K—If the MAX has the MultiRate option, these data services appear. These values are available only in call profiles and on a PRI line with MultiRate or GloBanD data services.

Dependencies: 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 specifies the rate at which the MAX routes data to the host for each channel in the connection. When Call Type=FT1-B&O or Call Type=FT1-AIM, the Data Svc parameter applies to the switched channels.

Location: Host/Dual (Host/AIM6) > Port*N* Menu > Directory, Ethernet > Connections > *Connection profile* > Telco Options, System > Dial Plan, Ethernet > Frame Relay, Ethernet > X.25

See Also: Call Type

Date

Description: Specifies the month, day, and year. You should set this parameter when installing the MAX.

Usage: Specify the current date in the format *month* /*day* /*year*. The default is 00/00/00.

Location: System > Sys Config

DBA Monitor

Description: Specifies how the MAX monitors the traffic over an MP+ connection. Only the initiating side of the call can add or subtract bandwidth. If both sides of the link have DBA Monitor set to None, Dynamic Bandwidth Allocation is disabled.

Usage: Specify one of the following values:

- Transmit—The MAX adds or subtracts bandwidth on the basis of the amount of data it transmits. Transmit is the default.
- Transmit-Recv—The MAX adds or subtracts bandwidth on the basis of the amount of data it transmits *and* receives.
- None—The MAX does not monitor traffic over the link.

Dependencies: DBA Monitor is supported only on MP+ calls.

Location: Ethernet > Connections > *Connection profile* > Encaps Options

See Also: Dyn Alg, Encaps, Idle Pct, Target Util

DCE Addr

Description: Specifies the address of the calling unit in the EU-UI header of packets that the calling unit sends.

Usage: Specify the DCE address. Contact your service provider for the correct address.

Dependencies: This parameter applies only to EU-UI connections.

Location: Ethernet > Connections > *Connection profile* > Encaps Options

See Also: DTE Addr, Encaps

DCE N392

Description: Specifies the number of errors during DCE N393 monitored events that causes the network side to declare the user-side procedures inactive.

Usage: Specify a value from 1 to 10 that is less than DCE N393.

Example: `DCE N392=5`

Dependencies: This parameter is N/A when FR Type is DTE.

Location: Ethernet > Frame Relay

DCE N393

Description: Specifies the DCE monitored event count (from 1 to 10).

Usage: Specify a value from 1 to 10 that is greater than DCE N392.

Example: `DCE N393=7`

Dependencies: This parameter is N/A when FR Type is DTE.

Location: Ethernet > Frame Relay

DeadInterval

Description: Specifies the number of seconds the MAX will wait before declaring its neighboring routers down after it stops receiving the router's Hello packets.

Usage: Specify a number. In a Connection profile, the default is 120 seconds. The default is 40 seconds.

Example: `DeadInterval=240`

Location: Ethernet > Connections > *Connection profile* > OSPF Options, Ethernet > Mod Config > OSPF Options

See Also: HelloInterval

Dec Ch Count

Description: Specifies the number of channels the MAX removes as a bundle when bandwidth changes either manually or automatically during a call. You cannot clear a call by decrementing channels.

If the data service is 384K/H0 or 384KR, this value should be divisible by 6, because 384 Kbps is 6x64 Kbps. If the data service is MultiRate or GloBanD and the service you select is a multiple of 64 Kbps, this value should be a multiple of 6.

Usage: Specify a number from 1 to 32. The default is 1.

Example: `Dec Ch Count=1`

Dependencies: This parameter does not apply if all channels of a link are nailed up. In a call profile, this parameter applies only if the Call Type parameter is set to AIM, FT1-AIM, FT1-B&O, or BONDING and if the Call Mgm parameter is set to Manual, Dynamic, or Mode 2.

Location: Host/Dual (Host/AIM6) > Port*N* Menu > Directory, Ethernet > Connections > *Connection profile* > Encaps Options

See Also: Base Ch Count, Inc Ch Count, Max Ch Count

Default Zone

Description: Specifies the default zone for nodes on an AppleTalk seed router's internet. All AppleTalk nodes on the seceded network use the default zone until a user explicitly selects a

different zone name. A zone is a multicast address containing an arbitrary subset of the AppleTalk nodes in an internet. Each node belongs to only one zone, but a particular extended network can contain nodes belonging to any number of zones. Zones provide departmental or other groupings of network entities that a user can easily understand.

Usage: Enter a zone name of up to 33 alphanumeric characters.

In a Lucent AppleTalk router, zone names are not case sensitive. However, some routers regard zone names as case sensitive, and you should be consistent in spelling zone names when you configure multiple connections or routers. Although AppleTalk permits the use of spaces in zone names, it does not consider an underscore to be the same as a space. Since some routers do equate the underscore and the space, or do not recognize a space as a valid character, it is advisable to use only the underscore in a network with routers other than Lucent routers.

Example: `Default Zone=SALES`

Dependencies: You must select the following:

- AppleTalk=Yes (in Ethernet > Mod Config)
- Route AppleTalk=Yes in the Connection profile (if the connection requires authentication using names and passwords)
- Values for the remaining parameters in the AppleTalk Options profile

Location: Ethernet > Mod Config > AppleTalk Options

See Also: AppleTalk, Route AppleTalk, AppleTalk Router, Zone Name #*N*, Net Start, Net End, Peer (AppleTalk Options)

Def Telnet

Description: Specifies whether the MAX will interpret a command that does not include a keyword as a hostname for a Telnet command. To display the terminal-server-command keywords, enter Help or a question mark (?) from the terminal-server command-line interface.

Usage: Specify Yes or No. Yes is the default.

Yes specifies that the MAX interprets any terminal-server command that does not begin with a keyword as though it began with the keyword Telnet. (That is, it interprets the string entered at the prompt as a Telnet hostname.)

No specifies that all terminal-server commands must begin with a keyword.

Example: `Def Telnet=Yes`

Location: Ethernet > Mod Config > TServ Options

Delay Dual

Description: Specifies whether the MAX inserts a 10 second delay between dialing the first and second calls in a dual-port call.

In a dual-port call, a codec performs inverse multiplexing on two channels so that a call can achieve twice the bandwidth of a single channel. Inverse multiplexing is a method of combining individually dialed channels into a single, higher-speed data stream.

The codec provides two ports, one for each channel. Two AIM ports on the MAX connect a dual-port call to the codec. These ports can be the V.35, RS-499, or X.21 ports on the MAX, and are called the primary port and the secondary port. Because the MAX places the two calls in tandem and clears the calls in tandem, it considers them a single call.

Usage: Specify Yes or No. No is the default.

Yes specifies that the MAX waits ten seconds before dialing the second call in a dual-port call.

No specifies that the MAX places both calls at the same time.

Example: `Delay Dual=Yes`

Location: System > Sys Config

Delete Digits

Description: Specifies the number of digits deleted from the beginning of the telephone number dialed by the device connected to line 2. Typically, a Private Branch Exchange (PBX) 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 was formerly be connected to a switch that supplied a T1 line, and that line is now supplied by the MAX. 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.

Usage: Specify the number of digits to delete from the beginning of the telephone number. You should specify the number of digits received from the PBX specific to the T1 switch the MAX is emulating.

Example: `Delete Digits=2`

Dependencies: This parameter applies only to T1 lines using PBX-T1 conversion.

Location: Net/T1 > Line Config > Line *N*

See Also: Sig Mode

Dest

Description: In a Static Rtes profile, Dest specifies the route's target IP address. This is the destination address that causes the MAX to bring up this route. In a Static Rtes profile, the default null address indicates the default route used for all destinations that have no explicit route in the routing table.

In an SNMP Traps profile, Dest is the IP address to which the MAX sends traps (the IP address of the station running an SNMP management utility). The default null address means that no traps are sent. If the Comm parameter is also null, traps are turned off altogether.

Usage: Specify the destination IP address. The default value is 0.0.0.0/0.

Example: `Dest=10.207.23.1`

Dependencies: This parameter does not apply if the MAX does not support IP routing.

Location: Ethernet > Static Rtes, Ethernet > SNMP Traps

See Also: Gateway

DestChanGroup

Description: Specifies the channel group for incoming calls to go out on. The DestChanGroup parameter provides a way to associate incoming calls with particular outgoing channels.

Usage: Specify a channel group number specified for ChanGroupID.

Example: `DestChanGroup=44`

Dependencies: This parameter does not apply if line usage is set to D&I, Nailed, or Unused, or if outgoing channel groups are not assigned ChanGroupID numbers.

Location: Net/T1 > Line Config > *Line Config profile* > Line *N* > Net2Net Incoming Calls, System > Answer Plan

See Also: Dial Plan, #DialPlanSelDigits, Ch *N* ChanGroupID

Dest Port

Description: Specifies the port to which traps are sent.

Usage: Specify a number from 1 to 65535. The default is 162.

Example: `Dest Port=20`

Location: Ethernet > SNMP Traps

See Also: Active, Message Proc Model, Notify Tag List, Security Level, Security Model, Security Name, Tag, Target Param Name

Dest VRouter

Description: Specifies whether or not there is a static route between VRouters and, if there is, the name of the destination VRouter.

Usage: Specify the name of the destination VRouter. You can specify the address of the main VRouter as the destination. The default is 0.0.0.0, which specifies that this is not a static route between VRouters.

Example: `Dest VRouter=vr2`

Dependencies: The default setting of 0.0.0.0 is correct if the gateway parameter, in the Static Rtes submenu, includes an IP address.

The Dest VRouter setting is valid only if the Sys Option Status display specifies VRouter Avail.

Location: Ethernet > Static Rtes > *any Static Rtes profile*

See Also: Active, Allow As Client DNS, Dest VRouter, Domain Name, Name, Pool#*N* Count, Pool#*N* Name, Pool#*N* Start, Pool Summary, Pri DNS, Sec DNS, Sec Domain Name, RIP Policy, RIP Summary, RIP Trigger, VRouter IP Adrs

Detect End of Packet

Description: Specifies whether the MAX buffers incoming data from TCP-CLEAR dial-in sessions that do not require V.120 processing.

Usage: Specify Yes or No. The default is No.

Yes—After authenticating the session, the MAX unit begins buffering incoming WAN data. The unit continues buffering data until it receives the specified End of Packet Pattern, until it reaches the timeout specified by Packet Flush Time, or until the data reaches the maximum packet length specified by Packet Flush Length, whichever occurs first.

No—The MAX unit does not buffer incoming data from a TCP-CLEAR dial-in session.

Example: `Detect End of Packet=No`

Location: Ethernet > Answer > TCP Clear Options, Ethernet > Connection > *any Connection profile* > Encaps Options

See Also: End of Packet Pattern, Packet Flush Length, Packet Flush Time

Dial

Description: Specifies how a call originates at the port. In addition to dialing through the MAX unit's user interface, you can use one of three dialing protocols to dial from the AIM port. The protocols are RS-366, V.25 bis, and X.21.

Note: The Dial parameter setting does not prevent you from dialing manually.

Usage: Specify one of the following values:

- Terminal (the default)—The MAX dials calls only when the user enters the DO 1 (DO Dial) command or presses Ctrl-D-1.
- DTR Active—The MAX dials the number in the current call profile when the DTR signal is asserted at the port.

  An AIM port 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 being sent determines the control-line state. For example, a device can send a signal to inform another party that it is ready to receive data. In this case, the control-line state is Data Transmit Ready (DTR). The process of sending control signals is called handshaking.

  When the device connected to the MAX unit's AIM port is ready to receive data, it sends an electrical signal over the DTR line to the MAX. When this signal is present, DTR is asserted.
- RS-366 ext1—The MAX dials calls through an RS-366 dialing service. The RS-366 dialing interface on the MAX meets the EIA RS-366 specification for dialing individual calls from an AIM port.
- RS-366 ext2—Supports RS-366 dialing, but has different message protocols than RS-366.

  If you choose this setting, you must also configure the RS-366 Esc parameter.

- V.25bis—V.25 bis handshaking controls dialing from your AIM port module. The V.25 bis dialing interface on the MAX meets the V.25 bis CCITT recommendation for the addressed call mode of dialing and answering local calls. This interface enables direct dialing and answering from an AIM port that uses the V.25 bis dialing protocol. The MAX unit's implementation of V.25 bis conforms to the extension of this standard published by Cisco Systems and Lucent Technologies.

  The port must support AIM functionality for this setting to have any effect. V.25bis does not appear if you have used the Dual Ports parameter in the Host-Interface profile to pair the port with another port.
- V.25bis-C—Identical to V.25bis, except that the Clear To Send (CTS) signal does not change its state during a call.
- X.21 ext1—The MAX dials calls under the control of the AIM port module as described in the CCITT Blue Book Rec. X.21. The X.21 dialing interface on the MAX is often used for direct dialing and answering from an attached codec, router, or other codec.
- X.21 ext1-P—Uses the same protocol as X.21 ext1, and is required when you are using a PictureTel X.21 dialer.
- X.21 ext2—Supports X.21 dialing, but has different message protocols than X.21 ext1.

Location: Host/Dual (Host/AIM6) > Port*N* Menu > Port Config

See Also: RS-366 Esc

Dial

Description: Specifies the number used to dial out this connection. The number can consist of up to 24 characters, which can include a dialing prefix that directs the connection to use a trunk group or dial plan (for example, 6-1-212-555-1212).

In call profiles, if the call type specifies a two-channel call, you can specify two telephone numbers, with a total of up to 49 characters. The two numbers must be separated by an exclamation mark (for example, 5551212!5551234).

Note: The telephone number can include a subaddress or trunk-group number. If the use of trunk groups is enabled in the System > Sys Config profile, this parameter must specify a trunk group as the first digit.

Usage: Specify a telephone number of up to 24 characters. The MAX sends only the numeric characters to place a call. You must limit the number to the following characters: 1234567890()[]!z-*#|

Example: `Dial #=6-1-808-555-1212`

Dependencies: This parameter is inapplicable for leased connections or connections using Frame Relay encapsulation.

Location: Host/Dual (Host/AIM6) > Port*N* Menu > Directory, Ethernet > Connections > *Connection profile*, Ethernet > Frame Relay, Ethernet > X.25

See Also: B*N* Trnk Grp, Call Type, Ch *N* Trnk Grp, Dial Plan, Encaps, Sub-Adr, Use Trunk Grps

Dial Enabled

Description: Enables or disables outbound dialing through a POTS port.

Usage: Specify Yes or No. The default is Yes.

- Yes—Enables dial-out from this port.
- No—Disables the port, and the user gets an error tone when the phone goes off-hook.

Location: Analog FXS > FXS Config > *FXS Configuration profile* > Line *N*

Dial Plan

Description: If the call matches a Call Routes profile in which a Dial Plan value is specified, the MAX applies the specified Dial Plan to the call.

Usage: Specify a value from 1 to 32. The default is 0, which does not apply a dial plan.

Location: System > Call Routes > *Call Routes profile*

See Also: Name, Call-By-Call, PRI # Type, NumPlanID

Dialer Type

Description: Specifies the type of redialer for incoming fax calls.

Note: This parameter applies only to MAX 6000 units.

Usage: Specify one of the following values:

- `Mitel` (the default)
- `Atlas`

Location: Ethernet > Mod Config > IP Fax Options

See Also: All Calls Are Fax, DID #N (N=1-4), InCall Type

Dial *N*# (*N*=1–6)

Description: Specifies the telephone numbers that reach the destination of the profile.

Usage: Specify a telephone number for each Dial *N*# parameter. You can enter up to 24 characters, and you must limit those characters to the following:

1234567890()[]!z-*#|

The MAX sends only the numeric characters to place a call. The default value is null.

In a call profile, when Call Type=2 Chnl, the Dial *N*# parameter accepts a single telephone number consisting of up to 49 characters, or two telephone numbers consisting of up to 24 characters each. The two telephone numbers must be separated by an exclamation point, as in this specification:

5551212!5551234

The first digit of the setting specified for Dial *N*# must match a trunk group specified by the Ch *N* Trnk Grp parameter in a Line *N* profile. For example, the first digit of Dial 1#=4-555-1234 is 4. The MAX places the call over the corresponding trunk group.

If the Dial Plan parameter specifies Trunk Grp, the digits following the first digit specified for Dial *N*# constitute an ordinary telephone number. If Dial Plan specifies Extended, the two digits that point to a Dial Plan profile come next, followed by an ordinary telephone number.

Dependencies: This parameter is inapplicable unless trunk groups are enabled in the System > Sys Config profile.

Location: System > Destinations

See Also: B*N* Trnk Grp, Ch *N* Trnk/Grp, Use Trunk Grps, Dial Plan

Dial Brdcast

Description: Specifies whether the MAX will dial this connection when it receives Ethernet broadcast packets. By default, the MAX does not use the dial-on-broadcast feature. It relies on its internal bridging table to bring up specific bridged connections.

If dial-on-broadcast is enabled in one or more Connection profiles, the MAX brings up all of those profiles whenever it receives Ethernet broadcast packets. It never uses a bridging table entry for those connections, even if one exists.

Usage: Specify Yes or No. No is the default.

Yes specifies that the MAX dials this connection if it is not online and the MAX receives a frame whose MAC address is set to broadcast.

No specifies that broadcast packets do not cause the MAX to dial this connection.

Dependencies: This parameter applies only if the Connection profile enables bridging and allows outgoing calls.

Location: Ethernet > Connections > *Connection profile*

See Also: Connection #, Bridge, AnsOrig

Dial Plan

Description: Specifies whether a module uses trunk groups or the extended dial plan. The extended dial plan is typically used to route calls from a terminating device on a Host BRI line out to a WAN that uses PRI channels. However, it can also be used to set up the PRI parameters for other outbound calls.

Usage: Specify one of the following values:

- Extended—The MAX uses the extended dial plan. When Dial Plan is set to Extended and the use of trunk groups is enabled in the System > Sys Config profile, the first digit of the setting for Dial # parameter or Dial *N*# parameter specifies a trunk group. The next two digits specify a Dial Plan profile containing the parameters the MAX uses to make the call. The parameters in the Dial Plan profile constitute the extended dial plan.

  Because the Dial Plan profile parameters apply only to PRI lines, choose Extended only if the MAX makes outgoing calls on PRI lines.

- Trunk Grp—The digits following the first digit define an ordinary telephone number. The first digit specifies a trunk group. If you choose this setting for calls on a T1 PRI line, the Dial Plan profile parameters default to Data Svc set to Inherit, Call-by-Call set to 0, and PRI # Type set to National.

Example: `Dial Plan=Trunk Grp`

Location: Ethernet > Mod Config > WAN Options, Host/BRI > Line Config > Line *N*, Host/Dual (Host/AIM6) > Port*N* Menu > Port Config, BRI/LT > Line Config > Line *N*

See Also: B*N* Trnk Grp, Call-by-Call, Ch *N* Trnk Grp, Data Svc, Dial #, Dial *N*#, PRI # Type

Dial Query

Description: Specifies whether the MAX places a call to the location indicated in the Connection profile when a workstation on the local IPX network looks for the nearest IPX server. More than one Connection profile can have this parameter set to Yes. As a result, several connections can occur at the same time.

Usage: Specify Yes or No. No is the default.

Yes specifies that the MAX places a call to the location specified in the Connection profile when a workstation looks for the nearest server.

Note that a workstation is likely to stop attempting to find a server before the MAX establishes any connections with the Dial Query mechanism.

No specifies that the MAX does not place a call to the location specified in the Connection profile when a workstation looks for the nearest server.

Dependencies: If there is an entry in the MAX unit's routing table for the location specified by the Connection profile, Dial Query has no effect.

Location: Ethernet > Connections > *Connection profile* > IPX Options

Dialout OK

Description: Specifies whether or not the Connection profile can be used to dial out using one of the MAX unit's digital modems.

Usage: Specify Yes or No. The default is No.

Yes—specifies that the Connection profile allows modem dialout.

No—specifies that the Connection profile does not allow modem dialout.

Example: `Dialout OK=Yes`

Dependencies: This parameter is not applicable unless Imm. Modem Access is set to User.

Location: Ethernet > Connections > *Connection profile* > Telco Options

See Also: Imm. Modem Access

DID #*N* (N=1-4)

Description: The value of this parameter will be compared to the incoming DID numbers to authenticate incoming calls. You can specify up to four DID numbers for authentication.

Note: This parameter applies only to MAX 6000 units.

Usage: Specify up to 24 digits.

Location: Ethernet > Mod Config > IP Fax Options

See Also: All Calls Are Fax, Dialer Type, DNIS #N, InCall Type

Direct Call X.121 Addr

Description: For DTE-initiated calls, specifies the default host's X.121 address.

Usage: Specify an alphanumeric string. You can enter up to 15 characters. The default is null.

Dependencies: None. This parameter is always applicable.

Location: Ethernet > Connections > *Connection profile* > Encaps Options
Ethernet > Answer > T3POS Options

Disc on Auth Timeout

Description: Specifies whether the MAX unit gracefully shuts down the PPP connection on an external authentication server timeout.

Usage: Specify Yes or No. No is the default.

Yes causes the unit to hang up a PPP connection when an external authentication server request times out.

No causes the unit to shut down cleanly when the external authentication server request times out.

Dependencies: This parameter applies only to PPP connections.

Location: Ethernet > Answer > PPP Options

See Also: PPP

DLCI

Description: Specifies a Frame Relay DLCI number for a gateway or circuit connection. A DLCI is a number between 16 and 991, which is assigned by the Frame Relay administrator. A DLCI is not an address, but a local label that identifies a logical link between a device and a Frame Relay switch. The switch uses the DLCI to route frames through the network, and the DLCI can change as frames are passed through multiple switches.

The MAX receives an incoming PPP call, examines the destination address, and brings up the appropriate Connection profile to that destination, as usual. If the Connection profile specifies frame-relay encapsulation, the Frame Relay profile, and a DLCI, the MAX encapsulates the packets in Frame Relay (RFC 1490) and forwards the data stream out to the Frame Relay

switch using the specified DLCI. The Frame Relay switch uses the DLCI to route the frames. This is known as gateway mode.

Usage: Specify a number from 16 to 991. The default is 16. Ask your Frame Relay network administrator for the value you should enter.

Example: `DLCI=17`

Dependencies: This parameter applies only to FR and FR_CIR encapsulated calls.

Location: Ethernet > Connections > *Connection profile* > Encaps Options

See Also: Encaps, FR Direct, FR DLCI

DM

Description: Specifies the subaddress associated with the MAX unit's digital modems. The MAX routes an incoming call whose subaddress matches the value of DM to the first available digital modem. The MAX handles such a call as a terminal-server call. If the subaddress matches the value of DM, but no digital modem is available, the MAX clears the call.

Usage: Specify a subaddress. You can specify a number from 0 to 99. The default is 0.

Dependencies: This parameter is ignored if the Sub-Adr parameter is not set to Routing.

Location: System > Sys Config

See Also: Ans *N*#, Sub-Adr

DNIS #N (N=1-4)

Description: Specifies four DNIS numbers to be defined for Fax recognition.

Usage: Specify up to 16 digits for each DNIS numbers.

Location: Ethernet >Mod Config > IP Fax Options

See Also: All Calls Are Fax, Dialer Type, DID #N, InCall Type

DNIS PW

Description: Specifies the DNIS authentication password the MAX unit requires before granting access to the calling device or dial-in user.

Usage: Specify 21 bytes of hidden text. The default is Ascend-DNIS.

Location: Ethernet > Mod Config > Auth

See Also: Ans *N*#, Ans Orig, Called #, Calling #, Id Auth, Login Prompt

Domain Name

Description: Specifies the local DNS domain name. The domain name is used for DNS lookups. When the MAX is given a hostname to look up, it tries various combinations

including appending the configured domain name. The secondary domain name (Sec Domain Name) can specify another domain name that the MAX can search using DNS.

Usage: Specify the domain name of the MAX. You can enter up to 63 characters.

Location: Ethernet > Mod Config > DNS

See Also: Pri DNS, Sec DNS, Sec Domain Name

Download

Description: Enables or disables permission to use the Save Cfg command to download the configuration of the MAX. Passwords are not saved to file.

Note: Passwords are not saved when you download the configuration. If you upload a saved configuration, all passwords are wiped out.

Usage: Specify Yes or No. No is the default.

Yes enables the user to download the MAX configuration (without the password values) by using the Save Cfg command in the Sys Diag menu.

No disables this permission.

Dependencies: This parameter is not applicable if the Operations parameter disables the operations permission.

Location: System > Security

See Also: *MAX Administration Guide*

DownMetric

Description: Specifies the metric for a route whose associated WAN connection is down.

Usage: Specify an integer. The higher the metric, the less likely that the MAX will use the route. The default metric for online WAN connections is 1. The default metric for offline WAN connections is 7. The metric you specify is in effect only as long as the WAN connection is down.

See Also: DownPreference

DownPreference

Description: Specifies the preference value for a route whose associated WAN connection is down.

Usage: Specify an integer. A higher preference number represents a less desirable route. The default preference for online WAN connections is 60. The default preference for offline WAN connections is 120. The preference you specify is in effect only as long as the WAN connection is down.

Dependencies: Make sure that routes for offline connections have a higher preference number than routes for online connections. The following table lists the factory default values for route preferences:

Route type	Default value
Interface	0
ICMP	30
RIP	100
OSPF ASE	150
OSPF Internal	10
Static	60
Down-Wan	120
Infinite	225

See Also: DownMetric

DS0 Min Rst

Description: Specifies when the MAX should reset accumulated DS0 minutes to 0 (zero). You can also use this parameter to specify that the MAX should disable the timer altogether.

A DS0 minute is the online usage of a single 56 Kbps or 64 Kbps switched channel for one minute. When the usage exceeds the maximum specified by the Max DS0 Mins parameter, the MAX cannot place any more calls, and takes any existing calls offline.

In a Sys Config profile, the accumulated minutes apply to all ports on the MAX and to the Ethernet module. In a Port Config profile, the accumulated minutes apply only to the associated AIM port.

Usage: Specify one of the following values:

- Daily—The MAX resets the accumulated DS0 minutes to 0 (zero) every day at 12 a.m.
- Monthly—The MAX resets the accumulated DS0 minutes to 0 (zero) on the first day of every month at 12 a.m.
- Off (the default)—The MAX disables the Max DS0 Mins parameter in the Sys Config profile or Port Config profile.

Location: Sys > Sys Config, Host/Dual (Host/AIM6) > Port*N* Menu > Port Config

See Also: Max Call Mins, Max DS0 Mins

Dst Adrs

Description: Specifies a destination IP address. After this value has been modified by applying the value specified for Dst Mask, it is compared to a packet's destination address.

Usage: Specify a destination IP address the MAX should use for comparison when filtering a packet. The zero address 0.0.0.0 is the default. If you accept the default, the MAX does not use the destination address as a filtering criterion.

Example: `Dst Adrs=10.62.201.56`

Dependencies: This parameter applies only to filters of type IP.

Location: Ethernet > Filters > Input Filters > In Filter *N* > IP, Ethernet > Filters > Output Filters > Out Filter *N* > IP

See Also: Dst Mask

Dst Chan Grp

Description: Specifies the destination MAXDAX channel group for a call. The MAX unit routes the outbound call to any channel configured to belong to the specified channel group.

Usage: Specify a value from 1 to 32,768. The default is 0, which disables MAXDAX functionality for the call.

Location: System > Call Routes > *Call Routes profile*

Dst Mask

Description: Specifies a mask to apply to the value of Dst Adrs before comparing the value to the destination address in a packet. You can use the mask to hide the host portion of an address, for example, or the host and subnet portion.

The MAX translates the mask and address specified by the Dst Adrs into binary format and then uses a logical AND to apply the mask to the address. Each binary 0 (zero) in the mask hides the bit in the corresponding position in the address. A mask of all zeros (the default) masks all bits, so all destination addresses match the Dst Adrs value. A mask of all ones (255.255.255.255) masks no bits, so the Dst Adrs values matches only the full destination address of a single host.

Usage: Specify the mask in dotted decimal format. The zero address 0.0.0.0 is the default. This setting indicates that the MAX masks all bits. To specify a single destination address, set Dst Mask to 255.255.255.255 and set Dst Adrs to the IP address that the MAX uses for comparison.

Example: `Dst Mask=255.255.255.0`

Dependencies: This parameter applies only to filters of type IP.

Location: Ethernet > Filters > Input Filters > In Filter *N* > IP, Ethernet > Filters > Output Filters > Out Filter *N* > IP

See Also: Dst Adrs

Dst Port

Description: Specifies the destination port for a call.

Usage: Specify a value from 1 to 8. The default is 0.

Dependencies:

- If both the Dst Port and Dst Slot parameters are set to nonzero values, the call is routed over the specified port/slot combination. If the Dst Port value is zero, and the value of Dst Slot is not zero, the call is routed over a port on the specified slot. You must not set Dst Port to a nonzero value if you set Dst Slot to 0 (zero).
- The Dst Port parameter applies only to POTS ports. Therefore, if you assign a value, it must specify a port on an installed MAXPOTS slot card.

Location: System > Call Routes > *Call Routes profile*

Dst Port Cmp

Description: Specifies the type of comparison the MAX makes when using the Dst Port # parameter.

Usage: Specify one of the following values:

- None—The MAX does not compare the packet's destination port to the value specified by Dst Port #. None is the default.
- Less—Port numbers with a value less than the value specified by Dst Port # match the filter.
- Eql—Port numbers equal to the value specified by Dst Port # match the filter.
- Gtr—Port numbers with a value greater than the value specified by Dst Port # match the filter.
- Neq—Port numbers not equal to the value specified by Dst Port # match the filter.

Dependencies: This parameter works only for TCP and UDP packets. You must set it to None if the Protocol parameter is not set to 6 (TCP) or 17 (UDP).

Location: Ethernet > Filters > Input filters > In filter *N* > IP, Ethernet > Filters > Output filters > Out filter *N* > IP

See Also: Dst Port #

Dst Slot

Description: Specifies the destination slot for the call.

Usage: Specify a value of 0 or 3 to 8. The default is 0.

Dependencies: If both Dst Slot and Dst Port parameters are set to nonzero values, the call is routed over the specified slot/port combination. If the Dst Slot value is not zero, and the Dst Port value is zero, then the call is routed over a port on the specified slot. You must not set Dst Slot to 0 (zero) if you set Dst Port to a nonzero value. If you assign a nonzero value, it must specify a MAXPOTS slot card.

Note: The Dst Slot parameter applies only to POTS ports. Therefore, if you assign a nonzero value, it must specify a port on an installed MAXPOTS slot card.

Location: System > Call Routes > *Call Routes profile*

Dst Trnk Grp

Description: Destination trunk group for the call. The call is routed over a channel belonging to the specified group.

Usage: Specify a value of 0 or 4 to 9. The default is 0, which does not designate a trunk call destination for a call.

Dependencies: This parameter applies only if Dst Chan Grp is zero (or NA) and Use Trunk Grps=Yes. If you set this parameter to a nonzero value, the call is routed over a channel belonging to the specified trunk group.

Location: System > Call Routes > *Call Routes profile*

DTE Addr

Description: Sets the address of the called unit in the EU-UI header of packets that the called unit sends.

Usage: Specify the address. Contact your service provider for the correct address.

Dependencies: This parameter applies only to EU-UI connections.

Location: Ethernet > Connections > *Connection profile* > Encaps Options

See Also: DCE Addr, Encaps

DTE Init. Mode

Description: For DTE-initiated calls, specifies the default data transfer mode. Note that the DTE can override this setting with an opening frame.

Usage: Specify one of the following values:

- Local (the default)—Error recovery is performed locally. In this mode, the MAX does not send supervisory frames (that is, ACKs and NAKs) across the X.25 network. The T3POS PAD is responsible for sending supervisory frames to the T3POS DTE.
- Transparent—The T3POS PAD does not provide any error recovery. In this mode, the DTE and the host system provide error recovery for the connection. In Transparent mode, however, the T3POS PAD does recognize a clear request command signal from the DTE (that is, DLE, EOT) and clears the call when it receives a DLE, EOT command.
- Blind—Same as Transparent mode except that the T3POS PAD does not clear a call when it receives a clear request command from the DTE. In this mode, the PAD or the host system must clear the call. The PAD passes all data *blindly*, without regard to the protocol in use. This mode provides a means to pass raw binary data between the DTE and the host system without reference to the protocol being used.
- Bin-Local—No error recovery is applied between the T3POS PAD and the host, but error recovery is applied between the PAD and the DTE. Like Blind mode, it passes data between the DTE and the host without reference to the protocol being used, but continues to use the T3POS protocol between the DTE and the PAD.

Dependencies: None. This parameter is always applicable.

Location: Ethernet > Connections > *Connection profile* > Encaps Options, Ethernet > Answer > T3POS Options

DTE N392

Description: Specifies the number of errors during DTE N393-monitored events that causes the user side to declare network-side procedures inactive.

Usage: Specify a value from 1 to 10 that is less than DTE N393.

Example: `DTE N392=3`

Dependencies: This parameter is not applicable when FR Type is DCE.

Location: Ethernet > Frame Relay

DTE N393

Description: Specifies the DTE monitored event count (from 1 to 10).

Usage: Specify a value from 1 to 10 that is greater than DTE N392.

Example: `DTE N393=5`

Dependencies: This parameter is not applicable when FR Type is DCE.

Location: Ethernet > Frame Relay

Dual Ports

Description: Specifies whether the AIM ports in a module or in the base system are paired for dual-port calls. If you are configuring the interface to an older model codec that does not support AIM, you can pair two AIM ports to provide double the bandwidth for a videoconferencing call. A dual-port call requires that the codec has a dual-port interface.

In a dual-port call, the codec performs its own inverse multiplexing on two channels so that a call can achieve twice the bandwidth of a single channel. A pair of AIM ports on the MAX connects to the codec. The pair includes a primary and secondary port. Because the MAX places the two calls in tandem and clears the calls in tandem, it considers them a single call.

Creating a dual-port configuration does not prevent you from dialing any other type of call from the primary host port of the pair, or from using either port for receiving any call type. Pairing ports does not disable RS-366 dialing at the secondary port.

Usage: Specify one of the following values:

- No Dual (the default)—No host ports are paired for dialing or receiving dual-port calls.
- 1&2 Dual—Host ports 1 and 2 are paired for dialing and receiving dual-port calls.

Example: `Dual Port=No Dual`

Location: Host/Dual (Host/AIM6) > Mod Config

Dyn Alg

Description: Specifies an algorithm for calculating average line utilization (ALU) over a certain number of seconds (Sec History).

Usage: Specify one of the following values:

- Quadratic (the default)—Gives more weight to recent samples of bandwidth usage than to older samples taken over the specified number of seconds. The weighting grows at a quadratic rate.
- Linear—Gives more weight to recent samples of bandwidth usage than to older samples taken over the specified number of seconds. The weighting grows at a linear rate.
- Constant—Gives equal weight to all samples taken over the specified number of seconds.

Location: Ethernet > Answer > PPP Options, Host/Dual (Host/AIM6) > Port*N* Menu > Directory, Ethernet > Connections > *Connection profile* > Encaps Options

See Also: Add Pers, Dec Ch Count, Dyn Alg, Inc Ch Count, Max Ch Count, Sec History, Sub Pers, Target Util

E

Early CD

Description: Specifies when the MAX raises Carrier Detect (CD) at its AIM port. An AIM port 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 being sent determines the control-line state. When a device receives a signal indicating that a sender has data to transmit, it raises CD. The process of sending synchronization signals between devices is called handshaking.

Usage: Specify one of the following values:

- None (the default)—The MAX raises CD after the completion of handshaking and an additional short delay.
- Answer—The MAX raises CD as soon as it answers a call, rather than waiting for the completion of handshaking. Choose Answer if your codec times out while waiting for CD.
- Originate—The MAX raises CD as soon as the remote end answers a call, rather than waiting for the completion of handshaking.
- Both—The MAX raises CD without waiting for the completion of handshaking whether it is answering or originating a call.

Example: `Early CD=None`

Location: Host/Dual (Host/AIM6) > Port*N* Menu > Port Config

Early Ringback Enable

Description: Enables the near-end MultiVoice Gateway to generate an early ringback tone on networks experiencing long call setup times. The near-end Gateway will play out a ringback tone for callers once a call connection is established with the far-end Gateway.

This feature is designed for use on networks experiencing long call setup times (that is, satellite IP networks, wireless networks, and networks using CAS trunks). Using it with other network configurations is not recommended, and can result in erroneous `ring->busy, ring->failure` announcements.

Usage: Early ringback is enabled or disabled by pressing Enter to toggle between `yes`, to enable the Gateway to play a ringback tone for the caller once the connection is established between the two calling Gateways, and `no`, the default, to have the caller wait to hear ringback from the far-end PSTN.

Example: `Early Ringback Enable=Yes`

ECM Enabled

Description: The ECM Enabled parameter enables error correction mode (ECM) for real-time fax calls. This allows fax frames to be retransmitted in the event that a frame is not received correctly.

Usage: Pressing [Enter] toggles the value of the ECM Enabled parameter between the following:

Value	Description
Yes	Enable fax frames to be retransmitted in the event a frame is not received correctly (default). ECM frames are relayed end to end between terminals.
No	ECM is disabled so fax frames containing errors are not corrected.

Dependencies: The ECM Enabled parameter has the following dependencies:

- This parameter defaults to `N/A` when a MultiVoice gateway is not hashed for real-time fax or T.38 fax processing is disabled (`T.38 Fax Enabled=No`).
- Changes to this parameter are effective with the next VoIP call.

Edit

Description: Enables you to customize which status windows are displayed in the VT100 interface at system startup. If you are running the simplified menus, the parameter determines which AIM port the MAX displays. If you enter a null value when running the simplified menus, the MAX displays host port #1.

Usage: Specify a slot and port address, using the format *XY-NNN*, where:

- X is the slot number. The slot numbers assigned to your MAX vary depending on which model you are using. In all cases, the system itself is assigned slot number 0 (00-000). For specific slot assignments, see the *Hardware Installation and Basic Configuration Guide* for your MAX.
- *Y* is the port number. Zero means any port on the slot.
- The three digits after the dash are the root number. A root number of 000 identifies a top-level branch of the menu tree. If *N* is not zero, the root number identifies a submenu.

Example: `Edit=00-000`

Location: System > Sys Config

Edit All Calls

Description: Enables or disables permission to edit all the parameters in all call profiles and Connection profiles. When the permission is disabled, the user is restricted to editing only the Dial # and Base Ch Count parameters in the current call profile. The user can access the profiles via Telnet, by local management, or by remote management.

Note: To restrict editing entirely, you must also set the Edit Cur Call parameter to disable that permission.

Usage: Specify Yes or No. Yes is the default.

- Yes specifies the user can edit all parameters in call and Connection profiles.
- No specifies the user can edit only the Dial # and Base Ch Count parameters in the current call profile.

Dependencies: This parameter does not apply if the Operations parameter disables the operations permission.

Location: System > Security

See Also: Edit Com Call, Edit Cur Call, Edit Own Call

Edit All Ports

Description: Enables or disables permission to edit all Port Config profiles. When the permission is disabled, the user is restricted to editing only the current Port Config profile. The user can access the profiles via Telnet, by local management, or by remote management.

Note: To restrict editing of Port Config profiles entirely, you must also set the Edit Own Port parameter to disable that permission.

Usage: Specify Yes or No. Yes is the default.

Yes specifies that the user can edit all parameters in call and Port Config profiles.

No specifies the user can edit only the current Port Config profile.

Dependencies: This parameter does not apply if the Operations permission is disabled.

Location: System > Security

See Also: Edit Own Port

Edit Com Call

Description: Specifies whether a user can edit call profiles that are not specific to any AIM port. These profiles are known as common call profiles. Numbers 201 through 216 denote port-specific call profiles. Numbers 217 through 232 denote common call profiles. The user can access the profiles via Telnet, by local management, or by remote management.

Note: To restrict editing common call profiles entirely, you must also set the Edit All Calls parameter to disable that permission.

Usage: Specify Yes or No. Yes is the default if Edit All Calls is set to No.

Yes specifies the user can edit call profiles that are not specific to any AIM port (common call profiles).

No disables this permission.

Dependencies: This parameter does not apply if the Operations parameter disables the operations permission or the Edit All Calls parameter is set to Yes.

Location: System > Security

See Also: Edit All Calls

Edit Cur Call

Description: Specifies whether a user can edit all the parameters in the current call profile. When the permission is disabled, the user is restricted to editing only the Dial # and Base Ch Count parameters in the current call profile. The user can access the profiles via Telnet, by local management, or by remote management.

Note: To restrict editing entirely, you must also set the Edit All Calls parameter to disable that permission.

Usage: Specify Yes or No. Yes is the default if Edit All Calls is set to No.

Yes specifies that the user can edit call profiles that are not specific to any AIM port (common call profiles).

No disables this permission.

Dependencies: This parameter does not apply if the Operations permission is disabled or the Edit All Calls parameter is set to Yes.

Location: System > Security

See Also: Edit All Calls

Edit Line

Description: Specifies whether a user can edit Line profiles. The user can access the profiles via Telnet, by local management, or by remote management.

Usage: Specify Yes or No. No is the default.

Yes specifies the user can edit all Line *N* profiles.

No specifies the user can edit only the current Line *N* profile.

Dependencies: This parameter does not apply if the Operations parameter disables the operations permission.

Location: System > Security

Edit Own Call

Description: Specifies whether a user can edit the call profile for the port that has been called. The user can access the profiles via Telnet, by local management, or by remote management.

Note: To restrict editing entirely, you must also set the Edit All Calls parameter to disable that permission.

Usage: Specify Yes or No. Yes is the default if Edit All Calls is set to No.

- Yes specifies the user can edit the call profile for the port that has been called.
- No disables this permission.

Dependencies: This parameter does not apply if the Operations parameter disables the operations permission or the Edit All Calls parameter is set to Yes.

Location: System > Security

See Also: Edit All Calls

Edit Own Port

Description: Enables or disables permission to edit the Port Config profile for the port that has been called.

Note: To restrict editing of Port profiles entirely, you must also disable Edit All Port.

Usage: Specify Yes or No. Yes is the default if Edit All Ports is set to No.

Yes specifies the user can edit the Port Config profile for the port that has been called.

No disables this permission.

Dependencies: This parameter does not apply if the Operations parameter disables the operations permission or the Edit All Ports parameter is set to Yes.

Location: System > Security

See Also: Edit All Ports

Edit Security

Description: Enables or disables permission to edit Security profiles.

Note: Do not set the Edit Security parameter to No in all Security profiles. If you do, you will be unable to edit any of them. This parameter is the most powerful security permission, because it gives the user the ability to modify his or her own permissions.

Usage: Specify Yes or No. Yes is the default.

Yes specifies the user can edit Security profiles.

No specifies the user cannot edit Security profiles.

Dependencies: This parameter does not apply if the Operations parameter disables the operations permission.

Location: System > Security

Edit System

Description: Enables or disables permission to edit the System profile and the Read Comm and R/W Comm parameters in the Ethernet > Mod Config > SNMP Options profile.

Usage: Specify Yes or No. Yes is the default.

Yes specifies the user can edit the System profile and SNMP community strings.

No disables this permission.

Dependencies: This parameter does not apply if the Operations parameter disables the operations permission.

Location: System > Security

Enable

Description: Specifies whether or not the Security profile allows SNMPv3 USM read/write access.

Usage: Specify Yes or No. No is the default.

Example: `Enable=No`

Location: System > Security > *any Security profile* > Snmpv3 USM Options

See Also: Auth Protocol, Message Type, Priv Protocol, R/W Enable, Security Level

Enable ASBR

Description: Specifies whether the MAX performs Autonomous System Boundary Router (ASBR) calculations.

ASBRs perform calculations related to external routes. Typically, when the MAX imports external routes from RIP (for example, when it establishes a WAN link with a caller that does not support OSPF), it performs the ASBR calculations for those routes. However, you can set the Enable ASBR parameter to No to prevent the MAX from performing ASBR calculations and advertising ASE entries.

Usage: Specify Yes or No. The default is Yes.

Yes specifies that the MAX performs ASBR calculations.

No specifies that the MAX does not perform ASBR calculations.

Example: `Enable ASBR=Yes`

Dependencies: This parameter applies only if the MAX supports OSPF routing.

Location: Ethernet > Mod Config > OSPF Global Options

Enabled

Description: Enables or disables an ISDN BRI line.

Usage: Specify Yes or No. Yes is the default.

Yes enables the line for use.

No specifies that the line is not available for use.

Location: Net/BRI > Line Config > Line *N*, BRI/LT > Line Config > Line *N*, Host/BRI > Line Config > Line *N*

Enable Local DNS Table

Description: Enables the use of a local DNS table that can provide a list of IP addresses for a specific host when the remote DNS server fails to resolve the hostname successfully. The local DNS table provides the list of IP addresses only if the hostname for the attempted connection matches a hostname in the local DNS table.

Usage: Set Enable Local DNS Table to Yes to enable the local DNS table. No disables the feature. No is the default.

Location: Ethernet > Mod Config > DNS

See Also: The *`dnstab entry`* terminal command.

Encaps

Description: Specifies the encapsulation method to use when exchanging data with a remote network. Both sides of the link must use the same encapsulation for the connection to be established.

Note: When you specify an encapsulation method, the Encaps Options subprofile displays a group of parameters relevant to your selection; you must set the appropriate parameters in the subprofile.

Usage: Specify one of the following values:

- PPP (Point-to-Point Protocol) for standard PPP
- MP (Multilink PPP) for fixed-bandwidth multilink PPP
- MPP (Multilink Protocol Plus) for PPP with Lucent extensions for dynamic bandwidth allocation. This setting applies only to multichannel links between two Lucent INS units.
- COMB (Combinet) for links to a Combinet bridge
- FR (Frame Relay)
- FR_CIR (Frame relay circuit)
- TCP-CLEAR (raw TCP using a proprietary encapsulation)
- ARA (AppleTalk Remote Access client dialins)
- X.25/PAD (X.25 connections to the PAD interface)
- X.25/IP (IP network connection over X.25)

Example: `Encaps=MPP`

Dependencies: The encapsulation type must be enabled in the Answer profile.

Location: Ethernet > Connections > *Connection profile*

See Also: MPP, MP, PPP, COMB, FR, X25/PAD, V.120, TCP-CLEAR, ARA, X25/IP

Encaps Type

Description: Specifies which encapsulation to use when calling the remote IP network across X.25. When receiving a call, the MAX will accept any of the three encapsulation types.

Usage: Specify one of the following values:

- RFC877 (the default) for backward compatibility.
- SNAP.
- NULL (multiplexing). Only the IP NLPID (0xCC) is supported in the NULL encapsulation.

Example: `Encaps Type=RFC877`

Dependencies: This parameter applies only to X.25/IP connections.

Location: Ethernet > Connections > *Connection profile* > Encaps Options

See Also: Encaps

Encoding

Description: Specifies the type of T1 PRI line encoding that the MAX unit uses. Your carrier can tell you which type of encoding your unit requires.

Usage: Specify one of the following values:

AMI (the default)—The MAX uses Alternate Mark Inversion encoding.

None— Identical to AMI, but without density enforcement.

B8ZS—The encoding is Bipolar with 8-Zero Substitution. This setting is often required for ISDN lines.

Example: `Encoding=AMI`

Dependencies: This parameter applies only to T1 lines.

Location: Net/T1 > Line Config > Line *N*

End Of Packet Pattern

Description: Defines a character pattern that signals the end of a packet. When the pattern matches the buffered data, the system immediately flushes the buffer by writing all data, up to and including the pattern, into TCP packets.

Usage: Specify up to 64 characters. The default is null. You can enter both ASCII characters and binary data, using the backslash (\) as an escape mechanism. For example:

- To insert a literal backslash in the pattern, enter two backslash characters (\\).
- To insert a 1- to 3-digit octal number, use a single backslash. (To avoid confusion between the literal ASCII characters 1 through 7 and an octal value, you can pad the octal value with leading zeroes.) For example, the pattern `\015` represents a carriage return (octal 15).
- To insert a 1- or 2-digit hexadecimal number in the pattern, precede the number with the pattern `\x`. For example, the pattern `\x0D` represents a carriage return (hex 0D).

Following are other special escape sequences:

Escape Sequence	Description	Value
`\a`	Alarm	7
`\b`	Backspace	8
`\f`	Form feed	12
`\n`	New line	10
`\r`	Carriage return	13
`\t`	Tab	9
`\v`	Vertical tab	11
`\\`	Backslash	92
`\'`	Apostrophe	44
`\"`	Double quote	34
`\?`	Wildcard	Matches any single character

Example: `End of Packet Pattern=\015`

Dependencies: If Detect End of Packet=No, End of Packet Pattern does not apply.

Location: Ethernet > Answer > TCP-CLEAR Options, Ethernet > Connection > *any Connection profile* > Encaps Options

See Also: Detect End of Packet, Packet Flush Length, Packet Flush Time

Enet Adrs

Description: In a Bridge Adrs profile, specifies the physical Ethernet address (MAC address) of a device at the remote end of the link. The Bridge Adrs profile correlates a remote MAC address with a Connection profile number, enabling the MAX to bring up the connection configured in that profile when it receives packets destined for the remote device.

Usage: Specify the physical address of the device on the remote network. An Ethernet address is a 12-digit hexadecimal number. The default setting is 000000000000.

Example: `Enet Adrs=0180C2000000`

Location: Ethernet > Bridge Adrs

See Also: Net Adrs

ENQ Handling

Description: Specifies whether the PAD should expect to receive an ENQ from the host when an X.25 virtual call is established. ENQ indicates that the host is ready to receive data.

Usage: Specify one of the following values:

- Off (the default)—The PAD does not expect to receive an ENQ before sending data to the host. The host is ready to receive data as soon as the X25 call is established.
- On—The PAD does not forward data it receives from the DTE to the host until it either receives an ENQ or the T3 POS timer expires. Note that the PAD does not forward the ENQ to the DTE.

Dependencies: This parameter is always applicable.

Location: Ethernet > Connections > *Connection profile* > Encaps Options, Ethernet > Answer > T3POS Options

EOC Address

Description: Specifies the Embedded Operations Channel (EOC) address from which the MAX rolls back the signal.

Usage: Specify one of the following values:

- 0 (the default)—The remote ISDN TA device.
- 1-6—The number of an ISDN repeater between the MAX and the remote TA. A value of 1 specifies the repeater nearest the MAX.
- 7—The EOC command should be broadcast to all the nodes on the IDSL connection.

Note: The EOC address setting reverts to its default value of 0 whenever you exit the Line Diag subprofile.

Location: BRI/LT > Line Diag > Line *N*

EU-RAW

Description: Specifies whether the MAX accepts EU-RAW calls, provided that they meet all other X.75 criteria.

Usage: Specify Yes or No. Yes is the default.

Yes specifies the MAX accepts EU-RAW encapsulated calls, provided that they meet all other connection criteria.

No specifies the MAX will not accept inbound EU-RAW calls.

Location: Ethernet > Answer > Encaps

EU-UI

Description: Specifies whether the MAX accepts EU-UI calls, provided that they meet all other X.75 criteria.

Usage: Specify Yes or No. Yes is the default.

Yes specifies that the MAX accepts EU-UI encapsulated calls, provided that they meet all other connection criteria.

No specifies that the MAX will not accept inbound EU-UI calls.

Location: Ethernet > Answer > Encaps

Excl Routing

Description: Enables or disables exclusive port routing. Exclusive port routing is a way to prevent the MAX from accepting calls for which it has no explicit routing destination. If Excl Routing is disabled (the default), the call is routed to a digital modem if the bearer service is voice. If the service is V.110, the call is routed to the first available V.110 module. If the service is data, the call is routed to the first available AIM port. If no AIM ports are available, the call is routed to the MAX unit's bridge/router. To prevent this service-based routing and instead reject the call, enable Excl Routing.

Usage: Specify Yes or No. No is the default.

Yes specifies that the MAX drops calls for which it has no explicit call-routing information (such as answer numbers or ISDN subaddressing).

No specifies that the MAX uses service-based routing to route voice calls to a digital modem and data calls to an AIM port or its bridge/router software.

Note: With MAXPOTS functionality, the default for Excl Routing is Yes.

Example: `Excl Routing=No`

Location: System > Sys Config

Exp Callback

Description: Specifies whether the MAX expects outgoing calls to result in a callback from the far-end device. If the MAX expects callback, a 90-second waiting period is required before attempting to reestablish a call that is disconnected. Use this parameter when the remote device requires callback security.

Usage: Specify Yes or No. No is the default.

Yes specifies that the MAX expects the connection to terminate and result in a call-back from the far-end device. This setting prevents problems that arise when CLID is set to Required on the device that is expected to call back. However, if a call fails for any reason, regardless of whether or not the called machine requires CLID and is attempting a callback, the call initiator will still have to wait 90 seconds before attempting to call the same number again if Exp Callback is set to Yes.

No specifies that the MAX does not expect callback for this connection.

Example: `Exp Callback=No`

Location: Ethernet > Connections > *Connection profile* > Telco Options

See Also: Callback

Ext. Clock * 1K

Description: Defines the maximum bandwidth that the unit uses for the nailed portion of a nailed/MP+ call. The unit cannot determine the bandwidth for the serial WAN line if it does not generate clocking for its serial WAN line. The unit must know the bandwidth of the nailed line for a nailed/MP+ session to operate properly.

Usage: Specify a number from 1 to 10000 to indicate the externally-generated clocking speed. The MAX multiplies the number that you specify by 1024 (1K). The default is 56.

Example: `Ext. Clock * 1K=56`

Dependencies: Ext. Clock * 1K applies only if the MAX uses the serial WAN in nailed/ MP+ connections.

Location: Serial WAN > Mod Config

F

Fail Action

Description: Specifies the action that the MAX takes when it cannot establish the base channels of a codec connection.

Usage: Specify one of the following values:

- Disc—The MAX clears the call entirely.
- Reduce (the default)—The MAX reduces the bandwidth allocated for the call, and then tries to establish the call with a number of channels lower than the amount specified by Base Ch Count.
- Retry—The call remains online with the bandwidth available while the MAX attempts to add channels to bring the count up to the value specified by Base Ch Count. Retry attempts continue for approximately 30 seconds, until the MAX achieves full bandwidth, or until you reduce the setting of the Base Ch Count parameter. If the MAX cannot make the channel count match the setting of Base Ch Count within 30 seconds, the call remains online.

Example: `Fail Action=Retry`

Location: Host/Dual (Host/AIM6) > Port*N* Menu > Directory

FDL

Description: Specifies the Facilities Data Link (FDL) protocol that the MAX uses. FDL is a protocol used by the telephone company to monitor the quality and performance of T1 lines. It provides information at regular intervals to your carrier’s maintenance devices.

You continue to accumulate D4 and 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.

Usage: Specify one of the following values:

- None (the default)—Disables FDL signaling.
- AT&T—Specifies AT&T FDL signaling.
- ANSI—Specifies ANSI FDL signaling.
- Sprint—Specifies Sprint FDL signaling.

Dependencies: This parameter does not apply to D4-framed T1 lines.

Location: Net/T1 > Line Config > Line *N*

See Also: Framing Mode

Field Service

Description: Enables or disables permission to perform Lucent-provided field service operations, such as uploading new system software. Field service operations are special diagnostic routines not available through MAX menus.

Usage: Specify Yes or No. Yes is the default.

Yes specifies that the user can upgrade the system software and perform other field service operations.

No disables this permission.

Example: `Field Service=No`

Dependencies: This parameter is not applicable if the Operations parameter disables the operations permission.

Location: System > Security

Filter

Description: Specifies the number of a data filter that plugs into the Ethernet profile. The data filter manages data flow on the Ethernet interface. The filter examines each incoming or outgoing packet and uses the Forward parameter to determine whether to forward or discard the packet.

Usage: Specify a number from 0 to 199. The number you enter depends on whether you are applying a filter you created through the VT100 interface, or a firewall you created with SecureConnect Manager (SCM).

If you are applying a filter created through the VT100 interface, enter the last 2 digits of the filter number as it appears in the Filters menu.

If you are applying a firewall created with SCM, add 100 to the last 2 digits of the firewall number as it appears in the Firewalls menu. For example, if the number of your firewall is 90-

601, specify 101. For information about downloading firewalls to the MAX, see your SCM documentation. The numbering scheme for filters and firewalls is:

- 0 indicates that no filtering is being used (this is the default).
- 1-99 indicates that a filter created through the VT100 interface is being used.
- 100-199 indicates that a filter created with SCM is being used.

When you set Filter to 0 (zero), the MAX forwards all data packets.

Example: `Filter=7`

Location: Ethernet > Mod Config > Ether Options

See Also: Call Filter, Data Filter

Filter Persistence

Description: Specifies whether the filter or firewall assigned to a Connection profile or the Answer profile should persist after the call has been disconnected.

Before SecureConnect Firewall was supported, the MAX simply constructed a filter on a WAN interface when the connection was established and destroyed the filter when the connection was brought down, even if the connection just timed out momentarily. This works fine for static packet filters, but does not accommodate a firewall. Filter persistence is needed to allow firewalls to persist across connection state changes, but it is not needed for filters. If you do set Filter Persistence for a static packet filter, the filter persists across connection state changes. For details, see the *MAX Security Supplement*.

Note: Firewalls must have persistence to work correctly, but filters do not.

Usage: Specify Yes or No. No is the default.

- Yes causes the filter or firewall to persist across connection state changes. This is not required for a data or call filter, but it is required for firewalls.
- No causes the filter or firewall to be torn down when a connection is brought down.

Example: `Filter Persistence=Yes`

Location: Ethernet > Answer > Session Options, Ethernet > Connections > *Connection profile* > Session Options

See Also: Call Filter, Data Filter, Name, Version, Length

Finger

Description: Enables or disables the Finger remote user information protocol (RFC 1288). Finger returns information about users currently logged in to the MAX. Note that for security reasons the MAX does not forward Finger requests.

Usage: Specify one of the following values:

Yes enables the MAX to respond to Finger requests.

No disables the Finger protocol on the MAX.

Location: Ethernet > Mod Config

First Retry Timer

Description: Specifies, in milliseconds, the initial interval the MAX unit waits before it resends an unacknowledged L2TP control message. Any change you make to this parameter is reflected as soon as the previous timer expires.

Usage: Enter a decimal number from 100 to 5000. The default is 1000.

Example: `First Retry Timer (ms)=1000`

Dependencies: First Retry Timer applies only if you have set L2TP Mode to LAC, LNS, or Both.

Location: Ethernet>Mod Config>L2 Tunneling Options

See Also: CC Establish Timer, Hello Timer, L2TP Mode, LAC In Call Timer, LNS In Call Timer, Retry Count

Fixed Packets

Description: The Fixed Packets parameter causes the MAX to enable the pre-9.0 fax packet scheme for real-time fax processing. When enabled, fax calls are processed using variable length packets that are zero terminated and allow class1 modems to underrun gracefully.

Usage: Press [Enter] to toggle the value for Fixed Packets between `yes`, enabling the pre-9.0 fax packet scheme, and `no`, enabling jitter buffering and packet redundancy for real-time fax processing. Press [Esc] to exit the profile, then write the changes to this profile.

Example: `Fixed Packets =2`

Dependencies: The following dependencies apply to this parameter:

- Once saved, the selected packeting scheme is enabled with the next fax call.
- When this value is set to `yes`, then `Packet Redundancy=N/A`.

Location: Ethernet > Mod Config > RT Fax Options

Flag Idle

Description: Specifies which bit pattern a dynamic call to an AIM port uses as the idle indicator: a flag pattern (01111110) or a mark pattern (11111111). Both patterns include enough 1 bits to maintain clock sychronization with the remote unit. Both ends must use the same pattern. Receipt of the specified pattern indicates to the local unit that the remote unit is not sending data.

Usage: Specify Yes or No. Yes is the default.

Yes specifies that the MAX uses a flag pattern (01111110) as the idle indicator on an AIM dynamic call.

No specifies that the MAX uses a mark pattern (11111111) as the idle indicator on an AIM dynamic call.

Example: `Flag Idle=Yes`

Location: Host/Dual (Host/AIM6) > Port*N* Menu > Directory

Force 56

Description: Specifies whether the MAX uses only the 56 Kbps portion of a channel, even when all 64 Kbps appear to be available.

Use this parameter when you receive calls from European or Pacific Rim countries and the complete path cannot distinguish between the Switched-56 and Switched-64 data services. This parameter is not required if you are receiving calls only from North America.

Note: The MAX uses the value specified by Force 56 in a Connection profile only if the call authenticates by means of CLID/DNIS. The MAX uses the value specified by Force 56 in the Answer profile if a call authenticates by means of name and password, or if a call is unauthenticated.

Usage: Specify Yes or No. No is the default.

Yes specifies that the MAX uses 56K of a channel that can provide up to 64K bandwidth.

No specifies that the MAX uses the full 64K bandwidth if it is available.

Dependencies: This parameter should not be enabled for calls within North America.

Example: `Force 56=No`

Location: Host/Dual (Host/AIM6) > Port*N* Menu > Directory, Ethernet > Connections > *Connection profile* > Telco Options, Ethernet > Answer

Forward

Description: Specifies whether the MAX discards or forwards packets that match the filter specification. When no filters are in use, the MAX forwards all packets by default. When a filter is in use, the default is to discard matching packets (Forward=No).

Usage: Specify Yes or No. No is the default.

- Yes specifies that the MAX forwards packets that match the filter.
- No specifies that the MAX discards packets that match the filter.

Example: `Forward=No`

Location: Ethernet > Filters > Input Filters > In filter *N* > IP, Ethernet > Filters > Output Filters > Out Filter *N* > IP

See Also: Call Filter, Data Filter, Filter, More

Forward Directed Bcast

Description: Specifies whether the MAX responds to directed-broadcast ICMP echo requests.

Usage: Specify Yes or No.

Yes specifies that the MAX responds to directed broadcast ICMP echo requests.Yes is the default.

No specifies that the MAX does not respond to directed broadcast ICMP echo requests.

Dependencies: Forward Directed Bcast applies only if the MAX supports IP routing.

Location: Ethernet > Mod Config

See Also: Reply DirectedBcast Pin

Forward Disc

Description: Specifies whether a far-end disconnect is forwarded.

Usage: Specify Yes or No. The default is No.

- Yes—Forwards the far-end disconnect indication. This allows locally connected equipment, such as faxes and answering machines, to notice that the connection has been terminated.

  Note: During forward disconnect, the MAX opens the analog loop for approximately 1 second if you set Signaling to Loopstart. If you set Signaling to Groundstart, the MAX unit opens the loop (onhook) and remains so until the next call.
- No—Disables forward disconnect.

Location: Analog FXS > FXS Config > *FXS Configuration profile* > Line *N*

Forwarding

Description: Enables multicast forwarding in the MAX.

Note: When you change the Forwarding parameter from No to Yes, the multicast subsystem reads the values in the Ethernet > Mod Config > Multicast profile and initiates the forwarding function. If you modify a multicast value in the Ethernet > Mod Config > Multicast profile, you must set this parameter to No and then set it to Yes again to force a read of the new value.

Usage: Specify Yes or No. No is the default.

Yes turns on multicast forwarding in the MAX.

No disables multicast forwarding.

Example: `Forwarding=Yes`

Location: Ethernet > Mod Config > Multicast

See Also: Mbone Profile, Multicast Client

FR

Description: Specifies whether the MAX accepts incoming Frame Relay-encapsulated calls.

Usage: Specify Yes or No. Yes is the default.

Yes specifies that the MAX accepts calls that use Frame Relay encapsulation, provided that they meet all other connection criteria.

No specifies that the MAX does not accept inbound calls using Frame Relay encapsulation.

Location: Ethernet > Answer > Encaps

See Also: Encaps, FR Prof, DLCI

Framing Mode

Description: Specifies the framing mode in use on the physical links of a T1, E1, or DS3 line. Your carrier can tell you which framing mode to choose.

Usage: For a T1 or E1 line, specify one of the following values:

- D4—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—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).

An E1 line supports the following additional Framing Mode values:

- G703—The trunk interface uses CRC-4.
- 2DS—The trunk interface does not use CRC-4.

A DS3 line supports only the following Framing Mode values:

- M13—An M23 application.
- C-Bit-Parity—A C-bit parity application.

Example: `set framing mode=esf`

Location: Net/E1 > Line Config > *Line N profile* > Line *N*

FR Direct

Description: Specifies whether the MAX redirects incoming packets to the Frame Relay switch without processing. An FR Direct connection is a dial-in IP routing connection (typically using PPP), for which the MAX simply forwards the packets automatically to the Frame Relay switch without examining destination addresses or its routing table. In effect, the MAX passes on the responsibility of routing those packets to a later hop on the Frame Relay network. This is known as FR Direct mode, and is not commonly used.

Note: An FR Direct connection is not a full-duplex tunnel between the PPP dial-in and the switch. The IP packets coming back from the Frame Relay switch are handled by the MAX router software, so to be routed correctly back across the WAN, they must contain the PPP caller's IP address.

Usage: Specify Yes or No. No is the default.

Yes specifies that this connection is an FR Direct connection.

No specifies that this is not an FR Direct connection.

Example: `FR Direct=No`

Dependencies: This parameter is not applicable for FR or FR_CIR encapsulated calls.

Location: Ethernet > Connections > *Connection profile* > Session Options

See Also: FR DLCI, FR Prof

FR DLCI

Description: Specifies a Frame Relay DLCI number to be used for FR Direct connections. An FR Direct connection is a dial-in IP routing connection (typically using PPP), for which the MAX simply forwards the packets automatically to the Frame Relay switch without examining destination addresses or its routing table. In effect, the MAX passes on the responsibility of routing those packets to a later hop on the Frame Relay network. This is known as FR Direct mode, and is not commonly used.

Note: More than one FR Direct PPP connection can share a Frame Relay DLCI number.

Usage: Specify the DLCI obtained from the Frame Relay administrator for FR Direct links.

Example: `FR DLCI=72`

Dependencies: This parameter is not applicable if Frame Relay encapsulation is in use.

Location: Ethernet > Connections > *Connection profile* > Session Options

See Also: FR Direct

FR Prof

Description: Specifies the name of the Frame Relay profile to use for forwarding this link on the Frame Relay network.

Usage: Specify the name of a configured Frame Relay profile. This is the string assigned in the Name parameter of the Frame Relay profile, specified exactly including case changes.

Example: `FR Prof=pacbell`

Location: Ethernet > Connections > *Connection profile* > Encaps Options, Ethernet > Connections > *Connection profile* > Session Options

See Also: FR Type, DLCI

FR Type

Description: Specifies the type of interface between the MAX and a Frame Relay switch or CPE (customer premises equipment) on the Frame Relay network.

Note: For NNI or UNI-DTE connections, the MAX is able to query the device at the other end of the link about the status of the DLCIs in the connection. If any of the DLCIs become

unusable and the DLCIs Connection profile has a specified Backup connection, the MAX dials the Connection profile specified in the Backup parameter in the Session Options submenu.

Usage: Specify one of the following values:

- NNI (Network to network interface)
  An NNI interface connection allows the MAX to appear as a Frame Relay network interface based on the NNI specifications. It performs both DTE and DCE link management, and allows two separate Frame Relay networks to connect via a common protocol.
- UNI-DCE (User to network interface—data communications equipment)
  UNI is the interface between an end-user and a network end point (a router or a switch) on the Frame Relay network. In a UNI-DCE connection, the MAX operates as a Frame Relay router communicating with a CPE device (customer premises equipment). To the DTE devices, it appears as a Frame Relay network end point.
- UNI-DTE (User to network interface—data terminal equipment)
  In a UNI-DTE connection, the MAX is configured as a UNI-DTE communicating with a Frame Relay switch. It acts as a Frame Relay *feeder* and performs the DTE functions specified for link management.

Example: `FR Type=NNI`

Location: Ethernet > Frame Relay

See Also: LinkUp, FR Prof, DLCI, Circuit

Frame Length

Description: Specifies the maximum number of bytes allowed in the information field by V.120 or X.75 terminal adapters that call the MAX.

Usage: For a V.120 TA, specify a number from 30 to 260. The default is 256. For an X.75 TA, specify a number from 128 to 1532. The default value is 1024.

Example: `Frame Length=256`

Location: Ethernet > Answer > V.120 Options, Ethernet > Answer > X.75 Options

See Also: K Window Size, N2 Retran Count, T1 Retran Timer, X.75

Framed Only

Description: Specifies whether the user is allowed access to all the terminal-server commands or to a subset of them.

Usage: Specify one of the following values:

- No (the default)—Terminal-server users connecting through this profile have unlimited access to the terminal server commands.
- Yes—Terminal-server users connecting through this profile have access only to the PPP, SLIP, CSLIP, and Quit terminal-server commands.

Dependencies: Keep the following additional information in mind:

- Framed Only has no affect if TS Enabled is set to No in the Ethernet > Mod Config > TServ Options subprofile.
- PPP, SLIP, and CSLIP must be enabled in the Ethernet > Mod Config > TServ Options subprofile before users can start a PPP, SLIP, or CSLIP session.

Location: Ethernet > Answer > Session Options, Ethernet > Connections > *Connection profile* > Session Options

Framed Addr Start

Description: Specifies whether the MAX sends a second accounting Start record to the RADIUS server when the Framed-Address and Framed-Protocol attributes are assigned to a user transferring to a framed protocol (such as PPP or SLIP).

Usage: You can specify Yes or No. No is the default.

Yes specifies that the MAX sends a second accounting Start record.

No specifies that the MAX does not send a second accounting Start record.

Location: Ethernet > Mod Config > Auth

Frames/Packet

Description: Specifies the number of voice frames that a MultiVoice Gateway inserts into each IP packet. Lowering the number reduces the delay and distortion introduced into any given voice call. But a lower number can also degrade performance, because it results in more IP packets per voice call.

Usage: Specify a number from 1 to 10. The default is 4.

Dependencies: Frames/Packet applies only if you set Ethernet > VOIP Options > Pkt Audio Mode to G.729.

Location: Ethernet > VOIP Options

See Also: Pkt Audio Mode

Framing Mode

Description: Specifies the framing mode the T1 or E1 physical layer uses. Your carrier can tell you which framing mode to choose.

Note: If the MAX has internal bantam test jacks, it can support a different framing mode for each line in a Drop-and-Insert application. If you set the second line to Drop-and-Insert and use Inband signaling, you can set Framing Mode to ESF on one line and to D4 on the other.

Usage: Specify one of the following values for a Net/T1 line:

- D4 —The D4 format, also known as the Superframe format, which consists of 12 consecutive frames, separated by framing bits. Do not use this setting with ISDN D-channel signaling. Doing so can result in false framing and Yellow Alarm emulation.

- ESF—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.

For a Net/E1 line, specify one of the following values:

- G.703 (the default)—The standard framing mode used by most E1 ISDN providers and by DASS 2.
- 2DS—A variant of G.703 required by most E1 DPNSS providers in the U.K.

Location: Net/T1 > Line Config > Line *N*, Net/E1 > Line Config > Line N

Front End

Description: Specifies the type of front end used on a MAX 3000 or MAX 6000 T1/PRI port. Specify CSU if you plan to use the MAX unit's internal CSU. Specify DSX if you plan to connect the port to other equipment that provides the interface to the WAN, for example, an external CSU, and disable the internal CSU.

Usage: Specify CSU or DSX for each port. CSU is the default.

CSU enables the internal CSU.

DSX disables the internal CSU.

Example: `Front End=DSX`

Location: Net/T1 > Line Config > *Line Config profile*> Line *N* > Front End, Net1/E1 > Line Config > *Line Config profile*> Line *N* > Front End

FT1 Caller

Description: Specifies whether the MAX 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. By the same token, if the remote end has FT1 Caller set to Yes, set it to No on the local MAX.

Usage: Specify Yes or No. No is the default.

Yes specifies that the MAX can initiate FT1-AIM, FT1-B&O, or Nailed/MPP calls on the connection configured in this Connection profile.

No specifies that the MAX cannot initiate these calls. No implies that the other end of the connection will always initiate the call.

Dependencies: This parameter applies only when the call type is FT1-AIM or FT1-B&O (in a Port*N* Menu profile) or Nailed/MPP (in a Connection profile). It should be set to Yes at only one side of the connection.

Location: Host/Dual (Host/AIM6) > Port*N* Menu > Directory, Ethernet > Connections > *Connection profile* > Telco Options

See Also: Call Type

G

Gateway

Description: Specifies the IP address of the next-hop router that a packet must go through to reach the route's destination address. A next-hop router is either directly connected (is on the Ethernet network) or is one hop away on a WAN link.

Usage: Specify the IP address of the next-hop router.

Example: `Gateway=200.207.23.1`

Dependencies: This parameter does not apply if the MAX does not support IP routing.

Location: Ethernet > Static Rtes

See Also: Dest

GK IP Adrs

Description: Specifies the IP address of the MultiVoice Access Manager. When the MAX, acting as a MultiVoice Gateway, receives voice calls, the MultiVoice Access Manager directs the MultiVoice Gateway in routing the call to a destination MultiVoice Gateway.

Usage: Specify the IP address of the MultiVoice Access Manager.

Example: `GK IP Adrs=10.10.10.1/24`

Dependencies: GK IP Adrs does not apply if the MAX does not support IP routing or does not act as a MultiVoice Gateway.

Location: Ethernet > Mod Config > VOIP Options

See Also: VPN Mode, Pkt Audio Mode

GK MLG Control

Description: Enables the MultiVoice gateway to accept and process call-specific administration instructions from a MultiVoice Access Manager, Release 3.0. When enabled, the gateway may apply call-specific processing instructions, for PIN authentication, single- or two-stage dialing, voice announcement playback, and configuring call timers for pre-paid billing. Values received from MVAM, or a third party billing system, will override parameter settings in the VOIP Options profile for processing the current VoIP call.

Rules used for performing call-specific administration are configured on MVAM, and are used when partitioning MultiVoice gateways into multiple logical gateways. This allows MVAM to administer a single physical gateway as if it were multiple gateways, partitioning the gateway according to trunk groups, DNIS, time of day, and so on.

Usage: This feature is enabled or disabled by pressing [Enter], toggling the value between `Yes`, enabling processing of call-specific administration instructions, and `No` (default), reverting to global administration of VoIP calls using the values set in the VOIP Options

profile. Once the desired value is selected, press [Esc] to exit the VOIP Options profile, then save the change.

Example: `GK MLG Control=Yes`

Dependencies: This parameter has the following dependencies:

- If `GK MLG Control=Yes`, the value of VPN Mode defaults to `N/A`.
- If `GK MLG Control=Yes`, the value of Single Dial Enable defaults to `N/A`.
- Changes to this parameter are effective with the next VoIP call.

Location: Ethernet>Mod Config> VOIP Options

GndStart Ring

Description: Specifies whether ringing voltage will be applied to the ground start line. Ringing in ground start is normally done by grounding the tip lead. A ringing voltage is usually not applied because it can confuse some ground start equipment. However, some key systems require this ringing voltage in addition to tip grounding.

Usage: Specify Yes or No. The default is No.

Dependencies: This parameter applies to each line uniquely and only when the Signaling parameter is set to Groundstart.

Location: Analog FXS > FXS Config > *FXS Configuration profile* > Line *N*

See Also: Signaling

Grp B Collect Signal

Description: Brazilian ISPs have the option of accepting or denying collect calls.

Usage: Specify one of the following values:

B-2—Indicates a busy line.

B-5—Indicates a line for which there is no fee.

B-7—Indicates a number that is not accessible or that a call will be forwarded to an answering machine. This value also indicates that the line does not accept collect calls.

Example: `Grp B Collect Signal=B7`

Dependencies: If Sig Mode is set to any value other than Brazil, then Grp B Collect Signal is NA.

Location: Net/E1 > Line Config > Line *N* profile

See Also: Sig Mode, Grp B No Match Signal

Group

Description: Assigns a group of nailed channels to a connection. For connections whose call type is Nailed/MPP, you can concatenate group numbers by separating them with a comma (for example, Group=1,3,5,7 assigns four groups of nailed channels.)

Note: Nailed channels are used for permanent connections, which are typically leased. It is important to keep those channels dedicated to the connection. Do not assign the same group number to more than one profile of any type.

Usage: Specify the group number assigned to nailed channels in a Line *N* profile.

Example: `Group=3`

Location: Host/Dual (Host/AIM6) > Port*N* Menu > Directory, Ethernet > Connections > *Connection profile* > Telco Options

See Also: Call Type, Ch *N* Prt/Grp, Ch *N*

Grp B Answer Signal

Description: Specifies the group B signal that the MAX sends immediately before answering an incoming call.

Usage: Specify Signal B 1, Signal B 2, and so on, up to Signal B 15. The default is Signal B 6, which is the recommended setting for E1 R2 Israeli signaling. The relevant specifications for E1 R2 Israeli signaling are in ITU-T recommendations Q.400 to Q.490 and Israeli MFC R2 Register Signaling documentation.

Systems in Mexico and Korea should set Group B Answer Signal to Signal B 1. Systems in Argentina should use Signal B 6 (the default). For information about the proper settings for other countries, please contact your carrier.

Location: Net/E1 Line Config > *Line Config profile* > Line *N* profile

See Also: Group II Signal, Group B Busy Signal

Grp B Busy Signal

Description: Specifies the group B signal that the MAX sends as a busy signal.

Usage: Specify Signal B 1, Signal B 2, and so on, up to Signal B 15. The default is Signal B 3, which is the recommended setting for E1 R2 Israeli signaling. The relevant specifications for E1 R2 Israeli signaling are in ITU-T recommendations Q.400 to Q.490 and Israeli MFC R2 Register Signaling documentation. For information about the proper settings for other countries, please contact your carrier.

Location: Net/E1 Line Config > *Line Config profile* > Line *N* profile

See Also: Group II Signal, Group B Answer Signal

Grp II Signal

Description: Specifies the group II signal, which the MAX sends on an outgoing call immediately after the called end acknowledges that it has received all the necessary address digits.

Usage: Specify Signal II 1, Signal II 2, and so on, up to Signal II 15. The default is Signal II 2. Systems in Mexico and Korea should use the default. Systems in Argentina should set Group II Signal to Signal II 1. For information about the proper settings for other countries, please contact your carrier.

Location: Net/E1 Line Config > *Line Config profile* > Line *N* profile

See Also: Group B Answer Signal, Group B Busy Signal

GRP Leave Delay

Description: Specifies the number of seconds the MAX waits before forwarding any IGMP, version 2, `leave group` message from any multicast client. If you specify a value other than 0, and the MAX receives a `leave group` message, the MAX sends an IGMP query to the WAN interface from which it received the `leave group` message. If the MAX unit does not receive a response on the WAN interface from an active multicast client that belongs to the same group from which the `leave group` message was received, the unit sends a `leave group` message when the time you specified for the GRP Leave Delay parameter has expired.

If you specify the default value of zero, the MAX forwards any `leave group` message immediately. If users might establish multiple multicast sessions for identical groups, you should set GRP Leave Delay to a value from 10 to 20 seconds.

Usage: Press Enter to open the text field. Then specify a number of seconds from 0 to 120. The default is 0.

`Example:` `GRP Leave Delay=15`

Dependencies: This parameter applies only if you set Forwarding to Yes and Multicast Client to Yes.

Location: Ethernet > Mod Config > Multicast

See Also: Forwarding, Multicast Client

H

Handle IPX

Description: Specifies IPX server or IPX client bridging.

Note: If NetWare servers are supported on both sides of the WAN connection, Lucent strongly recommends that you use an IPX routing configuration instead of bridging IPX. If you bridge IPX in that type of environment, client-server logins will be lost when the MAX brings down an inactive WAN connection.

Usage: Specify one of the following values:

- None (the default)—Disables IPX server or IPX client bridging.
- Client (for IPX client bridging)—IPX client bridging is used when the local Ethernet network supports NetWare clients but no servers. In an IPX client bridging configuration, you want the local clients to be able to bring up the WAN connection by querying (broadcasting) for a NetWare server on a remote network. You also want to filter IPX RIP and SAP updates, so the connections do not remain up permanently.
- Server (for IPX server bridging)—IPX server bridging is used when the local Ethernet network supports NetWare servers (or a combination of clients and servers) and the remote network supports NetWare clients only.

Example: `Handle IPX=Client`

Dependencies: This parameter does not apply if IPX routing is enabled for this connection.

Location: Ethernet > Connections > *Connection profile* > IPX Options

See Also: Dial Brdcast, NetWare VC

Handle IPX Type 20

Description: Specifies whether the MAX will propagate IPX VC Type-20 packets over all its interfaces. Some applications, such as NETBIOS, use IPX Type -0 packets to broadcast names over a network. By default, these broadcasts are not propagated over routed links, since Novell recommends not forwarding these packets over links that have less than 1 Mbps throughput. However, some applications, such as NetBIOS over IPX, require IPX Type-20 packets in order to work.

Usage: Specify Yes or No. No is the default.

Yes enables the MAX to propagate IPX Type-20 packets.

No specifies that IPX VC Type-20 packets are not propagated.

Dependencies: This parameter does not apply if the MAX does not support IPX routing.

Location: Ethernet > Mod Config > Ether VC options

HeartBeat Addr

Description: Specifies a multicast address. To perform heartbeat monitoring, the MAX unit listens for packets to and from the group that uses this address. When the unit is running as a multicast forwarder, it is continually receiving multicast traffic. The heartbeat-monitoring feature enables you to monitor possible connectivity problems by continuously polling for this traffic and generating an SNMP alarm trap if there is a traffic breakdown.

Note: All the HeartBeat parameters interact to enable heartbeat monitoring. Heartbeat monitoring is an optional function. It is not required for multicast forwarding.

Usage: Specify a multicast address to use for heartbeat monitoring.

Example: `HeartBeat Addr=224.1.1.1`

Location: Ethernet > Mod Config > Multicast

See Also: HeartBeat Udp Port, Source Addr, Source Mask, HeartBeat Slot Time, HeartBeat Slot Count, Alarm Threshold

HeartBeat Udp Port

Description: Specifies a UDP port number. To perform heartbeat monitoring, the MAX unit listens only to packets received on that port. When the unit is running as a multicast forwarder, it is continually receiving multicast traffic. The heartbeat-monitoring feature enables you to monitor possible connectivity problems by continuously polling for this traffic and generating an SNMP alarm trap if there is a traffic breakdown.

Note: All the HeartBeat parameters interact to enable heartbeat monitoring. Heartbeat monitoring is an optional function. It is not required for multicast forwarding.

Usage: Specify a UDP port to use for heartbeat monitoring.

Example: `HeartBeat Udp Port=16387`

Location: Ethernet > Mod Config > Multicast

See Also: HeartBeat Addr, Source Addr, Source Mask, HeartBeat Slot Time, HeartBeat Slot Count, Alarm Threshold

HeartBeat Slot Count

Description: Specifies how many times to poll for multicast traffic before comparing the number of heartbeat packets received to the value specified for Alarm Threshold. The MAX polls for multicast traffic the specified number of times, waits for the interval specified by the HeartBeat Slot Time parameter, and then polls again.

Note: All the HeartBeat parameters interact to enable heartbeat monitoring. Heartbeat monitoring is an optional function. It is not required for multicast forwarding.

Usage: Specify a number of seconds.

Example: `HeartBeat Slot Count=10`

Location: Ethernet > Mod Config > Multicast

See Also: HeartBeat Addr, Heartbeat Udp Port, Source Addr, Source Mask, HeartBeat Slot Time, Alarm Threshold

HeartBeat Slot Time

Description: Specifies how often (in seconds) the MAX should poll for multicast traffic. The MAX polls for multicast traffic, waits for this interval, and then polls again.

Note: All the HeartBeat parameters interact to enable heartbeat monitoring. Heartbeat monitoring is an optional function. It is not required for multicast forwarding.

Usage: Specify a number of seconds.

Example: `HeartBeat Slot Time=10`

Location: Ethernet > Mod Config > Multicast

See Also: HeartBeat Addr, Heartbeat Udp Port, Source Addr, Source Mask, HeartBeat Slot Count, Alarm Threshold

HelloInterval

Description: Specifies the number of seconds between sending OSPF Hello packets on the interface. OSPF routers use Hello packets to recognize when a router is down.

Usage: Specify a number. In a Connection profile, the default is 40 seconds. In the Ethernet > Mod Config profile, the default is 10 seconds.

Example: `HelloInterval=60`

Location: Ethernet > Connections > *Connection profile* > OSPF Options, Ethernet > Mod Config > OSPF Options

See Also: DeadInterval

Hello Timer

Description: Specifies the interval, in seconds, that an L2TP control connection must be idle before the MAX unit sends an L2TP Hello control message. Any change you make to the setting of this parameter is reflected as soon as the previous timer expires.

Usage: Specify a decimal number from 0 to 600. The default is 60. A value of 0 specifies that the MAX unit sends no Hello messages.

Example: `Hello Timer=60`

Dependencies: You can set this parameter only if you have set L2TP Mode to LAC, LNS, or Both.

Location: Ethernet>Mod Config>L2 Tunneling Options

CC Establish Timer, First Retry Timer, L2TP Mode, LAC In Call Timer, LNS In Call Timer, Retry Count

High BER

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

Usage: Specify one of the following values:

- 10**-3 (the default)
- 10**-4
- 10**-5

Location: System > Sys Config

See Also: High BER Alarm

High BER Alarm

Description: Specifies whether the back panel alarm relay closes when the bit-error rate exceeds the value specified by the High BER parameter.

The MAX has an alarm relay whose contacts remain open on the back panel's alarm relay terminal block during normal operation. If you enable, the alarm relay contacts close during loss of power, hardware failure, or a system reset. The High BER Alarm parameter specifies whether the contacts also close when the bit-error rate exceeds the High BER parameter value.

Usage: Specify Yes or No. No is the default.

Yes causes the MAX to close the back panel alarm relay when the bit-error rate exceeds the High BER value.

No causes the MAX to log the event but not close the alarm relay.

Location: System > Sys Config

See Also: High BER

Home Network Name

Description: Specifies the home network that the ATMP Foreign Agent sends to the ATMP Home Agent.

Usage: Specify a value of up to 21 case-sensitive characters.

Example: `Home Network Name=1234567890Abcdefgklm1`

Location: Ethernet > Mod Config > *any Connection profile* > Tunnel Options

See Also: Profile Type, Tunnel Protocol, Max Tunnels, ATMP HA RIP, UDP Port, Pri. Tunnel Server, Sec. Tunnel Server, Password, Client ID, Tunnel VRouter

Hop Count

Description: Specifies the number of hops to the destination IPX network. From the MAX, the local IPX network is one hop away. The IPX network at the remote end of the route is two hops away: one hop across the WAN and one hop to the local IPX network.

Usage: Specify a valid hop count from 1 to 15. A hop count of 16 is considered unreachable and is not valid for static routes.

Dependencies: This parameter does not apply if the MAX does not support IPX routing.

Location: Ethernet > IPX Routes

See Also: Route IPX

Host #1 Port

Description: Specifies the port to use for contacting the Telnet host specified in the Host #1 Addr parameter.

Usage: Specify a number from 0 to 65535. The default is 0.

Example: `Host#1 Port=50`

Dependencies: Host #1 Port is active only when the Host #1 Service parameter is set to `Telnet`.

Location: Ethernet > Mod Config >TServ Options

See Also: Host #1 Addr, Host #1 Service

Host #2 Port

Description: Specifies the port to use for contacting the Telnet host specified in the Host #2 Addr parameter.

Usage: Specify a number from 0 to 65535. The default is 0.

Example: `Host#2 Port=50`

Dependencies: Host #2 Port is active only when the Host #2 Service parameter is set to `Telnet`.

Location: Ethernet > Mod Config >TServ Options

See Also: Host #2 Addr, Host #2 Service

Host #3 Port

Description: Specifies the port to use for contacting the Telnet host specified in the Host #3 Addr parameter.

Usage: Specify a number from 0 to 65535. The default is 0.

Example: `Host#3 Port=50`

Dependencies: Host #3 Port applies only when Host #3 Service parameter is set to `Telnet`.

Location: Ethernet > Mod Config >TServ Options

See Also: Host #3 Addr, Host #3 Service

Host #4 Port

Description: Specifies the port to use for contacting the Telnet host specified in the Host #4 Addr parameter.

Usage: Specify a number from 0 to 65535. The default is 0.

Example: `Host#4 Port=50`

Dependencies: Host #4 Port applies only when the Host #4 Service parameter is set to `Telnet`.

Location: Ethernet > Mod Config >TServ Options

See Also: Host #4 Addr, Host #4 Service

Host #1 Service

Description: Specifies the type of service to use for the host specified in the Host #1 Addr parameter.

Usage: Specify one of the following values:

- `Telnet` (the default) specifies Telnet service.
- `RawTCP` specifies raw TCP service.
- `Rlogin` specifies Rlogin service.
- `PPP` specifies PPP service.

Example: `Host #1 Service=Rlogin`

Location: Ethernet > Mod Config >TServ Options

See Also: Host #1 Addr

Host #2 Service

Description: Specifies the type of service to use for the host specified in the Host #2 Addr parameter.

Usage: Specify one of the following values:

- `Telnet` (the default) specifies Telnet service.
- `RawTCP` specifies raw TCP service.
- `Rlogin` specifies Rlogin service.
- `PPP` specifies PPP service.

Example: `Host #2 Service=Rlogin`

Location: Ethernet > Mod Config >TServ Options

See Also: Host #2 Addr

Host #3 Service

Description: Specifies the type of service to use for the host specified in the Host #3 Addr parameter.

Usage: Specify one of the following values:

- `Telnet` (the default) specifies Telnet service.
- `RawTCP` specifies raw TCP service.
- `Rlogin` specifies Rlogin service.
- `PPP` specifies PPP service.

Example: `Host #3 Service=Rlogin`

Location: Ethernet > Mod Config >TServ Options

See Also: Host #3 Addr

Host #4 Service

Description: Specifies the type of service to use for the host specified in the Host #4 Addr parameter.

Usage: Specify one of the following values:

- `Telnet` (the default) specifies Telnet service.
- `RawTCP` specifies raw TCP service.
- `Rlogin` specifies Rlogin service.
- `PPP` specifies PPP service.

Example: `Host #4 Service=Rlogin`

Location: Ethernet > Mod Config >TServ Options

See Also: Host #4 Addr

Host #1 User

Description: Specifies the username for Rlogin sessions with the host specified in the Host #1 Addr parameter.

Usage: Specify a text string of up to 31 characters. The default is null.

Example: `Host #1 User=`**`robin`**

Dependencies: Host #1 User applies only when the Host #1 Service parameter is set to `Rlogin`.

Location: Terminal-Server > Menu-Mode-Options

See Also: Host #1 Addr, Host #1 Service

Host #2 User

Description: Specifies the username for Rlogin sessions with the host specified in the Host #2 Addr parameter.

Usage: Specify a text string of up to 31 characters. The default is null.

Example: `Host #2 User=`**`robin`**

Dependencies: Host #2 User applies only when the Host #2 Service parameter is set to `Rlogin`.

Location: Terminal-Server > Menu-Mode-Options

See Also: Host #2 Addr, Host #2 Service

Host #3 User

Description: Specifies the username for Rlogin sessions with the host specified in the Host #3 Addr parameter.

Usage: Specify a text string of up to 31 characters. The default is null.

Example: `Host #3 User=`**`robin`**

Dependencies: Host #3 User applies only when the Host #3 Service parameter is set to `Rlogin`.

Location: Terminal-Server > Menu-Mode-Options

See Also: Host #3 Addr, Host #3 Service

Host #4 User

Description: Specifies the username for Rlogin sessions with the host specified in the Host #4 Addr parameter.

Usage: Specify a text string of up to 31 characters. The default is null.

Example: `Host #4 User=`**`robin`**

Dependencies: Host #4 User applies only when the Host #4 Service parameter is set to `Rlogin`.

Location: Terminal-Server > Menu-Mode-Options

See Also: Host #4 Addr, Host #4 Service

Host Init. Mode

Description: For host-initiated calls, specifies the default data transfer mode. Note that the host can override the setting with a control frame.

Usage: Specify one of the following values:

- Local (the default)—Error recovery is performed locally. In this mode, the MAX does not send supervisory frames (that is, ACKs and NAKs) across the X.25 network. The T3POS PAD is responsible for sending supervisory frames to the T3POS DTE.
- Transparent—The T3POS PAD does not provide any error recovery. In this mode, the DTE and the host system provide error recovery for the connection. In Transparent mode, however, the T3POS PAD does recognize a clear request command signal from the DTE (that is, DLE, EOT) and clears the call when it receives a DLE, EOT command.
- Blind—Same as Transparent mode except that the T3POS PAD does not clear a call when it receives a clear request command from the DTE. In this mode, the PAD or the host system must clear the call. The PAD passes all data *blindly*, without regard to the protocol in use. This mode provides a means to pass raw binary data between the DTE and the host system without reference to the protocol being used.
- Bin-Local—No error recovery is applied between the T3POS PAD and the host, but error recovery is applied between the PAD and the DTE. Like Blind mode, it passes data

between the DTE and the host without reference to the protocol being used, but continues to use the T3POS protocol between the DTE and the PAD.

Dependencies: None. This parameter is always applicable.

Location: Ethernet > Connections > *Connection profile* > Encaps Options, Ethernet > Answer > T3POS Options

Host #*N* Addr (*N*=1–4)

Description: Specify the IP address of the first, second, third, and fourth hosts listed in the terminal-server menu-mode interface. These are the only hosts to which terminal–server users can Telnet or Rlogin if they are not allowed to use command mode. Note that you can use RADIUS to specify a longer list of hosts.

To specify hosts with which terminal-server users establish raw TCP sessions, enter the identifier `rawTcp` before the host address (or DNS name).

Usage: Specify the IP address of the host. The default value is 0.0.0.0/0.

To specify that the MAX is to establish raw TCP sessions instead of Telnet or Rlogin sessions, use the following format to set Host #*N* Addr:

`rawTcp` *`hostaddress portnumber`*

where:

- ***`hostaddress`*** indicates the IP address (or DNS name) of a raw TCP host.
- ***`portnumber`*** is the UDP port used for raw TCP sessions.

Example: `Host #N Addr=10.207.23.6/24`

Dependencies: This parameter is ignored if Remote Conf=Yes. It is not applicable if terminal services are disabled.

Location: Ethernet > Mod Config > TServ Options

See Also: Remote Conf

Host #*N* Text (*N*=1–4)

Description: Specify a text description of the first, second, third, and fourth hosts listed in the terminal-server menu-mode interface.

Usage: Specify a text description of the host.

Example: `Host #N Text=Database Server`

Dependencies: This parameter is ignored if Remote Conf=Yes. It is not applicable if terminal services are disabled.

Location: Ethernet > Mod Config > TServ Options

See Also: Remote Conf

Hunt-*N* # (*N*=1-3)

Description: Specify the hunt-group numbers associated with the T1 line in a specific Line *N* profile. An SNMP manager can retrieve these numbers from Lucent devices and store them in a table that identifies the devices from which information is retrieved and the hunt-group numbers in their WAN Line *N* profiles.

Usage: Enter the telephone number for the hunt group associated with the current line.

Example: `Hunt-1 #=847-4747`

Dependencies: The numbers specified in the Hunt-*N* # parameters must be the same as the numbers that are assigned to T1 channels, creating the hunt group.

Location: Net T1> *Line Config profile* > Line *N*

I

ICMP Redirects

Description: Specifies whether the MAX accepts or ignores Internet ICMP Redirect packets. ICMP was designed to dynamically find the most efficient IP route to a destination. ICMP Redirect packets are one of the oldest and least secure route discovery methods on the Internet. ICMP Redirects can be counterfeited to change the way a device routes packets.

Usage: Specify one of the following values:

- Accept (the default)—Process ICMP Redirects.
- Ignore—Drop ICMP Redirects.

Location: Ethernet > Mod Config

Id Auth

Description: Specifies how CLID (Calling Line ID) or DNIS (Dial Number Information Service) should be used for authentication.

Usage: Specify one of the following values:

- Ignore (the default)—Do not require a matching ID from incoming calls.
- Prefer—Authenticate using the CLID if available, otherwise use PAP or CHAP authentication. If CLID is available and CLID authentication fails, the MAX clears the call.
- Require—The CLID must be valid and match a value specified in a configured profile. If the profile also requires password authentication, perform that as well.
- Fallback—Authenticate using the CLID when RADIUS is available, otherwise use password authentication.
- Called Require—The called number must be valid and match the value of the Calling # parameter in a configured profile. If the profile also requires password authentication, perform that as well.

- Called Prefer—Authenticate using the value of the Calling # parameter in a configured profile if available, otherwise use password authentication.
- First—Authenticate using the CLID if available, otherwise use PAP or CHAP authentication. The MAX clears the call if both CLID authentication and PAP or CHAP authentication fail, or if CLID is not available and PAP or CHAP authentication fails.
- Called First—Authenticate using the value of the Called # parameter if available, otherwise use PAP or CHAP authentication. The MAX clears the call if both Called # authentication and PAP or CHAP authentication fail, or if the Called # value is not available and PAP or CHAP authentication fails.

Location: Ethernet > Answer

See Also: AnsOrig, Calling #, Called #

Id Auth Prefix

Description: Specifies the string inserted as a prefix to the telephone number that is presented to the RADIUS server in CLID or DNIS authentication requests.

This parameter can be used to distinguish a user authentication from a telephone number authentication by having the RADIUS server verify whether it matches a string it expects. The Id Auth Prefix parameter specifies a free-form value inserted as a prefix to the telephone number presented to the RADIUS server in CLID or DNIS authentication requests.

For example, the username is the dialed telephone number in CLID authentication and the calling telephone number in DNIS authentication. The prefix can be configured at your discretion. For example, if your telephone number is 510-747-1234 and the number you call to connect to the Internet is 1-800-1234, then, if your ISP is using CLID authentication, the ISP's MAX unit sends a RADIUS request to authenticate the username of 5107471234. And if, for example, the ISP has set the Id Auth Prefix parameter configured to `Caller`, the username attribute in the RADIUS request has a value of `Caller/5107471234.`

If you set Id Auth Prefix to a null value (the default), the MAX authenticates as before, using only the calling or called party number as the username in the authentication request.

Usage: Specify up to 16 characters. The default is null (authentication uses only the calling or called party number as the username in the authentication request).

Location: Ethernet > Mod Config > Auth

ID Fail Busy (previously CLID Fail Busy)

Description: Specifies whether to return User Busy or Normal Call Clearing as a Cause value in IDSN Disconnect messages when authentication fails because of a mismatch between the actual number and the expected number.

Usage: Press Enter to toggle between Yes and No. No is the default. If you choose Yes, and the ID authentication fails because of a mismatch between the actual number and the expected number, the Disconnect message will have the Cause value User Busy (decimal value 17). If you choose No, the Cause value will be Normal Call Clearing (decimal value 16).

Dependencies: This parameter is N/A if Auth=None or Auth=TACACS+ in this profile. The value specified for this parameter applies to both Caller ID and Called ID authentication.

This parameter is also N/A if `ID Auth=Ignore`.

Location: Ethernet > Mod Config > Auth

See Also: Timeout Busy

Idle

Description: In the Answer or Connection profile, specifies the number of seconds the MAX waits before clearing a call when a session is inactive. In a Port Config profile, specifies the action an AIM port takes when you turn on the power or if no call is active.

Usage: In the Answer profile or a Connection profile, specify the number of seconds a session can remain idle without being brought down. If you specify 0 (zero), MAX does not enforce a limit. An idle connection stays open indefinitely. The default setting is 120 seconds.

In a Port profile, specify one of the following values:

- None—The port waits for a user to establish a call. None is the default.
- Call—The port attempts to establish an outbound call whenever you turn on the power or when no call is active.

Dependencies: In a Port profile, this parameter is not applicable when the port's current call profile is configured for FT1 calls. If the MAX 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 MAX 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 end and the remote end must use the same combination of settings for these parameters. Further, if you set Idle to None and Dial to DTR, the hosts at both ends of the connection must activate the DTR (Data Terminal Ready) signal to enable the MAX to connect the switched channels.

Location: Ethernet > Answer > Session Options, Ethernet > Connections > *Connection profile* > Session Options, Host/Dual (Host/AIM6) > Port*N* Menu > Port Config

See Also: Call Type, Dial, Dual Ports, Profile Reqd

Idle Logout

Description: Specifies the number of minutes an administrative login can remain inactive before the MAX logs out and hangs up.

Usage: Specify a number from 0 to 60. The default setting is 0, which disables automatic logout.

Location: System > Sys Config

Idle Pct

Description: Specifies a percentage of bandwidth utilization below which the MAX clears an MP+ call. Bandwidth utilization must fall below this percentage *on both sides of the connection* before the MAX clears the call.

If the device at the remote end of the link has an Idle Pct setting lower than the value you specify, the MAX does not clear the call until bandwidth utilization falls below the lower

percentage. If either end of a connection has this parameter set to 0 (zero), the MAX ignores the parameter on both sides.

Note: When bandwidth utilization falls below the Idle Pct setting on both sides of the connection, the call disconnects regardless of whether the time specified by the Idle parameter has expired.

Usage: Specify a number from 0 to 99. The default value is 0, which causes the MAX to ignore bandwidth utilization when determining whether to clear a call.

Dependencies: This parameter applies only to MP+ calls.

Location: Ethernet > Answer > PPP Options, Ethernet > Connections > *Connection profile* > Encaps Options

See Also: Call Filter, Encaps, Idle

IF Adrs

Description: Specifies a numbered interface IP address for the MAX. Interface-based routing enables the MAX to operate more nearly the way a multihomed Internet host behaves. In addition to the system wide IP configuration, the MAX and the far end of the link have link-specific IP addresses. The MAX address for this connection is specified by the IF Adrs parameter. The far-end numbered interface address is specified by the WAN Alias parameter.

Usage: Specify the IP address of the numbered interface.

Example: `IF Adr=10.207.23.7/24`

Dependencies: This parameter does not apply if the MAX does not route IP.

Location: Ethernet > Connections > *Connection profile* > IP Options

See Also: WAN Alias, Route IP

Ignore Def Rt

Description: Specifies whether the MAX ignores the default route when applying RIP updates to its routing table. The default route specifies a static route to another IP router, which is often a local router such as a Lucent GRF400 or other kind of LAN router. When the MAX is configured to ignore the default route, RIP updates will not modify the default route in the MAX routing table.

Usage: Specify Yes or No. No is the default.

- Yes— Specifies that the MAX ignores advertised default routes. This setting is recommended.
- No—Specifies that the MAX can modify its default route on the basis of RIP updates.

Example: `Ignore Def Rt=Yes`

Dependencies: This parameter is not applicable if the MAX does not route IP.

Location: Ethernet > Mod Config > Ether Options

Imm. Modem Access

Description: Specifies the type of call restriction in use for the Immediate Modem feature.

Note: In previous software versions, you could set the Imm. Modem Pwd parameter to null to allow unlimited access to the Immediate Modem feature. In the current version, you should set Imm. Modem Access to None instead. For compatibility, however, the system still treats the combination of Imm. Modem Access=Global and a null Imm. Modem Pwd parameter as if Imm. Modem Access were set to None.

Usage: Specify one of the following values:

- None—Disables call restriction. All users can place outgoing calls.
- Global—A single password verifies dial-out. Anyone who knows that password can place outgoing calls. The Imm. Modem Pwd parameter specifies the password.
- User (the default)—Enables per-user Immediate Modem access. The MAX requests a login name before allowing any user to access the Immediate Modem feature. It then looks for a profile with that name. If it does not find a matching profile, the MAX closes the Telnet session and rejects the request for dialout. If it does find a matching profile, it requests the password (if any) associated with that profile. If the user enters the correct password, the MAX performs an additional check. It verifies that the Dialout-OK parameter is set to Yes in the Connection profile. The user is allowed access to a modem only if the user enters the proper password and has Dialout-OK set to Yes. Otherwise, the MAX closes the Telnet session and displays an appropriate message.

Example: `Imm. Modem Access=User`

Location: Ethernet > Mod Config > TServ Options

See Also: Dialout OK, Imm. Modem Pwd

Imm. Modem Port

Description: Specifies the port number for Immediate Modem dial-out.This setting informs the MAX that all Telnet sessions initiated with that port number require modem access.

Usage: Specify a port number (5000–65535). The default is 5000.

Location: Ethernet > Mod Config > TServ Options

Dependencies: This parameter is not applicable if terminal services are disabled.

See Also: Immediate Modem

Imm. Modem Pwd

Description: Specifies a password required to dial-out using the Immediate Modem service when Imm. Modem Access is set to Global. If this password is non-null, users will be prompted for a password before being allowed access to a modem and modem dial-out service will be denied if the user does not enter the proper password.

Usage: Specify a password of up to 64 characters.

Location: Ethernet > Mod Config > TServ Options

Dependencies: This parameter is not applicable if terminal services are disabled, if Immediate Modem is disabled, or if Imm. Modem Access is set to None or User.

See Also: Immediate Modem, Imm. Modem Access

Immed Host

Description: Specifies the host to use for terminal-server users' immediate service. Immediate service establishes the selected service as soon as the terminal-server connection is established.

Usage: If the immediate service is Telnet, Raw-TCP, or Rlogin, specify the IP address or DNS hostname. If the immediate service is X25-PAD, specify the X.121 address (or mnemonic) to call for access to the Packet Assembler/Disassembler (PAD).

Example: `Immed Host=host1.abc.com`

Dependencies: This parameter is not applicable if terminal services are disabled.

Location: Ethernet > Mod Config > TServ Options

See Also: Immed Port, Immed Service

Immed Port

Description: Specifies the TCP port on which immediate Telnet, raw TCP, or Rlogin sessions are established as soon as the terminal-server connection is established.

Usage: Specify the port number on the remote device. The default, 0 (zero), specifies port 23.

Dependencies: This parameter is not applicable if Immediate Service is set to X.25/PAD or if terminal services are disabled.

Location: Ethernet > Mod Config > TServ Options

See Also: Immed Host, Immed Service

Immed Service

Description: Enables a particular type of service for establishing an immediate host connection for dial-in terminal-server connections (*immediate mode*).

When you specify an immediate service, the MAX allows no other types of service (PPP, for example).

Usage: Specify one of the following values:

- None (the default)—Disables immediate mode.
- Telnet—You can set the Telnet Host Auth parameter to bypass terminal-server authentication and go right to a Telnet login prompt.
- Raw-TCP
- Rlogin

- X.25/PAD—The call is directed to the PAD, and the MAX makes an X.25 call request with the X.121 address specified by the Immed Host parameter. The Immed Port parameter does not apply.

Dependencies: This parameter requires a host specification for the Immed Host parameter. It is not applicable if terminal services are disabled.

Location: Ethernet > Mod Config > TServ Options

See Also: Immed Host, Immed Port

Immediate Modem

Description: Enables or disables the Immediate Modem service. If Immediate Modem service is enabled, users can Telnet to a MAX unit to access the MAX unit's modems, so that they can place outgoing calls without going through the MAX terminal-server interface. The MAXDial software offers the same outgoing call ability, but through a GUI interface.

Note: The MAX provides per-user control and accounting for both the Immediate Modem feature and MAXDial. For details, see Imm Modem Access or the MAXDial documentation.

Usage: Specify Yes or No. No is the default.

Yes enables Immediate Modem service.

No disables this service.

Location: Ethernet > Mod Config > TServ Options

Dependencies: This parameter is not applicable if terminal services are disabled.

See Also: Imm. Modem Port, Imm. Modem Access

Inactivity Timer

Description: The inactivity timer specifies the number of seconds to allow a connection to remain inactive before dropping the virtual circuit.

Usage: Specify a number of seconds. The default, 0 (zero), disables the inactivity timer.

Example: `Inactivity Timer=120`

Dependencies: This parameter applies only to X.25/IP connections

Location: Ethernet > Connections > any *Connection profile* > Encaps Options

Inc CallerID Info

Description: Specifies whether or not to include caller ID information for calls from this port.

Usage: Specify Yes or No. The default is No.

Dependencies: If the Inc CallerID Info parameter is set to Yes, then the value in Clid Number is passed to the Dst Port.

Location: Analog FXS > FXS Config > *FXS Configuration profile* > Line *N*

InCall Type

Description: Specifies whether the calls are redial-type fax calls or DID-type fax calls.

Note: This parameter applies only to MAX 6000 units.

Usage: Specify one of the following values:

- `redialer`—All fax calls are redialer-type calls. Redialer is the default.
- `did`—The MAX unit authenticates the call on the basis of DID numbers.

Dependencies: If the MAX unit utilizes a DID line, specify `did`.

A MAX unit authenticates a call on the basis of the values specified by the `InCall Type` and `All-Calls-Are Fax` parameters as follows:

If `InCall Type` is set to:	**And `All Calls Are Fax` is set to:**	**The MAX unit:**
`redialer`	`yes`	Receives any incoming call as a redialer type of fax call
`did`	`yes`	Treats any incoming call as a DID type of fax call
`did`	`no`	Authenticates calls against the (up to four) DID numbers specified by the `DID #N` parameters
`redialer`	`no`	Authenticates calls against the DNIS numbers specified by the `DNIS #N` parameters

Location: Ethernet > Mod Config > IP Fax Options

See Also: All Calls Are Fax, Dialer Type, DID #N, DNIS #N

Inc Ch Count

Description: Specifies the number of channels the MAX adds as a bundle when bandwidth changes either manually or automatically during a call.

If the call's data service is 384K/H0 or 384KR, the value you specify should be divisible by 6, because 384 Kbps is 6x64 Kbps. In this case, specify a value of 6, 12, 18, 24, or 30.

If the call's data service is MultiRate or GloBanD, and the service you select is a multiple of 64 Kbps, specify a value that is a multiple of 6.

MP+ calls cannot exceed 32 channels. The sum of Base Ch Count and Inc Ch Count cannot exceed the maximum number of channels available.

Usage: Specify a number of channels. The default is 1.

Example: `Inc Ch Count=3`

Dependencies: This parameter does not apply 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.

Location: Host/Dual (Host/AIM6) > Port*N* Menu > Directory, Ethernet > Connections > *Connection profile* > Encaps Options

See Also: Base Ch Count, Dec Ch Count, Max Ch Count

Input Sample Count

Description: 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 uses only one sample to decode signals from robbed-bit PBXs, because some PBX devices have a tone duration of 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 MAX can use two samples. Using two samples is recommended when the tone duration is longer than 70ms.

Usage: Specify one of the following values:

- One—Use one set of Goertzel samples.
- Two —Use two sets of Goertzel samples.

Example: `Input Sample Count=One`

Dependencies: This parameter applies only to T1 lines using PBX-T1 conversion.

Location: Net/T1 > Line Config > Line *N*

See Also: Sig Mode

Initial Scrn

Description: Specifies the type of user interface displayed at the start of a dial-in terminal-server connection.

Usage: Specify one of the following values:

- Cmd (the default)—Display the command-line interface (*terminal mode*).
- Menu—Display the menu interface (*menu mode*).

Location: Ethernet > Mod Config > TServ Options

InterDigit Timeout

Description: Controls how long a MultiVoice gateway will wait after receiving the last digit of a dial string before declaring DNIS/ANI collection complete. When using inband signaling (T1, MF R2), MAX will wait until this interval has elapsed to ensure it has received all audible tones used to transmit DNIS/ANI across the trunk.

Usage: The InterDigit Timeout parameter accepts values between 100 and 6000 millisecond (ms). This parameter defaults to 3000ms. (3 seconds). For configurations supporting E1 MRC R2 signaling, the InterDigit Timeout parameter accepts values between 200ms and 6000ms.

Example: The following illustrates how to configure the inter-digit timer on a MultiVoice gateway to wait one second (1000 ms.) in between dialed digits before continuing with call processing.

1 From the MAX administration menu, select the Net/E1 > Line Config > Line profile.

2 Scroll down to the appropriate Line, then select the Line Config > Line # profile. Press [Enter] to open this profile.

3 Scroll down to the InterDigit Timeout parameter, then press [Enter] to open the edit field for this parameter, as illustrated.

```
InterDigit Timeout=
[3000]
```

4 Type in 1000 in the edit field to set the new value to one second (1000ms.). Press [Enter] to close the edit field when finished.

5 Press [Esc] until the option to `Exit and accept` your changes appears; then save your changes.

Dependencies: E1 MFC-R2 signaling is country specific. The Sig Mode parameter, and the Country parameter in the System profile, must be set for the country-appropriate signaling in order for the MultiVoice gateway to properly detect dialed digits.

Location: Net/E1 > Line Config > Line *xx* > Line *x*

Interval

Description: Specifies the interval, in seconds, between the receipt or transmission of Combinet line-integrity packets. If the MAX does not receive a Combinet line-integrity packet within three of these intervals, it disconnects the call.

Usage: Specify a number of seconds from 5 to 50. The default is 10.

Example: `Interval=10`

Dependencies: This parameter applies only to Combinet connections.

Location: Ethernet > Answer > COMB Options, Ethernet > Connections > *Connection profile* > Encaps Options

See Also: COMB, Encaps

IP Addr Msg

Description: Specifies a string to be printed in front of the IP address when a terminal-server user initiates a PPP session.

Usage: Specify a text string of up to 20 characters. The default is *`IP address is`*:

Example: `IP Addr Msg=Your IP address is:`

Dependencies: This parameter is not applicable when terminal services are disabled.

Location: Ethernet > Mod Config > TServ Options

IP Adrs

Description: Specifies the LAN interface IP address.

Usage: Specify the IP address of the MAX on the local IP network or subnet.

Example: `IP Adrs=10.2.1.1/24`

Dependencies: This parameter does not apply if the MAX does not route IP.

Location: Ethernet > Mod Config > Ether Options

See Also: Encaps, Route IP

IP Direct

Description: Specifies the IP address of a local host to which all inbound IP packets on this link will be directed. When you specify an address for this parameter, the MAX bypasses all internal routing and bridging tables and sends each packet received from the remote end of the connection to the specified address. This parameter does not affect outbound traffic. Note that the IP direct host must be on the same local network as the MAX.

Usage: Specify an IP address. The default is 0.0.0.0. If you accept the default, the MAX does not redirect traffic coming from the remote end specified by the Connection profile.

Example: `IP Direct=10.2.3.4/24`

Location: Ethernet > Connections > *Connection profile* > Session Options

See Also: Bridge, Encaps, FR Direct, RIP, Route IP

IP Gateway Addr Msg

Description: Specifies the text the MAX displays before the MAX IP address field in the SLIP session startup message.

Usage: Specify a text message. You can enter up to 64 characters. The default is `Gateway:`

Dependencies: IP Addr Msg does not apply unless you set SLIP Info to Advanced.

Location: Ethernet > Mod Config > TServ Options

See Also: Slip Info, IP Netmask Msg

IP Netmask Msg

Description: Specifies the text the MAX displays before the netmask field in the SLIP session startup message.

Usage: Specify a text message. You can enter up to 64 characters. The default is `Netmask:`

Dependencies: IP Netmask Msg does not apply unless you set SLIP Info to Advanced.

Location: Ethernet > Mod Config > TServ Options

See Also: Slip Info, IP Gateway Addr Msg

IPX Alias#

Description: Specifies the IPX network number assigned to a point-to-point link. This parameter is used only when the MAX operates with a non-Lucent router that uses a numbered interface. It does not apply if you are routing from one MAX to another, or to a router that does not use a numbered interface.

Usage: Specify an IPX network number. The default value is 00000000. FFFFFFFF is invalid.

Dependencies: This parameter is not applicable if the MAX does not route IPX.

Location: Ethernet > Connections > *Connection profile* > IPX Options

See Also: Route IPX

IPX Enet

Description: Specifies the IPX network number for the Ethernet interface of the MAX. The easiest way to ensure that the number is correct is to leave the default null address. The null address causes the MAX unit to listen for its network number and acquire it from another router on the same interface. If you specify a number other than zero, the unit becomes a *seeding* router and other routers can learn their IPX network number from it. (For details about seeding routers, see the Novell documentation.)

Usage: Specify the IPX network number in use on the Ethernet segment to which the MAX is connected. The default 00000000 causes the MAX to learn its network number from other routers on that interface.

Example: `IPX Enet #=DE040600`

Dependencies: This parameter is not applicable if the MAX does not route IPX.

Location: Ethernet > Mod Config > Ether Options

IPX Frame

Description: Specifies the type of packet frame the MAX routes and spoofs (IEEE 802.2 by default). Base the setting of this parameter on the type of IPX frame used by the majority of NetWare servers on the Ethernet network. If some NetWare software transmits IPX in a frame type other than the type specified, the MAX drops those packets, or if bridging is enabled, it bridges them. (If you are not familiar with the concept of packet frames, see the Novell documentation.)

Usage: Specify one of the following values:

- 802.2 (NetWare 3.12 or later)—Specifies that IPX clients and servers on the local Ethernet network follow the IEEE 802.2 protocol for the MAC header. The framer contains the Logical Link Control (LLC) header in addition to the Media Access Control (MAC) header. This setting is the default.

- 802.3 (for NetWare 3.11 or earlier)—Specifies that IPX clients and servers on the local Ethernet network follow the IEEE 802.3 protocol for the MAC header (also called Raw 802.3). The frame does not contain the Logical Link Control (LLC) header in addition to the Media Access Control (MAC) header.
- SNAP—Specifies that IPX clients and servers on the local Ethernet network follow the SubNetwork Access Protocol (SNAP) for the MAC header. This specification includes the IEEE 802.3 protocol format plus additional information in the MAC header.
- Enet II— Specifies that IPX clients and servers on the local Ethernet network follow the Ethernet II protocol for the MAC header.
- None—The MAX can bridge or route IPX, but without watchdog spoofing or the automatic RIP and SAP handling.

Dependencies: This parameter is not applicable if the MAX does not route IPX.

Location: Ethernet > Mod Config > Ether Options

IPX Header Compression

Description: Specifies whether the MAX unit should use IPX header compression on the connection if the encapsulation method in use supports it. The compression does not include Shiva-type header compression, which is referenced by (though not defined by) RFC 1553. IPX header compression is interoperable with Windows 95 PPP stack and the Funk PPP dialer. The MAX supports IPX header compression to maintain consistency with MAX platforms and also to use as a toggle for enabling and disabling IPX header compression for a call if this parameter has not been set to Yes in the Connection profile.

Usage: Specify Yes to enable or No to disable IPX header compression in PPP (MP/MPP) sessions. Yes is the default.

Example: `IPX Header Compression=Yes`

Dependencies: This parameter is not applicable if the MAX does not route IPX.

Location: Ethernet > Connections > *Connection profile* > Encaps Options, Ethernet > Answer > PPP Options

IPX Net

Description: Specifies the network number of the remote-end router. If a number is specified, the MAX creates a static route to that device. A setting is needed only when the remote-end router requires that the MAX know its network number before connecting.

Usage: Specify the remote device's IPX network number. The default 00000000 is appropriate for most installations. The default causes the MAX not to advertise the route until it makes a connection to the remote network.

Dependencies: This parameter is not applicable if the MAX does not route IPX.

Location: Ethernet > Connections > *Connection profile* > IPX Options

See Also: Route IPX

IPX Pool#

Description: Enables each VRouter to maintain its own dial-in pool.

Usage: Specify an IPX network number that is unique in the IPX routing domain. All dial-in clients will be assigned addresses on this virtual network. The same IPX network number can be used as the IPX Pool# value for more than one VRouter. Within a VRouter profile, specify an IPX network number that is unique in the IPX routing domain. All dial-in clients belonging to a VRouter will be assigned addresses on the virtual network specified for that VRouter.

Example: `IPX Pool #=FF0000037`

Dependencies: This parameter is not applicable if the MAX unit does not route IPX.

Location: Ethernet > Virtual Routers > *any virtual router profile*

IPX RIP

Description: In a Connection profile, specifies how RIP packets are handled across the specified WAN connection. IPX RIP is set to Both by default, specifying that RIP broadcasts will be exchanged in both directions. You can disable the exchange of RIP broadcasts across a WAN connection, or specify that the MAX will only send or only receive RIP broadcasts on that connection.

Usage: Specify one of the following values:

- Both—Send and receive RIP updates. This setting is the default.
- Send—Send RIP updates but do not receive them.
- Recv—Receive RIP updates but do not send them.
- Off—Do not send or receive RIP updates.

Example: `IPX RIP=Both`

Dependencies: This parameter does not apply if Peer=Dialin or the MAX does not route IPX.

Location: Ethernet > Connection > *Connection profile* > IPX Options

See Also: IPX SAP, Peer

IPX Routing

Description: Enables or disables IPX routing mode. When you enable IPX routing in a MAX unit and close the Mod Config profile, the unit comes up in IPX routing mode, uses the default frame type 802.2 (which is the suggested frame type for NetWare 3.12 or later), and listens on the Ethernet network to acquire its IPX network number from other IPX routers on the same segment.

Usage: Specify Yes or No. No is the default.

Yes enables IPX routing in the MAX.

No disables IPX routing systemwide.

Example: `IPX Routing=Yes`

Dependencies: If IPX routing is disabled, the MAX can still bridge IPX packets, provided that Bridging is enabled.

Location: Ethernet > Mod Config

See Also: Active, Connection #, Dial Query, Hop Count, IPX Alias, IPX Enet#, Network, Node, Route IPX, Server Name, Server Type, Socket, Tick Count

IPX SAP

Description: In a Connection profile, specifies how SAP packets are handled across the specified WAN connection. IPX SAP is also set to Both by default, specifying that SAP broadcasts will be exchanged in both directions. If SAP is enabled to both send and receive broadcasts on the WAN interface, the MAX broadcasts its entire SAP table to the remote network and listens for SAP table updates from that network. Eventually, both networks have a full table of all services on the WAN. To control which services are advertised and where, you can disable the exchange of SAP broadcasts across a WAN connection, or specify that the MAX will only send or only receive SAP broadcasts on that connection.

Usage: Specify one of the following values:

- Both—Send and receive SAP updates. This setting is the default.
- Send—Send SAP updates but do not receive them.
- Recv—Receive SAP updates but do not send them.
- Off—Do not send or receive SAP updates.

Example: `IPX SAP=Both`

Dependencies: This parameter does not apply if Peer=Dialin or the MAX does not route IPX.

Location: Ethernet > Connections > *Connection profile* > IPX Options

See Also: IPX RIP, Peer

IPX SAP Filter

Description: Applies a SAP filter to the LAN or WAN interface. You can apply an IPX SAP filter to exclude or explicitly include certain remote services from the MAX SAP table. If you apply a SAP filter in a Connection profile, you can exclude or explicitly include services in both directions.

Usage: Specify the unique portion of the number preceding an IPX SAP Filter profile name in the IPX SAP Filters menu. The default 0 (zero), specifies that no filter is applied.

Example: `IPX SAP Filter=4`

Dependencies: This parameter does not apply if the MAX does not route IPX.

Location: Ethernet > Answer > Session Options, Ethernet > Connections > *Connection profile* > Session Options, Ethernet > Mod Config > Ether Options

See Also: IPX Enet #, IPX Routing, Server Name, Server Type, Type, Valid

ISDN TE/NT Mode

Description: Specifies whether the MAX functions as Terminal Equipment (TE) or as a Network Terminating (NT) device for ISDN T1 or E1 connections.

Usage: The default value of TE specifies that the MAX functions as ISDN Terminal Equipment (TE). To configure the MAX as an NT device for T1 or E1 connections, specify `NT`.

Example: `ISDN TE/NT mode=NT`

Dependencies: To specify `NT` for E1 connections, you must first set the Switch Type parameter to `Net 5`.

Location: Net/T1 > Line Config > Line *N*, Net/E1 > Line Config > Line *N*

K

K Window Size

Description: Establishes the maximum number of data packets that can be outstanding in an X.75 connection before acknowledgment is required.

Usage: Specify a number from 2 to 7. The default is 7.

Location: Ethernet > Answer > X.75 Options

See Also: Frame Length, N2 Retran Count, T1 Retran Timer, X.75

KeyID

Description: 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`.

Usage: Specify a number from 0 to 255.

Example: `KeyID=125`

Dependencies: KeyID does not apply unless you set AuthType to MD5.

Location: Ethernet > Connections > *Connection profile* > OSPF Options, Ethernet > Mod Config > OSPF Options

See Also: AuthType, MD5 Key

L

L2 End

Description: Specifies how the MAX unit's CCITT Layer 2 software differentiates between the acting network (PBX) side and the acting user (ET) side of a back-to-back DPNSS

connection. On a functional level, the L2 End parameter enables the DPNSS state machine to detect the difference between Layer 2 command messages and Layer 2 response messages.

Usage: Specify one of the following values:

- `b-side`—(the default).
- `a-side`—Layer 2 acts as ET.

Example: `L2 End=b-side`

Dependencies: This parameter applies only to DPNSS signaling.

Location: Net/E1 > Line Config > Line *N*

See Also: L3 End, Switch Type

L2TP Mode

Description: Specifies the systemwide type of L2TP functionality the MAX supports.

Usage: Specify one of the following values:

- LAC—The MAX can function as an LAC only.
- LNS —The MAX can function as an LNS only.
- Both—The MAX can function as either an LAC or an LNS.
- None—Disables L2TP functionality on the MAX. None is the default.

Example: `L2TP Enable=LAC`

Location: Ethernet > Mod Config > L2 Tunneling Options

See Also: Line *N* Tunnel Type, Route *N* Line

L2TP System Name

Description: Specifies a valid hostname to be used when the MAX establishes an L2TP session.

Usage: Enter an alphanumeric string of up to 31 characters. If you do not enter a value, the MAX unit's system name is used.

Example: `L2TP System Name=bungalow1912`

Dependencies: If the MAX unit's system name is longer than 31 alphanumeric characters, the hostname that is passed to the L2TP end point will be truncated and appended with the `+` character.

Location: Ethernet > Mod Config > L2 Tunneling Options >

L3 End

Description: Specifies which call (outbound or inbound) the MAX unit's CCITT Layer 3 software processes if a collision occurs. With the default setting (`x-side`), the unit processes

the outbound call and drops the inbound call. The default setting (`x-side`) is required for connection to a DPNSS or DASS2 switch.

Usage: Specify either `x-side` or `y-side`:

- `x-side`—When a call collision occurs, the unit processes the outbound call and drops the inbound call. The default is `x-side`.
- `y-side`—When a call collision occurs, the unit processes the inbound call and drops the outbound call.

Example: `L3 End=x-side`

Location: Net/E1 > Line Config > Line *N*

See Also: L2 End, Switch Type

LAC In Call Timer

Description: Specifies the maximum number of seconds that a MAX unit acting as an L2TP LAC waits for an incoming call setup negotiation with the LNS to be completed. Any change you make to the setting of this parameter is reflected as soon as the previous timer expires.

Usage: Specify a decimal number from 1 to 600. The default is 60.

Example: `LAC In Call Timer=60`

Dependencies: Keep in mind the following additional information:

- You can set this parameter only if you have set L2TP Mode to LAC, LNS, or Both.
- Any change you make to the setting of this parameter is reflected as soon as the previous timer expires.

Location: Ethernet > Mod Config > L2 Tunneling Options

CC Establish Timer, First Retry Timer, Hello Timer, L2TP Mode, LNS In Call Timer, Retry Count

LAPB K

Description: Specifies the maximum number of sequentially numbered frames that a given DTE/DCE link can have unacknowledged at any given time. This specification is also called the Level 2 Window Size or the Frame Window Size.

Usage: Specify a number from 1 to 7. The default is 7. A higher value enables faster throughput. The value you specify must be the same for both ends of the link.

Location: Ethernet > X.25

See Also: LAPB N2, LAPB T1, LAPB T2

LAPB N2

Description: Specifies the retry limit—the maximum number of times the MAX can resend a frame when the Link Access Protocol–Balanced (LAPB) T1 timer expires.

Usage: Specify a number from 0 to 255. The default is 20. A higher value increases the probability of a correct transfer of data. A lower value allows quicker detection of a permanent error condition.

Location: Ethernet > X.25

See Also: LAPB K, LAPB T1, LAPB T2

LAPB T1

Description: Specifies the maximum amount of time, in seconds, the transmitter should wait for an acknowledgment before initiating a recovery procedure.

On a transmission line between a user and the network, a particular frame or acknowledgment can be incorrectly transmitted or simply discarded. To keep the transmitter from waiting indefinitely for an acknowledgment, you can specify the maximum amount of time the transmitter should wait.

Usage: Specify a number from 1 to 255. The default is 3. When you specify a value for this parameter, you must take into account any frame transmission and processing delays you might encounter. In most cases, you should use the default value suggested by the network.

Location: Ethernet > X.25

See Also: LAPB K, LAPB N2, LAPB T2

LAPB T2

Description: Specifies the maximum number of milliseconds Link Access Protocol–Balanced (LAPB) waits for outgoing Information frames (I-frames) before sending a Restart-Request packet to the network. An I-frame is a frame that transports data over an access link.

Usage: Specify a number from 0 to 255. The default is 0 (zero).

Location: Ethernet > X.25

See Also: LAPB K, LAPB N2, LAPB T1

LAN

Description: Specifies the ISDN subaddress associated with the MAX unit's bridge/router module or terminal server. When a call is received that includes this subaddress as part of the dialed number, the call is routed to the LAN. This is one method of routing calls. Another way to route calls to the Ethernet network is to set the Ans *N*# parameter in the Ethernet > Mod Config > WAN Options profile.

Usage: Specify a subaddress number from 0 to 99. The default is 0.

Example: `LAN=3`

Dependencies: This parameter is not applicable if the Sub-Adr parameter is not set to Routing.

Location: System > Sys Config

See Also: Ans *N*#, Sub-Adr

LAN Adrs

Description: Specifies the IP address of the remote-end host or router.

Usage: Specify the IP address of the remote device.

Example: `LAN Adrs=200.207.23.101/24`

Dependencies: This parameter does not apply if the MAX does not support IP routing. No two calling Connection profiles should have the same value for LAN Adrs.

Location: Ethernet > Connections > *Connection profile* > IP Options

See Also: Encaps, IP Adrs, Route IP, Station

LCN

Description: Specifies the logical channel number (LCN) to use for a Permanent Virtual Connection (PVC) using X.25.

At the packet level, a number of logical channels are set up between a DTE and a DCE. Every packet exchange occurs on one of these logical channels. When a connection takes place, X.25 uses a logical channel to establish a PVC. The DCE maintains the correspondence between the logical channel and the PVC while the call takes place, and clears the PVC when the data exchange is over.

Usage: Specify a channel number. You can specify a number from 0 to 4095. The default is 0 (zero). If you accept the default, the X.25 link does not use a logical channel or PVC. The link is a Switched Virtual Connection (SVC).

Dependencies: This parameter applies only to X.25/PAD and X.25/IP connections.

Location: Ethernet > Connections > *Connection profile* > Encaps Options

Length

Description: In a T1 Line *N* profile, specifies the cable length of the line from the Channel Service Unit (CSU) or other network interface unit to the MAX. The value you specify should reflect the longest line length you expect to encounter in your installation.

In a Firewall profile, this parameter specifies the length of the firewall uploaded to the MAX from Secure Connect Manager (SCM). In Firewall profiles, the parameter is read-only.

In a filter of type Generic, this parameter specifies the number of bytes to test in a packet, starting with the byte specified by the Offset parameter. For example, with the following specification the filter tests the value of bytes three (97) through ten (99):

```
Filters
   Name=filter-name
   Input filters...
      In filter 01
         Generic...
            Forward=No
```

```
Offset=2
Length=8
Mask=0F FF FF FF 00 00 00 F0
Value=07 FE 45 70 00 00 00 90
Compare=Equals
More=No
```

and the following packet contents:

```
2A 31 97 FE 45 70 12 22 33 99 B4 80 75
```

Usage: In a Filter profile, enter a number from 0 to 8 to specify the number of bytes to use for comparison. The default, 0 (zero), specifies that no bytes are compared.

In a T1 Line *N* profile, specify one of the following values:

- 1–133 ft. (the default)
- 134–266 ft.
- 267–399 ft.
- 400–533 ft.
- 534–655 ft.

Location: Ethernet > Filters > Input filters > In filter *N* > Generic, Ethernet > Filters > Output Filters > Out Filter *N* > Generic, Ethernet > Firewalls, Net/T1 > Line Config > Line *N*

See Also: Offset, Mask, Value

Line *N* Tunnel Type

Description: Specifies whether the MAX should tunnel all calls received on the specified WAN line.

Usage: Specify one of the following values:

- L2TP—Directs the MAX to create L2TP tunnels for all calls received on the specified line.
- PPTP—Directs the MAX to create PPTP tunnels for all calls received on the specified line.
- None—Directs the MAX not to create tunnels on a per-line basis.
  None is the default.

Example: `Line 1 tunnel type=None`

Dependencies: This parameter applies only if you set L2TP Mode to LAC or Both.

Location: Ethernet > Mod Config > L2 Tunneling Options

See Also: L2TP Mode, Route *N* Line

Line Provision

Description: Specifies whether the line is provisioned for the H0, the H11 and/or H12 data service. The calling device uses this value to know which data services it can request from the called device.

Usage: Specify one of the following values:

- None (the default) specifies that the line has not been provisioned.
- H0 specifies that the line has been provisioned for the H0 data service only.
- H11 specifies that the line has been provisioned for the H11 data service only.
- H0 + H11 specifies that the line has been provisioned for both the H0 and H11 data services.
- H12 specifies that the line has been provisioned for H12 data service.

Location: Net/T1 > Line Config > Line *N*, Net/E1 > Line Config > Line *N*

Line Speed

Description: Specifies the speed at which data is clocked on the interface.

Usage: Specify one of the following values: 56Kbps, 64Kbps, 128Kbps, 256Kbps, 384Kbps, 512Kbps, 1Mbps, 2Mbps, 4Mbps, or 8Mbps

Dependencies: This parameter is N/A if the Line Type parameter is set to DTE.

Location: Serial WAN > Mod Config

Line Termination

Description: Specifies the physical and electrical characteristics of the interface. This parameter applies only to the MAX 3000.

Usage: Specify one of the following values: V.35, RS-232, X.21, RS-485, EIA-530A, RS-449, EIA-503, or V.36.

Location: Serial WAN > Mod Config

Line Type

Description: Specifies whether the serial WAN interface is a DCE or DTE device.

Usage: Specify DCE or DTE.

Note: The FR Type parameter in Ethernet > Frame Relay > *Frame Relay* has values of DCE, DTE, and NMI. This setting is unrelated to the physical mode of the interface. It is possible for a device specified as DCE in a Frame Relay profile to be a physical DTE device, and vice versa.

When you connect two serial devices together, one should be DCE and the other DTE. Usually your switch is the DCE and the MAX is the DTE. However, the MAX 3000 can also serve as a DCE device into which you can plug another unit. DCE and DTE have different pinouts and it is the DCE that supplies the clock.

Dependencies: If the Line Type parameter is set to DTE, the Line Speed parameter is N/A.

Location: Serial WAN > Mod Config

Link Access Type

Description: Specifies the type of the DTE connection.

Usage: Specify one of the following values:

- Dedicated (the default)—The DTE connection is a permanent, leased-line connection.
- Dial—The DTE connection is a dial-up connection.

Dependencies: None. This parameter is always applicable.

Location: Ethernet > Connections > *Connection profile* > Encaps Options
Ethernet > Answer > T3POS Options

Link Comp

Description: Specifies the link-compression method for PPP, MP, and MP+ calls.

Usage: Specify one of the following values:

- None—No compression, the default in the Answer profile.
- Stac—A Lucent-modified version of draft 0 of the CCP protocol.
- Stac-9—Draft 9 of the Stac LZS Compression protocol.
- MS-Stac—Microsoft/Stac compression (the method used by Windows95). If the caller does not acknowledge Microsoft/Stac compression, the MAX attempts to use standard Stac compression. If the caller does not acknowledge Stac, the MAX uses no compression.
- MPPC—Microsoft Point-to-Point Compression (MPPC). If the caller does not acknowledge MPPC, the MAX attempts to use standard Stac. If the caller does not acknowledge Stac, the MAX uses no compression.

Dependencies: This parameter applies only to PPP and its multilink variants. Both sides of the link must support the same kind of compression, or none is used.

Location: Ethernet > Answer > PPP Options, Ethernet > Connections > *Connection profile* > Encaps Options

See Also: Compression

Link Mgmt

Description: Specifies the link management protocol to use between the MAX and the Frame Relay switch. The Frame Relay administrator or service provider can tell you which value to use.

Usage: Specify one of the following values:

- None—No link management. The MAX assumes that the physical link is up and that all logical links (as defined by the DLCI and FR DLCI parameters) are active on the physical link. None is the default.
- T1.617D—The link management protocol defined in ANSI T1.617 Annex D.
- Q.933A—The link management protocol defined in Q.933 Annex A.

Location: Ethernet > Frame Relay

See Also: DLCI, FR DLCI

Link Status DLCI

Description: Specifies the DLCI to use for link management on the Frame Relay data link.

Usage: Specify DLCI0 (the default) or DLCI1023.

Location: Ethernet > Frame Relay

See Also: Link Mgmt

Link Type

Description: Specifies whether an ISDN BRI line is operating in point-to-point or multipoint mode. If the MAX uses only one channel of a multipoint ISDN BRI line and another device uses the other channel, you should specify that one channel is unused by setting B1 Usage or B2 Usage to Unused, and enter only one SPID. The device sharing the line must use the other SPID assigned to the line.

Usage: Check with your carrier to find out which setting you should specify for this parameter. You can specify one of the following values:

- P-T-P—Point-to-point mode, in which the MAX requires one telephone number and no SPIDs.
- Multi-—Multipoint mode, in which the MAX requires two telephone numbers and two SPIDs. This setting is the default.

Dependencies: All switch types use multipoint except the AT&T 5ESS switch.

Location: Net/BRI > Line Config > Line *N*

See Also: Pri SPID, Sec SPID, Switch Type

LinkUp

Description: Specifies whether the Frame Relay link is up or down when no DLCI is active.

Usage: Specify Yes or No. No is the default.

Yes causes the MAX to bring the link up automatically and keep it up even if there are no active DLCIs.

No specifies that the link does not come up unless a Connection profile (DLCI) brings it up and shuts it down after the last DLCI has been removed.

Dependencies: You can start and drop Frame Relay data-link connections by using the DO Dial and DO Hangup commands. If LinkUp is set to Yes, DO Dial brings the link down, but it will be automatically restarted.

Location: Ethernet > Frame Relay

See Also: FR Prof, DLCI, Circuit

List Attempt

Description: Enables or disables the DNS List Attempt feature for Telnet logins. DNS can return multiple addresses for a hostname in response to a DNS query, but it does not include information about availability of those hosts. Users typically attempt to access the first address in the list. If that host is unavailable, the user must try the next host, and so forth. However, if the access attempt occurs automatically as part of immediate services, the physical connection is torn down when the initial connection attempt fails. To avoid tearing down physical links when a host is unavailable, you can use the List Attempt parameter to enable the MAX unit to try one entry in the DNS list of hosts, and if that connection attempt fails, to try the next entry, and so on, without losing the WAN session. The List Size parameter specifies the maximum number of hosts listed.

Usage: Specify Yes or No. No is the default.

Yes maintains the physical connection so that a user can try the next host in the DNS list if the first host is unavailable.

No specifies the connection fails if the first Telnet attempt is refused. For dial-in users, the physical connection is torn down when the initial connection fails.

Dependencies: If `List Attempt=No` and `Enable Local DNS Table=Yes`, the local DNS table has only one entry.

Location: Ethernet > Mod Config > DNS

See Also: List Size, Enable Local DNS Table

Listen X.121 Addr

Description: Specifies a listen pattern for host-initiated calls. Setting this parameter is similar to entering the following command in the X.25 PAD:

`* listen addr=`*`pattern`*

The pattern is in the same format as an X.121 address or subaddress and can contain wild cards.

Usage: None. Specify an address of up to 15 characters.

Dependencies: This parameter is always applicable.

Location: Ethernet > Connections > *Connection profile* > Encaps Options,
Ethernet > Answer > T3POS Options

List Size

Description: Specifies the maximum number of DNS addresses that are made accessible to terminal-server sessions in response to a DNS query. List Size also specifies the maximum number of IP address entries in the local DNS table.

If List Attempt=Yes and the name server returns an IP address list, the list is copied into the local DNS table-entry that matches the hostname, up to the number of addresses you specify

for List Size. When a list of IP addresses for an entry is automatically updated, any existing list for that entry is discarded.

Note: The number of IP addresses displayed by the `dnstab entry` terminal command depends upon the value you specify for the List Size parameter.

Usage: Specify a number from 1 to 35. The default is 6.

Example: Following are three possible local DNS table situations:

- You have set `List Size` to `4`, and the remote DNS returns three addresses. The three addresses replace the entire list of four IP addresses in the local DNS table.
- You have set `List Size` to `35`, and the remote DNS server returns only four addresses. The MAX places the four IP addresses in the table and sets the remaining 31 addresses in the list to 0 (zero).
- You have just set `List Size` to `1`. Previously, you had set `List Size` to `10`. The next time the table entry for that one IP address is updated, only the first IP address will be retained in the table, and all nine others will be set to 0 (zero).

Dependencies: This parameter is applicable only when List Attempt=Yes. A local DNS table is created only if `Enable Local DNS Table=Yes`.

Location: Ethernet > Mod Config > DNS

See Also: List Attempt, Enable Local DNS Table

LNS In Call Timer

Description: Specifies the maximum number of seconds a MAX unit functioning as an L2TP LNS waits for an incoming call setup negotiation with the LAC to be completed. Any change you make to the setting of this parameter is reflected as soon as the previous timer expires.

Usage: Specify a decimal number from 1 to 600. The default is 60.

Example: `LNS In Call Timer=60`

Dependencies: This parameter applies only if you have set L2TP Mode to LAC, LNS, or Both.

Location: Ethernet > Mod Config > L2 Tunneling Options

See Also: CC Establish Timer, First Retry Timer, Hello Timer, L2TP Mode, LAC In Call Timer, Retry Count

Local Echo

Description: Enables or disables local echo mode for terminal-server sessions. Local echo mode is a line-by-line mode, in which the line that appears as it is typed is not actually transmitted until the user presses Enter. If local echo is enabled, the line transmitted is echoed on the local MAX terminal screen.

Local echo allows MAX terminal-server users to connect to nonstandard Telnet ports and programs. If the remote server turns local echo on or off in its option negotiation for a Telnet session, it overrides the Local Echo setting.

A terminal-server user can override the Local Echo setting from the command line for the current session by using the `-e` option of the Telnet command.

Usage: Specify Yes or No. No is the default.

Yes turns on local echo.

No disables local echo.

Dependencies: This parameter is not applicable if terminal services are disabled.

Location: Ethernet > Mod Config > TServ Options

Local Profiles First

Description: Specifies whether the MAX should attempt local authentication before remote (external) authentication. By default, the MAX first attempts to authenticate the connection by using local profiles. If that fails, the MAX tries to authenticate the connection using an external authentication server.

If this parameter is set to No, the MAX first tries to authenticate the connection using a remote authentication server. If that fails, the MAX attempts to authenticate the connection by using local profiles. In this case, some dynamic password challenges behave differently than when authentication is local. (PAP and CHAP work the same either way.)

Specify one of the following values:

- PAP-TOKEN—Authentication will not produce a challenge if there is a local profile. This defeats the security of using PAP-TOKEN.
- PAP-TOKEN-CHAP—Brings up one channel, but all other channels fail.
- CACHE-TOKEN—If the far end of the connection has ever authenticated using a challenge, CACHE-TOKEN will not work with local profiles. If the far end has not ever authenticated, there will be no problem with the local profiles.

Note: Because remote authentication is tried first if this parameter set to No, the MAX unit waits for the remote authentication to time out before attempting to authenticate locally. This timeout may take longer than the timeout specified for the connection and could cause all connection attempts to fail. To prevent this, set the authentication timeout value low enough to not cause the line to be dropped, but high enough to permit the unit to respond if it is able to. The recommended time is 3 seconds.

Usage: Specify Yes or No. Yes is the default.

- Yes retains the default authentication order.
- No reverses the default and attempts remote authentication first.

Example: `Local Profiles First=Yes`

Dependencies: This parameter is not applicable if Auth is set to None. See the preceding Note for related dependencies.

Location: Ethernet > Mod Config > Auth

See Also: Auth Timeout

Local Retransmit LSF

Description: Enables local retransmission of a low speed fax frame if no response is detected from the destination fax. This is designed to reduce fax transmission errors on low packet loss networks.

Usage: Pressing [Enter] toggles the value of the Local Retransmit parameter between the following:

Value	Description
Yes	Enables local retransmission of a low speed fax frame if no response is detected from the destination fax.
No	Disables local retransmission of a low speed fax frame.

Dependencies: The Local Retransmit parameter has the following dependencies:

- This parameter defaults to `N/A` when a MultiVoice gateway is not hashed for real-time fax or T.38 fax processing is disabled (`T.38 Fax Enabled=No`).
- Changes to this parameter are effective with the next VoIP call.

Location

Description: An SNMP-readable parameter that specifies the physical location of the MAX unit. It does not affect the unit's operations.

Usage: Specify a description of the MAX unit's location. You can enter up to 80 characters.

Location: System > Sys Config

See Also: Contact

Loc. DNS Tab Auto Update

Description: Enables or disables automatic updating of the local DNS table. If automatic updating is enabled, the list of IP addresses for each entry is replaced with a list from the remote DNS when the remote DNS successfully resolves a connection to a host named in the table.

Usage: Specify Yes to enable automatic updating of the IP addresses in the local DNS table. No disables automatic updating. No is the default.

Dependencies: The Enable Local DNS Table parameter must be set to Yes.

Location: Ethernet > Mod Config > DNS

Log Call Progress

Description: Enables you to turn off all Syslog progress-related Incoming Call messages. except for the End-of-Call message. This parameter controls the output of the MAX for the following call-progress messages: Incoming Call, Call Answered, Assigned to Port, Call Connected, LAN Session Up, Call Terminated, LAN Session Down, and Call Cleared.diagnostics:

Usage: Specify Yes or No.

Yes (the default)—Enables all call-progress messages.

No—Disables all call-related messages except End-of-Call.

Dependencies: Applicable only with RADIUS accounting features enabled. Log Call Progress does not affect any call-related warning or error messages.

Location: Ethernet > Mod Config > Log

Log Facility

Description: 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.

Usage: Specify one of the following values:

- Local0 (the default)
- Local1
- Local2
- Local3
- Local4
- Local5
- Local6
- Local7

Dependencies: This parameter applies only when Syslog=Yes.

Location: Ethernet > Mod Config > Log

See Also: Log Host, Syslog

Log Host

Description: Specifies the IP address of the Syslog host—a UNIX station to which the MAX sends system logs.

Usage: Specify the IP address of the Syslog host. The default value is 0.0.0.0.

Example: `Log Host=10.207.23.1`

Dependencies: This parameter applies only when Syslog=Yes.

Location: Ethernet > Mod Config > Yes

See Also: Log Facility, Syslog

Login Host

Description: Specifies the IP address or DNS hostname of the host to which raw TCP connections are directed.

Usage: Specify the IP address or hostname of the device.

Location: Ethernet > Connections > *any Connection profile* > Encaps Options

See Also: Login Port

Login Port

Description: Specifies the TCP port the raw TCP connection uses to connect to the specified host.

Usage: Specify the TCP port number on the login host. You can specify a value from 1 to 65535. The default is 1.

Location: Ethernet > Connection > *any Connection profile* > Encaps Options

See Also: Login Host

Login Prompt

Description: 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, you can 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 precede it with another backslash.

For example, to display the following text as a login prompt:

```
Welcome to
   \\Ascend Remote Server\\
Enter your user name:
```

you enter the following string:

```
Welcome to\n\t\\Ascend Remote Server\\\nEnter your user name:
```

Usage: Specify up to 31 characters. The default value is `Login`:

Example: `Login Prompt=`*`Enter your name:`*

Dependencies: This parameter does not apply if terminal services are disabled. If the Prompt Format parameter is set to No, this parameter is limited to 15 characters and cannot include newlines or tabs.

Location: Ethernet > Mod Config > TServ Options

Login Timeout

Description: Specifies the number of seconds a terminal-server user can use for logging in. After the specified number of seconds, the login attempt times out. A user has the total number

of seconds specified by the Login Timeout parameter to attempt a successful login. This means that the timer begins when the login prompt appears on the terminal-server screen, and continues (is not reset) when the user makes unsuccessful login attempts.

Usage: Specify from 0 to 300 seconds. The default is 300. A value of 0 (zero) disables the timer.

Example: `Login Timeout=300`

Dependencies: This parameter does not apply if terminal services are disabled.

Location: Ethernet > Mod Config > TServ Options

LoopAvoidance

Description: Specifies the number of transit PBX devices through which a call can be routed.

Usage: Specify a number from 1 to 26. The default value is 7.

Example: `LoopAvoidance=7`

Dependencies: This parameter applies only to E1 lines.

Location: Net/E1 > Line Config > Line *N*

See Also: NL Value

Low Latency Mode

Description: Enables low latency mode for real-time fax operations over networks with low packet loss and low latency characteristics. Low latency mode allows operation on networks with 2.5 seconds or less of aggregate latency between pages.

Usage: Pressing [Enter] toggles the value of the Low Latency Mode parameter between the following:

Value	Description
Yes	Enables real-time fax operations over networks with 2.5 seconds or less of aggregate latency between pages.
No	ECM is disabled. A minimum of 10 seconds delay is added to processing fax calls to allow interpretation of T.30 frames and implement spoofing.

Dependencies: The Low Latency Mode parameter has the following dependencies:

- This parameter defaults to `N/A` when a MultiVoice gateway is not hashed for real-time fax or T.38 fax processing is disabled (`T.38 Fax Enabled=No`).
- Changes to this parameter are effective with the next VoIP call.

LQM

Description: Specifies whether the MAX requests Link Quality Monitoring (LQM) when answering a PPP call. LQM counts the number of packets sent across the link and periodically asks the remote end how many packets it has received. Discrepancies are evidence of packet loss and indicate link quality problems.

Both sides of the link negotiate the interval between periodic link quality reports; however, the interval must fall between the minimum interval (LQM Min) and the maximum interval (LQM Max).

Usage: Specify Yes or No. No is the default.

- Yes enables link quality monitoring for PPP connections.
- No turns off LQM.

Location: Ethernet > Answer > PPP Options, Ethernet > Connections > *Connection profile* > Encaps Options

Dependencies: This parameter applies only to PPP and its multilink variants.

See Also: Encaps, LQM Max, LQM Min

LQM Max

Description: Specifies the maximum duration between link quality reports for PPP connections, measured in 10ths of a second.

Usage: Specify a number from 0 to 600. The default is 600.

Dependencies: This parameter applies only to PPP and its multilink variants. It is not applicable if LQM is set to No.

Location: Ethernet > Answer > PPP Options, Ethernet > Connections > *Connection profile* > Encaps Options

See Also: LQM, LQM Min

LQM Min

Description: Specifies the minimum duration between link quality reports for PPP connections, measured in 10ths of a second.

Usage: Specify a number from 0 to 600. The default is 600.

Dependencies: This parameter applies only to PPP and its multilink variants. It is not applicable if LQM is set to No.

Location: Ethernet > Answer > PPP Options, Ethernet > Connections > *Connection profile* > Encaps Options

See Also: LQM, LQM Max

LSA-Type

Description: Specifies the OSPF ASE (external link) type of this link-state advertisement.

Usage: Specify one of the following values:

- ExternalType-1 (the default)—A Type-1 external metric is expressed in the same units as the link-state metric (the same units as interface cost).
- ExternalType-2—A Type-2 external metric is considered larger than any link-state path. Use of Type-2 external metrics assumes that routing between autonomous systems is the major cost of routing a packet, and eliminates the need for conversion of external costs to internal link-state metrics.
- Internal—Specifies that this static route should be advertised in an internal LSA.

Dependencies: Keep this additional information in mind.

- The MAX advertises the static route only if the Static Route gateway has a corresponding setting in a Connection profile.
- If you set LSA-Type to Internal, the internal LSA static route appears as a stub area to external OSPF routers.

Location: Ethernet > Connections > *Connection profile* > OSPF Options, Ethernet > Mod Config > OSPF Options, Ethernet > Static Rtes

See Also: Ospf-Cost

M

Mask

Description: In a filter of type Generic, specifies an 8-byte mask to apply to the value specified by the Value parameter before the MAX compares it to the packet contents at the specified offset. You can set the parameter to specify exactly which bits you want to compare.

The MAX translates both the mask and the value specified by the Value parameter into binary format and then applies a logical AND to the results. A mask of all ones (FF FF FF FF FF FF FF FF) masks no bits, so the full value must match the packet contents. For example, with the following filter specification:

```
Filters
   Name=filter-name
   Input filters...
      In filter 01
         Generic...
            Forward=No
            Offset=2
            Length=8
            Mask=0F FF FF FF 00 00 00 F0
            Value=07 FE 45 70 00 00 00 90
            Compare=Equals
            More=No
```

and the following packet contents:

```
2A 31 97 FE 45 70 12 22 33 99 B4 80 75
```

the MAX applies the mask and compares the data as follows:

```
Value setting          07   FE   45    70    00   00   00   90
Mask                   OF  FF   FF   FF    00   00   00  F0
Result of mask         27    FE    45     70       9
```

Every bit specified by the Value parameter and not masked by the Mask setting matches the corresponding bit in the packet. Therefore, the MAX drops the packet, because the Forward parameter is set to No. The comparison works as follows:

- The MAX ignores 2A and 31 because of the two-byte offset.
- The 9 in the third byte is also ignored, because the mask has a 0 (zero) in its space. The 7 in the third byte matches the Value parameter's 7 for that byte.
- In the fourth byte, F and E match the fourth byte specified by the Value parameter.
- In the fifth byte, 4 and 5 matches the fifth byte specified by the Value parameter.
- In the sixth byte, 7 and 0 match the sixth byte specified by the Value parameter.
- The seventh (12), eighth (22), and ninth (33) bytes are ignored because the mask has zeroes in those places.
- In the tenth byte, 9 matches the Value parameter's 9 for that byte. The second 9 in the packet's tenth byte is ignored because the mask has a 0 (zero) in its place.

Usage: Specify an 8-byte hexadecimal number. The default of all zeroes means the MAX uses the data in the packet as is for comparison purposes.

Example: `Mask=0F FF FF FF 00 00 00 F0`

Location: Ethernet > Filters > Input Filters > In Filter *N* > Generic, Ethernet > Filters > Output Filters > Out Filter *N* > Generic

See Also: Length, Offset, Type, Value

Max ATMP Tunnels

Description: Defines the maximum number of active ATMP sessions for a unit configured as an ATMP Home Agent. Changes take effect after the Connection profile is saved, and the connection is cleared, then reestablished.

Usage: Press Enter to open the text field. Type the number of simultaneous ATMP sessions you want to allow through this ATMP gateway. The default, 0 (zero), disables the parameter.

Dependencies: Applies only to units configured as ATMP Home agents.

Location: Ethernet > Connections > *any Connection profi*le > Tunnel Options

See Also: ATMP Mode, ATMP gateway

MAX # ASE LSA

Description: Specifies the number of Link-State Advertisements (LSAs) the MAX unit stores before going into a state of database overload. If the unit reaches database overload, it does not accept new entries and discards self-originated entries.

Usage: Specify a value from 0 to 65536. The default is 0.

Location: Ethernet > Mod Config

See Also: OSPF

Max Baud

Description: Specifies the highest baud rate that V.34 digital modems on the MAX should attempt to negotiate. Typically, the digital modems start with the highest possible baud rate (3360) and negotiate down to the rate accepted by the far-end modem. You can adjust the maximum rate to bypass some of the negotiation cycles, provided that no inbound calls will use a baud rate higher than the rate you specify for Max Baud.

Usage: Specify the maximum baud rate. The default is 3360 baud (the highest setting).

Dependencies: This parameter is not applicable if terminal services are disabled.

Location: Ethernet > Mod Config > TServ Options

See Also: TS Enabled

Max. Block Size

Description: Specifies maximum length of a frame, in bytes, that the PAD must be able to accept from the DTE or host and process.

Usage: Specify one of the following values:

- 512 (the default)
- 1024

Dependencies: This parameter can apply even if both the host and DTE-initiated call default modes are nonlocal. This is because the mode can be changed through an opening frame.

Location: Ethernet > Connections > *Connection profile* > Encaps Options, Ethernet > Answer > T3POS Options

Max Call Duration

Description: Specifies the maximum duration, in minutes, of an established session for an incoming call. The connection is checked once per minute, so the actual time of the call will be slightly longer (usually less than a minute longer) than the actual time you set.

Usage: To set the timer, specify a value from 1 to 1440. The default is 0 (zero), which disables the timer.

Example: `Max Call Duration=0`

Location: Ethernet > Answer > Session Options, Ethernet > Connections > *Connection profile* > Session Options

Max Call Mins

Dependencies: Establishes the maximum number of minutes a call can be online at the port, regardless of bandwidth, before the MAX disconnects it. This maximum limits the usage of switched channels, even if the MAX combines these channels with nailed-up ones. Although the MAX disconnects the switched channels when a call exceeds the value of Max Call Mins, the nailed-up channels remain connected.

Usage: Specify a number from 0 to 2,142,270. The default is 0. Accepting the default disables the parameter.

Location: Host/Dual (Host/AIM6) > Port*N* Menu > Port Config

See Also: Max DS0 Mins

Max Ch Count

Description: Specifies the maximum number of channels that can be allocated to a multilink connection. For optimum performance, both sides of the connection should specify the same maximum channel count.

Usage: Specify a number from 1 to 32. The default setting is 1.

Example: `Max Ch Count=5`

Dependencies: In a Connection profile or Answer profile, this parameter applies only to MP+ calls. In a call profile, it applies only to dynamic AIM calls.

Location: Ethernet > Answer > PPP Options, Host/Dual (Host/AIM6) > Port*N* Menu > Directory > Time Period *N*, Ethernet > Connections > *Connection profile* > Encaps Options

See Also: Add Pers, Base Ch Count, Call Mgm, Encaps

Max DS0 Mins

Description: Specifies the maximum number of DS0 minutes a call can be online. In a Port Config profile, this parameter applies to calls from the AIM port within the specified time period. In the System > Sys Config profile, it applies to calls from all ports on the MAX and to the Ethernet module.

A DS0 minute is the online usage of a single 56Kbps or 64Kbps switched channel for one minute. For example, a 5-minute, 6-channel call uses 30 DS0 minutes. When the usage exceeds the maximum specified by the Max DS0 Mins parameter, the MAX cannot place any more calls, and takes any existing calls offline.

The Max DS0 Mins parameter limits usage of switched channels, even if the MAX combines these channels with nailed-up ones. Although the MAX disconnects the switched channels when a call exceeds the value of Max DS0 Mins, the nailed-up channels remain connected.

Usage: Specify a number specifying the maximum number of DS0 minutes a call can be online before the MAX disconnects it. A value of 0 (zero) is not valid for this parameter.

- In a Port Config profile, specify a number from 1 to 2,142,720 (default 1).
- In a System Sys Config profile, specify a number from 1 to 5,713,920 (default 1).

Example: `Max DS0 Mins=30`

Dependencies: This parameter does not apply if DS0 Min Rst=Off.

Location: Host/Dual (Host/AIM6) > Port*N* Menu > Port Config, System > Sys Config

See Also: DS0 Min Rst

Max Packet Length

Description: Specifies the maximum length of the packet that can be buffered.

Usage: Specify a value from 1 to 8192. If End Of Packet Detection is set to Yes and a packet has not been matched, the buffered data is flushed to TCP once the number of bytes specified by Max Packet Length is cleared.

Dependencies: Keep the following additional information in mind:

- Max Packet Length does not apply unless Encaps is set to TCP-CLEAR in the Connection profile or Detect End of Packet is set to Yes.
- Buffering a large packet size will impact the overall performance of the system, and can run the risk of running out of memory.

Location: Ethernet > Connections > *Connection profile* > Encaps Options.

See Also: Encaps, Detect End of Packet, End of Packet Pattern, Detect End of Packet, Packet Flush Time

Max Rate

Description: Allows MultiVoice to modify the rate negotiation between the originating and destination fax terminals. This improves the reliability of the fax transmission by reducing the number of lost or repeated packets which occur during high rate transmissions, and reduces the required bandwidth for fax transmissions.

Usage: Press [Enter] to toggle through a list of supported fax data transmission speeds to set the desired value. Press [Esc] to exit the profile, then write the changes to this profile. Values assigned to this parameter cause MultiVoice to do the following:

Parameter value	Specifies
14400	Default. Mask the fax capabilities in the DIS frame that support fax data transmission at rates higher than 14,400 bps.
9600	Mask the fax capabilities in the DIS frame that support fax data transmission at rates higher than 9,600 bps.
4800	Mask the fax capabilities in the DIS frame that support fax data transmission at rates higher than 4,800 bps.
2400	Mask the fax capabilities in the DIS frame that support fax data transmission at rates higher than 2,400 bps.

Example: `Max Rate =14400`

Dependencies: Changes made to this parameter are enabled for the next VoIP call

Location: Ethernet >Mod Config > RT Fax Options

Max. Time

Description: Specifies the maximum connect time, in minutes, for the ARA dial-in. The MAX initiates an ARA disconnect when the specified time is up. The ARA link goes down cleanly, but remote users are not notified. Users find out that the ARA link is gone only when they try to access a device.

Note: The Max. Time parameter is not associated with the MAX unit's idle timer.

Usage: Enter a number specifying the maximum number of minutes the connection should stay up. The default setting is 0 (zero). This setting specifies an unlimited connection time.

Dependencies: This parameter applies only to ARA connections.

Location: Ethernet > Connections > *Connection profile* > Encaps Options

See Also: Password, ARA, AppleTalk, Encaps

Max Tunnels

Description: Specifies the maximum number of tunnels that can be assigned to a Tunnel Options profile.

Usage: Specify a numerical value, from 0 to 65535. The default, 0 (zero), specifies there is no limit.

Example: `Max Tunnels=0`

Dependencies: For MAX units configured as Ascend Tunnel Management Protocol (ATMP) home agent gateways only.

Location: Ethernet > Mod Config > *any Connection profile* > Tunnel Options

See Also: ATMP HA RIP, Client ID, Home Network Name, Password, Pri. Tunnel Server, Profile Type, Sec. Tunnel Server, Tunnel Protocol, Tunnel VRouter, UDP Port

Max Leases

Description: Specifies the number of dynamic addresses to assign to Network Address Translation (NAT) clients using this connection. When NAT is used, an initial dynamic address is automatically assigned during the PPP negotiations. This address can be used to perform address translation for a single client on the LAN. When additional clients attempt to route packets through this connection, they must first be assigned their own dynamic address. The Max Leases parameter restricts the number of addresses to be given out through this connection, thus limiting the number of clients on the remote LAN who can access the Internet.

Usage: Specify the maximum number of addresses to assign to clients using this connection. The valid range is from 1 to 254. The default is 4.

Dependencies: This parameter does not apply if Reply Enabled is set to No.

Location: Ethernet > Answer > DHCP Options, Ethernet > Connections > *Connection profile* > DHCP Options

See Also: Reply Enabled

MaxTap Log Server

Description: Specifies whether to tap a connection, and indicates the IP address or symbolic hostname of the MaxTap notification server, that is, the server to which the system sends MaxTap session Start and Stop packets.

Usage: Specify an IP address in dotted-decimal notation, or a symbolic hostname of up to 31 characters. The default is null. If you specify a nondefault value, the connection will be tapped, and MaxTap session Start and Stop packets will be sent to the device you specify.

Location: Connection > *Connection profile* > Session Options

See Also: MaxTap Data Server

MaxTap Data Server

Description: Specifies the IP address or symbolic hostname of the device running the MaxTap data log server, that is, the server to which the system sends the tapped data.

Usage: Specify an IP address in dotted-decimal notation, or a symbolic hostname of up to 31 characters. The default is null. If you specify a nondefault value, the tapped data is sent to the device whose address or hostname you specify. If you accept the default, the device specified by MaxTap Log Server receives the tapped data.

Location: Connection > *Connection profile* > Session Options

See Also: MaxTap Log Server

Max Unsucc. Calls

Description: Specifies the maximum number of unsuccessful X.25 calls the MAX tries to place before dropping the modem connection.

Usage: Specify a number from 0 to 9999. The default is 10. A value of 0 (zero) specifies that the MAX never drops the modem connection because of unsuccessful X.25 calls.

Dependencies: This parameter applies only to X.25/PAD and X.25/IP connections.

Location: Ethernet > Connections > *Connection profile* > Encaps Options

Mbone Profile

Description: Specifies the name of a resident Connection profile for connection to a multicast router on the WAN. The specified Connection profile must be resident. (It cannot be accessed

via a RADIUS or TACACS server.) If the setting for Mbone Profile is null and Forwarding is turned on, the MAX assumes that its Ethernet interface is the MBONE interface.

Usage: Specify the name of the Connection profile for connection to a remote multicast router. If no name is specified, the MAX assumes the presence of a multicast router on its Ethernet interface.

Example: `Mbone profile=newyork`

Location: Ethernet > Mod Config > Multicast

Dependencies: This parameter does not apply if Forwarding is set to No.

See Also: Forwarding, Multicast Client

MD5 Key

Description: Specifies an authentication key (a password) used to allow OSPF routing. MD5 Key specifies a number from 0 to 255 that is inserted into the OSPF packet header. OSPF routers use the value of MD5 Key to allow or exclude packets from an area. The default value is `0`. The key can consist of as many as 16 characters.

Usage: Specify a key consisting of as many as 16 characters.

Example: `MD5 Key=234658902234658`

Dependencies: MD5 Key does not apply unless you set AuthType to MD5.

Location: Ethernet > Connections > *any Connection profile* > OSPF Options, Ethernet > Mod Config > OSPF Options

See Also: AuthType, Key ID

MDM Trn Level

Description: Specifies the default transmit level for a digital modem. When a modem calls the MAX unit, the unit attempts to connect at the transmit level you specify. The transmit level is the amount of attenuation, in decibels, the MAX should apply to the line, causing the line to lose power. Transmitting at a higher level of attenuation helps certain modems with near-end-echo problems. Generally, you do not need to change the transmit level. However, when the carrier is aware of line problems or irregularities, you might need to alter the modem's transmit level.

Rockwell modem code has been modified to make the transmit level programmable, so users can change the default setting for their specific connections. Transmitting at higher level of attenuation helps certain modems with near-end-echo problems.

Usage: Specify a value from -13 dB to -18 dB. The default is -13 dB.

Example: `MDM Trn Level=-13db`

Dependencies: This parameter does not apply if terminal services are disabled.

Location: Ethernet > Mod Config > TServ Options

Message Type

Description: Specifies the SNMP version (s) that the MAX unit's SNMP agent supports.

Usage: 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.

Example: `Message Type=v1-and-v3`

Location: Ethernet > Mod Config > SNMP Options

See Also: Active (SNMPv3 USM Users), Auth Protocol, Name (SNMPv3 USM Users), Passwd (SNMPv3 USM Users), Priv Protocol, R/W Access, Security Level

Message Proc Model

Description: Specifies the message-processing model to use when generating SNMP messages.

Usage: Specify one of the following values:

- V1 (the default) specifies SNMP version 1.
- V3 specifies SNMP version 3. For SNMPv3 Notifications support, specify V3.

Example: `Message Proc Model=V3`

Location: Ethernet > SNMPv3 Target Params

See Also: Active, Dest Port, Notify Tag List, Security Level, Security Model, Security Name, Tag, Target Param Name

Message Type

Description: Specifies the SNMP version(s) that the MAX unit's SNMP agent supports.

Usage: 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.

Example: `Message Type=v1-and-v3`

Location: Ethernet > Mod Config > SNMP Options

See Also: Active (SNMPv3 USM Users), Auth Protocol, Name (SNMPv3 USM Users), Passwd (SNMPv3 USM Users), Priv Protocol, R/W Access, Security Level

Method of Host Notif

Description: For DTE-initiated calls, specifies how the host is notified of the mode of the call.

Usage: Specify one of the following values:

- None (the default)—The host is not notified of the mode of the call and any data in the CUD is discarded.
- CRP—The host is informed of the mode of the call by the DTE sending a Call Request Packet (CRP) in the Call User Data (CUD) field of a control frame.
- MSF—The host is informed of the mode of the call by the DTE sending a Mode Switch Frame (MSF) after the call has been established.

Dependencies: This parameter does not apply if the opening frame is a general frame, in which case the default DTE-initiated mode is not changed.

Location: Ethernet > Connections > *Connection profile* > Encaps Options, Ethernet > Answer > T3POS Options

Metric

Description: In a Connection or Static Rtes profile, specifies a RIP metric (a virtual hop count) associated with the IP route. In the Answer profile, this parameter specifies the RIP metric of the IP link when the MAX uses RADIUS or TACACS to validate an incoming call and Use Answer as Default is enabled.

The specified metric is a virtual hop count. The actual hop count includes the metric of each switched link in the route.

If two routes have the same preference value, the MAX chooses the route with the lower metric. If you enable Routing Information Protocol (RIP) across the WAN in a Connection profile or an Answer profile, the hop count for the route can differ from the value of the Metric parameter in the Static Rtes profile, because the MAX always uses the lower hop count.

Usage: Specify a number from 1 to 15. The default setting is 7. The higher the number you specify, the less likely that the MAX will bring the link or route online.

Example: `Metric=4`

Dependencies: This parameter does not apply if the MAX does not route IP. In the Answer profile, the Use Answer as Default parameter must also be enabled.

Location: Ethernet > Answer > IP Options, Ethernet > Connections > *Connection profile* > IP Options, Ethernet > Static Rtes

See Also: Private, RIP

Min Ch Count

Description: Specifies the minimum number of channels that can be established for a multilink call. If this number of channels is not available, the multilink session is not established. For optimum performance, both sides of the multilink connection should set this parameter to the same value.

Usage: Specify a number no lower than 1 and no higher than the maximum channel count. The default setting is 1.

Example: `Min Ch Count=1`

Location: Ethernet > Answer > PPP Options, Ethernet > Connections > *Connection profile* > Encaps Options, Host/Dual (Host/AIM6) > Port*N* Menu > Directory > Time Period *N*

See Also: Call Mgm, Max Ch Count

Modem #*N* (1-8, 1-12, 1-16, 1-24, and 1-30)

Description: Quiesces a digital modem or enables a quiesced modem. Quiescing a modem is disabling it 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 to service. When you reenable the quiesced modem, a delay of up to 20 seconds can occur before the modem becomes available for service.

Usage: SpecModem—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.

- 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.

Dependencies: If ModemSlot is disabled, all the Modem #*N* parameters are unavailable.

Location: V.34 Modem > Mod Config, K56 Modem > Mod Config

See Also: ModemSlot

Modem Dialout

Description: Specifies whether a user can use this MAX unit's V.34 digital modems to dial out from the terminal-server interface. Once the connection is established, the user can issue AT commands to the modem as if connected locally to the modem's asynchronous port. If you set this parameter to No while users have active dial-out connections, those connections are not affected. However, no new modem dial-outs will be allowed.

Usage: Specify Yes or No. No is the default.

Yes enables terminal-server users to dial out using the MAX unit's digital modems.

No disables modem dial-out.

Dependencies: This parameter does not apply if terminal services are disabled.

Location: Ethernet > Mod Config > TServ Option

See Also: TS Enabled, Immediate Modem

Modem: Call-by-Call

Description: Specifies a value for call-by-call services for an outgoing modem call.

Usage: Valid entries are 0 through 31. The default value is 0. If the service provider is AT&T, the following call-by-call services are available:

- 0 (Disable call-by-call service)
- 1 (SDN, including GSDN)
- 2 (Megacom 800)
- 3 (Megacom)
- 6 (ACCUNET Switched Digital Services)
- 7 (Long Distance Service, including AT&T World Connect)
- 8 (International 800-I800)
- 16 (AT&T MultiQuest)

If the service provider is Sprint, the following VPN and GVPN call-by-call services are available:

- 0 (Reserved)
- 1 (Private)
- 2 (Inwatts)
- 3 (Outwatts)
- 4 (FX)
- 5 (Tie Trunk)

If the service provider is MCI, the following call-by-call services are available:

- 1 (VNET/Vision)
- 2 (800)
- 3 (PRISM1, PRISM II, WATS)
- 4 (900)
- 5 (DAL)

Dependencies: This parameter applies only to calls placed by the digital modems in the MAX, that is, modem dial-out. The setting of the Call-by-Call parameter in the Connection > *Connection profile*> Telco Options profile overrides the setting of the Modem: Call-by-Call parameter in the Sys Config profile.

See Also: System > Sys Config

Modem:NumPlanID

Description: 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 about when

to use each of the following settings. This parameter specifies the value of the NumberPlanID field in the called party's information element.

Note: This parameter applies only to calls placed by the digital modems in the MAX, that is, modem dial-out.

Usage: Specify one of the following values:

- Unknown—NumberPlanID=0
- ISDN (the default)—NumberPlanID=1
- Private—NumberPlanID=9

Location: Net/T1 > Line Config > Line *N*)

See Also: Modem:PRI # Type, NumPlanID (for call and Connection profiles), T1-PRI:NumPlanID (in System Dial Plan profile)

Modem:PRI # Type

Description: 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 about when to use each of the following settings. This parameter specifies the value of the TypeOfNumber field in the called party's information element.

Note: This parameter applies only to calls placed by the digital modems in the MAX, that is, modem dial-out.

Usage: Specify one of the following values:

- National—Telephone numbers within the U.S. (TypeOfNumber=2)
- Intl—Telephone numbers outside the U.S. (TypeOfNumber=1)
- Local—Telephone numbers within your Centrex group. (TypeOfNumber=4)
- Abbrev.—The telephone number is abbreviated. (TypeOfNumber=6)
- NetSpecific (currently not implemented)—The network you are connected to understands the telephone number. (TypeOfNumber=3)
- Unknown (the default)—The telephone number is none of the above. (TypeOfNumber=0)

Location: Net/T1 > Line Config > Line *N*)

See Also: Modem:NumPlanID, NumPlanID (for call and Connection profiles), T1-PRI:NumPlanID (in System Dial Plan profile)

Modem Ringback

Description: Specifies whether the MAX generates a ringback tone. By default, when the MAX answers an analog modem call, it generates a ringback tone that the calling modem hears, and then begins the modem protocol. Most modems ignore the ringback tone. However, some older modems require the MAX to generate a ringback tone.

Usage: Specify Yes or No. Yes is the default.

Yes specifies that the MAX generates a ringback tone.

No specifies that the MAX does not generate a ringback tone.

Location: Ethernet > Mod Config

ModemSlot

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

Usage: Specify one of the following values:

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

Location: V.34 Modem > Mod Config, K56 Modem > Mod Config

See Also: Modem *#N*

Module Name

Description: In the Ethernet Mod Config profile, assigns an optional name to the Ethernet interface. In Host/Dual (Host/AIM6) > Mod Config profile, this parameter assigns a name to an AIM port module, which is sent to the remote end of the connection.

Usage: Specify a name consisting of up to 16 characters. For the Ethernet interface, you can leave this parameter blank.

Location: Ethernet > Mod Config, Host/Dual (Host/AIM6) > Mod Config, Serial WAN > Mod Config

More

Description: In a filter of type Generic, specifies whether the MAX applies the conditions specified in the next In Filter *N* or Out Filter *N* subprofile before determining whether the packet matches the filter. If More is set to Yes, the MAX links the current set of filter conditions linked to the one immediately following it, so the filter can examine multiple noncontiguous bytes within a packet before the forwarding decision is made. In effect, this parameter *marries* the current filter to the next one, so that the MAX applies the next filter before making the forwarding decision. The match occurs only if *both* noncontiguous bytes contain the specified values.

Usage: Specify Yes or No. No is the default.

Yes links the current filter rule (set of conditions) to the next one, so the next filter is applied before the forwarding decision is made.

No does not link the current filter rule. The forwarding decision is based solely on the rule.

Example: `More=Yes`

Dependencies: The next filter must be enabled.

Location: Ethernet > Filters > Input Filters > In Filter *N* > Generic, Ethernet > Filters > Output Filters > Out Filter *N* > Generic

See Also: Forward, Length, Offset, Type, Value, Valid

MP

Description: Enables incoming Multilink Protocol (MP) connections, which use RFC 1990 encapsulation. MP enables the MAX to interact with MP-compliant equipment from other vendors to use multiple channels for a call. Both connection sides must support MP.

Usage: Specify Yes or No. Yes is the default.

Yes specifies that the MAX answers MP calls if they meet all other connection criteria.

No specifies that the MAX will not accept inbound MP calls.

Location: Ethernet > Answer > Encaps

See Also: Encaps

MPP

Description: Enables incoming Multilink Protocol Plus (MP+) connections, which use PPP encapsulation with Lucent extensions. MP+ enables the MAX to use multiple channels to connect to another MAX unit.

Usage: Specify Yes or No. Yes is the default.

Yes specifies that the MAX answers MP+ calls if they meet all other connection criteria.

No specifies that the MAX will not accept inbound MP+ calls.

Location: Ethernet > Answer > Encaps

See Also: Encaps, MP

MRU

Description: Specifies the maximum number of bytes the MAX can receive in a single frame. Usually the default is the proper setting, unless the far end requires a lower number.

Third-party devices can calculate MRU differently. If you connect to a non-Lucent device, you might need to specify a different MRU to match frame size between the two devices.

Usage: Specify a number lower than the default MRU if the far end requires it.

- In the Answer profile or a Connection profile, specify a number from 1 to 1524.
- In a Frame Relay profile, specify a number from 128 to 1600.
- In an X.25 profile, specify a number from 1 to 1500.

Example: `MRU=1524`

Location: Ethernet > Answer > PPP Options, Ethernet > Connections > *Connection profile* > Encaps Options, Ethernet > Frame Relay

See Also: Encaps

Multicast Addr

Description: Specifies a valid class D address, which enables IP multicasting in a stacked-MAX environment.

Usage: Specify, in dotted-decimal format, a valid class D address from 224.0.0.0 to 239.255.255.255. The default setting is 239.192.74.72, an IP address that is within the local scope of the organization.

Example: `Multicast Addr=224.2.24.61`

Dependencies: If the multicast address you specify is not a valid Class D address, the following error message appears:

```
Stack Multicast Address
should be in CLASSD
address range.
```

If the address you specify is already in use by some other application, the following error message appears:

```
Stack Multicast Address
already exists in routing
table.  Choose another.
```

Location: Ethernet > Mod Config > Stack Options

Multicast Client

Description: Enables the MAX to respond to multicast clients on the WAN link. Clients cannot be supported on the MBONE interface, which means another WAN link or the local Ethernet network supports a multicast router.

When this parameter is set to Yes, the MAX begins handling IGMP requests and responses on the interface. It does not begin forwarding multicast traffic until the rate limit is set.

Usage: Specify Yes or No. No is the default.

Yes enables the MAX to respond to IGMP client requests and responses on the interface.

No specifies the MAX does not respond to multicast clients on the interface.

Example: `Multicast Client=Yes`

Dependencies: This parameter is not applicable if the Connection profile in which it resides is the Mbone profile (linking to a remote multicast router). See Multicast Rate Limit for related dependencies.

Location: Ethernet > Connections > *Connection profile* > IP Options

See Also: Multicast Rate Limit

Multicast Grp Leave Delay

Description: Specifies the number of seconds the MAX waits before forwarding an IGMP version 2 `leave group use` message from a multicast client.

Usage: Specify a number of seconds from 0 to 120. The default is 0 (zero). If you specify a value other than the default and the MAX unit receives a `leave group` message, the unit sends an IGMP query to the WAN interface or client from which it received the `leave group` message. If the MAX does not receive a response from an active multicast client that belongs to the client group, it sends a `leave group` message when the time you specify expires.

If you accept the default, the MAX forwards a `leave group` message immediately. If users might establish multiple multicast sessions for identical groups, set Multicast Grp Leave Delay to a value of 10 to 20 seconds.

Example: `Multicast Grp Leave Delay=15`

Location: Ethernet > Connections > *Connection profile* > IP Options

Multicast Rate Limit

Description: Specifies the rate at which the MAX accepts multicast packets from clients on this interface. This parameter does not affect the MBONE interface.

Note: By default, this parameter is set to 100, *which disables multicast forwarding on the interface.* The forwarder handles IGMP packets, but does not accept packets from clients or forward multicast packets from the MBONE router.

To begin forwarding multicast traffic on the interface, you must set the rate limit to less than 100. For example if you set it to 5, the MAX accepts a packet from multicast clients on the interface every 5 seconds. Subsequent packets received in that 5-second window are discarded.

Usage: Specify a value of less than the default of 100 to begin forwarding multicast traffic.

Example: `Multicast Rate Limit=5`

Dependencies: This parameter has no effect when applied to the MBONE interface.

Location: Ethernet > Connections > *Connection profile* > IP Options

See Also: Multicast Client

N

N2 Retran Count

Description: Specifies the retry limit—the maximum number of times the MAX can retransmit a frame on an X.75 connection when the T1 Retran Timer expires.

Usage: Specify a number from 2 to 15. The default value is 10. A higher value increases the probability of a correct transfer of data. A lower value allows for quicker detection of a permanent error condition.

Location: Ethernet > Answer > X.75 Options

See Also: Frame Length, K Window Size, T1 Retran Timer, X.75

N391

Description: Specifies the interval at which the MAX requests a Full Status Report on a Frame Relay link.

Usage: Specify a number from 1 to 255 seconds. The default is 6.

Example: `N391=15`

Dependencies: This parameter does not apply if FR Type is set to DCE.

Location: Ethernet > Frame Relay

See Also: Link Mgmt

Nailed Grp

Description: In a serial WAN profile, specifies the group number that supports the serial WAN connection. When you configure a nailed connection, you must assign a group number to each nailed channel. Nailed channels can share group numbers. In a Frame Relay or X.25 profile, this parameter assigns those channels to the link represented by the profile. Only one active link can be assigned to use a particular group number.

Usage: In a serial WAN profile, specify a number from 1 to 60 (default 1). In a Frame Relay or X.25 profile, specify the number assigned to a nailed T1 line or serial WAN.

Example: `Nailed Grp=5`

Location: Ethernet > Frame Relay, Serial WAN > Mod Config, Ethernet > X.25

See Also: Activation, Call Type, Ch *N* Prt/Grp, Group

Name

Description: Specifies the name of a profile, host, Dial Plan, or user.

Note: When the Name parameter specifies an existing host, user, the MAX system itself, or a Firewall profile, the name is case sensitive. The name you specify must be unique within the

list of profiles of the same type. In addition, Lucent strongly recommends that you do not use the same name for a Names/Passwords profile and a Connection profile.

Usage: Specify a name.

- In most profiles, the name can consist of up to 16 characters.
- In the X.25 profile, the name is limited to 15 characters.
- In the Names/Passwords profile, Static Rtes profile, and SNMP Traps profile, the name can consist of up to 31 characters.

Example: `Name=PacBell`

Location: Host/Dual (Host/AIM6) > Port*N* Menu > Directory, Host/BRI > Line Config, Net/BRI > Line Config, Net/T1 > Line Config, Net/E1 > Line Config, BRI/LT > Line Config, System > Destinations, System > Dial Plan, Ethernet > Filters, Ethernet > Firewalls, Ethernet > Frame Relay, Ethernet > IPX SAP Filters, Ethernet > Static Rtes, System > Security, Ethernet > SNMP Traps, System > Sys Config, Ethernet > X.25, Ethernet > Names/Passwords

Name (FXS Config)

Description: Specifies the name of a profile.

Usage: Specify a name. The name can be up to 15 (0-15) characters in length. The default is null.

Location: Analog FXS > FXS Config > *FXS Configuration profile;* System > Numbering Plan > *Numbering Plan profile;* System > Call Routes > *Call Routes profile*

Name (SNMPv3 USM Users)

Description: Specifies the user (in the SNMPv3 USM Users profile) for whom the MAX unit exchanges an SNMPv3 USM message.

Note: When the Name parameter specifies an existing host, user, the MAX unit, or a Firewall profile, the name is case sensitive. The name you specify must be unique within the list of profiles of the same type. In addition, do not use the same name for a Names/Passwords profile and a Connection profile.

Usage: Specify a name that contains up to 16 characters.

`Example:` `Name=PacBell`

Location: Ethernet > SNMPv3 USM Users > *any SNMPv3 USM Users profile*

See Also: Active (SNMPv3 USM Users), Auth Protocol, Message Type, Passwd (SNMPv3 USM Users), Priv Protocol, R/W Access, Security Level

NAS Port Type

Description: Specifies the type of calls that can be received.

Usage: Specify Analog, Digital, or Any (the default, which specifies both types).

Following are the settings for the RADIUS NAS-Port-Type attribute and the analogous settings for the NAS Port Type parameter:

Attribute setting	Parameter settings
Async	Analog, Any
Sync	Digital, Any
ISDN_Sync	Digital, Any
ISDN_Async_V120	Digital, Any
ISDN_Asyn_V110	Digital, Any
Virtual	Any
ISDN_Async_V32	Digital, Any
ISDN_Async_VDSP	Any

Example: `NAS Port Type=Digital`

Location: Ethernet > Connections > *Connection profile* > Telco Options

Net Adrs

Description: In a Bridge Adrs profile, specifies the IP address of a device at the remote end of the link. If you are bridging between two segments of the same IP network, you can use the Net Adrs parameter in a Bridge Adrs profile to enable the MAX to respond to ARP requests while bringing up the bridged connection. If an ARP packet contains an IP address that matches the setting of the Net Adrs parameter in a Bridge Adrs profile, the MAX responds to the ARP request with the Ethernet (physical) address specified in the Bridge Adrs profile and brings up the specified connection. In effect, the MAX acts as a proxy for the node that actually has that address.

Usage: Specify the IP address of the device on the remote network.

Example: `Net Adrs=10.207.23.101/24`

Location: Ethernet > Bridge Adrs

See Also: Enet Adrs

NetWare t/o

Description: Specifies the number of minutes the MAX will enable clients to remain logged into a NetWare server even though their IPX connection has been torn down.

NetWare servers send out NCP watchdog packets to monitor which logins are active and logout inactive clients. Only clients that respond to watchdog packets remain logged in.

Repeated watchdog packets would cause a WAN connection to stay up, but if the MAX simply filtered those packets, client logins would be dropped by the remote server. To prevent repeated client logouts while allowing WAN connections to be brought down in times of inactivity, the MAX responds to NCP watchdog requests as a proxy for clients on the other

side of an offline IPX routing or IPX bridging connection. Responding to these requests is commonly called watchdog spoofing.

To the server, a spoofed connection looks like a normal, active client login session, so it does not log the client out. The timer begins counting down as soon as the link goes down. At the end of the selected time, the MAX stops responding to watchdog packets and the client-server connections can be released by the server. If there is a reconnection of the WAN session before the end of the selected time, the timer is reset.

Note: The MAX filters watchdog packets automatically on all IPX routing connections and all IPX bridging connections that have watchdog spoofing enabled. The MAX applies a call filter implicitly, which prevents the Idle timer from resetting when IPX watchdog packets are sent or received. This filter is applied after the standard data and call filters.

Usage: Specify a number of minutes from 0 to 65535. The default value is 0 (zero); when you accept the default, the MAX responds to server watchdog requests indefinitely.

Example: `NetWare t/o=30`

Dependencies: This parameter does not apply if the MAX does not support IPX.

Location: Ethernet > Connections > *Connection profile* > IPX Options

See Also: Handle IPX

Net End

Description: Used in conjunction with Net Start to indicate the end of the zone range that defines the networks available for packets that are to be routed to this static route. If the MAX is an AppleTalk router, it brings up the line when it receives packets addressed to the network number (defined by Net Start and Net End) or zone name specified for the remote connection, and routes packets to the appropriate network or zone.

Usage: Valid entries for this field are in the range from 1 to 65199. If there are other AppleTalk routers on the network, it is necessary to configure the network ranges to coincide with the other routers on the LAN.

Dependencies: The following must be true:

- AppleTalk=Yes in the Ethernet Configuration menu.
- AppleTalk Router=On in the profile's AppleTalk Options submenu.
- Peer=Router in the profile's AppleTalk Options submenu.
- A valid value is entered for Net Start.

Location: Ethernet > Connections > *Connection profile* > AppleTalk Options

See Also: Peer (AppleTalk), Net Start, AppleTalk, AppleTalk Router, Route AppleTalk

Net Start

Description: Used in conjunction with Net End to indicate the beginning of the zone range that defines the networks available for packets that are to be routed to this static route. If the MAX is an AppleTalk router, it brings up the line when it receives packets addressed to the

network number (defined by Net Start and Net End) or zone name specified for the remote connection, and routes packets to the appropriate network or zone.

Usage: Valid entries for this field are in the range from 1 to 65199. If there are other AppleTalk routers on the network, it is necessary to configure the network ranges to coincide with the other routers on the LAN.

Dependencies: The following must be true:

- AppleTalk=Yes in the Ethernet Configuration menu.
- AppleTalk Router=On in the profile's AppleTalk Options submenu.
- Peer=Router in the profile's AppleTalk Options submenu.
- A valid value is entered for Net End.

Location: Ethernet > Connections > *Connection profile* > AppleTalk Options

See Also: Peer (AppleTalk), Net End, AppleTalk, AppleTalk Router, Route AppleTalk

Network

Description: Specifies the network that can be reached through this static IPX route. If this is an external IPX network number, do not set Server Name or Server Type. If the network number is an internal network number of a server, make sure you specify Server Name and Server Type. If you are not familiar with internal network numbers, see Novell documentation.

Usage: Specify the NetWare network number. The values 00000000 and ffffffff are not valid.

Example: `Network=A00100001`

Dependencies: This parameter does not apply if the IPX routing is not enabled.

Location: Ethernet > IPX Routes

See Also: Route IPX

New NASPort ID

Description: Specifies the format the MAX recognizes for the NAS-Port (5) RADIUS attribute.

Usage: Specify one of the following:

- Yes specifies that the MAX recognizes the format that specifies a shelf, slot, line, and channel number. This format is the one recognized by the MAX TNT.
- No specifies that the MAX recognizes the five-digit format that specifies the type of service in use, and the line and channel number. The default value is No.

Location: System > Sys Config

NFAS ID num

Description: Establishes an interface ID for a line using Non-Facility Associated Signaling (NFAS). You must assign a different interface ID for each NFAS line.

Usage: Specify a number between 0 and 31. The default is 1 for line #1 and 2 for line #2.

Dependencies: This applies only if the signaling mode is ISDN_NFAS.

Location: Net/T1 > Line Config > Line *N*

See Also: Sig Mode

NL Value

Description: Specifies the number of retransmissions to send on an E1 line. The default value is required when the line connects to a DPNSS or DASS-2 switch.

Usage: Specify a number between 1 and 255. The default is 64.

Example: `NL Value=64`

Dependencies: This parameter applies only to E1 lines. It must be set to its default value when the line connects to a DPNSS or DASS-2 switch.

Location: Net/E1 > Line Config > Line N

See Also: Switch Type

Node

Description: Specifies the node address on the internal network number of the server that will be reached through this static IPX route. If you are not familiar with internal network numbers, see the Novell documentation.

Usage: Specify the server's node address on its own internal network. Typically, a server running NetWare 3.11 or later has a node number of 0000000000001.

Dependencies: This parameter does not apply if the IPX routing is not enabled.

Location: Ethernet > IPX Routes

See Also: Route IPX, Network

Non-Multicast

Description: Specifies whether all multicast packets are remapped to a directed neighbor address.

Usage: Specify Yes or No. The default is No.

- Yes specifies that all multicast packets are remapped to a directed neighbor address, enabling adjacencies to form between neighbors. This setting is ignored on Ethernet (a broadcast network). Its use is not recommended for unnumbered interfaces. If you specify it for a non-numbered interface, the MAX drops the packets.
- No specifies that multicast packets are not remapped to a directed neighbor address.

Example: `NonMulticast=yes`

Location: Ethernet > Connections > *Connection profile* > OSPF options

No Trunk Alarm

Description: Specifies whether the back panel alarm relay closes when all T1 PRI lines (or trunks) go out of service. The MAX has an alarm relay whose contacts remain open on the back panel's alarm relay terminal block during normal operation. If you enable them, the alarm relay contacts close during loss of power, hardware failure, or a system reset. The No Trunk Alarm parameter enables you to specify whether the contacts also close when all T1 PRI lines go out of service.

Usage: Specify Yes or No. No is the default.

- Yes specifies the MAX closes the back panel alarm relay when all trunks go out of service.
- No specifies the MAX records the event in the log but does not close the alarm relay.

Location: System > Sys Config

Notify Tag List

Description: Specifies the tag list indicated by the Tag value in each SNMPv3 Notifications submenu.

Usage: Specify the Tag value(s) you indicated in one or more SNMPv3 Notifications submenus.

Example: `Notify Tag List=default1`

Location: Ethernet > SNMP Traps

See Also: Active, Dest Port, Message Proc Model, Security Level, Security Model, Security Name, Tag, Target Param Name

NSSA-Type

Description: Specifies whether or not area border routers convert this ASE type-7 to an ASE type-5 LSA. It applies only when the MAX is routing within an OSPF NSSA (that is, where AreaType is set to NSSA on all interfaces running OSPF). ASE type-7s can be imported only from static route definitions. NSSAs are described in RFC 1587.

Usage: Specify one of the following values:

- N/A (the default)
- Advertise (for area border routers to convert this type-7 to a type-5)
- DoNotAdvertise (for area border routers not to convert this type-7 to a type-5)

Dependencies: Keep this additional information in mind:

- Third Party is not applicable when the MAX is configured as an NSSA.
- NSSA-Type is not applicable unless Area-Type is set to NSSA.

Location: Ethernet > Static Rtes > *any Static Rtes profile*

NUI

Description: Specifies the set of Network User Identification (NUI) related facilities to use in the next call request. NUI provides information to the network for purpose of billing, security, network management, or to invoke subscribed facilities.

Usage: Specify the NUI to use in the next call request.You can specify up to six digits. The default is null.

Dependencies: Encaps must be set to X25/PAD for NUI to be applicable.

Location: Ethernet > Connections > *Connection profile* > Encaps options, Ethernet > Answer > PAD options, Ethernet > Answer > T3POS options

NUI prompt

Description: The Network User Identification (NUI) prompt parameter specifies the NUI prompt for a PAD application.

Usage: You can specify up to 15 characters. The default is null. A value in NUI prompt overrides any value entered in the NUI setting.

Dependencies: Encaps must be set to X25/PAD for NUI to be applicable.

Location: Ethernet > Connections > *Connection profile* > Encaps options

NUI PW prompt

Description: The NUI PW prompt specifies the Network User Identification (NUI) password prompt for a PAD application. This parameter is used as Call User Data in the outbound Call Request Packet.

Usage: You can specify up to 12 characters. The default is null.

Location: Ethernet > Connections > *Connection profile* > Encaps options

Number Digits

Description: Specifies the exact number of digits in a phone number matching this profile's Dial Prefix setting.

Usage: Specify a value from 1 to 24.

Location: System > Numbering Plan > *Numbering Plan profile*

NumPlanID

Description: 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 following settings. This parameter specifies NumberPlanID field in the called party's information element.

Usage: Specify one of the following values:

- Unknown (NumberPlanID=0)
- ISDN (the default) (NumberPlanID=1)
- Private (NumberPlanID=9)

Dependencies: The value you specify for NumPlanID in the Dial Plan profile overrides the value of NumPlanID in the call profile and Connection profile if you have enabled the unit's Dial Plan profiles.

Location: Host/Dual (Host/AIM6) > Port*N* Menu > Directory (Call profiles), Ethernet > Connections > *Connection profile*, System > Dial Plan, Ethernet > Frame Relay, Ethernet > X.25

See Also: PRI # Type, Call-by-Call, T1-PRI:NumPlanID (Line profiles), Modem:NumPlanID (System profile)

O

Offset

Description: In a filter of type Generic, specifies a byte-offset from the start of a frame to the data in the packet to be tested against this filter. For example, with this filter specification:

```
Filters
   Name=filter-name
   Input filters...
      In filter 01
         Generic...
            Forward=No
            Offset=2
            Length=8
            Mask=0F FF FF FF 00 00 00 F0
            Value=07 FE 45 70 00 00 00 90
            Compare=Equals
            More=No
```

and the following packet contents:

```
2A 31 97 FE 45 70 12 22 33 99 B4 80 75
```

The first two byes in the packet (2A and 31) are ignored due to the two-byte offset.

Note: If the current filter is linked to the previous one (if More=Yes in the previous filter), the offset starts at the endpoint of the previous segment.

Usage: Specify a number indicating a byte-offset.

Example: `Offset=2`

Location: Ethernet > Filters > Input filters > In filter *N* > Generic, Ethernet > Filters > Output filters > Out filter *N* > Generic

See Also: Length, Mask, More

Operations

Description: Enables or disables permission to view MAX profiles and to change the value of any parameter. When it is disabled, users can view MAX profiles, but cannot change the value of any parameter (read-only security). In addition, when this permission is disabled, users cannot access most DO commands. Only DO Esc, DO Close Telnet, and DO password are available.

Note: If this permission is disabled, all other permissions are disabled as well.

Usage: Specify Yes or No. Yes is the default.

- Yes specifies the user can view and edit profiles.
- No disables this permission as well as all other permissions in the Security profile.

Example: `Operations=No`

Location: System > Security

Option

Description: Specifies the criteria the MAX uses to select a trunk group when it places a call from a Destination profile. Each Destination profile contains six Call-by-Call N and Dial N# parameters. Therefore, you can configure up to six options for reaching the destination device. The Option parameter helps the MAX select which option to use.

Usage: Specify one of the following values:

- 1st Avail specifies that the MAX selects the first trunk group that has enough available bandwidth to meet the base bandwidth requirements of the call profile (as defined by the Base Ch Count parameter).

  If no group has enough bandwidth, the MAX drops the call.

  1st Avail is the default.
- 1st Active specifies the first trunk group that has at least one available channel.

  If you choose this setting, set the Port profile parameter Fail Action=Reduce so that the MAX does not disconnect the call even if the full base bandwidth specified by Base Ch Count is not available.
- Any specifies that the MAX uses any combination of circuits from any trunk group to make the call.

  Note that the MAX does not allow you to combine channels from trunk groups of different carriers to obtain a full base bandwidth.

Location: System > Destinations

See Also: B1 Trnk Grp, B2 Trnk Grp, Base Ch Count, Call-by-Call *N*, Ch *N* Trnk Grp, Dial *N#*, Fail Action

OSPF

Description: Enables OSPF traps.

Usage: Specify Yes or No. The default is No.

Dependencies: 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.

Location: Ethernet > SNMP Traps > *any profile*

See Also: MAX # ASE LSA

OSPF ASE Preference

Description: Specifies the OSPF ASE Preference the MAX uses when importing an ASE.

Usage: Specify a value from 0 to 255. A value of 255 means that the MAX never puts any ASEs into the routing table.

Example: The default route preferences are:

- `Connected routes 0`
- `OSPF internal routes 10`
- `ICMP routes 30`
- `Static routes 60`
- `RIP routes 100`
- `Unconnected WAN routes 120`
- `OSPF ASE 150`
- `Do not use route 255`

Dependencies: When specifying a preference for a route, make sure that routes that are learned from more reliable sources have a lower preference (and are therefore more likely to be used).

When specifying a preference for a route, you should set a lower preference for connected routes than for disconnected routes.

Location: Ethernet > Mod Config > Route Pref

OSPF If AuthFailure

Description: 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.

Usage: Specify Yes or No. The default is No.

Dependencies: This parameter does not apply if you set Ethernet > SNMP Traps > *any profile* > OSPF to No.

Location: Ethernet > SNMP Traps > Enable Traps

See Also: OSPF

OSPF If ConfigError

Description: 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.

Usage: Specify Yes or No. The default is No.

Dependencies: This parameter does not apply if you set Ethernet > SNMP Traps > *any profile* > OSPF to No.

Location: Ethernet > SNMP Traps > Enable Traps

See Also: OSPF

OSPF If RxBadPacket

Description: Sends the OSPF If RxBadPacket trap when the MAX unit receives an OSPF packet on a nonvirtual interface that cannot be parsed.

Usage: Specify Yes or No. The default is No.

Dependencies: This parameter does not apply if you set Ethernet > SNMP Traps > *any profile* > OSPF to No.

Location: Ethernet > SNMP Traps > Enable Traps

See Also: OSPF

OSPF If StateChange

Description: Sends the OSPF If StateChange trap when there has been a change in the state of a nonvirtual OSPF interface.

Usage: Specify Yes or No. The default is No.

Dependencies: This parameter does not apply if you set Ethernet > SNMP Traps > *any profile* > OSPF to No.

Location: Ethernet > SNMP Traps > Enable Traps

See Also: OSPF

OSPF LsdbApprchngOvrflw

Description: Sends the OSPF LsdbApprchngOvrflw trap when the number of LSAs in the router's link-state database has exceeded ninety percent of `ospfExtLsdbLimit`.

Usage: Specify Yes or No. The default is No.

Dependencies: This parameter does not apply if you set Ethernet > SNMP Traps > *any profile* > OSPF to No.

Location: Ethernet > SNMP Traps > Enable Traps

See Also: OSPF

OSPF LsdbOverflow

Description: Sends the OSPF LsdbOverflow trap when the number of LSAs in the router's link-state database has exceeded `ospfExtLsdbLimit`.

Usage: Specify Yes or No. The default is No.

Dependencies: This parameter does not apply if you set Ethernet > SNMP Traps > *any profile* > OSPF to No.

Location: Ethernet > SNMP Traps > Enable Traps

See Also: OSPF

OSPF MaxAgeLsa

Description: Sends the OSPF MaxAgeLsa trap when the age of one of the LSAs in the router's link-state database reached the MaxAge value.

Usage: Specify Yes or No. The default is No.

Dependencies: This parameter does not apply if you set Ethernet > SNMP Traps > *any profile* > OSPF to No.

Location: Ethernet > SNMP Traps > Enable Traps

See Also: OSPF

OSPF Nbr StateChange

Description: Sends the OSPF Nbr StateChange trap when there has been a change in the state of a nonvirtual OSPF neighbor.

Usage: Specify Yes or No. The default is No.

Dependencies: This parameter does not apply if you set Ethernet > SNMP Traps > *any profile* > OSPF to No.

Location: Ethernet > SNMP Traps > Enable Traps

See Also: OSPF

OSPF OriginateLsa

Description: Indicates the number of new Link-State Advertisements (LSAs) that have been originated.

Usage: Specify Yes or No. The default is No.

Dependencies: This parameter does not apply if you set Ethernet > SNMP Traps > *any profile* > OSPF to No.

Location: Ethernet > SNMP Traps > Enable Traps

OSPF

OSPF Preference

Description: Specifies the preference value for routes learned from the OSPF protocol.

When choosing which routes to put in the routing table, the router first compares the OSPF Preference values, preferring the lower number. If the OSPF Preference values are equal, the router compares the Metric values, using the route with the lower Metric. These are the default values for other types of routes:

- Routes learned from ICMP Redirects=30
- Routes learned from RIP=100
- Static routes from IP address pools, RADIUS authentication, and the terminal server iproute add command=100
- Static routes in an IP Route profile or Connection profile=100

Usage: Specify a number between 0 and 255. The default value is 10. Zero is the default for connected routes (such as the Ethernet). The value of 255 means *Do not use this route*.

Location: Ethernet > Mod Config > Route Pref

OSPF TxRetrans

Description: Sends the OSPF TxRetransmit trap when the MAX unit retransmits an OSPF packet on a nonvirtual interface.

Usage: Specify Yes or No. The default is No.

Dependencies: This parameter does not apply if you set Ethernet > SNMP Traps > *any profile* > OSPF to No.

Location: Ethernet > SNMP Traps > Enable Traps

See Also: OSPF

OSPF VirtIf AuthFailure

Description: 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.

Usage: Specify Yes or No. The default is No.

Dependencies: This parameter does not apply if you set Ethernet > SNMP Traps > *any profile* > OSPF to No.

Location: Ethernet > SNMP Traps > Enable Traps

See Also: OSPF

OSPF VirtIf ConfigError

Description: 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.

Usage: Specify Yes or No. The default is No.

Dependencies: This parameter does not apply if you set Ethernet > SNMP Traps > *any profile* > OSPF to No.

Location: Ethernet > SNMP Traps > Enable Traps

See Also: OSPF

OSPF VirtIf StateChange

Description: Sends the OSPF VirtIf StateChange trap when there has been a change in the state of an OSPF virtual interface.

Usage: Specify Yes or No. The default is No

Dependencies: This parameter does not apply if you set Ethernet > SNMP Traps > *any profile* > OSPF to No.

Location: Ethernet > SNMP Traps > Enable Traps

See Also: OSPF

OSPF VirtIf RxBadPacket

Description: Sends the OSPF VirtIf RxBadPacket trap when the MAX unit receives, on a virtual interface, an OSPF packet that cannot be parsed.

Usage: Specify Yes or No. The default is No.

Dependencies: This parameter does not apply if you set Ethernet > SNMP Traps > *any profile* > OSPF to No.

Location: Ethernet > SNMP Traps > Enable Traps

See Also: OSPF

OSPF VirtIf TxRetransmit

Description: Sends the OSPF VirtIf TxRetransmit trap when the MAX unit retransmits an OSPF packet on a virtual interface.

Usage: Specify Yes or No. The default is No.

Dependencies: This parameter does not apply if you set Ethernet > SNMP Traps > *any profile* > OSPF to No.

Location: Ethernet > SNMP Traps > Enable Traps

See Also: OSPF

OSPF VirtNbr StateChnge

Description: Sends the OSPF VirtNbr StateChnge trap when there has been a change in the state of an OSPF virtual neighbor.

Usage: Specify Yes or No. The default is No.

Dependencies: This parameter does not apply if you set Ethernet > SNMP Traps > *any profile* > OSPF to No.

Location: Ethernet > SNMP Traps > Enable Traps

See Also: OSPF

Ospf-Cost

Description: Specifies the cost of an OSPF route. The interpretation of this cost depends on the type of external metrics set in the ASE-type parameter. 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. Any Type 2 metric is considered greater than the cost of any path internal to the AS (autonomous system).

Usage: Specify a number greater than zero. The default is 1.

Example: `Ospf-Cost=1`

Location: Ethernet > Static Rtes > *any profile*

See Also: ASE-type, ASE-tag

Overlap Receiving

Description: Enables or disables overlap receiving for incoming calls on the PRI line. Overlap receiving affects the procedure of establishing an incoming call received on a T1 or E1 PRI line on the unit. When using overlap receiving, the unit can use a series of information messages to gather the complete called-number from the network switch, enabling the use of features such as called-number authentication.

The Q.931 specification permits either en-bloc receiving or overlap receiving for an incoming call. With en-bloc receiving, the Setup message received from the network switch must contain all information required to process the call. With overlap receiving, the Setup message can contain incomplete called-number information, with the remainder (if any) sent in one or more additional Information messages after the network switch receives a Setup Acknowledge message from the called unit.

Usage: Specify Yes or No. The default is No.

Example: `Overlap Receiving=Yes`

Dependencies: Overlap Receiving is N/A if Sig Mode is not configured as ISDN for T1, ISDN_NFRAS for T1, or ISDN for E1.

Net/T1 > Line Config > *any Net/T1 line* > Line 1

Own Port Diag

Description: Enables or disables permission to perform the commands in the Port Diag menu for the AIM port that was called.

Note: To completely disable the user's ability to perform diagnostics for the called port, you must also disable All Port Diag.

Usage: Specify Yes or No. Yes is the default if All Port Diag is set to No.

- Yes specifies the user can use the diagnostic commands in the Port Diag menu for the AIM port that was called.
- No disables this permission.

Dependencies: This parameter is not applicable if the Operations permission is disabled or if All Port Diag is set to Yes.

Location: System > Security

See Also: All Port Diag

P

Packet Characters

Description: Specifies the minimum number of bytes of received data that should accumulate before the data is passed up the protocol stack for encapsulation.

Usage: Specify an integer between 0 and 500. The default value is 0 (zero).

Dependencies: If your application is so specialized that it demands you use this parameter, be sure to set the Packet Wait Time parameter to an appropriate value. This parameter does not apply if terminal services are disabled.

Location: Ethernet > Mod Config > TServ Options

See Also: Packet Wait Time

Packet Flush Length

Description: Specifies the maximum number of bytes to buffer when handling incoming TCP-Clear data that does not require V.120 processing. If the system buffers the specified number of bytes without matching the End of Packet Pattern value, the MAX flushes the buffer by writing the data into TCP packets.

Usage: Specify an integer from 1 to 8192. The default is 256. Note that buffering large packets consumes a larger amount of system resources than buffering small packets.

Example: `Packet Flush Length=300`

Dependencies: If Detect End of Packet=No, Packet Flush Length does not apply.

Location: Ethernet > Answer > TCP-CLEAR options

See Also: Detect End of Packet, End of Packet Pattern, Packet Flush Time

Packet Flush Time

Description: Specifies the amount of time (in milliseconds) to buffer TCP-Clear data that does not require V.120 processing. The timer begins counting down upon receiving the first byte of buffered data. If the specified number of milliseconds elapses before the buffered data matches the End of Packet Pattern value, the MAX flushes the buffer by writing the data into TCP packets.

Usage: Specify an integer from 1 to 1000. The default is 20.

Example: `Packet Flush Time=300`

Dependencies: If Detect End of Packet=No, Packet Flush Time does not apply.

Location: Ethernet > Answer > TCP-CLEAR options, Ethernet > Connection > *any Connection profile* > Encaps Options

See Also: Detect End of Packet, End of Packet Pattern, Packet Flush Length

Packet Redundancy

Description: Causes the MAX to append a designated number of previously sent packets onto the current packet. On networks experiencing measurable packet loss, this improves the reliability of the fax transmission.

Usage: Press [Enter] to the edit field for Packet Redundancy, then enter a value between `0` and `5`. Press [Enter] again to save the new value for this parameter. Press [Esc] to exit the profile, then write the changes to this profile. Values assigned to this parameter cause MultiVoice to do the following:

Parameter value	Specifies
0	No change from the default packet behavior.
1	Append and send the previous fax packet with the current fax packet.
2	Append and send the two previous fax packets with the current fax packet.
3	Append and send the three previous fax packets with the current fax packet.
4	Append and send the four previous fax packets with the current fax packet.
5	Append and send the five previous fax packets with the current fax packet.

Example: `Packet Redundancy =2`

Dependencies: The following dependencies apply to this parameter:

- Once saved, packet redundancy is enabled with the next VoIP call.
- This value is set to `N/A` when `Fixed Packets=No`.

Location: Ethernet > Mod Config > RT Fax Options

Packet Wait time

Description: Specifies the maximum amount of time in milliseconds that any received data can wait before being passed up the protocol stack for encapsulation.

Usage: Specify an integer between 0 and 600 milliseconds. The default value is 0 (zero).

Dependencies: If your application is so specialized that it demands you use this parameter, be sure to take into account your modem speeds when calculating its value. This parameter does not apply if terminal services are disabled.

Location: Ethernet > Mod Config > TServ Options

See Also: Packet Characters

PAD Alias *N*

Description: Specifies a string for single-command substitution. For one command string (including a space) to be treated as equivalent to another, you must enter a slash (/) between the two strings.

Usage: You can specify three aliases of up to 40 characters each. The default is null.

Dependencies: Encaps must be set to X25/PAD for PAD Alias to be applicable.

Location: Ethernet > Connections > *Connection profile* > Encaps options

PAD banner msg

Description: Specifies the banner message that the user or a calling device sees when starting an X.25 PAD (Triple-X) session on the MAX. The PAD user can either be a user or a calling device running a script.

Usage: You can specify up to 32 characters. The default is null.

Dependencies: Encaps must be set to X25/PAD for PAD banner msg to be applicable.

Location: Ethernet > Connections > *Connection profile* > Encaps options

PAD prompt

Description: Specifies the PAD prompt.

Usage: You can specify up to 12 characters. The default is null.

Dependencies: Encaps must be set to X25/PAD for PAD prompt to be applicable.

Location: Ethernet > Connections > *Connection profile* > Encaps options

Palmtop

Description: Specifies whether the MAX enables or disables access to AIM ports through the Palmtop Controller. If it is restricted, the user cannot use commands specific to an AIM port, cannot access the System menus, Network menus, and Host-interface profiles, and cannot edit parameters specific to an AIM port, unless the user is doing so through the base system's Palmtop port and the Palmtop Port # parameter enables access to the port.

If you are operating a MAX through a Palmtop port, you can change your access from Full to Restrict, but you cannot change your access from Restrict to Full. Only a terminal connected to the Control port (the back panel's DE-9 connector) can provide full access.

Usage: Specify one of the following values:

- Full (the default) specifies that access to the Palmtop port is unrestricted.
- Restricts specifies that the MAX restricts user access to a Palmtop port.

Location: Host/Dual (Host/AIM6) > Mod Config

See Also: Palmtop Port #

Palmtop Menus

Description: Specifies whether the user of a Palmtop Controller connected to a Palmtop port has access to the standard set of menus, the command-line interface, or the simplified menus.

Usage: Specify one of the following values:

- Standard (the default) means the Palmtop port has access to the standard set of menus.
- MIF specifies that the Palmtop port has access to the command-line interface.
- Limited specifies that the Palmtop port has access to the simplified menus.

Location: Host/Dual (Host/AIM6) > Mod Config

Palmtop Port

Description: Specifies the AIM port to which a Palmtop port has access if Palmtop access is restricted.

Usage: Specify the number of an AIM port. If you enter 0 (zero), the user of the Palmtop port has access to any AIM port.

Location: Host/Dual (Host/AIM6) > Mod Config

See Also: Palmtop

Password (Security)

Description: Specifies the password that an incoming call or session must include.

Note: Passwords are case-sensitive.

Usage: Specify up to 20 characters.

Dependencies: In a Connection profile, this parameter is not applicable unless Encaps is set to ARA. In the Ethernet profile, it is not applicable unless ATMP is enabled and the ATMP Mode is Home.

Location: Ethernet > Connections > Encaps Options, Ethernet > Mod Config > ATMP Options, Security

See Also: AppleTalk, ARA, ATMP Gateway, ATMP Mode, Encaps, Type, UDP Port Priv Protocol

Passwd (SNMPv3 USM Users)

Description: 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.

Usage: Specify up to 20 characters.

Dependencies: In the SNMPv3 USM Users profile, you must specify a password if the Auth Protocol parameter is set to a value other than `none`.

Location: Ethernet > SNMPv3 USM Users > *any SNMPv3 USM Users profile*

See Also: Active (SNMPv3 USM Users), Auth Protocol, Message Type, Name (SNMPv3 USM Users), Priv Protocol, R/W Access, Security Level

Password (Tunnel Options)

Description: Specifies the password the MAX unit uses to establish a tunnel.

Usage: Specify a value of up to 21 case-sensitive characters.

Example: `Password=1234567890Abcdefgklm1`

Dependencies: This parameter does not apply if Profile Type is set to Disabled or Tunnel Protocol is set to PPTP.

Location: Ethernet > Mod Config > *any Connection profile* > Tunnel Options

See Also: ATMP HA RIP, Client ID, Home Network Name, Max Tunnels, Pri. Tunnel Server, Profile Type, Sec. Tunnel Server, Tunnel Protocol, Tunnel VRouter, UDP Port

Parallel Dial

Description: Specifies the number of channels that the MAX can dial simultaneously over the T1 PRI line, or that the MAX can disconnect simultaneously. Although you can specify any number of channels, the initial number of channels in a connection never exceeds the value of the Base Ch Count parameter. Similarly, when the MAX adds or subtracts channels, the values for Max Ch Count and Min Ch Count override any setting for Parallel Dial.

Note: If calls from the U.S. to another country have trouble establishing an initial connection at the full bandwidth, reduce the Parallel Dial parameter to a value of 2 or 1.

Usage: Specify a number between 1 and 12. The default is 5.

Location: System profile: System > Sys Config

See Also: Base Ch Count

Passwd

Description: Specifies the terminal-server password (Ethernet profile) or the password required to authenticate a Security profile (Security profile). The first Security profile, Default, has no password.

Note: Passwords are case-sensitive.

Usage: Specify up to 20 characters.

Dependencies: In the Ethernet profile, this parameter does not apply if terminal services are disabled.

Location: Ethernet > Mod Config > TServ Options, System > Security

See Also: Edit Security, TS Enabled

Passwd Prompt

Description: Specifies the prompt the terminal server displays when asking the user for his or her password.

Usage: Specify up to 31 characters. The default value is *Password:*

Dependencies: This parameter does not apply if terminal services are disabled.

Location: Ethernet > Mod Config > TServ Options

Password

Description: Specifies the password that an incoming ARA caller must supply (Connection profile) or the password the foreign agent must specify under ATMP (Ascend Tunnel Management Protocol) in order to access this unit (Ethernet profile).

Note: Passwords are case-sensitive.

Usage: Specify up to 20 characters.

Dependencies: In a Connection profile, this parameter is not applicable unless Encaps is set to ARA. In the Ethernet profile, it is not applicable unless ATMP is enabled and the ATMP Mode is Home.

Location: Ethernet > Connections > *Connection profile* > Encaps Options, Ethernet > Mod Config > ATMP Options

See Also: AppleTalk, ARA, ATMP Gateway, ATMP Mode, Encaps, Type, UDP Port

Password Reqd

Description: Specifies that a password will be required to authenticate Combinet connections.

Usage: Specify Yes or No. No is the default.

- Yes specifies the MAX requires a password from all incoming calls from a Combinet bridge.
- No specifies a password is not required for Combinet calls.

Example: `Password Reqd=Yes`

Dependencies: This parameter applies only to Combinet connections.

Location: Ethernet > Answer > COMB Options, Ethernet > Connections > *Connection profile* > Encaps Options

See Also: COMB, Encaps, Recv PW, Send PW, Station

Passwd (SNMPv3 USM Users)

Description: 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.

Usage: Specify up to 20 characters.

Dependencies: In the SNMPv3 USM Users profile, you must specify a password if the Auth Protocol parameter is set to a value other than `none`.

Location: Ethernet > SNMPv3 USM Users > *any SNMPv3 USM Users profile*

See Also: Active (SNMPv3 USM Users), Auth Protocol, Message Type, Name (SNMPv3 USM Users), Priv Protocol, R/W Access, Security Level

Pbx Type

Description: Specifies the signaling conversion the MAX provides when the signaling mode is PBX T1 for the second T1 line.

Usage: Specify one of the following values:

- Leased 1:1 specifies that line #1 uses inband signaling and that line #2 consists entirely of nailed-up and unused channels.

  Each channel of line #1 must have a unique telephone number. When any unused channel on line #1 indicates that it has an incoming call, the MAX answers the call and connects it to the same channel in line #2, if that channel is nailed up. If the channel on line #2 is unused, the MAX handles the call in the usual manner. The call remains connected until the caller hangs up.
- Voice specifies that line #1 uses ISDN D-channel signaling and that line #2 uses inband signaling.

  The device connected to line #2 views the MAX as a switch. A switch is the device that connects the calling party to the answering party. The MAX switches an incoming call on line #1 to line #2 only if it is a voice-service call.

- Data specifies that line #1 uses ISDN D-channel signaling and that line #2 uses inband signaling.

  When you set PBX Type=Data, the MAX 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.

Dependencies: The setting you specify for PBX Type affects the Ans Service parameter in these ways:

- If you choose PBX Type=Leased 1:1, the Ans Service parameter does not apply.
- If you choose PBX Type=Voice, Ans Service must be set to Voice.
- If you choose PBX Type=Data, Ans Service can have any valid value, including Voice; however, the MAX does not generate call progress tones, and does not send call information messages.

Location: Net/T1 > Line Config > Line *N*

See Also: Ans Service, Ans #, Sig Mode

Peer

Description: Specifies whether the remote IPX caller is a router or a dialin client. The Answer profile > IPX Options > Peer parameter specifies how the MAX negotiates IPX, with callers that have no configured Connection profile, assuming them to be either IPX routers or IPX clients.

Usage: Specify one of the following values:

- Router (the default) specifies that the caller is an IPX router.
- Dialin specifies a dialin client.

  Dial-in NetWare clients do not have an IPX network address. To allow those clients an IPX routing connection to the local network, the MAX must assign the client an IPX network address from a virtual IPX network defined in the IPX Pool parameter.

  For dialin clients, the MAX does not send RIP and SAP advertisements across the connection and ignores RIP and SAP advertisements received from the far end. However, it does respond to RIP and SAP queries received from dial-in clients

Dependencies: This parameter does not apply if IPX routing is not enabled. It requires that a virtual IPX network number be provided in the IPX Pool parameter.

Location: Ethernet > Connections > *Connection profile* > IPX Options
Ethernet > Answer > IPX Options

See Also: IPX Pool#

Peer (AppleTalk Options)

Description: Indicates whether the connection for this profile is a single-user PPP connection or a router.

Usage: Select Peer=Dialin to indicate that the profile is for a single user PPP connection. All other fields in the AppleTalk options menu are N/A. If you select Peer=Dialin, you have completed the configuration; close the AppleTalk Options menu and save your changes.

Select Peer=Router to indicate that the profile is for a connection with a router (such as an Lucent Pipeline unit).

Dependencies: If you select Peer=Router, you will need to configure the other fields in the AppleTalk options menu. You must select the following:

- Route Appletalk=Yes in the PPP options menu of the Answer profile.
- AppleTalk=Yes in the Ethernet Configuration menu.
- AppleTalk Router=On in the profile's AppleTalk Options submenu.

Location: Ethernet > Connections > *Connection profile* > AppleTalk Options

See Also: Net Start, Net End, AppleTalk, AppleTalk Router, Route AppleTalk, Zone Name

Perm Conn Update

Description: Specifies under what circumstances the MAX performs nonintrusive remote updates of the configurations of permanent connections.

Usage: Specify one of the following values:

- All (the default) specifies that, if they are fetched from the RADIUS server, all existing permanent connections will be torn down and reestablished following the update. This setting causes service interruption every time any nailed profile is updated or added.
- Changed specifies that only changed permanent connections will be torn down and reestablished.

Location: System > Sys Config

Phone Number

Description: Specifies the phone number pattern against which the destination phone number of the call will be matched to determine if the call route applies. If this value is not zero, then the destination phone number must match the specified phone number.

Usage: Enter up to 24 characters. By default, this parameter has a null value, which does not require the phone number to match the specified phone number. The phone number can include any of the following characters:

0-9	Regular phone number digits.
#	The number sign.
*	A literal * (asterisk) as in *69.
*	Matches multiple characters.
^	Start of line marker. If present, must be at the start of the pattern. Indicates that the following pattern must be at the start of the dial string to match.
$	End of line marker. If present, must be at the end of the pattern. Indicates that the proceeding pattern must be at the end of the dial string to match.

.	Matches any single character. In this case, a period.

Sample Setting	Description of action
5551212	Matches dial strings containing 5551212
^5551212$	Matches only the dial string 5551212
^555	Matches all dial strings starting with 555 (including the string 555)
55512.2	Matches dial strings 5551202, 5551212, 5551222, ... , 5551292, 55512#2, 55512*2
*69	Matches dial strings containing *69
^*69$	Matches only the dial string *69
.....	Matches all dial strings at least seven digits long
^.....$	Matches all seven-digit dial strings

Location: System > Call Routes > *Call Routes profile*

PID selection

Description: For DTE-initiated calls, this specifies which Protocol Identifier (PID) the PAD includes in the call request packet it sends to the host.

Usage: Specify one of the following values:

- X.29 (the default)
  Specifies that the PAD sets the protocol identifier in the CUD field to X.29.
- T3POS
  Specifies that the PAD sets the protocol identifier in the CUD field to T3POS.

Dependencies: This parameter is always applicable.

Location: Ethernet > Connections > *Connection profile* > Encaps options,
Ethernet > Answer > T3POS options

Pkt Audio Mode

Description: Configures the preferred audio codec a MultiVoice gateway uses to compress/decompress analog speech into packetized voice for transmission across a packet network. Starting with Release 8.0-118, this parameter may be used to enable use of the Full Rate GSM audio codec on a MultiVoice gateway.

Usage: The Pkt Audio Mode parameter now accepts the following value:

Parameter value	Usage
FRGSM	Assigning this value configures the MultiVoice gateway to select the Full Rate GSM as the preferred audio codec for processing voice data for VoIP calls.

Example: The following example illustrates how to configure a MultiVoice gateway to use Full Rate GSM as the preferred audio codec for processing voice data for VoIP calls:

1. From the MAX administration menu, select the `Ethernet` > `Mod Config` profile.
2. Scroll down to the VOIP Options, then press [Enter] to open this profile.
3. Scroll down to the Pkt Audio Mode parameter, then press [Enter] to toggle the value of this parameter, as illustrated.

   ```
   Pkt Audio Mode=FRGSM
   ```
4. Press [Esc]; then, when prompted, select the option to `Exit and Save` your changes.

Dependencies: Changes to the Pkt Audio Mode parameter take effect with the next VoIP call.

Location: Ethernet > Mod Config > VOIP Options

See Also: GK IP Adrs, VPN Mode

Pool

Description: Specifies an IP address pool from which the caller will be assigned an IP address. If the Pool parameter is null but all other configuration settings enable dynamic assignment, the MAX gets IP addresses from the first defined address pool.

You can define up to 10 IP address pools in the vt100 interface. RADIUS supports up to 50 address pools.

Usage: Specify the number of the pool. The default is 1.

Location: Ethernet > Connections > *Connection profile* > IP Options

See Also: Assign Adrs, Pool # Count, Pool # Start

Pool #N count (N=1–10)

Description: Specifies how many IP addresses are in the numbered pool (up to 254). N represents the number of the pool, which can be 1 through 10.

Note: Addresses in a pool do not accept a netmask modifier, because they are advertised as host routes. If you allocate IP addresses on a separate IP network or subnet, make sure you inform other IP routers about the route to that network or subnet.

Usage: For each pool, specify a number between 0 and 254.

Dependencies: The starting address must be specified in the Pool #N start parameter.

Location: Ethernet > Mod Config > WAN Options

See Also: Pool only, Pool #N start

Pool only

Description: Instructs the MAX to hang up if a caller rejects the dynamic assignment. During PPP negotiation, a caller can reject the IP address offered by the MAX and present its own IP address for consideration. Connection profiles compare IP addresses as part of authentication, so the MAX would automatically reject such a request if the caller has a Connection profile. However, Names/Passwords profiles have no such authentication mechanism, and could potentially allow a caller to spoof a local address.

Usage: Specify Yes or No. No is the default.

- Yes specifies the caller must accept dynamic assignment. This is recommended if Names/Passwords profiles are in use.
- No specifies the MAX allows the caller to reject the IP address offered by the MAX and present its own IP address for consideration.

Dependencies: At least one address pool must be defined, and addresses must be available.

Location: Ethernet > Mod Config > WAN Options

See Also: Pool # Count, Pool # Start

Pool #N name (N=1-10)

Description: Specifies the name of an IP address pool

Usage: Specify a name. You can enter up to 10 characters. The first character cannot be a number.

Location: Ethernet > Mod Config > WAN Options

Pool #N start (N=1–10)

Description: Specifies the first address in a block of contiguous addresses on the local network or subnet. The Pool #1 count parameter specifies the number of contiguous addresses in that pool.

Usage: Specify the first IP address in the pool. The address you specify does not need to be on the same LAN segment as the MAX. The default is 0.0.0.0.

Example: `Pool #1 Start=200.207.23.1`

Dependencies: The number of addresses in the pool must be specified in the Pool #N count parameter.

Location: Ethernet > Mod Config > WAN Options

See Also: Pool #N count, Pool only

Pool Number

Description: Specifies the IP address pool to use to assign addresses to NAT (Network Address Translation) clients.

Usage: Specify the IP address pool to use to assign IP addresses to clients using this connection. The valid range is from 0 to 150 (RADIUS) or 0 to 10 (pool configuration in the Ethernet profile). The default is 0. A value of 0 means the MAX will assign any address from any available pool.

Dependencies: This parameter does not apply if Reply Enabled is set to No.

Location: Ethernet > Answer > DHCP options, Ethernet > Connections > *Connection profile* > DHCP options

See Also: Reply Enabled

Pool OSPF Adv Type

Description: Specifies how to import summarized pool addresses into OSPF.

Usage: Specify one of the following values:

- Type-1 (the default) instructs the MAX to import the pool addresses into OSPF as external Type-1 routes.
- Type-2 instructs the MAX to import the pool addresses into OSPF as external Type-2 routes.
- Internal instructs the MAX to import the pool addresses into OSPF as Intra-Area routes.

Dependencies: Pool OSPF Adv Type applies if you set Pool Summary=Yes and enable OSPF. For a change in the Pool OSPF Adv Type setting to take effect, you must reset the MAX.

Location: Ethernet > Mod Config > WAN Options

See Also: Active, Pool Summary

Pool Summary

Description: Indicates that network summarization is in use.

Network summarization reduces the size of route advertisements by summarizing a series of host routes into a network advertisement. Packets destined for a valid host address on that network are routed to the host, and packets destined for an invalid host address are rejected with an ICMP “host unreachable” message. To use the pool summary feature, create a network-aligned pool and set the Pool Summary parameter to Yes.

To be network-aligned, the Pool Start address must be the first host address. Pool Start address –1 is used to determine the network address (the zero address on the subnet). To have a power of two size, the Pool Count value must be two less than a power of two; for example, 2, 6, 14, 30, 62, 126. The Pool Count value + 2 is used to create a netmask. For example:

```
Pool Summary=Yes
Pool#1 start=10.12.253.1
Pool#1 count=126
```

The network alignment address is Pool Start address –1: 10.12.253.0 and the netmask is Pool Count +2 addresses: 255.255.255.128. The resulting address pool network is:

```
10.12.253.0/25
```

Usage: Specify Yes or No. No is the default.

- Yes indicates that network summarization is in use. The Pool Count and Pool Start values must be set up as described above.
- No indicates that host routes will not be summarized.

Example: `Pool Summary=Yes`

Dependencies: The Pool Count and Pool Start values must be set up as described above.

Location: Ethernet > Mod Config > WAN Options

See Also: Pool #N start, Pool #N count

Port

Description: Specifies whether the MAX traps AIM port state changes and sends traps-PDUs (Protocol Data Units) to the SNMP manager. For details on the events that cause the MAX to send a traps-PDU, see the Ascend Enterprise Traps MIB.

Usage: Specify Yes or No. No is the default.

- Yes specifies the MAX traps AIM port state changes and send traps-PDUs to the SNMP manager.
- No specifies the MAX does not generate traps for port changes.

Example: `Port=Yes`

Location: Ethernet > SNMP Traps

Port N/N Dual (N/N=1/2, 3/4, 5/6)

Description: Specifies whether the MAX pairs ports for dual-port or FT1-B&O calls on a Host/AIM6 module. In a dual-port call, a codec performs inverse multiplexing on two channels so that a call can achieve twice the bandwidth of a single channel. Inverse multiplexing is a method of combining individually dialed channels into a single, higher-speed data stream.

The codec provides two ports, one for each channel. Two AIM ports on the MAX connect a dual-port call to the codec; these ports can be the V.35, RS-499, or X.21 ports on the MAX, and are called the primary port and the secondary port. Because the MAX places the two calls in tandem and clears the calls in tandem, it considers them a single call.

Usage: Specify Yes or No. No is the default.

- Yes pairs the specified ports for a dual-port call.

  Port 1/2 Dual pairs ports 1 and 2 for a dual-port call.

  Port 3/4 Dual pairs ports 3 and 4 for a dual-port call.

  Port 5/6 Dual pairs ports 5 and 6 for a dual-port call.
- No does not pair the ports.

Dependencies: For a dual-port call, the call type is 2-channel. For an FT1-B&O call, the call type is FT1-B&O.

Location: Host/Dual (Host/AIM6) > Mod Config

Port Name

Description: Specifies a name for the Port profile. This name replaces *PortN Menu* as a menu title. For example, if it is set to *Lucent* for AIM port #1, the menu called *21-000 Port1 Menu* becomes *21-100 Lucent*.

Usage: Specify the name. You can specify up to 16 alphanumeric characters.

Example: `Port Name=Lucent`

Location: Host/Dual (Host/AIM6) > Port*N* Menu > Port Config

Port Password

Description: Specifies the password for incoming AIM or BONDING calls. Authentication is used only if the calling unit has a password defined in the Call profile. If the Call profile in the calling unit does not have a password defined, the units connect without authentication even though the originating unit can have sent parameters. Note that the MAX only authenticates AIM and BONDING calls; dual-port calls are not authenticated.

Usage: Enter a password of nine characters or less.

Example: `Port Password=Lucent`

Location: Host/Dual (or Host/AIM6 > Port*N* Menu > Port Config

See Also: Call Password

POTS Digit Timeout

Description: Specifies the maximum time (in seconds) the MAX will wait for additional digits. If this time is exceeded, the unit considers the phone number complete and attempts to place the call.

Usage: Specify a value from 2 to 60. The default is 10.

Dependencies: This parameter applies only to POTS ports.

Location: System > Sys Config

PPP

Description: In the Answer profile, this enables incoming PPP (Point-to-Point Protocol) connections. PPP sessions are single-channel connections to any remote device running PPP software. In the Ethernet profile, this enables terminal server users to initiate a framed PPP session from the terminal-server command line interface.

Usage: Specify Yes or No. Yes is the default in the Answer profile. No is the default in the Ethernet profile.

- Yes in the Answer profile means the MAX accepts inbound PPP calls, provided that they meet all other connection criteria. No specifies it will not accept inbound PPP connections.
- Yes in the Ethernet profile enables terminal-server users to invoke a PPP session. No prevents them from initiating a PPP session.

Dependencies: In the Ethernet profile, this parameter does not apply if terminal services are disabled.

Location: Ethernet > Answer > Encap, Ethernet > Mod Config > TServ Options

See Also: TS Enabled

PPP Delay

Description: Specifies the number of seconds the MAX waits for PPP packets before transitioning to terminal server mode. Note that this applies to incoming modem, V.110, or V.120 asynchronous calls.

Usage: Specify a number between 1 and 60. The default is 5 seconds.

Dependencies: This parameter does not apply if terminal services are disabled.

Location: Ethernet > Mod Config > TServ Options

PPP Direct

Description: Specifies whether to start PPP negotiation immediately after a user enters the PPP command in the terminal server interface, or to wait to receive a PPP packet from an application. (Some applications expect to receive a packet first.)

Usage: Specify Yes or No. No is the default.

- Yes specifies the MAX begins PPP/LCP negotiation immediately after a user enters PPP at the command line.
- No specifies the MAX waits to receive PPP packets from the remote peer.

Dependencies: This parameter does not apply if terminal services are disabled.

Location: Ethernet > Mod Config > TServ Options

See Also: PPP, PPP Delay

PPP Info

Description: Specifies what message is displayed when a terminal server user initiates a framed PPP session from the command line.

Usage: Specify one of the following values:

- None (the default) specifies that no message appears.
- Mode specifies that the banner reads:

```
Entering PPP Mode
IP address is <ipaddr >
MTU is 1524
```

<ipaddr > is the caller's IP address. The value 1524 is the default size of a link's Maximum Transfer Unit.

- Session specifies that the banner reads:

```
Entering PPP Session
IP address is <ipaddr >
MTU is 1524
```

Dependencies: This parameter does not apply if terminal services are disabled.

Location: Ethernet > Mod Config > TServ Options

See Also: TS Enabled

PPTP Enabled

Description: Enables or disables Point-to-Point Tunneling Protocol (PPTP) functionality in the MAX. When PPTP is enabled, the MAX can bring up a PPTP tunnel with a PPTP Network Server (PNS) and respond to a request for a PPTP tunnel from a PNS. You must specify the IP address of the PNS in one or more of the Route Line parameters.

Usage: Specify Yes or No. No is the default.

- Yes enables PPTP, enabling the MAX to bring up a PPTP tunnel to a PNS or respond to a tunnel request.
- No disables PPTP.

See Also: Route Line *n*, Line *n* tunneling type

Location: Ethernet > Mod Config > L2 Tunneling Options submenu

Precedence

Description: Specifies the priority level of the data stream.

Usage: The three most significant bits of the Type-of-Service (TOS) byte are priority bits used to set precedence for priority queuing. When TOS is enabled, you can set those bits (most significant bit first) to one of the following values:

- 000—Normal priority (the default).
- 001—Priority level 1.
- 010—Priority level 2.
- 011—Priority level 3.
- 100—Priority level 4.
- 101—Priority level 5.
- 110—Priority level 6.
- 111—Priority level 7 (the highest priority).

Example: `Precedence=001`

Dependencies: If `TOS Enabled=No`, the Precedence setting is not applicable.

Location: Ethernet > Connections > *Connection profile* > IP options

See Also: Apply To, TOS, TOS Enabled, TOS Filter

Preempt

Description: Specifies the number of idle seconds the MAX waits before using one of the channels of an idle link for a new call.

Usage: Specify a number between 0 and 65535. The MAX sets no time limit if you enter 0 (zero). The default setting is 60.

Location: Ethernet > Answer > Session Options, Ethernet > Connections > *Connection profile* > Session Options

See Also: Call Type

Preference

Description: Specifies the preference value for a route. RIP is a distance-vector protocol, which uses a hop count to select the shortest route to a destination network. OSPF is a link-state protocol, which means that OSPF can 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. Because these two metrics are incompatible, the MAX supports route preferences.

When choosing which routes should be put in the routing table, the router first compares preference values, preferring the lower number. If the preference values are equal, then the router compares the metric field, using the route with the lower metric.

- Connected routes have a default preference of 0
- OSPF routes have a default preference of 10
- ICMP redirects have a default preference of 30
- RIP routes have a default preference of 100
- Static routes have a default preference of 100
- ATMP routes have a default preference of 100

Usage: Specify a number between 0 and 255. Zero is the default for connected routes (such as the Ethernet). The value of 255 means *Do not use this route*; this value is meaningful only for Connection profiles.

Location: Ethernet > Connections > *Connection profile* > IP Options, Ethernet > Static Rtes

PrependDigits

Description: Specifies digits to add in front of an outgoing call.

Example: `PrependDigits=9`

Location: System > Dial Plan

PRI # Type

Description: PRI # Type 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 following settings. This parameter specifies the TypeOfNumber field in the called party's information element.

Usage: Specify one of the following values:

- National (the default) specifies telephone numbers within the U.S. (TypeOfNumber=2)
- Intl specifies telephone numbers outside the U.S. (TypeOfNumber=1)
- Local specifies telephone numbers within your Centrex group. (TypeOfNumber=4)
- Abbrev. specifies that the telephone number is abbreviated. (TypeOfNumber=6)
- NetSpecific (currently not implemented) specifies that the network you are connected to understands the telephone number. (TypeOfNumber=3)
- Unknown specifies that the telephone number is none of the above. (TypeOfNumber=0)
- Inherit (Dial Plan profile only) applies to calls placed by a device connected to a local T1 PRI line supplied by a Host/BRI module. If you choose this setting, the caller on the WAN requests the same TypeOfNumber as the caller on the local ISDN BRI line.

Dependencies: 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.

Location: Host/Dual (Host/AIM6) > Port*N* Menu > Directory (Call profiles), Ethernet > Connections > *Connection profile*, System > Dial Plan, Ethernet > Frame Relay, Ethernet > X.25

See Also: NumPlanID, Call-by-Call, T1-PRI:PRI # Type (Line profiles), Modem:PRI# Type (System profile)

Pri DNS

Description: Specifies the IP address of the primary domain name server. You can specify a primary and secondary name server of each type. The secondary server is accessed only if the primary one is inaccessible.

Usage: Specify the IP address of the primary domain name server. The default value is 0.0.0.0. Accept this default if you do not have a domain name server.

Example: `Pri DNS=10.207.23.1`

Location: Ethernet > Mod Config > DNS

See Also: Domain Name, Sec DNS

Pri Num

Description: Specifies the primary add-on number for the ISDN BRI line. When the MAX receives a multichannel AIM, BONDING, or MP+ call, it reports the primary add-on number (Pri Num) and the secondary add-on number (Sec Num) to the calling party. The calling MAX can then add more channels. If you do not specify an add-on number and the calling MAX

needs to add more channels, it redials the telephone number it used to make the first connection. For example, suppose that 777-3330 is the primary number for line #1, and 777-3331 is the secondary number for line #1. Set Pri Num=30 and Sec Num=31. (See "Ch N (N=1–24, 1–32)" on page 4-67" for more detail on add-on numbers.)

Usage: Specify a telephone number with a limit of 24 characters, which can include the following characters: 1234567890()[]!z-*#|. The default is null.

Example: `Pri Num=30`

Location: Net/BRI > Line Config > Line *N*

See Also: Sec Num, Sub-Adr

Pri. Tunnel Server

Description: Specifies the IP address or hostname of the primary tunnel server used by ATMP, PPTP, L2F, and L2TP tunnels.

Usage: Enter a dotted-decimal IP address or hostname.

Example: `Pri. Tunnel Server=123.123.123.1`

Location: Ethernet > Mod Config > *any Connection profile* > Tunnel Options

See Also: Profile Type, Tunnel Protocol, Max Tunnels, ATMP HA RIP, UDP Port, Home Network Name Sec. Tunnel Server, Password, Client ID, Tunnel VRouter

Priority

Description: Specifies the priority of this router with respect to the designated router and backup designated router elections under OSPF. When two routers attached to a network attempt to become the designated router, the one with the highest Priority value takes precedence. A router whose Priority is set to 0 (zero) is ineligible to become the designated router on the attached network.

Usage: Specify a number. The default value is 5.

Location: Ethernet > Connections > *Connection profile* > OSPF Options, Ethernet > Mod Config > OSPF Options

Pri SPID

Description: Specifies the primary Service profile Identifier (SPID) for the ISDN BRI line. The SPIDs assigned to a BRI line operating in multipoint mode are numbers used at the central switch to identify services provisioned for your ISDN line. A SPID is derived from a telephone number and should be supplied by your carrier.

Note: Not all telephone companies include a suffix on their SPIDs. When receiving SPIDs from your telephone company, ask them to verify whether or not suffixes are included. The SPID formats described in the next sections have been agreed upon by most telephone companies.

For example, for an AT&T switch in multipoint mode, SPIDs have one of these formats:

01*nnnnnnn*0

01*nnnnnnn*00

In the AT&T SPID formats, *nnnnnnn* is the 7-digit telephone number (not including the area code). For example, if the telephone number is 555-1212, the SPID will be 0155512120 or 01555121200.

For a Northern Telecom switch, SPIDs have one of these formats:

aaannnnnnnSS

*aaannnnnnnSS*00

In the Northern Telecom SPID formats, *aaannnnnnn* is the 10-digit telephone number (including the area code). SS is an optional suffix—if specified it is a one or two-digit number differentiating the channels. For example, if the telephone numbers are 212-555-1212 and 212-555-1213, the SPIDs can be:

21255512121

21255512132

or:

212555121201

212555121302

or one of the above formats followed by 00 (for example, 21255512130200).

Usage: Specify up to 16 characters; you must limit those characters to numbers, hyphens, and parentheses. The default value is 0 (zero).

Location: Net/BRI > Line Config > Line profile > Line *N*

See Also: B1 Usage, B2 Usage, Link Type, Pri Num, Sec Num, Sec SPID, Switch Type

Private

Description: Specifies whether the MAX will disclose the existence of this route when queried by RIP or another routing protocol. Private routes are used internally but are not advertised.

Usage: Specify Yes or No. No is the default.

- Yes makes the route private. The MAX does not advertise the route.
- No specifies the route is advertised via routing protocols.

Dependencies: This parameter does not apply if the IP routing is not enabled.

Location: Ethernet > Connections > *Connection profile* > IP Options, Ethernet > Static Rtes

See Also: LAN Adrs, Metric, RIP, Route IP

Priv Key

Description: Specifies a privacy key for SNMPv3 USM users.

Usage: In most cases, you do not set this string directly. Instead, use the snmpPrivPass command to generate the value. If you have permission to view passwords, the privacy key appears on your screen as a hexadecimal value for save and restore purposes. Otherwise, the privacy key appears as a row of asterisks. The default is null.

If you change the value of Priv Key directly, keep in mind that the first byte indicates the length of the field. This value must be 10 (16d in hexadecimal) if Message Digest 5 (MD5) is in use and 14 (20d in hexadecimal) if the Secure Hash Algorithm (SHA) is in use. If you specify an invalid value, the unit uses the previous key, if any, to communicate with the SNMP manager. If no previous key exists, this USM user cannot communicate with the network until a valid key is generated by means of the snmpPrivPass command.

Example: Suppose you use the snmpPrivPass command to generate the following 16-byte string:

```
27 0a dc 75 f8 98 e5 7c 4c 03 22 7d dd ac 0d ef
```

The system displays it as the following Priv Key value:

```
10270adc75f898e57c4c03227dddac0def00000000
```

Dependencies: Consider the following:

- You must generate the privacy key by means of the snmpPrivPass command before the SNMPv3 USM Users profile can be used for communication with the SNMP manager.
- If you change the privacy protocol from MD5 to SHA (or vice versa), you must change the privacy key by means of the snmpPrivPass command. The previous protocol-and-key combination is used until you specify a new one.
- If Priv Protocol is set to No-Auth, Priv Key does not apply.

Location: Ethernet > SNMPv3 USM Users

See Also: Auth Key

Priv Protocol

Description: 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.

Usage: N/A is the default setting. You cannot change the default setting.

Example: `Priv Protocol=N/A`

Dependencies: The MAX unit's SNMPv3 engine does not support encryption/decryption.

Location: Ethernet > SNMPv3 USM Users > *any SNMPv3 USM Users profile*

See Also: Active (SNMPv3 USM Users), Auth Protocol, Message Type, Name (SNMPv3 USM Users), Passwd (SNMPv3 USM Users), R/W Access, Security Level

Pri WINS

Description: Specifies the IP address of the primary Windows Internet Name Service (WINS) server.

Usage: Specify an IP address in dotted decimal notation. The default is 0.0.0.0.

Dependencies: Pri WINS applies only to Telnet and raw TCP connections running under the MAX unit's terminal server interface.

Location: Ethernet > Mod Config > DNS

See Also: Sec WINS

ProcProgInd

Description: Configures the type of call progress events which are captured and reported in the Q.931 Proceeding message progress indicator information element by the MultiVoice gateway. Once configured, MultiVoice gateways report when specific call routing events occur for VoIP calls passing from the packet network and the switched telephone network.

Usage: The ProcProgInd parameter may be assigned the following values:

Parameter value	Usage
`No Indicator`	Assigning this value, the default, disables alert reporting of call routing events on the egress switched telephone network.
`Non End2End ISDN`	Assigning this value, the egress MultiVoice gateway reports when calls are connected to an egress switched telephone network which does not use ISDN signaling. The egress switched telephone network may support robbed-bit or detectable DTMF.
`Non ISDN Dest`	Assigning this value, the egress MultiVoice gateway reports when calls are connected to an egress switched telephone network which does not use ISDN signaling, such as a transit network or private network, which does not return call progress signals to the MultiVoice gateway.
`Non ISDN Orig`	Assigning this value, the ingress MultiVoice gateway reports when calls are received from a local switched telephone network which does not use ISDN signaling, such as a transit network or private network, which does not provide call progress signals to the MultiVoice gateway.
`Return to ISDN`	Assigning this value, the egress MultiVoice gateway reports when calls connected across a transit network are routed back on to trunk supporting ISDN signaling.

Parameter value	Usage
`Interworking`	Assigning this value, the egress MultiVoice gateway reports if interworking occurs upon connecting a call to the switched telephone network. Such events occur when the selected bearer capability is not supported or when a resource or route with the preferred capability is not available.
`Inband Info`	Assigning this value, the egress MultiVoice gateway reports if inband call progress signaling or other supported non-ISDN signaling is available from the switched telephone network for the connected call.

Example: The following example illustrates how to report when calls are proceeding on a far-end switched telephone network which does not use ISDN signaling:

1 From the MAX administration menu, select the `Ethernet` > `Mod Config` profile.

2 Scroll down to the PSTN Options, then press [Enter] to open this profile. The following menu appears on your screen:

```
90-C00 Mod Config            x
x PSTN Options...            x
x >Cause Code Enabled=No     x
x  AlertProgInd=No Indicator x
x  ProcProgInd=No Indicator  x
x  Bearer Info=Speech        x
```

3 Scroll down to the ProcProgInd parameter, then press [Enter] to toggle the value of this parameter, as illustrated.

```
ProcProgInd=Non ISDN Dest
```

4 Press [Esc]; then, when prompted, select the option to `Exit and Save` your changes.

Dependencies: Changes to the ProcProgInd parameter take effect with the next VoIP.

Location: Ethernet > Mod Config > PSTN Options

Profile Reqd

Description: Specifies whether the MAX rejects incoming calls for which it could find no Connection profile and no entry on a remote authentication server. If you do not require a configured profile for all callers, the MAX builds a temporary profile for unknown callers. Many sites consider this a security breach.

Note: Setting Profile Reqd to Yes disables Guest access for ARA connections.

Usage: Specify Yes or No. No is the default.

- Yes specifies a configured profile is required for all callers.
- No specifies that if a configured profile is not found, the MAX builds a temporary profile for the unknown caller.

Dependencies: This parameter does not apply to terminal server calls.

Location: Ethernet > Answer

See Also: AppleTalk, Encaps, Recv Auth, Route IP

Profile Type

Description: Specifies whether this profile supports no tunneling, the mobile-client end of a tunnel, or a tunneling gateway.

Usage: Specify one of the following values:

- Disabled (the default)—The Connection profile is not used for tunneling.
- Mobile-client—The Connection profile is for a tunnel's mobile client, such as an ATMP FA or L2TP LAC.
- gateway—The Connection profile is for an ATMP tunnel's gateway, such as an ATMP HA.

Example: `Profile type=Mobile-client`

Location: Ethernet > Mod Config > *any Connection profile* > Tunnel Options

See Also: ATMP HA RIP, Client ID, Home Network Name, Max Tunnels, Password, Pri. Tunnel Server, Sec. Tunnel Server, Tunnel Protocol, Tunnel VRouter, UDP Port

Prompt

Description: Specifies the prompt the MAX displays during a terminal server session.

Usage: Specify a string containing up to 15 characters. The default is *ascend%*.

Dependencies: This parameter is not applicable if terminal services are disabled.

Location: Ethernet > Mod Config > TServ Options

See Also: TS Enabled

Prompt Format

Description: Determines whether you are able to use the multi-line format for the terminal server login prompt.

Usage: Specify Yes or No. No is the default.

- Yes causes the MAX to interpret carriage-return/line-feed and tab characters in the string specified as the Login Prompt.
- No specifies the MAX does not interpret the line feed/carriage return character or the tab character.

Example: `Prompt Format=No`

Dependencies: This parameter is not applicable if terminal services are disabled.

Location: Ethernet > Mod Config > TServ Options

See Also: TS Enabled, Login Prompt

Protocol

Description: In a filter of type IP, specifies the protocol number to which the MAX compares a packet's protocol number. If you specify a protocol number, the MAX compares it to the protocol number field in packets to match them to this filter. The default protocol number of zero matches all protocols. Common protocols are listed below, but protocol numbers are not limited to this list. For a complete list, see the section on Well-Known Port Numbers in RFC 1700, *Assigned Numbers*, by Reynolds, J. and Postel, J., October 1994.

- 1: ICMP
- 5: STREAM
- 8: EGP
- 6: TCP
- 9: Any private interior gateway protocol (such as Cisco's IGRP)
- 11: Network Voice Protocol
- 17: UDP
- 20: Host Monitoring Protocol
- 22: XNS IDP
- 27: Reliable Data Protocol
- 28: Internet Reliable Transport Protocol
- 29: ISO Transport Protocol Class 4
- 30: Bulk Data Transfer Protocol
- 61: Any Host Internal Protocol
- 89: OSPF

Usage: Specify the number of the protocol. You can enter a number between 0 and 255. The default setting is 0 (zero). When you accept the default, the MAX disregards the Protocol parameter when applying the filter.

Location: Ethernet > Filters > Input filters > In filter *N* > IP, Ethernet > Filters > Output filters > Out filter *N* > IP

See Also: Type, Valid

Proxy Mode

Description: Specifies under what conditions the MAX 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, Proxy ARP is enabled when the MAX supplies IP addresses dynamically to dial-in users, and both of the following conditions exist:

- The MAX-supplied IP addresses are in the same local subnet as the MAX
- Hosts on the local subnet must send packets to the dial-in clients.

You should not need to enable Proxy ARP, because most routing protocols (including those used over the Internet) are designed to propagate subnet mask information.

Usage: Specify one of the following values:

- Off disables proxy ARP. This is the default.
- Always specifies that the MAX responds to an ARP request with its own MAC address if the ARP request is sent to a host to which the MAX has a route.
- Active specifies that the MAX responds to an ARP request with its own MAC address if the ARP request is sent to a host to which the MAX has an active connection.
- Inactive specifies that the MAX responds to an ARP request with its own MAC address if the ARP request is sent to a host to which the MAX has an inactive connection.

  Note: Proxy ARP does not apply to inactive user profiles stored in RADIUS.

Dependencies: This parameter does not apply if IP routing is not enabled.

Location: Ethernet > Mod Config > Ether Options

See Also: Net Adrs, Route IP

Q

Queue Depth

Description: The maximum number of unprocessed SNMP requests which the MAX saves. If SNMP requests arrive at a rate faster than they can be processed, then a backlog builds up. This parameter sets the maximum depth of the queue. If the queue fills, further packets destined for it are discarded.

Usage: Enter an integer value from 0 to 1024. If you enter 0, the MAX saves SNMP requests until it runs out of memory. The default is 0.

Note: Setting Queue Depth to 0 is not recommended. An unlimited queue depth could result in an out-of-memory error on the MAX if it receives a flood of packets on its SNMP port.

Location: Ethernet > Mod Config > SNMP options

See Also: Rip Queue Depth

R

RD Mgr*N* (*N*=1-8)

Description: Specifies up to eight IP addresses of SNMP managers that have SNMP read permission. The MAX responds to SNMP Get and Get Next commands from these SNMP managers only.

Usage: Specify the IP address of a host running an SNMP manager. The default is 0.0.0.0. Do not include subnets as a part of the IP address you specify.

Example: `RD Mgr1=10.5.6.7`

Dependencies: The Security parameter must be set to Yes for the RD Mgr1-8 parameters to have any effect. If the Security parameter is set to Yes, only SNMP managers at the IP addresses you specify can execute the SNMP Get and Get-Next commands.

Location: Ethernet > Mod Config > SNMP Options

See Also: Security, WR Mgr*N*

Recv Name

Description: Specifies the PPP called device's name during outgoing calls. Because bidirectional authentication provides a way to formally authenticate the called device during an outgoing call, the name of the device must be checked against a locally defined name. The name can be the dialout profile name, or a substituted name.

Usage: Specify a string of up to 23 characters. The default is null.

Dependencies: Consider the following:

- The value you specify for Recv Name is used only during outgoing calls that use bidirectional authentication.
- If you accept the default of null for Recv Name, the name of the called device is checked against the dialout profile name.
- Recv Name allows an additional RADIUS lookup during an outgoing call.
- Because Recv Name represents the called device's real name, it is sent in RADIUS accounting Start and Stop messages.
- Recv Name is not applicable if PPP is not enabled, if Receive Auth is set to None, PAP, PAP-Token, or PAP-Token-CHAP, or if Bi-Dir Auth is set to None.

Location: Ethernet > Connection > PPP Options

See Also: Bi-Dir Auth

R/W Access

Description: Specifies whether or not the MAX unit grants the SNMPv3 USM user read and write access to the unit's MIB (Management Information Base) settings.

Usage: Specify Yes or No. No is the default.

Example: `R/W Access=No`

Location: Ethernet > SNMPv3 USM Users > *any SNMPv3 USM Users profile*

See Also: Active (SNMPv3 USM Users), Auth Protocol, Message Type, Name (SNMPv3 USM Users), Passwd (SNMPv3 USM Users), Priv Protocol, Security Level

R/W Comm Enable

Description: Enables and disables the use of SNMP set commands.

Usage: Press Enter to select Yes or No.

- Yes enables the use of SNMP set commands. To use a set command, you must know the SNMP read-write community string specified in the R/W Comm parameter.
- No disables the use of set commands.

Location: Ethernet > Mod Config > SNMP Options

See Also: R/W Comm, Read Comm

R/W Comm

Description: Specifies a read/write SNMP community name. If an SNMP manager sends this community name, it can access the Get, Get-Next, and Set SNMP agents.

Usage: Specify the community name that the MAX will use for authenticating the SNMP management station for read-write access. You can enter letters and numbers, up to a limit of 31 characters. The default is Write.

Location: Ethernet > Mod Config > SNMP Options

See Also: Read Comm, R/W Comm Enable

R/W Enable

Description: Specifies whether or not the MAX unit enables modifications to Snmpv3 USM options profile.

Usage: Specify Yes or No.

Example: `R/W Enable-No`

Location: System > Security > *any Security profile* > Snmpv3 USM options

See Also: Auth Protocol, Enable, Message Type, Priv Protocol, Security Level

Rate Limit

Description: Specifies the rate at which the MAX accepts multicast packets from clients on this interface. It does not affect the MBONE interface.

Note: By default, the Rate Limit parameter is set to 100. *This disables multicast forwarding on the interface.* If multicast forwarding is enabled on the interface but the Rate Limit parameter is left at the default 100, the forwarder handles IGMP packets, but does not accept packets from clients or forward multicast packets from the MBONE router.

To begin forwarding multicast traffic on the interface, you must set the rate limit to a number less than 100. For example if you set it to 5, the MAX accepts a packet from multicast clients on the interface every 5 seconds. Any subsequent packets received in that 5-second window are discarded.

Usage: Specify a number lower than the default 100 to begin forwarding multicast traffic on the interface.

Example: `Multicast Rate Limit=5`

Dependencies: This parameter has no effect when applied to the MBONE interface.

Location: Ethernet > Mod Config > Multicast

See Also: Forwarding, Mbone Profile, Multicast Client, Multicast Client, Multicast Rate Limit

RD MgrN (N=1–5)

Description: Specifies up to five IP addresses of SNMP managers that have SNMP read permission. The MAX responds to SNMP get and get-next commands from these SNMP managers only.

Usage: Specify the IP address of a host running an SNMP manager. The default is 0.0.0.0.

Dependencies: The Security parameter must be set to Yes for the RD Mgr1-5 parameters to have any effect. If the Security parameter is set to Yes, only SNMP managers at the IP addresses you specify can execute the SNMP get and get-next commands.

Location: Ethernet > Mod Config > SNMP Options

See Also: Security, WR Mgr1-5

Read Comm

Description: Specifies a read-only SNMP community name. If an SNMP manager sends this community name, it can access the Get and Get-Next SNMP agents.

Usage: Specify the community name that the MAX uses for authenticating the SNMP management station for read-only access. You can enter up to 16 alphanumeric characters. The default is Public.

Location: Ethernet > Mod Config > SNMP Options

See Also: R/W Comm, R/W Comm Enable

Recv Auth

Description: Specifies the authentication protocol the MAX uses to receive and verify a password for an incoming PPP connection.

Usage: Specify one of the following values:

- None (the default) means the MAX does not use an authentication protocol to validate incoming calls.
- PAP indicates the Password Authentication Protocol.

  PAP provides a simple method for a host to establish its identity in a two-way handshake. Authentication takes place only upon initial link establishment, and does not use encryption. The remote device must support PAP.
- CHAP indicates the Challenge Handshake Authentication Protocol.

  CHAP is more secure than PAP. It provides a way to periodically verify the identity of a host using a three-way handshake and encryption. Authentication takes place upon initial

link establishment; the MAX can repeat the authentication process any time after the connection is made. The remote device must support CHAP.

- MS-CHAP means the connection must use Microsoft's extension of CHAP.
  MS-CHAP was designed mostly for Windows NT/Lan Manager platforms. For details, see `ftp://ftp.microsoft.com/DEVELOPR/RFC/chapexts.txt`.)
- Either specifies any of the supported authentication schemes.
  When you select Either, the MAX allows authentication if the remote peer can authenticate using any of the designated authentication schemes.

Dependencies: If you specify an authentication method, you must also specify a password in the caller's profile. For a nailed connection, you must set Recv Auth and Send Auth to the same value at both ends of the connection.

Location: Ethernet > Answer > PPP Options

See Also: Auth Host, Recv PW, Send Auth, Send PW

Recv PW

Description: Specifies the password that the MAX expects to receive from the far-end while the connection is being authenticated. If this password is not sent by the far-end device, authentication fails. For PPP links, the password can contain up to 20 characters. For X.25/PAD, it can contain 48 characters.

If the link uses Combinet bridging, and the Answer profile requires a Combinet password, specify a password using all lowercase letters.

Usage: Specify a password. The password is case sensitive. The default is null.

Dependencies: This parameter does not apply if Recv Auth is set to None.

Location: Ethernet > Connections > *Connection profile* > Encaps Options, Ethernet > Names/Passwords

See Also: Encaps, Password Reqd, Recv Auth, Send Auth, Send PW

Remote Conf

Description: Specifies whether a RADIUS server configures the login banner and a list of Telnet hosts for the terminal-server menu mode.

Usage: Specify Yes or No. No is the default.

- Yes specifies the MAX obtains the configuration for these items from RADIUS. The local configuration for these items is ignored.
- No specifies it uses the local configuration for these items.

Location: Ethernet > Mod Config > TServ Options

See Also: Banner, Host # Addr, Host # Text, Upd Rem Cfg

Remote Mgmt

Description: Specifies whether the user at the far end of an AIM call can manage the MAX remotely using the DO Beg/End Rem Mgm command. In remote management, the MAX uses bandwidth between sites over the management subchannel established by the AIM protocol. If remote management is disabled and the remote user attempts to invoke that DO command, the message "Remote Management Denied" is displayed.

Usage: Specify Yes or No. Yes is the default.

- Yes allows remote management of the MAX unit via AIM call.
- No prevents remote management.

Dependencies: This parameter applies only when Call Type is set to AIM, FT1-B&O, or FT1-AIM. It does not apply if Call Mgm=Static.

Location: System > Sys Config

See Also: Call Mgm, Call Type

Remote X.121 Addr

Description: Specifies the X.121 address of the remote X.25 host to which this profile connects. The remote host is assumed to also support RFC1356 encapsulation of IP packets.

Note: This field cannot be left empty if Call Mode is set to Both or Outgoing.

Usage: Specify the X.121 address of the remote X.25 host. An X.121 address contains between 1 and 15 decimal digits, such as 031344159782738.

Example: `Remote X.121 Addr=031344159782111`

Location: Ethernet > Connections > *Connection profile* > Encaps Options

See Also: Call Mode

Reply DirectedBcast Ping

Description: Specifies whether the MAX forwards directed broadcast traffic to the Ethernet interface.

Usage: Specify Yes or No.

- Yes directs the MAX to forward directed broadcast traffic.
  Yes is the default.
- No directs the MAX to drop directed broadcast packets, preventing them from propagating to intermediary networks.

Dependencies: Reply DirectedBcast Ping applies only if the MAX supports IP routing.

Location: Ethernet > Mod Config

See Also: Forward Directed Bcast

Reply Enabled

Description: Specifies whether the MAX processes DHCP packets and acts as a DHCP server on this connection.

Usage: Specify Yes or No. No is the default.

- Yes specifies that the MAX will process DHCP packets.
  If the connection to the MAX is over a bridged connection the MAX will respond to all DHCP requests. If the connection is over any other type of connection, the MAX will only respond to NAT (Network Address Translation) DHCP packets.
- No specifies that the MAX will not process DHCP packets; it routes or bridges DHCP packets as any other packet.

Location: Ethernet > Answer > DHCP options, Ethernet > Connections > *Connection profile* > DHCP options

Retransmit Interval

Description: Specifies the number of seconds between retransmissions of OSPF packets. OSPF uses this value for LSA transmissions and when retransmitting Database Description and Link State Request Packets.

Usage: Specify a number greater than zero. The default is 5.

Example: `Retransmit Interval=15`

Location: Ethernet > Connections > *Connection profile* > OSPF Options, Ethernet > Mod Config > OSPF Options

Retry Count

Description: Specifies the maximum number of times that the MAX unit sends an L2TP control message. Any change you make to this parameter is reflected as soon as the previous timer expires.

Usage: Specify a decimal number from 1 to 10. The default is 10.

Example: `Retry Count=10`

Dependencies: Retry Count only applies if you have set L2TP Mode to either LAC, LNS, or Both.

Location: Ethernet>Mod Config>L2 Tunneling Options

See Also: CC Establish Timer, First Retry Timer, Hello Timer, L2TP Mode, LAC In Call Timer, LNS In Call Timer

Retry limit

Description: Specifies the number of times in a row, per connection, that the PAD allows the DTE to send a frame or frame acknowledgment in error before it disconnects the call. For a dial-up connection, the Retry Limit specifies how many times the PAD will allow the DTE to

try to establish a call that fails because the X.25 virtual call to the host could not be established. When the DTE exceeds the Retry Limit, the PAD disconnects the call.

Usage: Specify a value between 1 and 15. The default is 3.

Dependencies: This parameter is always applicable.

Location: Ethernet>Connections>*any Connection profile*>Encaps options,
Ethernet > Answer > T3POS options

Reverse Charge

Description: Specifies whether the call packet should include a reverse charge request facility parameter.

Usage: Specify one of the following values:

- Yes
  Specifies that the call packet includes a reverse charge request facility parameter.
- No (the default)
  Specifies that the call packet does not include a reverse charge request facility parameter.

Dependencies: This parameter is always applicable.

Location: Ethernet > Connections > *Connection profile* > Encaps options,
Ethernet > Answer > T3POS options

Rewrt Pattn

Description: Specifies the phone number pattern against which the destination phone number of the call will be matched to determine whether the phone number should be rewritten.

Usage: Enter up to 24 characters. The default is null, which specifies that there is no rewrite pattern for a phone number. The possible components of a pattern are:

0-9	Regular phone number digits.
#	The number sign.
*	A literal * (asterisk) as in *69.
*	Matches multiple characters.
^	Start of line marker. If present, must be at the start of the pattern. Indicates that the following pattern must be at the start of the dial string to match.
$	End of line marker. If present, must be at the end of the pattern. Indicates that the proceeding pattern must be at the end of the dial string to match.
.	Matches any single character. In this case, a period.

Sample Setting	Description of action
P=^1201 R=1973	Replaces dial strings starting with 1201 with 1973. For example, if the user dials 12015551212, the phone number is changed to 19735551212.

P=^ R=9	Prepends a 9 to every dial string. For example, if the user dials 5551212, the phone number is changed to 95551212.
P=^. R=	Strips the first digit of every dial string. For example, if the user dials 95551212, the phone number is changed to 5551212.

Location: System > Call Routes > *Call Routes profile*

See Also: Rewrt Replce

Rewrt Replce

Description: Specifies the phone number that replaces the actual digits entered by the POTS user.

Usage: Enter up to 24 characters. The default is null, which specifies that there is no replacement for a phone number. The possible components of a pattern can be any of the following:

Character	Description
0-9	Regular phone number digits.
#	The number sign.
*	Asterisk as in *69

Location: System > Call Routes > *Call Routes profile*

See Also: Rewrt Pattn

RIP

Description: Specifies how the MAX handles RIP update packets on the interface.

Note: Lucent recommends that all routers and hosts run RIP-v2 instead of RIP-v1. The IETF has voted to move RIP version 1 into the *historic* category and its use is no longer recommended.

Usage: Specify one of the following values:

- Off specifies that the MAX does not transmit or receive RIP updates. Off is the default.
- Recv-v2 indicates that the MAX receives RIP-v2 updates on the interface but does not send RIP updates.
- Send-v2
  This setting indicates that the MAX sends RIP-v2 updates on the interface but does not receive RIP updates.
- Both-v2 means the MAX sends and receives RIP-v2 updates on the interface.
- Recv-v1 indicates that the MAX receives RIP-v1 updates on the interface but does not send RIP updates.
- Send-v1
  This setting indicates that the MAX sends RIP-v1 updates on the interface but does not receive RIP updates.

- Both-v1 means the MAX sends and receives RIP-v1 updates on the interface.

Dependencies: This parameter does not apply if the MAX does not route IP.

Location: Ethernet > Answer > Session Options, Ethernet > Connections > *Connection profile* > IP Options, Ethernet > Mod Config > Ether Options

See Also: Route IP

RIP2 Use Multicast

Description: Enables or disables the default RIP-v2 behavior of using the multicast address (224.0.0.9) to send or receive updates to the routing table.

Usage: Specify Yes or No. The default is No.

- No disables the use of the multicast address for RIP updates. The updates are sent to and received from the broadcast address. Use this setting if you must use the broadcast address for backward compatibility with other systems.
- Yes enables RIP-v2 to send updates to and receive them from the multicast address (224.0.0.9) instead of the broadcast address.

Example: `RIP2 Use Multicast=Yes`

Dependencies: The parameter does not apply to RIP-v1.

Location: Ethernet > Connections > *Connection profile* > IP options

RipASEType

Description: Specifies how RIP routes are propagated into OSPF.

Usage: Specify one of the following values:

- Type1 is a metric expressed in the same units as the link-state metric (the same units as interface cost).
- Type2 is considered larger than any link-state path.

  Type 2 is the default. It assumes that routing between autonomous systems is the major cost of routing a packet, and eliminates the need for conversion of external costs to internal link-state metrics.

Dependencies: This parameter does not apply if the MAX does not route OSPF.

Location: Ethernet > Mod Config > Route Pref

RIP Policy

Description: Specifies a split horizon or poison reverse policy to handle update packets that include routes that were received on the same interface on which the update is sent. Split-horizon means that the MAX does not propagate routes back to the subnet from which they were received. Poison-reverse means that it propagates routes back to the subnet from which they were received with a metric of 16.

Usage: Specify Split Hrzn or Poison Rvrs. Poison Rvrs is the default.

Example: `RIP Policy=Poison Rvrs`

Dependencies: This parameter does not apply to RIP-v2. It applies only to RIP-v1 packets.

Location: Ethernet > Mod Config

Rip Preference

Description: Specifies the preference value for routes learned from the RIP protocol.

When choosing which routes to put in the routing table, the router first compares the Rip Preference values, preferring the lower number. If the Rip Preference values are equal, the router compares the Metric values, using the route with the lower Metric.

Usage: Specify a number between 0 and 255. The default value is 100. Zero is the default for connected routes (such as the Ethernet). The value of 255 means *Do not use this route*.

Dependencies: These are the default values for other types of routes:

- Routes learned from OSPF=10
- Routes learned from ICMP Redirects=30
- Static routes from IP address pools, RADIUS authentication, and the terminal server iproute add command=100
- Static routes in an IP Route profile or Connection profile=100

Location: Ethernet > Mod Config > Route Pref

Rip Queue Depth

Description: The maximum number of unprocessed RIP requests which the MAX saves. If RIP requests arrive at a rate faster than they can be processed, then a backlog builds up. This parameter sets the maximum depth of the queue. If the queue fills, further packets destined for it are discarded. This limit applies to each RIP socket, so if RIP is running on multiple interfaces, this parameter limits the number of requests stored per interface.

Usage: Enter an integer value from 0 to 1024. If you enter 0, the MAX saves RIP requests until it runs out of memory. The default is 50.

Note: Setting Queue Depth to 0 is not recommended. An unlimited queue depth could result in an out-of-memory error on the MAX if it receives a flood of packets on its RIP port.

Dependencies: This parameter does not apply if the MAX does not listen to RIP updates.

Location: Ethernet > Mod Config > Route Pref

See Also: Queue Depth, RIP

RIP Summary

Description: Specifies whether to summarize subnet information when advertising routes. If the MAX summarizes RIP routes, it advertises a route to all the subnets in a network of the same class; for example, the route to 200.5.8.13/28 (a class C address) would be advertised as

a route to 200.5.8.0. When the MAX does not summarize information, it advertises each route in its routing table "as-is;" in our example, the MAX advertises a route only to 200.5.8.13.

Usage: Specify Yes or No. Yes is the default.

- Yes causes the MAX to summarize RIP-v1 subnet information.
- No specifies the MAX advertises each route as-is.

Dependencies: This parameter does not apply to RIP-v2. It applies only to RIP-v1 packets. In addition, note that RIP Summary does not affect host routes.

Location: Ethernet > Mod Config

Rip Tag

Description: Assigns a specific tag to all routes propagated from RIP into OSPF. A tag is a 32-bit hexadecimal number border routers can use to filter this record.

Usage: Specify a 32-bit hexadecimal number. The default is c0000000.

Dependencies: This parameter does not apply if the MAX does not route OSPF.

Location: Ethernet > Mod Config > Route Pref

Rlogin

Description: Specifies whether an Rlogin session can be invoked from the terminal-server command line.

Usage: Specify Yes or No. No is the default.

- Yes enables Rlogin sessions.
- No specifies terminal-server users cannot invoke Rlogin.

Example: `Rlogin=Yes`

Dependencies: This parameter does not apply if terminal services are disabled.

Location: Ethernet > Mod Config > TServ Options

See Also: TS Enabled

Rob Ctl

Description: Specifies the robbed-bit call control mechanism that the MAX uses for inband signaling or a PBX that is not of type Leased 1:1. For inband signaling, the MAX places and answers calls using the call control mechanism you specify.

For PBX T1 conversion, the MAX emulates the WAN switch, and the PBX places and answers calls using the call control mechanism you specify.

Note: The call control mechanisms are based on the AT&T Special Access Connections specification for ACCUNET T1.5 services (AT&T TR 41458). Regardless of the type of call control mechanism you specify, the switch should not forward dialed digits to the MAX; doing so disrupts the handshaking process during multichannel calls.

Usage: Specify one of the following values:

- Wink-Start—Specifies that the MAX goes off-hook and waits for a 200-millisecond (ms) wink before dialing. The default is Wink-Start.

  In a wink, the answering device transmits an off-hook signal for a few hundred milliseconds. After receiving the wink, the calling device begins dialing.
- Idle-Start—Specifies that neither device sends a wink before either dialing or answering, and that off-hook dialing alone initiates a call.
- Inc-W-400—Specifies that each device sends a 400ms wink before dialing or answering a call. This is the appropriate setting when a MAX is connected back-to-back with another MAX, or when it is connecting to a PBX.
- Inc-W-200—Specifies that each device sends a 200ms wink before dialing or answering a call.
- Loop-Start—Specifies that the MAX uses loop start signaling instead of wink signaling.

  If you specify this setting, only MP+ and PPP provide an indication of call establishment or call termination. Using this setting for other types of calls is strongly discouraged. Specify it only if you cannot get wink signaling on your T1 access line.

  Loop-Start is not available when for PBX T1 conversion.

Location: Net/T1 > Line Config > Line *N*

See Also: PBX Type, Sig Mode

Route AppleTalk

Description: This parameter enables or disables the routing of AppleTalk data packets on the interface. AppleTalk routing must be set on both sides of the connection.

Usage: Specify Yes or No. No is the default.

- Yes enables AppleTalk routing.
- No specifies the MAX will not route AppleTalk for this connection (if set in the Connection profile) or accept inbound AppleTalk routing calls (if set in the Answer profile).

Location: Ethernet > Answer > PPP Options, Ethernet > Connections

See Also: Net Start, Net End, AppleTalk, AppleTalk Router, Route AppleTalk, Zone Name

Route IP

Description: Enables or disables the routing of IP data packets on the interface. IP routing must be enabled on both sides of the connection, and the MAX unit must be configured with an IP address in the Ethernet profile. To establish an inbound connection, IP routing must also be enabled in the Answer profile.

Usage: Specify Yes or No. Yes is the default.

- Yes enables IP routing.
- No specifies the MAX will not route IP for this connection (if set in the Connection profile) or accept inbound IP routing calls (if set in the Answer profile).

Dependencies: If you have a MAX running Multiband Simulation, Route IP is disabled.

Location: Ethernet > Answer > PPP Option, Ethernet > Connections

See Also: Bridge, Encaps, Profile Reqd

Route IPX

Description: This parameter enables or disables the routing of IPX data packets on the interface. IPX routing must be enabled on both sides of the connection, and the MAX unit must be configured with an IPX network address and frame type in the Ethernet profile. Note that the MAX will route and spoof only one IPX frame type. Other frame types will be bridged if bridging is enabled.

Usage: Specify Yes or No. No is the default.

- Yes enables IPX routing.
- No specifies the MAX will not route IPX for this connection (if set in the Connection profile) or accept inbound IPX routing calls (if set in the Answer profile).

Dependencies: If you have a MAX running Multiband Simulation, Route IPX is disabled.

Location: Ethernet > Answer > PPP Options, Ethernet > Connections

See Also: Bridge, IPX Frame, IPX Net

Route line *n*

Description: Specifies the IP address of the L2TP Network Server (LNS) if you set Line *n* tunnel type to L2TP, or the IP address of the PPTP Network Server (PNS) if you set Line *n* tunnel type to PPTP.

Usage: Specify an IP address. The default is 0.0.0.0. If you accept the default, the MAX does not tunnel any call received on the WAN line specified in Line *n* tunnel type.

Example: `Route Line 1=10.10.10.10`

Dependencies: When configuring L2TP, Route line *n* applies only if you set L2TP Mode to LAC or Both. When configuring PPTP, Route line *n* applies only if you set PPTP Enabled to Yes. You must also set the corresponding Line *n* tunnel type parameter to PPTP or L2TP, as applicable.

Location: Ethernet > Mod Config > L2 Tunneling Options

See Also: L2TP Mode, PPTP Enabled, Line *n* tunnel type

RPOA

Description: Specifies the set of Recognized Private Operating Agency (RPOA) user facilities to use in the next call request. The RPOA facilities provide the data network identification code for the requested initial RPOA transit network and is in the form of four decimal digits.

Usage: Specify the RPOA user facilities to use in the next call request. You can specify up to four digits. The default is null.

Dependencies: Encaps must be set to X25/PAD for RPOA to be applicable.

Location: Ethernet > Connections > *Connection profile* > Encaps options, Ethernet > Answer > PAD options, Ethernet > Answer > T3POS options

RS-366 Esc

Description: Specifies the escape character the MAX uses during RS-366 ext2 dialing or during X.21 ext2 dialing.

Usage: Specify an escape character. You can enter one of these characters:

```
* # 5 6 7 9 0 00
```

The default is #.

Location: Host/Dual (Host/AIM6) > Port*N* Menu > Port Config

See Also: Dial

Run OSPF

Description: Enables or disables OSPF on the interface. When OSPF is active, the MAX sends update packets out on the interface. These packets set the correct link state for the interface and make sure that the local link-state database is an exact copy of the database maintained by other OSPF routers.

Usage: Specify Yes No. No is the default.

- Yes turns on OSPF routing on the interface. There is currently no spoofing for running active OSPF over dial-on-demand links, so periodic OSPF traffic will bring up the link almost continuously. OSPF is meant to run on nailed connections.
- No turns off OSPF on the interface.

Dependencies: If you have a MAX running Multiband Simulation, Run OSPF is disabled.

See Also: Ethernet > Connections > *Connection profile* > OSPF Options, Ethernet > Mod Config > OSPF Options

Rx Gain

Description: Specifies the gain applied to the signal received from the connected equipment.

Usage: Specify a value from 0 to -6 db to weaken the signal. Specify a value from +1 to +12 db to strengthen the signal. The default is -3 dB.

Location: Analog FXS > FXS Config > *FXS Configuration profile* > Line *N*

S

SAP HS Proxy

Description: This parameter specifies whether the MAX performs SAP Home Server Proxy.

Usage: Press Enter to cycle through the choices.

- Yes enables NetWare SAP Home Server Proxy.
- No disables NetWare SAP Home Server Proxy.

  No is the default.

Dependencies: The SAP HS Proxy parameter does not apply (SAP HS Proxy=N/A) if IPX routing is disabled (Route IPX=No).

Location: Ethernet > Connections > *Connection profile* > IPX Options

SAP HS Proxy Net#n (n=1-6)

Description: Specifies an IPX network to which SAP broadcasts should be directed.

Usage: Press Enter to open a text field. Then, type an IPX network number using an 8-digit (4-byte) hexadecimal value. The default is 00000000.

Dependencies: The SAP HS Proxy Net#*N* parameter does not apply (SAP HS Proxy Net#*N*=N/A) if either IPX routing is disabled (Route IPX=No) or if SAP Home Server Proxy is disabled (SAP HS Proxy=No).

Location: Ethernet > Connections > *Connection profile* > IPX Options

SAP Reply

Description: Enables or disables a home agent's ability to reply to the mobile node's IPX Nearest Server Query if the home agent knows about a server on the home network. It is used only when accessing this unit as a home agent.

Usage: Specify Yes or No. No is the default.

- Yes enables the MAX configured as ATMP home agent to reply to a mobile node's Nearest Server Query with the address of a server on the home network.
- No specifies the MAX will not respond to these queries from a mobile node.

Location: Ethernet > Mod Config > ATMP Options

See Also: ATMP Gateway, ATMP Mode

Sealing Current

Description: Sealing Current allows you to enable *sealing* on the loop. Sealing refers to the ability of the IDSL card to send some current (40V) on the line when enabled. You typically use this feature to keeps the physical connection from corroding. This could occur if there is no activity on the line such as when there is no device connected on the other end.

Usage: Specify Yes to enable sealing. The default value is Off.

Dependencies: Note that the Sealing Current setting is not saved to the MAX permanent memory. This means that whenever you reboot the MAX, the Sealing Current parameter reverts to its default value of 0.

Location: BRI/LT > Line Diag > line *n*

Sec DNS

Description: Specifies the IP address of the secondary domain name server. It will be accessed only if the primary DNS server is unavailable.

Usage: Specify the IP address of the secondary domain name server. The default is 0.0.0.0. Accept this default if you do not have a secondary domain name server.

Example: `Sec DNS=200.207.23.1`

Location: Ethernet > Mod Config > DNS

See Also: Domain Name, Pri DNS

Sec Domain Name

Description: Specifies a secondary domain name that the MAX can search using DNS. The MAX performs DNS lookups in the domain configured in Domain Name first, and then in the domain configured in Sec Domain Name.

Usage: Specify a secondary domain name. You can enter up to 63 characters.

Example: `Sec Domain Name=xyz.com`

Location: Ethernet > Mod Config > DNS

See Also: Domain Name

Sec History

Description: Specifies a number of seconds to use as the basis for calculating average line utilization (ALU). The ALU is used in calculating when to add or subtract bandwidth from a multi-channel call that supports dynamic bandwidth management.

The number of seconds you choose for the Sec History parameter depends on your device's traffic patterns. For example, if you want to average spikes with normal traffic flow, you can want the MAX to establish a longer historical time period. If, on the other hand, traffic patterns consist of many spikes that are short in duration, you can want to specify a shorter period of time; doing so assigns less weight to the short spikes.

If you specify a small value for the Sec History parameter, and increase the values of the Add Pers parameter and the Sub Pers parameter relative to the value of Sec History, the system becomes less responsive to quick spikes.

The easiest way to determine the proper values for Sec History, Add Pers, and Sub Pers is to observe usage patterns; if the system is not responsive enough, the value of Sec History is too high.

Usage: Specify a number between 1 and 300. The default value for MP+ calls is 15 seconds; the default value for dynamic AIM calls is 30 seconds.

Dependencies: This parameter applies only to multilink calls that support dynamic management.

Location: Ethernet > Answer > PPP Options, Host/Dual (Host/AIM6) > Port*N* Menu > Directory, Ethernet > Connections > *Connection profile* > Encaps Options

See Also: Add Pers, Call Mgm, Dec Ch Count, Dyn Alg, Encaps, Inc Ch Count, Sub Pers, Target Util

Sec Num

Description: Specifies the secondary add-on number for the Net BRI line. When the MAX receives a multichannel AIM, BONDING, or MP+ call, it reports the primary add-on number (Pri Num) and the secondary add-on number (Sec Num) to the calling party. The calling MAX can then add more channels. If you do not specify an add-on number and the calling MAX needs to add more channels, it redials the telephone number it used to make the first connection. (See "Ch N (N=1–24, 1–32)" on page 4-67 for more detail on add-on numbers.)

Usage: Specify a telephone number with a limit of 24 characters, which can include the following characters: 1234567890()[]!z-*#|. The default is null.

Dependencies: This parameter does not apply when Link Type=P-T-P (point-to-point mode).

Location: Net/BRI > Line Config > Line *N*

See Also: Pri Num, Sub-Adr

Sec SPID

Description: Specifies the SPID (Service Profile Identifier) associated with the secondary telephone number for the Net BRI line. The carrier supplies both the telephone number and the associated SPID.

If the MAX uses only one channel of a multipoint ISDN BRI line and another device uses the other channel, you can choose to operate in single-terminal mode. Set one channel to unused, and enter only one SPID. The device sharing the line must enter the other assigned SPID.

Note: The MAX appends the value of the SPID with a TID if you are connected to a Northern Telecom switch running NI-1.

Usage: Specify up to 16 characters; you must limit those characters to numbers, hyphens, and parentheses. The default value is 0 (zero).

Dependencies: This parameter does not apply when the line is serviced by an AT&T switch in point-to-point mode.

Location: Net/BRI > Line Config > Line *N*

See Also: B1 Usage, B2 Usage, Link Type, Pri Num, Pri SPID, Sec Num, Switch Type

SecurID DES Encryption

Description: Specifies whether the server uses standard DES or the native encryption provided by SecurID.

Usage: Specify Yes or No. No is the default.

- Yes specifies the server uses standard DES encryption.

- No specifies the server uses the native encryption provided by SecurID.

Dependencies: This parameter does not apply unless Auth specifies SECURID.

Location: Ethernet > Mod Config > Auth

See Also: Auth, SecurID Host Retries, SecurID NodeSecret

SecurID Host Retries

Description: Specifies the number of times the MAX attempts to contact the SecurID host before timing out.

Usage: Specify an integer. The default value is 3.

Dependencies: This parameter does not apply unless Auth specifies SECURID.

Location: Ethernet > Mod Config > Auth

See Also: Auth, SecurID DES Encryption, SecurID NodeSecret

SecurID NodeSecret

Description: On the first successful authentication attempt, the SecurID host informs the MAX of a secret value, theoretically only known to the MAX, to be used in subsequent interactions between the MAX and the SecurID host. This value appears in the SecurID NodeSecret parameter. The user must have sufficient permissions in the active Security profile to view the value of this parameter.

Note: After the SecurID server sets the value of this parameter, if you later reset the parameter to null, you must reinitialize the interface to the MAX in the SecurID server by using the *Client Edit* menu selection in the ACE server's *sdadmin* utility. Then, the server sends a new NodeSecret at the next successful authentication.

Usage: The initial value must be null (the default). After the first SecurID authentication occurs, the value is set by the server.

Dependencies: This parameter does not apply unless Auth specifies SECURID.

Location: Ethernet > Mod Config > Auth

See Also: Auth, SecurID Host Retries, SecurID NodeSecret

Security

Description: Enables or disables a kind of security, which differs depending on which subprofile the parameter appears in.

Usage: Specify one of the following values.

For SNMP address security:

- Yes—The unit compares the source IP address of packets containing SNMP commands against a list of qualified IP addresses specified by the RD Mgr1-8 and WR Mgr1-8

parameters. (The MAX always checks the version and community strings before making source IP address comparisons. The Security parameter does not affect those checks.)

- No (the default) —The unit does not compare IP addresses, so address-security is not used.

For SNMP traps:

- Yes—The unit generates traps for Security events (such as failed login attempts) and sends the trap-PDU to the SNMP manager.
- No (the default) —The unit does not generate traps based on Security events.

For terminal-server security:

- Full—The unit prompts you for a name and password upon initial login and when you switch between terminal mode and menu mode.
- Partial—The unit prompts you for a name and password only when entering terminal mode, not for menu mode.
- None (the default) —The unit does not prompt you for a login name and password to enter the terminal-server interface.

Location: Ethernet > Mod Config > TServ Options, Ethernet > Mod Config > SNMP Options, Ethernet > SNMP Traps

See Also: Initial Scrn, Max DS0 Mins, Passwd, RD Mgr*N*, Toggle Scrn, WR Mgr*N*

Security Level

Description: Specifies the level of security to use when generating messages.

Usage: Specify one of the following settings:

- None (the default) specifies no authentication and no privacy.
- Auth, NoPriv specifies authentication and no privacy.
- Auth & Priv specifies authentication and privacy.

Example: `Security Level=Auth & Priv`

Dependencies: For Auth & Priv to apply, you must set the Priv Protocol and Priv Password parameters in the Ethernet > SNMPv3 USM Users submenu.

Location: Ethernet > SNMPv3 Target Params

See Also: Active, Dest Port, Message Proc Model, Notify Tag List, Security Model, Security Name, Tag, Target Param Name

Security Model

Description: Specifies the security model to use when generating SNMP messages.

Usage: Specify one of the following values:

- V1 (the default) specifies the SNMP version 1 security model.
- V3-USM specifies the SNMP version 3 User-Based Security Model (USM). For SNMPv3 Notifications support, specify V3-USM.

Example: `Security Model=V3-USM`

Dependencies: Consider the following:

- You can specify V1 only when you have also set Message Proc Model to V1.
- You can specify V3-USM only when you set Message Proc Model to V3.
- When Security Model is set to V3-USM, you must configure the Ethernet > SNMPv3 USM Users submenu with the name specified for the Security Name parameter in order for the SNMPv3 Target Params profile to have any effect.

Location: Ethernet > SNMPv3 Target Params

See Also: Active, Dest Port, Message Proc Model, Notify Tag List, Security Level, Security Name, Tag, Target Param Name

Security Name

Description: Specifies a security name that identifies the user on whose behalf SNMPv3 USM messages are generated.

Usage: Specify up to 22 characters. The default is null.

Example: `Security Name=newuser`

Dependencies: Security Name applies only if Security Model is set to V3-USM.

Location: Ethernet > SNMPv3 Target Params

See Also: Active, Dest Port, Message Proc Model, Notify Tag List, Security Level, Security Model, Tag, Target Param Name

Sec. Tunnel Server

Description: Specifies a secondary tunnel server the unit uses if the primary tunnel server is unavailable.

Usage: Specify a dotted-decimal IP address or hostname.

Example: `Sec. Tunnel Server=123.123.12.12`

Dependencies: This parameter is not applicable if the Profile Type parameter is set to Disabled or the Tunnel Protocol parameter specifies PPTP.

Location: Ethernet > Mod Config > *any Connection profile* > Tunnel Options

See Also: ATMP HA RIP, Client ID, Home Network Name, Max Tunnels, Password, Pri. Tunnel Server, Profile Type, Sec. Tunnel Server, Tunnel Protocol, Tunnel VRouter, UDP Port

Sec WINS

Description: Specifies the IP address of the secondary NetBIOS server.

Usage: Specify an IP address. The default is 0.0.0.0.

Example: `Sec WINS=10.2.3.4`

Location: Ethernet > Mod Config > DNS

See Also: Pri WINS

Send Auth

Description: Specifies the authentication protocol that the MAX uses to send a password to the far-end of a PPP connection.

Usage: Specify one of the following values:

- None (the default) means the MAX does not use an authentication protocol to validate incoming calls.
- PAP indicates the Password Authentication Protocol.

  PAP provides a simple method for a host to establish its identity in a two-way handshake. Authentication takes place only upon initial link establishment, and does not use encryption. The remote device must support PAP, and you must specify a password in the Send PW parameter.
- CHAP indicates the Challenge Handshake Authentication Protocol.

  CHAP is more secure than PAP. It provides a way to periodically verify the identity of a host using a three-way handshake and encryption. Authentication takes place upon initial link establishment; the MAX can repeat the authentication process any time after the connection is made. The remote device must support CHAP, and you must specify a password in the Send PW parameter.
- PAP-TOKEN is an extension of PAP authentication.

  In PAP-TOKEN, the user making outgoing calls from the MAX authenticates his or her identity by entering a password derived from a hardware device, such as a hand-held security card. The MAX prompts the user for this password, possibly along with a challenge key. The NAS (Network Access Server) obtains the challenge key from a security server that it accesses through RADIUS.

  If you specify PAP-TOKEN-CHAP, you must enter a password in the Aux Send PW parameter; this password must match the password in the RADIUS entry for authenticating the call. If you do not enter identical passwords in the Aux Send PW parameter and the RADIUS entry, the MAX cannot extend the MP+ call beyond a single channel.
- PAP-TOKEN-CHAP is PAP-TOKEN for the base channel with CHAP for subsequent channels.

  For multilink PPP calls where the answering unit requires security card authentication, PAP-TOKEN and PAP-TOKEN-CHAP begin identically when authenticating the first channel of an MP+ call. However, when the MAX adds additional channels to the MP+ call, PAP-TOKEN requires security-card authentication for each new channel, while PAP-TOKEN-CHAP uses CHAP authentication for all new channels. CHAP authentication works automatically, without the use of a hand-held security card.
- CACHE-TOKEN begins authentication using a hand-held security card, and fills a token cache set up for you on the RADIUS server.

  CHAP authenticates your subsequent calls without using your hand-held security card. After a period of time configured in your entry in the RADIUS users file, the token cache expires and the next call you place must again be authenticated using your hand-held security card.

If you request CACHE-TOKEN, the Send PW parameter must match the Ascend-Receive-Secret attribute in the RADIUS entry that authenticated the call. If you do not enter identical passwords in the Send PW parameter and Ascend-Receive-Secret attribute, CACHE-TOKEN calls are rejected after initial access through hand-held security card authentication.

Dependencies: For a nailed connection, you must set Recv Auth and Send Auth to the same value at both ends of the connection. PAP-TOKEN and PAP-TOKEN-CHAP require configuration of a SAFEWORD or ACE entry in the NAS's RADIUS users file with the caller's name. See the *MAX Security Supplement* for details.

Location: Ethernet > Connections > *Connection profile* > Encaps Options

See Also: APP Host, APP Port, APP Server, Call Type, Dial Brdcast, Encaps, Recv Auth, Recv PW, Send PW

Send Disc

Description: Specifies the number of seconds the MAX waits from the time a call is presented before it clears the call. The value selected must be less than the T310 timer value used by the switch servicing the MAX.

Usage: Press Enter to open a text field. Then, type the number of seconds the MAX should wait from the time a call is presented to it before it clears the call. The timer is cancelled if the MAX sends a ISDN Alerting message or ISDN Disconnect message or if the network switch sends an ISDN Disconnect message. You can specify a number from 0 to 60. The value of 0 (zero) disables this parameter. The default is 0 (zero).

Dependencies: Send Disc does not apply if the MAX does not support ISDN signaling.

Location: Net/T1 > Line Config > Line *N*

See Also: Timeout Busy

Send Name

Description: When a user dials into a MAX using CHAP authentication, the MAX by default uses the system name (System > Sys Config > Name parameter) during CHAP authentication. Alternatively, you can set the Send Name parameter, Send Name in Ethernet Answer > PPP Options to specify the name to be used during CHAP authentication. If you set the Send Name parameter, the MAX ignores the value of the System > Sys Config > Name parameter.

Usage: Specify up to 16 characters. If you do not change the default, null value, the MAX uses the System > Sys Config > Name parameter for CHAP verification.

Location: Ethernet >Answer > PPP Options

Send PW

Description: Specifies the password that the MAX sends to the far-end while the connection is being authenticated. If this password is not received by the far-end device, authentication fails. If the link uses Combinet bridging and the far-end Answer profile specifies that a

password is required (Password Reqd=Yes), you must enter a password using all lowercase letters.

Usage: Specify a password, up to 20 characters. The password is case sensitive. The default is null.

Dependencies: This parameter does not apply if Send Auth is set to None.

Location: Ethernet > Connections > *Connection profile* > Encaps Options

See Also: Encaps, Password Reqd, Recv Auth, Recv PW, Send Auth

Serial

Description: Specifies an ISDN subaddress associated with the MAX unit's AIM ports. ISDN subaddressing is used for routing inbound calls to the appropriate destination in the MAX unit.

Usage: Specify a number between 0 and 99. The default is 0.

Location: System > Sys Config

See Also: Ans *N*#

Server

Description: Enables or disables the on-board RADIUS server, or specifies the IP address of a BOOTP server, depending on where the parameter appears.

In the RADIUS Server submenu of the Ethernet profile, it enables or disables the on-board RADIUS server, which enables the MAX to appear as a server to some client requests.

In the BOOTP Relay submenu of the Ethernet profile, it specifies the IP address of a BOOTP server for handling BOOTP requests. If a server is on the same local-area network as the MAX, BOOTP requests from other networks are relayed to the server. If a server is on another network, BOOTP requests from clients on the same local-area network as the MAX are relayed to the remote server. If you specify two BOOTP servers, the MAX that relays the BOOTP request determines when each server is used. The order of the BOOTP servers in the BOOTP Relay menu does not necessarily determine which server is tried first.

Usage: To enable the on-board RADIUS server, specify Yes. The default setting is No.

To enable the MAX to communicate with a BOOTP server, specify the server's IP address. The default is 0.0.0.0.

Location: Ethernet > Mod Config > RADIUS Server, Ethernet > Mod Config > BOOTP Relay

See Also: Client #, Server Key, Server Port BOOTP Relay Enable

Server Key #N (N=1–9)

Description: Specifies up to nine RADIUS server keys, shared with the RADIUS clients. It is used to validate the authenticator field on requests and generate the authenticator on responses. You should specify a key for each client address. For example:

- Client #1= 125.65.5.0/24
  Server Key #1=bob
- Client #2= 125.5.0.0/16
  Server Key #2=bob
- Client #3= 135.50.248.76/32
  Server Key #3=sue

Usage: Specify a string containing the shared secret. You can enter up to 20 characters. For security purposes, the string is hidden when the parameter is displayed. The default is null.

Dependencies: This parameter does not apply if the on-board RADIUS server is disabled.

Location: Ethernet > Mod Config > RADIUS Server

See Also: Client #N, Server, Server Port, *TAOS RADIUS Guide and Reference*

Server Name

Description: Specifies the name of a NetWare server. In an IPX Route profile, it is the server that will be reached via the specified route.

In an IPX SAP Filters profile, it is the name of a local or remote NetWare server. If the server is on the local network and this is an Output filter, Server Name specifies whether to include or exclude advertisements for this server in SAP response packets. If the server is on the remote IPX network and this is an Input filter, the Server Name parameter specifies whether to include or exclude this server in the MAX service table.

Usage: Specify a NetWare server name. In an IPX SAP filter, you can use the wildcard characters * and ? for partial name matches.

Dependencies: These parameters do not apply if IPX routing is not in use.

Location: Ethernet > IPX Routes, Ethernet > IPX SAP Filters > Input SAP Filters > In filter *N*, Ethernet > IPX SAP Filters > Output SAP Filters > Out filter *N*

See Also: Route IPX, Server Type

Server Port

Description: This parameter indicates the UDP port number to use for the on-board RADIUS server.

Usage: Specify a number between 1 and 65535. The default is 1700. Although the value can match the port setting for RADIUS authentication or accounting, we recommend that you specify a different port.

Dependencies: This parameter does not apply if the on-board RADIUS server is disabled.

Location: Ethernet > Mod Config > RADIUS Server

See Also: Client #, Server, Server Key

Server Type

Description: Specifies a Service Advertising Protocol (SAP) type. SAP advertises services by a type number. For example, NetWare file servers are SAP Service type 0004. For complete information on SAP service types, refer to your Novell NetWare documentation.

In an IPX Route profile, specifies the type of service advertised by the server that will be reached via the specified route.

In an IPX SAP Filters profile, the Server Type parameter specifies whether to include or exclude advertisements for the specified service type in SAP response packets. In an Input filter, it specifies whether to include remote services of this type in the MAX service table.

Usage: Specify a hexadecimal number that represents a valid SAP service type.

Location: Ethernet > IPX RoutesEthernet > IPX SAP Filters > Input SAP Filters > In filter *N*, Ethernet > IPX SAP Filters > Output SAP Filters > Out filter *N*

See Also: Server Name, Type, Valid

Sess Timer

Description: When set for RADIUS accounting, this parameter sets the amount of time the MAX waits for a response to a RADIUS accounting request. You can set this parameter globally and for each connection. If it does not receive a response within that time, the MAX sends the accounting request to the next server's address (for example, server #2). If all RADIUS accounting servers are busy, the MAX stores the accounting request and tries again at a later time. It can queue up to 154 requests.

When set for RADIUS/LOGOUT authentication, Sess Timer specifies the interval at which session reports will be sent to the RADIUS/LOGOUT authentication server. For example, if you wish the MAX to send Session Events at one-minute (60-second) intervals, set Auth to RADIUS/LOGOUT and Sess Timer to 60.

Usage: When setting the timer for RADIUS accounting, specify a number from 1 to 10. The default value in the Ethernet profile is 0. The default in a Connection profile is 1.

When setting the timer for RADIUS/LOGOUT authentication, specify a number between 0 and 655353. The default is 0, which means that no Session Events will be sent.

Example: `Sess Timer=10`

Dependencies: For accounting, this parameter applies only to RADIUS—because TACACS+ uses TCP, it has its own timeout method. For authentication, this parameter applies only to RADIUS/LOGOUT.

Location: Ethernet > Mod Config > Accounting, Ethernet > Mod Config > Auth

See Also: Acct, Auth

Session Key

Description: Specifies whether or not all new session entries are assigned a session key in RADIUS.

Usage: Specify Yes or No. No is the default.

- Yes specifies session keys will be assigned to all new session entries.
- No specifies session keys will not be assigned.

Example: `Session Key=Yes`

Dependencies: This parameter is not applicable if Server is set to No. See the Attributes parameter for information about specifying which attributes will be required for identification of a session.

Location: Ethernet > Mod Config > RADIUS Server

See Also: Attributes

Shared Prof

Description: The MAX can force terminal server users to connect using unique profiles. The Shared Prof parameter in the Ethernet > Mod Config profile or in a Connection profile specifies:

- Whether multiple users can share a single Connection profile or a single RADIUS user profile *or*
- Whether a single user can have multiple sessions active

This parameter enables multiple incoming calls to share a local Connection profile or a RADIUS users file with Connection profile parameters. Sharing a profile cannot result in two IP addresses sharing the same interface, so this parameter is typically used to share profiles when the caller is assigned an IP address dynamically, which ensures that each caller is assigned a unique address.

Usage: Specify Yes or No. No is the default.

- Yes specifies the MAX will allow more than one caller to share the same profile, provided that no IP address conflicts will result.
- No specifies the MAX will not allow shared profiles.

Note: If Shared Prof is set to No and a user attempts to log in to the MAX terminal server with the same username and password as an already active session, the following message is displayed and the MAX disconnects the user: `***Account Already In Use`

Dependencies: This parameter does not apply to Combinet links or connections that have hard-coded IP addresses. For the Ascend-Shared-Profile-Enable attribute to apply, you must disable shared profiles for the MAX as a whole with Ethernet > Mod Config > Shared Prof=No.

Location: Ethernet > Mod Config, Ethernet > Connections > *Connection profile*

See Also: Encaps, Name, Pool #*N* Count, Pool #*N* Start, Recv PW

Sig Mode

Description: Specifies the type of signaling used on the T1 or E1 line.

Usage: In a Net/T1 profile, specify one of the following values:

Value	Description
Inband (the default)	The line uses 8 Kbps of each 64-Kbps channel for WAN synchronization and other signaling. The remaining 56 Kbps handle the transmission of user data. Another term for inband signaling is *robbed-bit* signaling. *Robbed-bit* refers to the 8 Kbps used for signaling on each channel. Switched-56 lines and T1 lines containing one or more switched channels use inband signaling. If you specify inband signaling, you must set the Rob Ctl parameter to specify a call control mechanism.
ISDN	The D channel handles WAN synchronization and other signaling, and the B channels carry the user data. Another term for ISDN D-channel signaling is out-of-band signaling. T1 PRI and Net BRI lines containing one or more switched channels use ISDN D-channel signaling.
NFAS (Non-Facility Associated Signaling)	A special case of ISDN D-channel signaling. When you use NFAS, two or more T1 PRI lines use the same D channel, and you can add a backup D channel. NFAS is required for the Switched-1536 data service because all 24 channels of the T1 PRI line carry user data and therefore the D channel must be on another line.
PBX T1	Specifies that line #2 can access the WAN through line #1. When Sig Mode=PBX T1, the MAX emulates the WAN switch and the PBX connected to the line #2 port uses the call control mechanism you specify for Rob Ctl to place and answer calls. If you set Sig Mode to PBX T1, keep in mind the following information: • If line #2 uses inband signaling and line #1 uses ISDN D-channel signaling, set PBX Type to Voice or PBX Type to Data. • Any calls placed to a device connected to line #2 are switched to line #1 of the expansion module or to any line configured for ISDN, that is, to any line for which Sig Mode=ISDN. • If line #2 consists entirely of nailed-up and unused channels, and line #1 uses inband signaling, set PBX Type to Leased 1:1.
PBX T1 *(continued)*	• The MAX connects calls received on line #1 to the corresponding nailed-up channels of line #2, or it handles them in the usual manner when the corresponding channel of line #2 is unused. • If PBX Type=Voice, the MAX switches only incoming voice calls to line #2. • If PBX Type=Data, the Ans # and Ans Service parameters determine which incoming calls on the T1 PRI line the MAX switches to line #2. • Line #2 typically connects to a PBX or other type of device that uses inband signaling. Do not use line #2 for data calls.

In a Net/E1 profile, specify one of the following values:

- None—A leased line.

- ISDN—ISDN signaling using the D channel. You must designate the 32nd channel of the E1 line as the D channel.
- DPNSS—The interface supports DPNSS or DASS 2 signaling.
- DTMF_R2— DTMF R2 signaling detection and processing. Once selected, DTMF R2 detection is enabled with the next VoIP call. DTMF R2 detection is only supported when R2 signal processing is enabled for this MultiVoice gateway.
- R2—R2 signaling.
- Metered—Metered R2 signaling protocol, used in Brazil and South Africa.
- Chinese—A version of the R2 signaling protocol, used in China.
- Philippines—A version of the R2 signaling protocol with CLID processing, used in the Philippines.
- Argentina—A version of the R2 signaling protocol with CLID processing, used in Argentina.
- Brazil—A version of the R2 signaling protocol with CLID processing, used in Brazil.
- India—A version of the R2 signaling protocol with CLID processing, used in India.
- Malaysia—A version of the R2 signaling protocol with CLID processing, used in Malaysia.
- Czech—A version of the R2 signaling protocol, used in the Czech Republic.
- Korean—A version of the R2 signaling protocol, used in Korea.
- P7—P7 protocol signaling.
- New Zealand—A version of the R2 signaling protocol with CLID processing, used in New Zealand.
- Thailand—A version of the R2 signaling protocol with CLID processing, used in Thailand.
- Israel—A version of the R2 signaling protocol with CLID processing, used in Israel.
- Kuwait—A version of the R2 signaling protocol with R2 register signaling, used in Kuwait.
- Mexico—A version of the R2 signaling protocol with CLID processing, used in Mexico.

Location: Net/T1 > Line Config > *any profil*e > Line *N*, Net/E1 > Line Config > *any profil*e > Line *N*

Signaling

Description: Specifies signaling on an analog loop.

Usage: Specify Groundstart or Loopstart. Regular phones use Loopstart, which is the default.

Location: Analog FXS > FXS Config > *FXS Configuration profile* > Line *N*

Silent

Description: Suppresses status messages when interactive users establish a terminal-server connection.

Usage: Specify Yes or No. No is the default.

- Yes suppresses status messages upon connection of interactive terminal-server sessions.
- No sends all status messages.

Example: `Silent=Yes`

Dependencies: This parameter is not applicable when terminal services are disabled.

Location: Ethernet > Mod Config > TServ Options

Single Answer

Description: Specifies whether the MAX completes the answering and routing of one call before answering and routing the next call.

Usage: Specify Yes or No. Yes is the default.

- Yes specifies the MAX will answer and route one call before answering and routing the next call. Yes is the default, and should be used if the MAX is not configured for dual-port calls, or if an incoming call is explicitly routed.
- No specifies the MAX will answer and route an incoming call immediately.

Example: `Single Answer=Yes`

Location: System > Sys Config

See Also: Ans #, B1 Prt/Grp, B2 Prt/Grp, Ch *N* Prt/Grp

SLIP

Description: Specifies whether a Serial Line IP (SLIP) session can be invoked from the terminal-server command line.

Usage: Specify Yes or No. No is the default.

- Yes enables users to invoke SLIP sessions from the terminal-server.
- No disables this use of SLIP.

Dependencies: This parameter does not apply if terminal services are disabled.

Location: Ethernet > Mod Config > TServ Options

See Also: TS Enabled

SLIP BOOTP

Description: Specifies whether or not the MAX responds to BOOTP within SLIP sessions. If a unit dials into the MAX unit's terminal server and runs SLIP, it can get an IP address through a BOOTP request. This IP address is taken from the MAX unit's IP address pool or by the Ascend-IP-Pool-Definition attribute in the RADIUS database.

Usage: Specify Yes or No. No is the default.

- Yes enables the MAX to respond to a BOOTP request from the calling unit during a SLIP session.

- No disables BOOTP for SLIP sessions.

Dependencies: This parameter does not apply if terminal services are disabled or if SLIP is set to No.

Location: Ethernet > Mod Config > TServ Options

See Also: Pool # Count, Pool # Start, TS Enabled

SLIP Info

Description: Specifies the type of information the MAX reports to SLIP users.

Usage: Specify one of the following values:

- Basic (the default)

  Specifies that the MAX only reports the SLIP user's IP address and the Maximum Transmission Unit (MTU).

- Advanced

  Specifies that the MAX reports the SLIP user's IP address, the MTU, the Netmask, and the Gateway to SLIP users. Note that the gateway is the MAX unit's IP address.

Example: The MAX now reports the following information whenever a user connects:

```
Entering SLIP Mode
IP address is 192.1.1.1
MTU is 1500
Netmask: 255.255.255.0
Gateway: 192.168.6.181
```

The Netmask label identifies the subnet mask the MAX is using. The Gateway label identifies the MAX unit's IP address.

Location: Ethernet > Mod Config > TServ Options

See Also: IP Addr Msg, IP Netmask Msg

SNTP Enabled

Description: Enables or disables the MAX to use SNTP (Simple Network Time Protocol—RFC 1305) to set and maintain its system time by communicating with an SNTP server. SNTP must be enabled for the MAX to communicate using that protocol.

When enabled, the MAX polls the SNTP server every 50 seconds.

Usage: Specify Yes or No. No is the default.

- Yes enables the MAX to use an SNTP server to maintain its time.
- No disables SNTP.

Dependencies: If enable SNTP, you must specify at least one SNTP server address.

Location: Ethernet > Mod Config > SNTP Server

See Also: SNTP Host #N, Time Zone

SNTP Host #N (N=1–3)

Description: Specifies the IP address of up to three SNTP servers. The MAX polls the SNTP Host every 50 seconds. If the server specified by SNTP Host #1 is not active, the MAX sends its requests to SNTP Host #2. If that server is not active, the MAX sends its requests to SNTP Host #3.

Usage: Specify an IP address. The default is 0.0.0.0.

Dependencies: This parameter does not apply if SNTP is not enabled.

See Also: Ethernet > Mod Config > SNTP Server

Location: SNTP Enabled, Time Zone

Socket

Description: Specifies a well-known socket number.

Usage: Specify the socket number for the server.

Example: `Socket=0000`

Dependencies: This parameter does not apply if the MAX does not route IPX.

Location: Ethernet > IPX Routes

See Also: Route IPX

Source Addr

Description: Specifies an IP address. If specified, the MAX ignores packets from that source for monitoring purposes. If a Source Mask is also specified, the MAX uses the combined address and mask to ignore packets from the specified source.

Note: Heartbeat monitoring is optional. It is not required for multicast forwarding.

Usage: Specify an IP address.

Example: `Source Addr=10.2.3.4`

Dependencies: To set up heartbeat monitoring, you must configure several parameters that define what packets are monitored, how often and for how long multicast packets are polled, and the threshold for generating an alarm. These parameters do not apply if multicast forwarding is not in use.

Location: Ethernet > Mod Config > Multicast

See Also: HeartBeat Addr, Heartbeat Udp Port, Source Mask, HeartBeat Slot Time, HeartBeat Slot Count, Alarm Threshold

SourceIP Check

Description: Enables or disables anti-spoofing for the session.

Usage: Specify Yes or No. The default is No.

- Yes specifies that the system checks all packets received on the interface to ensure that their source IP address matches the combination of address and subnet mask specified by the LAN Adrs value, or the address agreed upon in IPCP negotiation. If Remote-Address specifies a subnet, packets that originate on that subnet are accepted. If Remote-Address specifies a 32-bit mask, only packets from that host are accepted. Packets sent from an address that does not match are discarded.
- No disables anti-spoofing for the session.

Example: `SourceIP Check=Yes`

Location: Ethernet > Connections > *any Connection profile* > IP options

See Also: IP Adrs, LAN Adrs

Source Mask

Description: Specifies an IP netmask. If specified, the MAX uses the combined address and mask to ignore packets from the specified source for heartbeat monitoring purposes.

Note: Heartbeat monitoring is optional. It is not required for multicast forwarding.

Usage: Specify a netmask.

Example: `Source Mask=255.255.255.248`

Dependencies: To set up heartbeat monitoring, you must configure several parameters that define what packets will be monitored, how often and for how long to poll for multicast packets, and the threshold for generating an alarm. These parameters do not apply if multicast forwarding is not in use.

Location: Ethernet > Mod Config > Multicast

See Also: HeartBeat Addr, Heartbeat Udp Port, Source Addr, HeartBeat Slot Time, HeartBeat Slot Count, Alarm Threshold

Split Code.User

Description: Divides the PIN and CODE of a user and their USERNAME by a period. If the CHAP field cannot accommodate the full PIN+CODE.USER, you can enable this feature. The MAX splits the passcode into two pieces with the information following the period becoming the CHAP Name, overriding the name of the router.

Usage: Specify one of the following values:

- Yes—Enables PIN, CODE and USERNAME to be divided.
- No— Disables this feature. No is the default.

Example: `Split Code.User=No`

Location: Ethernet > Connections > *Connection profile* > Encaps Options

Src Adrs

Description: Specifies a source IP address. After this value has been modified by applying the specified Src Mask, it is compared to a packet's source address.

Usage: Specify a source IP address the MAX should use for comparison when filtering a packet. The zero address 0.0.0.0 is the default. If you accept the default, the MAX does not use the source address as a filtering criterion.

Example: `Src Adrs=10.62.201.56`

Dependencies: This parameter applies only to filters of type IP.

Location: Ethernet > Filters > Input filters > In filter *N* > IP, Ethernet > Filters > Output filters > Out filter *N* > IP

See Also: Src Mask

Src Mask

Description: Specifies a mask to apply to the Src Adrs before comparing it to the source address in a packet. You can use it to mask out the host portion of an address, for example, or the host and subnet portion.

The MAX applies the mask to the address using a logical AND after the mask and address are both translated into binary format. The mask hides the portion of the address that appears behind each binary 0 (zero) in the mask. A mask of all zeros (the default) masks all bits, so all source addresses are matched. A mask of all ones (255.255.255.255) masks no bits, so the full source address to a single host is matched.

Usage: Specify the mask in dotted decimal format. The zero mask 0.0.0.0 is the default; this setting indicates that the MAX masks all bits. To specify a single source address, set Src Mask=255.255.255.255 and set Src Adrs to the IP address that the MAX uses for comparison.

Example: `Src Mask=255.255.255.0`

Dependencies: This parameter applies only to filters of type IP.

Location: Ethernet > Filters > Input filters > In filter *N* > IP, Ethernet > Filters > Output filters > Out filter *N* > IP

See Also: Src Adrs

Src Port

Description: Specifies a value to compare with the source port number in a packet. The default setting (zero) indicates that the MAX disregards the source port in this filter. Port 25 is reserved for SMTP; that socket is dedicated to receiving mail messages. Port 20 is reserved for FTP data messages, port 21 for FTP control sessions, and port 23 for telnet.

Note: The Src Port Cmp parameter specifies the type of comparison to be made.

Usage: Specify a number between 0 and 65535.

Example: `Src Port #=25`

Dependencies: This parameter applies only to filters of type IP.

Location: Ethernet > Filters > Input filters > In filter *N* > IP, Ethernet > Filters > Output filters > Out filter *N* > IP

See Also: Dst Port #, Dst Port Cmp, Src Port Cmp

Src Port Cmp

Description: Specifies the type of comparison the MAX makes when filtering for source port numbers using the Src Port # parameter.

Usage: Specify one of the following values:

- None (the default) means the MAX does not compare source port numbers.
- Less means the comparison succeeds if the number is less than the value of Src Port #.
- Eql means the comparison succeeds if the number equals the value of Src Port #.
- Gtr means the comparison succeeds if the number is greater than the value of Src Port #.
- Neq means the comparison succeeds if the number is not equal to the value of Src Port #.

Location: Ethernet > Filters > Input filters > In filter *N* > IP, Ethernet > Filters > Output filters > Out filter *N* > IP

See Also: Src Port #

Src Port

Description: Specifies the source port number for calls that match the profile.

Usage: Specify a value from 1 to 8. The default is 0, which matches calls from all source ports.

Location: System > Call Routes > *Call Routes profile*

Src Slot

Description: Specifies the source slot number for calls that match the profile.

Usage: Specify a value from 1 to 8. The default is 0, which matches calls from all source slots.

System > Call Routes > *Call Routes profile*

Stacking Enabled

Description: Enables the MAX to communicate with other members of the same stack. A MAX can belong to only one stack. All members of the stack use the same stack name and UDP port. A MAX can support up to 40 stacked channels, that is, channels that originate on another MAX but are bundled with channels on the current MAX. The total number of

channels in a stack is limited by the performance considerations of the network because stacking MAX units causes extra traffic on the Ethernet.

If the local network supports more than one MAX, you can *stack* them to enable inbound multilink PPP connections to distribute bandwidth across the multiple MAX units. The stacked units must all have access to the same authentication information, typically on a RADIUS server. Every member of a stack must reside on the same physical LAN. A MAX unit can only belong to a single stack, but does not have to belong to any stack. Multiple stacks can exist on the same LAN by simply having different stack names.

Usage: Specify Yes or No. No is the default.

- Yes enables stacks in this MAX.
- No disables stacks in this MAX.

Location: Ethernet > Mod Config > Stack Options

See Also: Stack Name, UDP Port

Stack Name

Description: Specifies a stack name. Add a MAX to an existing stack by specifying that name. The stack name must be unique among all MAX stacks that can communicate with each other. You can create a new stack by specifying a new stack name.

Usage: Specify the name of the Stack to which this MAX belongs. A stack name must 16 characters or less.

Example: `Stack Name=Stack-1`

Dependencies: This parameter does not apply if stacks are not enabled.

Location: Ethernet > Mod Config > Stack Options

See Also: Stacking Enabled, UDP Port

Static Preference

Description: Specifies the default preference value for statically configured routes.

Usage: Specify a number between 0 and 255. The default value is 100. Zero is the default for connected routes (such as the Ethernet). The value of 255 means *Don't use this route*.

Example: `Static Preference=100`

Dependencies: These are the default route preference values:

- Routes learned from OSPF=10
- Routes learned from ICMP Redirects=30
- Routes learned from RIP=100
- Static routes in an IP Route profile or Connection profile=100

Location: Ethernet > Mod Config > Route Pref

Station

Description: Specifies the name of the far-end device in this Connection profile. If the connection uses Combinet encapsulation, it is the MAC address of the far-end Combinet bridge.

Note: If this Connection profile specifies a nailed link to the home network for a MAX acting as an ATMP home agent in gateway mode, the Station name must match the Ascend-Home-Network-Name attribute in the foreign agent's RADIUS configuration.

Usage: Specify the name of the far-end device. You can enter up to 31 characters. Make sure you specify the name exactly, including case changes.

For a Combinet link, specify the 12-digit hexadecimal MAC address of the far-end device.

Example: `Station=NewYork`

Location: Ethernet > Connections

See Also: ATMP Mode, Type

Status N (N=1–8)

Description: Enables you to customize the status windows in the VT100 interface so that particular screens appear at startup. The numbers 1 through 8 indicate the position of the status window, starting with the upper left. You can also use Ctrl-D-M to automatically configure the Status parameter.

Usage: Specify a window number in the format *XY-NNN*.

- *X* is the module number, and indicates a virtual or real module.
- The slot numbers and virtual or real modules assigned to your MAX vary depending on which model you are using. In all cases, the system itself is assigned slot number 0 (00-000). Refer to the *Hardware Installation and Basic Configuration Guide* for your MAX for specific assignments.
- *Y* is the port number.

  Zero indicates information pertinent to any portion of the module. A nonzero value indicates the AIM port to which the window applies. For system and T1 PRI network windows, the port number is always 0.
- The three digits after the dash are the root number.

  A root number of 000 identifies a top-level branch of the tree. If *N* is not 0 (zero), the root number identifies a window lower in the tree.

Example: `Status 1=20-100`

Location: System > Sys Config

Sub-Adr

Description: Specifies how the MAX treats incoming calls based on whether they convey an ISDN subaddress.

Usage: Specify one of the following values:

- Termsel specifies that the MAX must use an ISDN subaddress to determine whether a call is answered.

  The called-party number must have a subaddress that matches a subaddress in the Line profile of the line on which the MAX receives the call. Otherwise, the MAX ignores the call. If the MAX accepts the call, the subaddress becomes part of the incoming telephone number, and the MAX uses it in Ans # comparisons.

  This setting is intended for a scenario in which equipment is connected to a multidrop ISDN BRI line.
- Routing specifies that the called-party number can or cannot have a subaddress.

  If a subaddress is present, it becomes part of the incoming telephone number. The MAX matches it against the value of the Serial, LAN, DM, and V.110 parameters in the Sys Config menu in order to determine the interface to which it should route the call. If no match is found, the MAX uses the subaddress in Ans # comparisons.
- None specifies that the MAX does not use subaddressing.

Location: System > Sys Config

See Also: Ans #, DM, LAN, Serial, V.110

Sub Pers

Description: Specifies a number of seconds for which the ALU (average link utilization) must persist below the Target Util threshold before the MAX subtracts bandwidth.

When utilization falls below the threshold for a period of time greater than the value of the Sub Pers parameter, the MAX attempts to remove the number of channels specified by the Dec Ch Count parameter. However, the MAX never subtracts enough bandwidth to clear the call or cause the channel count to fall below the specified minimum. Setting the Add Pers and Sub Pers parameters prevents the system from continually adding and subtracting bandwidth, and can slow down the process of allocating or removing bandwidth.

Add Pers and Sub Pers have little or no effect on a system with a high Sec History value. However, if the value of Sec History is low, the Add Pers and Sub Pers parameters provide an alternative way to ensure that spikes persist for a certain period of time before the system responds.

Usage: Specify a number between 1 and 300. When the MAX is using MP+, the default value is 10. When the MAX is using dynamic AIM, the default value is 20.

Example: `Sub Pers=15`

Location: Ethernet > Answer > PPP Options, Host/Dual (Host/AIM6) > Port*N* Menu > Directory, Ethernet > Connections > *Connection profile* > Encaps Options

See Also: Add Pers, Dec Ch Count, Dyn Alg, Min Ch Count, Sec History, Target Util

Suppress Host Routes

Description: Specifies whether the MAX advertises host routes in each update, which can cause excessive routing overhead:

Usage: Specify Yes or No. The default is No.

- Yes specifies that host routes are suppressed,
- No specifies that host routes are advertised.

Example: `Suppress Host Routes=No`

Dependencies: If you set Suppress Host Routes to Yes, routes are suppressed according to the following rules:

- If a Connection profile specifies a Remote Address setting with a subnet mask of less than 32 bits, host routes for the interface are suppressed while the session is being negotiated. After the session is established, only network routes are advertised for the interface.
- If a Connection profile specifies a Remote Address setting with a subnet mask of /32, host routes for the interface are not suppressed.

Location: Ethernet > Mod Config

See Also: Pool Summary

Switch Type

Description: Specifies the carrier switch type that services the Net/T1, Net/E1, Net/BRI for T1 MAX units, Net/BRI for E1 MAX units, or Host/BRI lines.

Usage: Specify the carrier switch type according to the following guidelines for selecting values.

Net/T1

In a Net/T1 profile, specify one of the following switch types:

- AT&T (the default)
- GloBanD (Q.931W GloBanD data service)
  Although GloBanD can appear in the list of switch types available for ISDN, it is currently not supported on any T1 PRI switches in the U.S. However, some T1 PRI switches do support MultiRate, which is a service similar to GloBanD that allows data service bandwidths higher than 64 Kbps. For specific information, contact your T1 PRI service provider.
- IDSL (Identical to AT&T Point-to-Point, but has support for Q.931 en-bloc dialing)
- Japan
- NI-2 (National ISDN-2)
- NT1 (Northern Telecommunications, Inc.)

Net/E1

In a Net/E1 profile, specify one of the following switch types:

- Australian (Australia only)
- CAS (New Zealand)
- DASS 2 (U.K. only)
- French (VN3 ISDN PRI)
- German (1TR6)

- GloBanD (Q.931W GloBanD data service)
- ISDX (DPNSS switch type)
- ISLX (DPNSS switch type)
- Mercury (DPNSS switch type)
- NET 5 (Euro ISDN services in Belgium, the Netherlands, Switzerland, Sweden, Denmark, and Singapore)
- NI-1 (National IDSN-1)

Net/BRI

In a Net/BRI Line profile for a MAX T1 unit, specify one of the following switch types:

- AT&T (the default)
- NI-1 (National ISDN-1)
- NT1 (Northern Telecommunications, Inc.)

In a Net/BRI Line profile for a MAX E1 units, specify one of the following switch types:

- AUSTR (Australia and New Zealand)
- BELGI (Belgium: Pre-Euro ISDN Belgacom Aline)
- DUTCH (Netherlands 1TR6 version: PTT Netherlands BRI)
- FRANC (France: FT Numeris)
- GERMA (Germany 1TR6 version: DBP Telecom)
- JAPAN (Japan: NTT INS-64)
- MP GERMAN (Germany: 1TR6 multipoint)
- NET3 (Same as U.K. NET3; is also known as Euro-ISDN)
- NET3 PTP (A variation of EURO-ISDN signaling used in Germany)
- SWISS (Switzerland: Swiss Net 2)
- U.K. (Also known as Euro-ISDN. United Kingdom: ISDN-2; Hong Kong: HKT Switchline BRI; Singapore: ST BRI; Euro ISDN countries: Austria, Belgium, Denmark, Finland, Italy, Netherlands, Portugal, Spain, Sweden)

Note: All international switch types except German operate in multipoint mode. Some MAX units can support both North American and international switch types for Net/BRI.

Host/BRI

In a Host/BRI profile, specify one of the following switch types:

- AT&T (default for T1 MAX units)
- NET3 (Euro-ISDN, the default for E1 MAX units)
- NI-1 (National ISDN-1)

Example: `Switch Type=AT&T`

Location: Net/T1 > Line Config > Line *N*, Net/BRI > Line Config > Line *N*

Switch Version

Description: Identifies a particular version of a switch in order to handle minor variations in switch protocols.

Usage: Specify one of the following values:

Generic— No protocol variations. Generic is the default.

DefinityG3V4—The DefinityG3V4 switch.

Location: Net/E1 > Line Config > Line *N* profile

Sys Diag

Description: Enables or disables permission to perform all system diagnostics.

Usage: Specify Yes or No. Yes is the default.

- Yes specifies the user can use the commands in the Sys Diag menu.
- No specifies that a user cannot use any of those commands.

Location: System > Security

See Also: *MAX Administration Guide*

Syslog

Description: Specifies whether the MAX sends warning, notice, and CDR (Call Detail Reporting) records from the system logs to the Syslog host.

Usage: Specify Yes or No. No is the default.

- Yes enables the MAX to communicate with the Syslog host.
- No disables this function.

Dependencies: If you enable Syslog, you must enter the IP address of the Syslog host in the Log Host parameter.

Location: Ethernet > Mod Config

See Also: Log Facility, Log Host

T

T-Online

Description: This parameter specifies whether the MAX performs T-Online routing.

Usage: Specify Yes or No.

- Yes specifies that the MAX performs T-Online routing.
- No specifies that the MAX does not perform T-Online routing.

The default value is No.

Dependencies: If T-Online=Yes, you can not use lines 3 and 4 on the MAX for any purpose other than PRI-PRI switching.

Location: System > Sys Config

See Also: T302 Timer

T1-PRI:PRI # Type

Description: T1-PRI:PRI # Type 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 following settings. This parameter specifies the TypeOfNumber field in the called party's information element.

Note: This parameter applies only to calls placed by devices terminating the inband T1 lines provided by the MAX in a T1-PRI conversion configuration.

Usage: Specify one of the following values:

- National specifies telephone numbers within the U.S. (TypeOfNumber=2)
- Intl specifies telephone numbers outside the U.S. (TypeOfNumber=1)
- Local specifies telephone numbers within your Centrex group. (TypeOfNumber=4)
- Abbrev. specifies that the telephone number is abbreviated. (TypeOfNumber=6)
- NetSpecific (currently not implemented) specifies that the network you are connected to understands the telephone number. (TypeOfNumber=3)
- Unknown (the default) specifies that the telephone number is none of the above. (TypeOfNumber=0)

Dependencies: The value you specify for PRI # Type in the Dial Plan profile overrides the value of T1-PRI:PRI # Type in the Line profile if you have enabled the unit's Dial Plan profiles.

Location: Net/T1 > Line Config (Line profile)

See Also: T1-PRI:NumPlanID, NumPlanID (Call and Connection profiles), Modem:NumPlanID (System profile)

T1-PRI:NumPlanID

Description: 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 following settings. This parameter specifies NumberPlanID field in the called party's information element.

Note: This parameter applies only to calls placed by devices terminating the inband T1 lines provided by the MAX in a T1-PRI conversion configuration.

Usage: Specify one of the following values:

- Unknown (NumberPlanID=0)
- ISDN (the default) (NumberPlanID=1)

- Private (NumberPlanID=9)

Dependencies: The value you specify for NumPlanID in the Dial Plan profile overrides the value of T1-PRI:NumPlanID in the Line profile if you have enabled the unit's Dial Plan profiles.

Location: Net/T1 > Line Config (Line profile)

See Also: T1-PRI:PRI # Type, NumPlanID (Call and Connection profiles), Modem:NumPlanID (System profile)

T1 Retran Timer

Description: Specifies the maximum amount of time in ticks the transmitter should wait for an acknowledgment before initiating a recovery procedure.

Usage: Specify a number between 500 and 2000. The default value is 1000 (1 second).

Location: Ethernet > Answer > X.75 Options

See Also: Frame Length, K Window Size, N2 Retran Count, X.75

T302 Timer

Description: This parameter specifies the duration of the ISDN Q.931 layer 3 SETUP_ACK timer.

When the MAX receives the layer 3 SETUP message, the SETUP message consists of many IEs (Information Elements), such as Bearer Capability IE, Channel Identifier IE, Caller Number IE, Called Number IE, Sending Complete IE, and so on. The MAX checks for the Sending Complete IE upon receiving the SETUP message from the switch. If the Sending Complete IE is not in the SETUP message, the MAX starts the T302 timer and waits for an INFO message from switch. If the INFO message consists of Sending Complete IE, MAX stops the T302 timer. If no Sending Complete IE appears, the MAX restarts the T302 timer.

Usage: You can specify a value between 100 and 3000 one-hundredths of a second (1 to 30 seconds). The default value is 1800 (18 seconds).

Dependencies: T302 Timer does not apply if T-Online=No.

Location: System Profile: System>Sys Config

See Also: T-Online

T.38 Fax Enabled

Description: The T.38 Fax Enabled parameter is used to enable T.38 fax call processing on a MultiVoice gateway. This allows a MultiVoice gateway to switch over from a voice session to fax upon detection of a CED tone or V.21 HDLC flag.

Usage: Pressing [Enter] toggles the value of the T.38 FAX Enabled parameter between the following:

Value	Description
Yes	Enables T.38 fax call processing on a MultiVoice gateway. This allows a MultiVoice gateway to switch over from a voice session to fax upon detection of a CED tone or V.21 HDLC flag.
No	Disables T.38 fax processing (default). Fax tones are ignored, unless the transparent fax/modem options are enabled in the VOIP Options profile.

Dependencies: The T.38 Fax Enabled parameter has the following dependencies:

- This parameter defaults to `N/A` when a MultiVoice gateway is not hashed for real-time fax.
- Changes to this parameter are effective with the next VoIP call.

T391

Description: Specifies the number of seconds between Status Enquiry messages.

Usage: Specify a number between 5 and 30. The default is 10.

Dependencies: This parameter applies only if Link Mgmt=T1.617D and T392 is set to a nonzero value.

Location: Ethernet > Frame Relay

See Also: Link Mgmt

T392

Description: Specifies the number of seconds the MAX waits for a Status Enquiry message before recording an error. If you specify zero, the MAX does not process WAN-side Status Enquiry messages. If you specify a nonzero value, the MAX uses T1.617D (a link management protocol defined in ANSI T1.617 Annex D) to monitor another MAX over a nailed-up connection.

Usage: Specify 0 (zero), or a number between 5 and 30. The default is 15.

Dependencies: The T392 parameter applies only if Link Mgmt=T1.617D.

Location: Ethernet > Frame Relay

See Also: Link Mgmt

T3POS T1

Description: Specifies the Char-to-Char timer. This timer indicates the maximum amount of time permitted between characters sent from the DTE to the PAD.

Usage: Specify a value between 1 and 20 (tenths of seconds). The default is 5.

Dependencies: This parameter is always applicable.

Location: Ethernet > Connections > *Connection profile* > Encaps options,
Ethernet > Answer > T3POS options

T3POS T2

Description: 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.

Usage: Specify a value between 10 and 100 (tenths of seconds). The default is 40.

Dependencies: Keep in mind that the T2 timer only applies to the opening frame and to Local or Bin-Local mode.

Location: Ethernet > Connections > *Connection profile* > Encaps options
Ethernet > Answer > T3POS options

T3POS T3

Description: Specifies the ENQ handling timer. This timer indicates the amount of time the PAD waits for an ENQ from the host.

Usage: Specify a value between 5 and 50 (tenths of seconds). The default is 15.

Dependencies: Keep in mind that this parameter is not applicable when you set ENQ Handling to Off.

Location: Ethernet > Connections > *Connection profile* > Encaps options
Ethernet > Answer > T3POS options

T3POS T4

Description: 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.

Usage: Specify a value between 10 and 100 (tenths of seconds). The default is 40.

Dependencies: This parameter is always applicable.

Location: Ethernet > Connections > *Connection profile* > Encaps options
Ethernet > Answer > T3POS options

T3POS T5

Description: Specifies the DLE, 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; it is disabled in both Local mode and Bin-Local mode.

Usage: Specify a value between 50 and 3000 (tenths of seconds). The default is 2400 (four minutes).

Dependencies: Keep this additional information in mind.

- The T5 timer can 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.

Location: Ethernet > Connections > *Connection profile* > Encaps options
Ethernet > Answer > T3POS options

T3POS T6

Description: Specifies the Frame Arrival timeout. This timer 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.

Usage: Specify a value between 50 and 3000 (tenths of seconds). The default is 300 (30 seconds).

Dependencies: This parameter is always applicable.

Location: Ethernet > Connections > *Connection profile* > Encaps options
Ethernet > Answer > T3POS options

Tag

Description: Specifies a value that links the SNMPv3 Notifications submenu with the SNMP Traps parameter setting specifying the host address to which notification messages are sent.

Usage: Specify up to 255 characters. The default is null.

Example: `Tag=newtag`

Location: Ethernet > SNMPv3 Notifications

See Also: Active, Dest Port, Message Proc Model, Notify Tag List, Security Level, Security Model, Security Name, Target Param Name

Target Param Name

Description: Specifies the value indicated by the Name parameter setting in the SNMPv3 Target Params submenu.

Usage: Specify up to 22 characters.

Example: `Target Param Name=profile1`

Location: Ethernet > SNMP Traps

See Also: Active, Dest Port, Message Proc Model, Notify Tag List, Security Level, Security Model, Security Name, Tag

Target Util

Description: Specifies a percentage of line utilization to use as a threshold for determining when to add or subtract bandwidth. When the value is 70%, the device adds bandwidth when it exceeds a 70 percent utilization rate, and subtracts bandwidth when it falls below that number.

Usage: Specify a number between 0 and 100. The default is 70 (70% utilization).

Example: `Target Util=70`

Dependencies: In a Call profile, this parameter applies only to dynamic AIM calls. It specifies the target percentage of bandwidth utilization for a dynamic time period.

Location: Ethernet > Answer > PPP Options, Host/Dual (Host/AIM6) > Port*N* Menu > Directory > Time Period *N*, Ethernet > Connections > *Connection profile* > Encaps Options

See Also: Add Pers, Call Mgm, Call Type, Dec Ch Count, Dyn Alg, Inc Ch Count, Sec History, Sub Pers

TCP-Clear

Description: Specifies whether the MAX can answer calls that use a proprietary encapsulation method and rely on raw TCP sessions to a local host for processing that encapsulation.

Usage: Specify Yes or No. Yes is the default.

- Yes specifies the MAX will answer TCP-Clear connections, provided they meet all other connection criteria.
- No specifies the MAX will not accept inbound calls of this type.

Location: Ethernet > Answer > Encaps

See Also: Encaps

TCP Estab

Description: In a filter of type IP, specifies whether the filter should match only established TCP connections. You can use it to restrict the filter to packets in an established TCP session.

You can only use it if the Protocol number has been set to 6 (TCP); otherwise, it does not apply.

Usage: Specify Yes or No. No is the default.

- Yes specifies the filter matches only packets that are part of established TCP connections.
- No removes this restriction.

Dependencies: This parameter does not apply if the Protocol field is set to a value other than 6 (TCP).

Location: Ethernet > Filters > Input filters > In filter *N* > IP, Ethernet > Filters > Output filters > Out filter *N* > IP

TCP Modem Enabled

Description: Specifies whether the MAX allows TCP modem access.

Usage: Specify one of the following values:

- Yes indicates the MAX answers TCP modem connections.
- No indicates the MAX does not answer TCP modem connections over the port specified by TCP Modem Port.

  No is the default.

Location: Ethernet > Mod Config > TCP Modem Options

TCP Modem Port

Description: Specifies the port for TCP modem access.

Usage: Specify a TCP port. The default is 6150.

Location: Ethernet > Mod Config > TCP Modem Options

TCP timeout

Description: Specifies the length of time the MAX attempts to connect to an IP host in the list provided by the DNS server.

Since the first host on the list can not be available, the timeout should be short enough to allow the MAX to go on to the next address on the list before the client software times out.

This feature applies to all TCP connections initiated from the MAX, including telnet, rlogin, tcp-clear, and the TCP portion of DNS queries.

Usage: Enter a value from 0 to 200. The value specifies the number of seconds after which the MAX will stop attempting to connect to an IP address and will proceed to the next address on the list.

When the MAX has sent the maximum number of messages to an address on the DNS list it will stop attempting to make a connection to that address, even if the maximum time set in DNS Timeout has not yet elapsed.

The default for DNS Timeout is 0. If you set TCP timeout to 0, the MAX retries connecting to the address at increasingly larger intervals until it sends the maximum number of start-connection messages. This takes approximately 170 seconds, but can take longer if the MAX is running large number of other tasks. If the client software times out before the MAX makes a connection or proceeds to the next address on the DNS list, the physical connection is dropped.

Dependencies: The List Attempt parameter in the DNS submenu of the Mod Config menu in the Ethernet Profile must be enabled. This permits the MAX to attempt the IP addresses. On a list, if the DNS server provides such a list. The List Attempt parameter does not apply if Telnet and Immediate Telnet are both disabled.

Location: Ethernet > Mod Config

TEI

Description: Specifies the Terminal Endpoint Identifier (TEI). Your service provider should provide you with the appropriate value.

Usage: Specify a TEI value from 0 to 63. The default value is 23. If you set TEI to 0, the MAX requests a TEI assignment from the network.

Location: Ethernet > X.25 > *any X.25 profile*

Telnet

Description: Enables or disables the Telnet command from the terminal server interface.

Usage: Specify Yes or No. No is the default.

- Yes specifies users can invoke Telnet sessions from the terminal-server interface.
- No disables the use of Telnet in the terminal server.

Example: `Telnet=Yes`

Dependencies: This parameter is not applicable when terminal services are disabled.

Location: Ethernet > Mod Config > TServ Options

See Also: TS Enabled

Telnet Host Auth

Description: Specifies whether immediate Telnet sessions require local authentication in the terminal server or if authentication is the responsibility of the Telnet host.

Usage: Specify Yes or No. No is the default.

- Yes specifies rely on the Telnet host for authentication.
- No specifies the immediate Telnet session must be authenticated locally first.

Example: `Telnet Host Auth=Yes`

Dependencies: This parameter is not applicable when terminal services are disabled.

Location: Ethernet > Mod Config > TServ Options

See Also: Immed Service

Telnet Mode

Description: Specifies the default Telnet mode for terminal-server Telnet users.

Usage: Specify one of the following values:

- ASCII

  Standard 7-bit mode. In 7-bit mode, bit 8 is set to 0 (zero); 7-bit telnet is also known as NVT (Network Virtual Terminal) ASCII. This is the default if no other mode is specified.

- Binary

  The MAX attempts to negotiate the telnet 8-bit binary option with the server at the remote end. You can run X -Modem and other 8-bit file transfer protocols using this mode.

  In 8-bit binary mode, the telnet escape sequence does not operate. The telnet session can close only if one end of the connection quits the session. If you are a local user not connected through a digital modem, the remote-end user must quit.

  A user can override the binary setting on the Telnet command line.

- Transparent

  You can send and receive binary files without having to be in Binary mode. You can run the same file transfer protocols available in Binary mode.

  Select Transparent if the hosts to which you connect do not fully comply with the Binary Telnet standard.

Example: `Telnet mode=ASCII`

Dependencies: This parameter is not applicable when terminal services are disabled. Also, consider the following:

- In 8-bit binary mode, the Telnet escape sequence does not operate. The Telnet session can close only if one end of the connection quits the session. If you are a local user not connected through a digital modem, the remote-end user must quit.
- A user can override the Binary setting on the Telnet command line.
- If terminal services are disabled, Telnet-Mode does not apply.
- Not all devices support the Binary mode option. Some devices partially follow the Telnet RFC, but do not enforce the Telnet restriction of using only 7-bit ASCII. They accept 8-bit data and, after doing the appropriate processing, forward all data received. If you specify Transparent for these devices, you can escape the IAC character and add a null after every CR to cause the devices to work.

Location: Ethernet > Mod Config > TServ Options

See Also: TS Enabled

Telnet PW

Description: Specifies the password users must enter to access the MAX unit through Telnet. If you specify a password, users are allowed three tries of 60 seconds each to enter the correct password.

Usage: Specify a password containing up to 20 characters. The default is null. If you leave this parameter blank, the MAX does not prompt users for a password.

Example: `Telnet PW=Lucent`

Location: Ethernet > Mod Config

Telnet Security

Description: Enables the MAX to use a RADIUS server to authenticate a MAX Telnet session. The MAX first attempts authentication with a RADIUS profile. If that fails, the MAX tries to match a Security profile to the login and password. The MAX allows the user three login attempts before it closes the Telnet session.

Usage: Specify one of the following values:

- None—Telnet authentication is disabled.
- Global—Password-only authentication that uses the default Security profile. The behavior is the same as if the value `None` had been selected.
- Profile—The MAX requires both a login name and password. If the login name matches the name of a security profile, the MAX compares that security profile's password with the user-provided password. A password mismatch or an unmatched name results in the error message `Incorrect login or password`.
- Auth Setting—The MAX uses the RADIUS authentication settings in the Ethernet > Mod Config > Auth menu (Auth=RADIUS or Auth=RADIUS/LOGOUT). If the Auth parameter is set to anything other than RADIUS or RADIUS/LOGOUT, the MAX does not accept Telnet requests.

  Note: The Auth Setting value deletes the Security Prof parameter from the Ethernet > Connections > *Connection profile* menu.

Dependencies: Telnet PW does not apply if you specify None, Profile or Auth Setting.

Location: Ethernet > Mod Config

See Also: Telnet PW, Auth

Template Connection

Description: Specifies a Connection profile to use a *template* Connection profile instead of the Answer profile settings to build the session for this Name-password profile. You specify the unique portion of the profile's number here. The default zero instructs the MAX to use the Answer profile settings. Note that the specified Connection profile must be active.

Template connections can be used to enable or disable group logins. For example, you can specify a Connection profile for the Sales group to use when dialing in, then configure a Name-password profile for each individual salesperson. You can prevent a single salesperson from dialing in by setting Active to No in the Name-password profile, or you can prevent the entire group from logging in by setting Active to No in the Connection profile.

Usage: Specify the unique part of the Connection profile's number in the Connections menu.

Example: `Template Connection #=99`

Dependencies: The specified Connection profile must be active.

Location: Ethernet > Names/Passwords

Term Rate

Description: Specifies the bit rate of a MAX serial port. When you modify the bit rate of a serial port, you also need to change the data rate setting of the terminal accessing that port.

Usage: Specify one of the following values:

- 57600
- 38400
- 19200
- 9600 (the default)
- 4800
- 2400

Example: `Term Rate=9600`

Location: System > Sys Config

Term Timing

Description: Specifies whether the MAX uses the Terminal Timing signal from the codec to clock data it receives from the codec. Terminal Timing is a clock signal specified in the V.35, X.21, and RS-449 serial interfaces that compensates for the phase difference between Send Data and Send Timing.

For the MAX to use the Terminal Timing signal from the codec, the AIM port module must support Terminal Timing and the codec must use Terminal Timing if the distance between the MAX and the host is greater than the distances described next.

- With a maximum cable length of 25 feet and a serial data rate of 3 mbps
- With a maximum cable length of 75 fee and a serial data rate of 2 mbps
- With a maximum cable length of 150 feet and a serial data rate of 512 Kbps

Usage: Specify Yes or No. No is the default.

- Yes specifies the MAX will use the Terminal Timing signal from the codec.
- No specifies the MAX uses its Send Timing signal to clock data it receives from the codec.

Example: `Term Timing=No`

Location: Host/Dual (Host/AIM6) > Port*N* Menu > Port Config

Term Type

Description: Specifies the default terminal type for Telnet and Rlogin sessions.

Usage: Specify the terminal type. You can enter up to 15 characters. The default is vt100.

Example: `Term Type=vt100`

Dependencies: This parameter is not applicable when terminal services are disabled.

Location: Ethernet > Mod Config > TServ Options

See Also: TS Enabled

Third-Party

Description: This enables OSPF third-party routing for a static route. When enabled, the gateway address is used as the third-party router for this route. Third-party routing enables an OSPF router to advertise a route to a destination network through a remote router (Router-A advertises a route to Network-B via Router-C). This is accomplished by specifying the address of the remote router (Router-C) in the next-hop field of an LSA.

Note: In some cases, third-party routing results in more efficient routes, because other OSPF routers (such as Router-D and Router-E) might be able to trim one hop off of the packet's path and send it to the specified address (Router-C) directly. In practice, it requires that the third-party router is on an Ethernet that is running OSPF, and that its designated router is advertising that network into the OSPF cloud.

Usage: Specify Yes or No. No is the default.

- Yes enables third-party routing for the OSPF router.
- No disables third-party routing.

Example: `Third-Party=Yes`

Dependencies: Third-Party does not apply to NSSAs.

Location: Ethernet > Static Rtes

See Also: Gateway

Tick Count

Description: Specifies the distance to the destination network in IBM PC clock ticks (18 Hz). This value is for round-trip timer calculation and for determining the nearest server of a given type.

Usage: Specify an appropriate value. In most cases, the default value (12) is appropriate.

Dependencies: This parameter is not applicable if the MAX does not route IPX >

Location: Ethernet > IPX Routes

See Also: Route IPX

Time

Description: Specifies the time of day.

Usage: Specify the time of day in the format <hour > :<minutes > :<seconds > . The default is 00:00:00.

Example: `Time=13:24:24`

Location: System > Sys Config

Timeout Busy (previously CLID Timeout Busy)

Description: Specifies whether to return User Busy or Normal Call Clearing as a Cause in IDSN DISCONNECT messages when ID authentication fails due to a RADIUS timeout.

Usage: Press Enter to toggle between Yes and No. No is the default. If you choose Yes, and the ID authentication fails due to a RADIUS timeout, the DISCONNECT message will have the Cause value User Busy (decimal value 17). If you choose No, the Cause value will be Normal Call Clearing (decimal value 16).

Dependencies: This parameter will be N/A if Auth=None or Auth=TACACS+ in the this profile. The value set in this parameter applies to both Caller ID and Called ID authentication.

This parameter is N/A if ID Auth=Ignore.

Location: Ethernet Profile: Ethernet > Mod Config > Auth

See Also: IDFail Busy,

Time Period N (N=1–4)

Description: This subprofile contains up to four dynamic time periods, each of which can be configured with different bandwidth management settings.

Dependencies: The Time Period subprofile applies only to dynamic AIM calls.

Location: Host/Dual (Host/AIM6) > Port*N* Menu > Directory

See Also: Activ, Call Mgm, Max Ch Count, Min Ch Count, Target Util

Time zone

Description: Specifies your time zone as an offset from the UTC (Universal Time Configuration) to enable the MAX to update its system time from an SNTP server. UTC is in the same time zone as Greenwich Mean Time (GMT), and the offset is specified in hours using a 24-hour clock. Because some time zones, such as Newfoundland, cannot use an even hour boundary, the offset includes four digits and is stated in half-hour increments. For example, Newfoundland is 1.5 hours behind UTC and is represented as follows:

```
UTC-0130
```

San Francisco is eight hours behind UTC and is represented as follows:

```
UTC-0800
```

Frankfurt is one hour ahead of UTC and is represented as follows:

```
UTC+0100
```

Usage: Specify one of the following values to represent your time zone:

```
utc-1130
utc-1100
```

```
utc-1030
utc-1000
utc-0930
utc-0900
utc-0830
utc-0800
utc-0730
utc-0700
utc-0630
utc-0600
utc-0530
utc-0500
utc-0430
utc-0400
utc-0330
utc-0300
utc-0230
utc-0200
utc-0130
utc-0100
utc-0030
utc+0000
utc+0030
utc+0100
utc+0130
utc+0200
utc+0230
utc+0300
utc+0330
utc+0400
utc+0430
utc+0500
utc+0530
utc+0600
utc+0630
utc+0700
utc+0730
utc+0800
utc+0830
utc+0900
utc+0930
utc+1000
utc+1030
utc+1100
utc+1130
utc+1200
```

Example: `Time zone=UTC-0700`

Dependencies: This parameter is not applicable unless SNTP Enabled is Yes.

Location: Ethernet > Mod Config > SNTP Server

See Also: SNTP Enabled, SNTP Host #

Toggle Scrn

Description: Specifies whether an interactive user is allowed to switch between menu mode and the terminal server command line. Users switch to menu mode by using the terminal server Menu command, and switch from menu mode to the command line by pressing the zero key. If this parameter is set to No, the menu command and 0 command are disabled.

Usage: Specify Yes or No. Yes is the default.

- Yes specifies terminal-server users can switch between terminal mode and menu mode.
- No specifies users have access only to the screen configured to come up initially.

Example: `Toggle Scrn=No`

Dependencies: This parameter is not applicable when terminal services are disabled.

Location: Ethernet > Mod Config > TServ Options

See Also: Initial Scrn

TOS

Description: Specifies the type of service for the data stream.

Usage: The three most significant bits of the Type-of-Service (TOS) byte are priority bits indicating precedence for priority queuing. The next four bits of the TOS byte are used to choose a link on the basis of the type of service. When TOS is enabled, you can set one of the following values in the packet:

- Normal (the default)—Specifies that the MAX unit applies normal TOS service. Normal is the default.
- Cost—The unit minimizes monetary cost.
- Reliability—The unit maximizes reliability.
- Throughput—The unit maximizes throughput.
- Latency—The unit minimizes delay.

Example: `TOS=Normal`

Dependencies: If `TOS Enabled=No`, the TOS setting is not applicable.

Location: Ethernet > Connections > *Connection profile* > IP options

See Also: Apply To, Precedence, Source IP Check, TOS Enabled, TOS Filter

TOS Enable

Description: Specifies whether to apply TOS settings to TOS filtering to IP packets.

Usage: Specify Yes or No. The default is No.

- Yes—Type of service is active for this connection.
- No—Disables type of service for this connection.

Example: `TOS Enabled=Yes`

Location: Ethernet > Connections > *Connection profile* > IP options

See Also: Apply To, Precedence, Source IP Check, TOS, TOS Filter

TOS Filter

Description: Specifies Type of Service (TOS) policy. In a Connection profile that has both its own local policy and an enabled TOS filter, the policy defined in the TOS filter takes precedence. Applying a TOS filter to a TOS connection enables administrators to define one priority setting for incoming packets on the connection and another for incoming packets addressed to a particular destination (the destination in a TOS filter).

Usage: Specify a number from 0 to 99999. The default is 0.

Example: `TOS Filter=12345`

Dependencies: Keep in mind the following additional information:

- If `TOS Enabled=No`, the TOS setting is not applicable.
- The TOS Filter setting applies the data stream(s) specified by the Apply To parameter. For example, if Apply To=Incoming, the TOS filter setting applies only to the incoming data stream.

Location: Ethernet > Connections > C*onnection profile* > IP options

See Also: Apply To, Precedence, Source IP Check, TOS, TOS Enabled

Transfer to Operator

Description: Defines the dial string a caller enters when requesting operator assistance. This parameter may be up to five digits long.

Usage: The Transfer to Operator feature is enabled by assigning a two-to-five digit dial string containing an asterisk (`*`) in either the first or second position to this parameter. Valid entries for the Transfer to Operator parameter are the asterisk (`*`) plus any number(s) 0 through 9. By default this value is `*0`. This feature is disabled by assigning a NULL value to the Transfer to Operator parameter.

Example: The following procedure illustrates how to set the value of the Transfer to Operator parameter:

1. From the Main Edit menu of the MAX administration interface, select Ethernet > Mod Config > Voip Options.-
2. Using the arrow keys, scroll to the Transfer to Operator parameter.
3. Press [ENTER] to open the edit field, as illustrated:

```
Transfer to Operator
[*0]
```

4. Enter a new two-to-five digit dial string containing an asterisk (`*`), as illustrated:

```
Transfer to Operator
[*5432]
```

5. Press [ENTER] to close the edit field, and save your change.

To disable the operator assistance feature, set the value of the Transfer to Operation parameter as illustrated:

```
Transfer to Operator=N/A
```

Dependencies: The Transfer to Operator parameter has the following dependencies:

- The first or second digit of the dial string must always be an asterisk (*).
- A MultiVoice gateway must be configured for two-stage dialing (`Single Dial Enable=no`).
- This feature requires MultiVoice Access Manager Release 3.1.0 be installed and running on the gatekeeper.
- A translation rule must be defined in one of the ingress translation tables used by MVAM that contains the actual dialed number used to connect calls to operator assistance.

Location: Ethernet > Mod Config > VOIP Options

Transit

Description: 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.

Usage: Specify one of the following dialing prefixes:

- 288 (AT&T)
- 222 (MCI)
- 333 (Sprint)

Example: `Transit #=222`

Dependencies: 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.

Location: Host/Dual (Host/AIM6) > Port*N* Menu > Directory, Ethernet > Connections > *Connection profile* > Telco Options, Ethernet > Frame Relay, System > Dial Plan, Ethernet > X.25

See Also: B1 Trnk Grp, B2 Trnk Grp, Ch *N* Trnk Grp

TransitDelay

Description: Specifies the estimated number of seconds it takes to transmit a Link State Update (LSU) Packet over this interface. Before transmission, LSAs (link state advertisements) contained in the LSU packet have their ages incremented by the amount you specify.

Usage: Specify a number greater than 0 (zero). This value should take into account transmission and propagation delays. The default is 1.

Example: `TransitDelay=1`

Location: Ethernet > Connections > *Connection profile* > OSPF Options, Ethernet > Mod Config > OSPF Options

True Connect Enable

Description: Enables or disables true connect signaling for VoIP calls. When enabled, the ingress MultiVoice gateway will delay PSTN alerting and sending connect messages to match the equivalent H.323 alerting and connect messages.

Usage: Press [Enter] to toggle between the following values for True Connect Enable parameter:

Value	Description
`Yes`	When assigned this value, an alerting message is sent to the ingress PSTN switch only when an H.323 alerting message is received on the ingress MultiVoice gateway, and a PSTN connect message is sent only when the H.323 VoIP call has been answered. This ensures that no charges are incurred for incomplete calls.
`No`	When assigned this value, the default, an alerting message is sent to the ingress PSTN switch as soon as the connection is established with the ingress MultiVoice gateway. This behavior results in the caller incurring a PSTN charge at the time of connection to the near-end gateway, before the called party has received and answered the call from the far-end MultiVoice gateway.

Example: The following procedure enables delayed PSTN alerting and connect messages (true connect signaling).

1. From the MAX Main Edit menu, select: `Ethernet` > `Mod Config` > `VOIP Options`.
2. Scroll down to the True Connect Enable parameter:

   ```
   True Connect Enable=No
   ```

3. Press [Enter], changing the value to `Yes`:

   ```
   True Connect Enable=Yes
   ```

4. Continue by pressing [Esc] until you are prompted to exit and save your changes, then save this change.

   True connect signaling takes affect with the next VoIP call.

Dependencies: The True Connect Enable parameter has the following dependencies:

- The Call Type parameter in the T1/E1 > Line # profile must be set to `VoIP Call` for T1 or E1 trunks used for VoIP calls that require true connect signaling. Setting this parameter to `VoIP Call` causes *all* calls received on the trunk to be mapped to VoIP.
- With ISDN trunks, it is recommended to set T310 on the Telco switch or PBX to 30 seconds or greater when using the true connect feature. The T310 timeout includes the time that the called party's phone is ringing, so a 10-second timeout can cause the near-end gateway to tear down the call too soon.
- When the true connect feature is enabled and a VoIP call fails before the PSTN call is fully connected, the MultiVoice gateway is still able to send an appropriate tone or voice announcement to the caller.

TS Enabled

Description: This enables or disables the terminal server.

Usage: Specify Yes or No. No is the default.

- Yes enables the terminal server.
- No disables the terminal server. Note that terminal services must be enabled to support incoming calls from analog modems or V.120 terminal adapters.

Example: `TS Enabled=Yes`

Location: Ethernet > Mod Config > TServ Options

TS Idle

Description: Specifies the number of seconds that a terminal server connection must be idle before the MAX disconnects the session.

Usage: Specify a value between 0 and 65535. The default is 120. A setting of 0 (zero) means that the line can be idle indefinitely.

Example: `TS Idle=60`

Dependencies: This parameter applies only to terminal server sessions.

Location: Ethernet > Answer > Session Options, Ethernet > Connections > *Connection profile* > Session Options

See Also: Encaps, TS Idle Mode

TS Idle Mode

Description: Specifies whether the MAX uses the terminal server idle timer and, if so, whether both the user and host must be idle before the MAX disconnects the session.

Usage: Specify one of the following values:

- None disables the idle timer.
- Input (the default) specifies that the MAX disconnects the session if the user is idle for a length of time greater than the value of the TS Idle parameter.
- Input/Output specifies that the MAX disconnects the session if both the user and the host are idle for a length of time greater than the value of the TS Idle parameter.

Example: `TS Idle Mode=Input/Output`

Dependencies: This parameter applies only to terminal server sessions.

Location: Ethernet > Answer > Session Options, Ethernet > Connections > *Connection profile* > Session Options

See Also: Encaps, TS Idle

Tunnel Protocol

Description: Specifies the type of tunneling protocol the MAX unit uses to establish a tunnel.

Usage: Specify one of the following values:

- ATMP (the default)—Ascend Tunnel Management Protocol
- PPTP—Point-to-Point Tunneling Protocol
- L2F—Layer 2 Forwarding
- L2TP—Layer 2 Tunnel Protocol

Example: `Tunnel protocol=ATMP`

Location: Ethernet > Mod Config > *any Connection profile* > Tunnel Options

See Also: ATMP HA RIP, Client ID, Home Network Name, Max Tunnels, Password, Pri. Tunnel Server, Profile Type, Sec. Tunnel Server, Tunnel VRouter, UDP Port

Tunnel VRouter

Description: Specifies the name of the VRouter the unit uses for the tunnel.

Usage: Specify up to 23 characters of text.

Example: `Tunnel VRouter=abcdefghijklmnopqrstuvw`

Location: Ethernet > Mod Config > *any Connection profile* > Tunnel Options

See Also: ATMP HA RIP, Client ID, Home Network Name, Max Tunnels, Password, Pri. Tunnel Server, Profile Type, Sec. Tunnel Server, Tunnel Protocol, Tunnel VRouter, UDP Port

Tx Gain

Description: Specifies the gain of the signal transmitted to the equipment.

Usage: Specify a value from 0 to -7 db. The default is -7 db.

Location: Analog FXS > FXS Config > *FXS Configuration profile* > Line *N*

Type

Description: Specifies the type of ATMP functionality supported in the MAX, or if it appears in a filter, the action performed by the filter.

Usage: Specify one of the following values:

In an Ethernet profile:

- Router specifies that the MAX is an ATMP home agent in routing mode (the default for ATMP home agents).
- Gateway specifies that the MAX is an ATMP home agent in gateway mode.

In a Filter profile:

- Generic means the filter examines byte and offset values within packets, regardless of which protocol is in use (the default in Filter profiles).
- IP means the filter examines the IP-specific fields within packets.

In an IPX SAP Filter profile:

- Exclude means the filter excludes the service defined in the filter (the default).
- Include specifies that the filter includes the service in the service table (if inbound) or in SAP response packets (if outbound).

Location: Ethernet > Mod Config > ATMP Options, Ethernet > Filters > Input filters > In filter N, Ethernet > Filters > Output filters > Out filter N, Ethernet > IPX SAP Filters > Input SAP Filters > In filter *N*, Ethernet > IPX SAP Filters > Output SAP Filters > Out filter *N*

See Also: ATMP Gateway, ATMP Mode, Password, Server Name, Server Type, Station, UDP Port, Valid

U

UDP Cksum

Description: This enables or disables the use of UDP checksums on this interface. If enabled, the MAX generates a checksum whenever it sends out a UDP packet. It sends out UDP packets for queries and responses related to the following protocols:

- ATMP
- SYSLOG
- DNS
- ECHOSERV
- RADIUS
- TACACS
- RIP
- SNTP
- TFTP

Note: You can enable this parameter if data integrity is of the highest concern for your environment, and having redundant checks is important; this setting is also appropriate if your UDP-based servers are located on the remote side of a WAN link that is prone to errors.

Usage: Specify Yes or No. No is the default.

- Yes generates UDP checksums for queries and responses related to protocols that use UDP.
- No disables UDP checksums.

Example: `UDP Cksum=Yes`

Location: Ethernet > Mod Config

UDP Port

Description: Specifies the destination UDP port number for ATMP packets.

Usage: Specify a numerical value from 0 through 65535. The default value is 5150.

Example: `UDP Port=5150`

Dependencies: This parameter is not applicable if the Profile Type parameter is disabled, the Tunnel Protocol parameter is set to any setting but ATMP, or ATMP is not enabled on the unit.

Location: Ethernet > Mod Config > *any Connection profile* > Tunnel Options

See Also: ATMP HA RIP, Client ID, Home Network Name, Max Tunnels, Password, Pri. Tunnel Server, Profile Type, Sec. Tunnel Server, Tunnel Protocol, Tunnel VRouter

Upload

Description: Enables or disables permission to upload the MAX configuration from another device.

Usage: Specify Yes or No. Yes is the default.

- Yes specifies the user can upload the MAX configuration from another device. This has the potential of clearing all passwords in the MAX.
- No disables this permission.

Example: `Upload=Yes`

Dependencies: This parameter is not applicable if the Operations permission is disabled.

Location: System > Security

See Also: Restore Cfg

Use Answer as Default

Description: Indicates whether the Answer profile should override the factory default Internet profile when the MAX validates an incoming call using RADIUS or TACACS.

Usage: Specify Yes or No. No is the default.

- Yes instructs the MAX to use the Answer profile for default values.

  When set to Yes, the MAX falls back to the value specified in the Answer profile for options that are not specified in a given external authentication profile. This does not affect Connection profiles in any way.
- No specifies the MAX uses the factory default Internet profile instead.

  When set to No, the MAX uses factory defaults for options not specified in an external authentication profile, rather than the values set in the Answer profile.

Example: `Use Answer as Default=Yes`

Location: Ethernet > Answer

Use Trunk Grps

Description: 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.

Usage: Specify Yes or No. No is the default.

- Yes specifies all channels must be assigned a trunk group number to be available for outbound calls.

- No specifies trunk groups will not be used.

Example: `Use Trunk Grps=Yes`

Dependencies: When this parameter is set to Yes, channel configurations must specify trunk-group assignments.

Location: System > Sys Config

See Also: B1 Trnk Grp, B2 Trnk Grp, Call Type, Ch *N* Trnk Grp, Dial #, Dial Plan

V

V.110

Description: Specifies the subaddress associated with the MAX unit's V.110 modems. The MAX routes an incoming call whose subaddress matches the value of V.110 to the first available V.110 modem; the MAX handles such a call as a terminal server call.

Usage: Specify a subaddress. You can specify a number between 0 and 99. The default is 0.

Dependencies: This parameter is ignored if the Sub-Adr parameter is not set to Routing.

Location: System > Sys Config

See Also: DM, LAN, Serial, Sub-Adr

V.120

Description: Specifies whether or not the MAX accepts incoming calls using V.120 encapsulation, provided they meet all other criteria.

Usage: Specify Yes or No. Yes is the default.

- Yes enables the MAX to accept incoming V.120 calls, provided that they meet all other connection criteria.
- No specifies the MAX will not accept inbound calls of this type.

Example: `V.120=Yes`

Location: Ethernet > Answer > Encaps

V42/MNP

Description: The digital modems negotiate LAPM/MNP error control with the analog modem at the other end of the connection according to how this parameter is set. The MAX can request LAPM/MNP and accept the call anyway if it is not provided, request it and drop the call if it is not provided, or not use LAPM/MNP error control at all.

Usage: Specify one of the following values:

- Will (the default)
  Request LAPM/MNP, but accept the call anyway if it is not provided.

- Won't
  Do not use LAPM/MNP at all.
- Must
  Request LAPM/MNP, and drop the call if it is not provided.

Example: `V42/MNP=Will`

Dependencies: This parameter is not applicable when terminal services are disabled.

Location: Ethernet > Mod Config > TServ Options

VA FileSpec

Description: Identifies the file path to the voice announcement files, used by the tftp command to retrieve the voice announcement files from the TFTP server. This is an ASCII text file which maps the message file names on the TFTP server to the voice announcement names used by MultiVoice. Changes to this parameter are effective with the next VoIP call.

Usage: Pressing [Enter] opens the edit field for the Voice Ann Serv parameter. This parameter accepts any valid IP address. This address should identify the TFTP server where the MAX will find the voice announcement files.

Dependencies: This parameter has the following dependencies:

- This parameter is ignored unless voice announcements are enabled (`Voice Ann Enbl=Yes`).
- When this parameter is enabled, the Voice Ann Serv parameter must be defined for voice announcements to work.

Location: Ethernet > Mod Config > VOIP Options

Valid

Description: Enables or disables the current input or output filter. When it is set to No, that input or output filter is skipped when filtering the data stream. You must set this parameter to Yes to configure the filter specification.

Usage: Specify Yes or No. No is the default.

- Yes activates the filter and enables its configuration.
- No disables the filter, causing the MAX to skip it when filtering the data stream.

Location: Ethernet > Filters > Input filters > In filter *N*, Ethernet > Filters > Output filters > Out filter *N*, Ethernet > IPX SAP Filters > Input SAP Filters > In filter *N*, Ethernet > IPX SAP Filters > Output SAP Filters > Out filter *N*

See Also: Server Name, Server Type, Type

Value

Description: Specifies a hexadecimal number to be compared to specific bits contained in packets after the Offset, Length, and Mask calculations have been performed. The MAX

compares only the unmasked portion of a packet to the Value parameter. The length of the Value parameter must contain the number of bytes specified by the Length parameter.

Usage: Specify a hexadecimal number up to 12 bytes.

Example: `Value=e0e0030000000000`

Location: Ethernet > Filters > Input filters > In filter *N* > Generic, Ethernet > Filters > Output filters > Out filter *N* > Generic

See Also: Length, Mask, Offset

VC Timer enable

Description: This enables or disables the Virtual Call Establishment (VCE) timer on a per-user basis. The VCE timer specifies the number of seconds to maintain a connection to a character-oriented device (such as the terminal server) that has not established a virtual call.

Usage: Specify Enable (to activate the VC timer for this connection) or Disable. Disable is the default.

Dependencies: This parameter applies only to X.25/PAD connections. If the X.25 profile disables the VC timer, this parameter has no effect.

Location: Ethernet > Connections > *Connection profile* > Encaps Options

See Also: Max Unsucc.Calls, VC Timer Val

VCE Timer Val

Description: Sets the Virtual Call Establishment (VCE) timer by specifying the number of seconds to maintain a connection to a character-oriented device (such as a terminal server) that has not established a virtual call. This timer value is link-wide. Each X.25 PAD connection has a parameter to enable or disable this timer on a per-connection basis.

Usage: Specify a number of seconds between 0 and 9999. A value of 0 disables this timer system-wide regardless of the value of the VC timer enable flag per connection. The default is 300 seconds.

Location: Ethernet > X.25

See Also: VC Timer

Version

Description: Specifies the version number of a Secure Access Firewall. Each firewall contains a version number to ensure that any firewall that is uploaded to the router will be compatible with the firewall software on the MAX. Secure Access Manager (SAM) checks the version number before uploading a firewall. In the event that a MAX with a stored firewall profile receives a code update that makes the existing firewall incompatible, a default firewall is enabled, permitting only Telnet access to the MAX.

Usage: This parameter cannot be edited.

Location: Ethernet > Firewalls

Virtual Router

Description: Specifies the name of the Vrouter for which the MAX unit creates a static route.

Usage: Specify the name of a VRouter. The default is null, which specifies that the unit uses the global virtual router (main).

Example: `Virtual Router=SL2`

Dependencies: The Virtual Router parameter is valid only if the Sys Option Status display specifies VRouter Avail.

Location: Ethernet > Static Rtes > *any Static Rtes profile*, Ethernet > Connections> *any Connection profile* > IP Options

See Also: Active, Allow As Client DNS, Dest VRouter, Domain Name, Name, Pool*#N* Count, Pool*#N* Name, Pool*#N* Start, Pool Summary, Pri DNS, Sec DNS, Sec Domain Name, RIP Policy, RIP Summary, RIP Trigger, VRouter IP Adrs

VJ Comp

Description: Specifies whether Van Jacobson IP header compression should be negotiated on incoming calls using encapsulation protocols that support this feature. VJ Comp applies only to packets in TCP applications, such as Telnet. Turning on header compression is most effective in reducing overhead when the data portion of the packet is small.

Usage: Specify Yes or No.

- Yes enables VJ compression for TCP packets.
  This is the default.
- No disables VJ compression.

Location: Ethernet > Answer > PPP Options, Ethernet > Connections > *Connection profile* > Encaps Options

Voice Ann Serv

Description: Identifies the TFTP server where the voice announcement files used for call progress reporting and pre-paid billing messages are stored. This parameter specifies the IP address of TFTP server where audio files are stored.

Usage: Pressing [Enter] opens the edit field for the Voice Ann Serv parameter. This parameter accepts any valid IP address. This address should identify the TFTP server where the MAX will find the voice announcement files.

Dependencies: This parameter has the following dependencies:

- This parameter is ignored unless voice announcements are enabled (`Voice Ann Enbl=Yes`).
- When this parameter is enabled, the VA FileSpec parameter must be defined for voice announcements to work.

- Using the default value for this parameter, 0.0.0.0, will prevent the MAX from retrieving message files from the TFTP server. Voice announcements will not be played out by this gateway, even when `Voice Ann Enbl=Yes`.

Location: Ethernet > Mod Config > VOIP Options

Voice Ann Dir

Description: Identifies the directory location where the voice announcement files are stored on the MAX. This value defaults to the `/current` directory on pc-flash card 1.

Usage: Pressing [Enter] opens an edit field used to specify the file path to the directory location containing the VoIP voice announcement files. This may be a string of 40 characters or less beginning with "/". This parameter defaults to N/A when `Voice Ann Enbl=No`. Changes to this parameter are effective with the next VoIP call.

Once the directory is created, voice announcement files can be copied from a TFTP server to the external flash memory card.

Example: To configure the voice announcement directory:

1. Create a directory on the flash card for the announcements. For example, the following commands create a directory named `messages` and a subdirectory named `announce` on the flash card in slot 1:

   ```
   > mkdir 1/messages
   > mkdir 1/messages/announce
   ```

2. The following command loads a voice-announcement file named `busy.au` from a TFTP server at 10.10.10.10 to the `/current` directory on flash card 1 (flash card 1 is the default):

   ```
   > load file network 10.10.10.10 busy.au
   ```

3. The following command moves the `busy.au` file to the new subdirectory on flash card 1:

   ```
   > mv 1/current/busy.au 1/messages/announce/busy.au
   ```

   Repeat this Step 2 and Step 3 for all voice announcement files.

4. Verify that the files have all been copied to that directory:

   ```
   > ls
   ```

Dependencies: This parameter has the following dependencies:

- This parameter is ignored unless voice announcements are enabled (`Voice Ann Enbl=Yes`).
- This parameter is ignored when the default values for VA FileSpec or Voice Ann Serv parameters are changed.

Location: Ethernet > Mod Config > VOIP Options

Voice Ann Enc

Description: Specifies either the G.711 U-Law or G.729 encoding of voice announcements played out by a MultiVoice gateway where voice announcements are used for reporting call progress to callers.

Usage: When a MultiVoice gateway uses voices announcements to report call progress to callers, selecting `G.711 U Law` as the value for the Voice Ann Enc parameter will enable use of G.711-U-Law encoding for voice announcement play out. Selecting `G.729` as the value for this parameter will enable use of G.729 encoding for voice announcement play out.

Example: The following example illustrates how to configure a MultiVoice gateway to use G.729 encoding for voice announcement play out.

1 From the MAX administration menu, select the `Ethernet` > `Mod Config` profile.

2 Scroll down to the VOIP Options, then press [Enter] to open this profile.

3 Scroll down to the Voice Ann Enc parameter, then press [Enter] to toggle the value of this parameter, as illustrated.

```
Voice Ann Enc=G.729
```

4 Press [Esc]; then, when prompted, select the option to `Exit and Save` your changes.

Dependencies: Changes to the Voice Ann Enc parameter take effect with the next VoIP.

Location: Ethernet > Mod Config > VOIP Options

VPN Mode

Description: Specifies whether or not the MultiVoice Access Manager (specified by the IP address in the GK IP Adrs parameter) requires callers to authenticate by means of a PIN number.

Usage: Specify Yes or No.

- Yes enables VPN mode. The MultiVoice Access Manager does *not* require callers to authenticate by means of a PIN number.

  This is the default.
- No disables VPN mode. Every caller must authenticate by means of a PIN number, and to complete a call, the caller's PIN must match a PIN in the database of the MultiVoice Access Manager.

Dependencies: VPN Mode applies only if the MAX acts as a MultiVoice Gateway.

Location: Ethernet > Mod Config > VOIP Options

See Also: GK IP Adrs, Pkt Audio Mode

VRouter IP Adrs

Description: When the MAX unit supports a Vrouter domain, VRouter IP Adrs specifies the default local IP address the unit uses for any outgoing packets generated by the VRouter.

Usage: Specify an IP address in dotted decimal notation. The default is 0.0.0.0.

Example: VRouter IP Adrs=0.0.0.0

Dependencies: The VRouter IP Adrs parameter is valid only if the Sys Option Status display specifies VRouter Avail.

Location: Ethernet > Virtual Routers > *any Virtual Routers profile*

See Also: Active, Allow As Client DNS, Dest VRouter, Domain Name, Pool#*N* Count, Pool#*N* Name, Pool#*N* Start, Pool Summary, Pri DNS, Sec DNS, Sec Domain Name, RIP Policy, RIP Summary, RIP Trigger, Virtual Router

W

WAN Alias

Description: Specifies the IP address of the link's remote interface to the WAN. It is used to identify a numbered interface at the remote end of the link. If an address is specified for WAN alias, the following events occur:

- Host routes are created both to the Lan Adrs and the WAN Alias address. The WAN Alias will be listed in the routing table as a gateway (next hop) to the Lan Adrs.
- A route is created to the remote system's subnet, showing the WAN Alias as the next hop.
- Incoming PPP/MP+ calls must report their IP addresses as the WAN Alias (rather than the Lan Adrs). That is, the caller must be using a numbered interface, and its interface address must agree with the WAN Alias on the receiving side.

If you want to create static routes to hosts at the remote end, you can use the WAN Alias address as the "next hop" (gateway) field. (The Lan Adrs address will also work, as would be used for system-based routing.)

Usage: Specify the IP address of the remote interface. The default is 0.0.0.0/0.

Example: `WAN Alias=10.207.23.7/24`

Dependencies: This parameter does not apply if the connection does not route IP.

Location: Ethernet > Connections > *Connection profile* > IP Options

See Also: Route IP, IF Adrs

WR Mgr*N* (*N*=1-8)

Description: Specifies up to eight IP addresses of SNMP managers that have SNMP write permission. A MAX unit responds to SNMP Set, Get, and Get-Next commands from these SNMP managers only, provided that the Security parameter is set to Yes.

Usage: Specify the IP address of a host running an SNMP manager. The default setting is 0.0.0.0, which specifies no host. Do not include subnets as a part of the IP address you specify.

Example: `WR Mgr1=10.5.6.7`

Dependencies: The Security parameter must be set to Yes for these parameters to restrict read-write access to the MAX.

Location: Ethernet > Mod Config > SNMP Options

See Also: Security, RD Mgr*N* (*N*=1-8)

X

X.121 src addr

Description: Specifies the X.121 source address is the MAX unit's source address for logical links using this X.25 profile. An X.121 address contains between 1 and 15 decimal digits, such as 031344159782738.

Usage: Specify an X.121 address.

Example: `X.121 src addr=031344159782738`

Location: Ethernet > X.25

X.25 Clear/Diag

Description: Specifies whether Clear-Request packets include the diagnostic field.

The DTE sends a Clear-Request packet to initiate clearing procedures for a call. The DCE accomplishes the same task by using a Clear-Indication packet. The DTE can send a Clear-Request packet to refuse an incoming call, or to clear a call once the data exchange is complete. Once the DTE or DCE receives a Clear-Confirmation packet, the call is cleared and the logical channel is available for other calls.

A Clear-Request packet has a required Cause field and an optional Diagnostic field. If the Cause field indicates that the remote DTE did not request the reset, the diagnostic field has standard values. If the Cause field indicates that the remote DTE requested the reset, the diagnostic field contains information specified in the Cause field by the remote DTE.

Usage: Specify Yes or No. No is the default.

- Yes causes the MAX to include the diagnostic field in Clear-Request packets.
- No specifies the optional diagnostic field is not included in Clear-Request packets.

Location: Ethernet > X.25

See Also: X.25 Reset/Diag, X.25 Restart/Diag

X.25 highest PVC

Description: Specifies the highest Permanent Virtual Circuit (PVC) number in a range defined by the X.25 lowest and X.25 highest PVC parameters. The range of PVCs can be between 1 and 4096. If the lowest PVC number is zero, no PVCs are supported.

Usage: Specify the high number in the range of PVCs available for this X.25 profile. The default is zero. The number you specify must be greater than or equal to the value specified by the X.25 lowest PVC parameter.

Example: `X.25 highest PVC=128`

Dependencies: If X.25 lowest PVC is zero, no PVCs are supported regardless of this setting.

Location: Ethernet > X.25

See Also: X.25 lowest PVC

X.25 highest SVC

Description: Specifies the highest Switched Virtual Circuit (SVC) number in a range defined by the X.25 lowest and X.25 highest SVC parameters. The range of SVCs can be between 1 and 4096. If the lowest SVC number is zero, no SVCs are supported.

Usage: Specify a number between 0 and 4095. The default is 8. The number you specify must be greater than or equal to the value specified by the X.25 Lowest SVC parameter.

Example: `X.25 highest SVC=8`

Dependencies: If X.25 lowest SVC is zero, no SVCs are supported regardless of this setting.

Location: Ethernet > X.25

See Also: X.25 lowest SVC

X.25 Link Setup Mode

Description: Specifies whether the X.25 link comes up in active or passive disconnect mode. In ACTIVE disconnect mode (the default) the link layer comes up sending a DISC, and the packet layer sends a Restart-Request packet at initialization. In PASSIVE disconnect mode the link layer comes up sending SABM(E), and issues a restart to the network only upon receipt of a request restart token. It will not issue a Restart-Request packet upon initialization, but responds to restart packets it receives.

Usage: Specify one of the following values:

- ACTIVE specifies active disconnect mode. Active is the default.
- PASSIVE specifies passive disconnect mode.

Example: `X.25 Link Setup Mode=ACTIVE`

Location: Ethernet > X.25

X.25 lowest PVC

Description: Specifies the lowest Permanent Virtual Connection (PVC) number in a range defined by the X.25 lowest and X.25 highest PVC parameters. The range of PVCs can be between 1 and 4096. If the lowest PVC number is zero, no PVCs are supported.

Usage: Specify a number between 0 and 4095. The default is 0 (zero), which means that no PVCs are available.

Example: `X.25 lowest PVC=1`

Dependencies: The upper limit of the range is defined by the X.25 highest PVC parameter.

Location: Ethernet > X.25

See Also: X.25 highest PVC

X.25 lowest SVC

Description: Specifies the lowest Switched Virtual Connection (SVC) number in a range defined by the X.25 lowest and X.25 highest SVC parameters. The range of SVCs can be between 1 and 4096. If the lowest SVC number is zero, no SVCs are supported.

Usage: Specify a number between 0 and 4095. The default is 0 (zero), which means that no SVCs are available.

Example: `X.25 lowest SVC=1`

Dependencies: The upper limit of the range is defined by the X.25 highest SVC parameter.

Location: Ethernet > X.25

See Also: X.25 highest SVC

X.25 Max pkt size

Description: Specifies the maximum number of bytes in the data field of a data packet when negotiating the packet size with a remote X.25 switch. Note that a large packet size improves throughput by reducing the overhead associated with header transmission. However, a large packet size also increases the probability of transmission errors, causes increased transmission delays on the network, and is associated with processing delays at the host.

Usage: Specify one of the following values:

- 64
- 128 (the default)
- 256
- 512
- 1024
- 2048
- 4096

Location: Ethernet > X.25

See Also: X.25 pkt size, X.25 Min pkt size, X.25 window size

X.25 Min pkt size

Description: Specifies the minimum number of bytes in the data field of a data packet when negotiating the packet size with a remote X.25 switch.

Usage: Specify one of the following values:

- 64
- 128 (the default)
- 256
- 512
- 1024

- 2048
- 4096

Location: Ethernet > X.25

See Also: X.25 pkt size, X.25 Max pkt size, X.25 window size

X.25 Network Type

Description: Specifies the type of network used by the link. At present, only the CCITT network type is supported.

Usage: CCITT specifies that the link uses a CCITT network.

Example: `X.25 Network Type=CCITT`

Location: Ethernet > X.25

X.25 Node Type

Description: Specifies whether the MAX interacts with the remote end of the connection as a DTE (the default) or DCE. A DTE is a device that a user uses, such as a computer or a terminal. A DCE is a device that connects the DTE to a communications channel.

Usage: Specify one of the following values:

- DTE if the MAX interacts with the remote end of the X.25 connection as a DTE. This is the default.
- DCE if the MAX interacts with the remote end of the X.25 connection as a DCE

Example: `X.25 Node Type=DTE`

Dependencies: For proper X.25 operation, the two ends of a link must be of opposite types.

Location: Ethernet > X.25

X.25 options

Description: Specifies X.25 packet-level options.

Usage: Specify one of the following values:

- None specifies that no packet-level options are enabled. None is the default.
- NPWS specifies that the X.25 protocol negotiates packet and window size.
  The window size establishes the maximum number of data packets that can be outstanding between a DTE and a DCE before acknowledgment is required.

Example: `X.25 options=None`

Location: Ethernet > X.25

See Also: X.25 pkt size, X.25 Max pkt size, X.25 Min pkt size, X.25 window size

X.25 pkt size

Description: Specifies the default number of bytes in the data field of a data packet.

Usage: Specify one of the following values:

- 64
- 128 (the default)
- 256
- 512
- 1024
- 2048
- 4096

Location: Ethernet > X.25

See Also: X.25 Max pkt size, X.25 Min pkt size, X.25 window size

X.25 Prof

Description: Specifies the name of an X.25 profile to use for this connection. To guard against misconfiguration, the MAX does not allow you to save an active Connection profile specifying X.25 encapsulation unless the named X.25 profile is defined and active.

Usage: Specify the name of an X.25 profile, which can contain up to 15 characters.

Dependencies: This parameter applies only to X.25/PAD and X.25/IP connections.

Location: Ethernet > Connections > *Connection profile* > Encaps Options

X.25 R20

Description: Determines the limit for Restart Retries—that is, the number of times the MAX transmits a Restart-Request packet before waiting indefinitely for a response. At the packet layer, a Restart-Request packet clears all virtual circuits. When the sending device receives a Restart-Confirmation packet, it can again issue a call to establish a virtual circuit.

Usage: Specify a number between 0 and 255. The default is 0 (zero). This default indicates that the MAX always waits indefinitely for a response.

Dependencies: The value you specify is not meaningful if X.25 T20=0.

Location: Ethernet > X.25

See Also: X.25 R22, X.25 R23, X.25 T20

X.25 R22

Description: Determines the limit for Reset Retries—that is, the number of times the MAX retransmits a Reset-Request packet before clearing a call. At the packet layer, a Reset-Request packet resets the packet sequence number for the logical channel to 0 (zero), and removes any

outstanding data and Interrupt packets from the virtual circuit. Once the sending device receives a Reset-Confirmation packet, it can send data on the logical channel.

Usage: Specify a number between 0 and 255. The default is 0 (zero).

Dependencies: The value you specify is not meaningful if X.25 T22=0.

Location: Ethernet > X.25

See Also: X.25 R20, X.25 R23, X.25 T22

X.25 R23

Description: Determines the limit for Clear-Request Retries—that is, the number of times the MAX sends a Clear-Request before waiting indefinitely for a response.

The DTE can send a Clear-Request packet to refuse an incoming call, or to clear a call once the data exchange is complete. The DCE accomplishes the same task by using a Clear-Indication packet. Once the DTE or DCE receives a Clear-Confirmation packet, the call is cleared and the logical channel is available for other calls.

Usage: Specify a number between 0 and 255. The default is 0 (zero).

Dependencies: The value you specify is not meaningful if X.25 T23=0.

Location: Ethernet > X.25

See Also: X.25 R20, X.25 R22, X.25 T23

X.25 Reset/Diag

Description: Specifies whether Reset-Request packets include the diagnostic field. At the packet layer, a Reset-Request packet resets the packet sequence number for the logical channel to 0 (zero), and removes any outstanding data and Interrupt packets from the virtual circuit. Once the sending device receives a Reset-Confirmation packet, it can send data on the logical channel.

A Reset-Request packet has a required Cause field and an optional Diagnostic field. If the Cause field indicates that the remote DTE did not request the reset, the diagnostic field has standard values. If the Cause field indicates that the remote DTE requested the reset, the diagnostic field contains information specified in the Cause field by the remote DTE.

Usage: Specify Yes or No. No is the default.

- Yes causes the MAX to include the diagnostic field in Reset-Request packets.
- No specifies the optional diagnostic field is not included in Reset-Request packets.

Location: Ethernet > X.25

See Also: X.25 Clear/Diag, X.25 Restart/Diag

X.25 Restart/Diag

Description: Specifies whether Restart-Request packets include the diagnostic field. At the packet layer, a Restart-Request packet clears all virtual circuits. When the sending device receives a Restart-Confirmation packet, it can again issue a call to establish a virtual circuit.

A Restart-Request packet has a required Cause field and an optional Diagnostic field. If the Cause field indicates that the remote DTE did not request the restart, the diagnostic field has standard values. If the Cause field indicates that the remote DTE requested the restart, the diagnostic field contains information specified in the Cause field by the remote DTE.

Usage: Specify Yes or No. No is the default.

- Yes causes the MAX to include the diagnostic field in Restart-Request packets.
- No specifies the optional diagnostic field is not included in Restart-Request packets.

Location: Ethernet > X.25

See Also: X.25 Clear/Diag, X.25 Reset/Diag

X.25 Seq Number Mode

Description: Specifies whether the MAX uses modulo 8 or modulo 128 sequence number mode. At the frame level, X.25 allows a sender to transmit a certain number of frames before requiring an acknowledgment of the first frame. The protocol increments a sequence number in the frame header, and places the value into the next outgoing frame. The sequence number identifies each frame that has not yet been acknowledged.

Usage: Specify one of the following values:

- NORMAL specifies modulo 8 mode.

  In modulo 8 mode, the sequence number can contain three bits, allowing eight frames to be identified with a single sequence number.

  Normal is the default.
- EXTENDED specifies module 128 mode.

  When substantial delays in transmission can occur, you can specify Extended so that the sequence number is enlarged to seven bits. When you choose this setting, 128 frames can be identified with a unique sequence number.

Example: `X.25 Seq Number Mode=NORMAL`

Location: Ethernet > X.25

X.25 T20

Description: Determines the duration of the Restart timer—that is, the number of one-second ticks the MAX waits before retransmitting a Restart-Request packet. At the packet layer, a Restart-Request packet clears all virtual circuits. When the sending device receives a Restart-Confirmation packet, it can again issue a call to establish a virtual circuit.

Usage: Specify a number between 0 and 255. The default is 0 (zero). This default setting disables the timer.

Location: Ethernet > X.25

See Also: X.25 R20, X.25 T21, X.25 T22, X.25 T23

X.25 T21

Description: Determines the duration of the Call-Request timer—that is, the number of one-second ticks the MAX waits before clearing an outgoing call that has not been accepted. When a device makes an outgoing call, it sends a Call-Request packet. If the remote DTE accepts the call, it sends back a Call-Connected Packet; if the DTE refuses the call, it sends back a Clear-Request packet.

Usage: Specify a number between 0 and 255. The default is 0 (zero). This default setting disables the timer.

Location: Ethernet > X.25

See Also: X.25R21, X.25 T20, X.25 T22, X.25 T23

X.25 T22

Description: Determines the duration of the Reset-Request timer—that is, the number of one-second ticks the MAX waits before retransmitting a Reset-Request packet. At the packet layer, a Reset-Request packet resets the packet sequence number for the logical channel to 0 (zero), and removes any outstanding data and Interrupt packets from the virtual circuit. Once the sending device receives a Reset-Confirmation packet, it can send data on the logical channel.

Usage: Specify a number between 0 and 255. The default is 0 (zero). This default setting disables the timer.

Location: Ethernet > X.25

See Also: X.25 R22, X.25 T20, X.25 T21, X.25 T23

X.25 T23

Description: Determines the duration of the Clear-Request timer—that is, the number of one-second ticks the MAX waits before retransmitting a Clear-Request packet. When a device makes an outgoing call, it sends a Call-Request packet. If the remote DTE accepts the call, it sends back a Call-Connected Packet; if the DTE refuses the call, it sends back a Clear-Request packet.

Usage: Specify a number between 0 and 255. The default is 0 (zero). This default setting disables the timer.

Location: Ethernet > X.25

See Also: X.25 R23, X.25 T20, X.25 T21, X.25 T22

X.25 window size

Description: Specifies the maximum number of data packets that can be outstanding between a DTE and a DCE before acknowledgment is required.

Usage: Specify a number between 1 and 7. The default is 7.

Dependencies: The value you specify applies to all of the user's virtual circuits. However, the user can use the FACILITIES command at the PAD prompt to alter the window size on a per-call basis.

Location: Ethernet > X.25

See Also: X.25 Default Packet Size, X.25 Max Packet Size, X.25 Min Packet Size

X25/PAD

Description: Specifies whether the MAX accepts incoming X.25/PAD calls.

Usage: Specify Yes or No. Yes is the default.

- Yes specifies the MAX accepts X.25/PAD calls, provided that they meet all other connection criteria.
- No specifies the MAX will not accept inbound X.25/PAD calls.

Location: Ethernet > Answer > Encaps

See Also: Encaps

X.3 Custom

Description: This parameter specifies a string containing X.3 profile parameters. The MAX parses this string into X.3 profile parameters when a user uses the PAD.

Usage: Specify a string using this format:

```
X.3 Custom=[ref:]val,[ref:]val, ... ,[ref:]val
```

where:

`ref` is the number of an X.3 parameter as defined in the ITU X.3 specification. You can specify a value between 1 and 22. By default, `ref` starts at 1 and is incremented by 1 after each comma. Unless you wish to specify fewer X.3 parameters than the maximum, you do not need to enter a value for `ref`.

`val` is the value associated with the X.3 parameter.

The MAX silently ignores invalid parameters.

You can enter up to 64 characters for the entire X.3 Custom specification. By default, the X.3 Custom parameter contains the X.3 parameter values set in the CRT profile.

Dependencies: The X.3 Custom parameter does not apply if X.3 Param Prof is not set to CUSTOM.

Location: Ethernet > Answer > X.25 Options, Ethernet > Connections > *Connection profile* > Encaps Options

See Also: X.3 Param Prof

X.3 Param Prof

Description: Specifies the default X.3 profile for setting up the PAD for this connection. Note that a user can specify a profile using a PAD command. In this case the profile specified on the command line overrides this default for the length of the current session.

Usage: Specify one of the following values:

- CRT (the default)
- INFONET
- DEFAULT
- SCEN
- CC_SSP
- CC_TSP
- HARDCOPY
- HDX
- SHARK
- NULL

Dependencies: This parameter applies only to X.25/PAD connections.

Location: Ethernet > Connections > *Connection profile* > Encaps Options

X.75

Description: Specifies whether the MAX accepts incoming calls that use X.75 encapsulation.

Usage: Specify Yes or No. Yes is the default.

- Yes indicates that the MAX accepts incoming X.75 calls.
- No indicates that the MAX does not accept incoming X.75 calls.

Location: Ethernet > Answer > Encaps

See Also: Frame Length, K Window Size, N2 Retran Count, T1 Retran Timer

Z

Zone Name #N

Description: Specifies the name of the AppleTalk zone to which the MAX belongs. If the local Ethernet network supports an AppleTalk router with configured zones, you can place the MAX in one of those zones.

A zone is a multicast address containing an arbitrary subset of the AppleTalk nodes in an internet. Each node belongs to only one zone, but a particular extended network can contain nodes belonging to any number of zones. Zones provide departmental or other groupings of network entities that a user can easily understand. If the MAX is an AppleTalk router, it brings up the line when it receives packets addressed to the network number (defined by Net Start and

Net End) or zone name specified for the remote connection, and routes packets to the appropriate network or zone.

Usage: Specify the name of a zone that has been configured on the local Ethernet network. Enter up to 33 alphanumeric characters.

If you do not specify a name and AppleTalk=Yes, the MAX acquires its zone(s) from the seed router on the network, including the default zone.

In a Lucent AppleTalk router, zone names are not case sensitive. However, some routers regard zone names as case sensitive, and you should be consistent in spelling zone names when you configure multiple connections or routers. Although AppleTalk permits the use of spaces in zone names, it does not consider an underscore to be the same as a space. Since some routers do equate the underscore and the space, or do not recognize a space as a valid character, it is advisable to use only the underscore in a network with routers other than Lucent routers.

Example:

```
Default Zone=SALES
Zone Name #1=MKTG
Zone Name #2=ENGINEERING
Zone Name #3=ADMIN
Zone Name #4=BRANCH
```

Dependencies: If AppleTalk is disabled, the Zone Name parameter does not apply.

Location: Ethernet > Mod Config > AppleTalk

See Also: Default Zone, AppleTalk, Route AppleTalk, Net Start, Net End, AppleTalk Router

Index

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y