

# **MAX Reference Guide**

*Ascend Communications, Inc.  
Part Number: 7820-0647-001  
For software version 7.0.0*

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

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

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

---

# ***Ascend Customer Service***

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

## **Obtaining technical assistance**

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

### ***Enabling Ascend to assist you***

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

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

### ***Calling Ascend from within the United States***

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

#### ***Priority Technical Assistance***

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

#### ***Ascend Advantage Pak***

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

#### ***Other telephone numbers***

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

---

## *Calling Ascend from outside the United States*

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

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

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

## *Obtaining assistance through correspondence*

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

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

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

## **Finding information and software on the Internet**

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

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

# Contents

Ascend Customer Service ..... iii

**About This Guide ..... vii**

How to use this guide ..... vii  
What you should know ..... vii  
Documentation conventions ..... viii  
Documentation set ..... ix  
Related publications ..... ix

**Chapter 1      MAX Alphabetic Parameter Reference ..... 1**

Numeric ..... 2  
A ..... 5  
B ..... 33  
C ..... 40  
D ..... 62  
E ..... 80  
F ..... 89  
G ..... 98  
H ..... 99  
I ..... 105  
K ..... 117  
L ..... 118  
M ..... 130  
N ..... 141  
O ..... 147  
P ..... 150  
Q ..... 168  
R ..... 168  
S ..... 179  
T ..... 200  
U ..... 215  
V ..... 218  
W ..... 221  
X ..... 222  
Z ..... 231

**Index ..... Index-1**



# About This Guide

## *How to use this guide*

This guide contains a single chapter, the “MAX Alphabetic Parameter Reference” that explains parameters in alphabetical order. This guide also includes an index.



## *What you should know*

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

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

## Documentation conventions

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

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

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



## Documentation set

The MAX documentation set consists of the following manuals:

- *Administration Guide for your MAX*
- *Hardware Installation Guide for your MAX*
- *Network Configuration Guide for your MAX*
- *MAX Reference Guide (this guide)*
- *MAX Security Supplement*
- *MAX RADIUS Configuration Guide*

## Related publications

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

Here are some related publications that you may find useful:

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



# MAX Alphabetic Parameter Reference

# 1

The MAX supports a variety of software loads which are customized to particular purposes. The installed software may not support all of the parameters described in this reference.

Numeric .....	1-2
A.....	1-5
B.....	1-33
C.....	1-40
D.....	1-62
E.....	1-80
F.....	1-89
G.....	1-98
H.....	1-99
I .....	1-105
K.....	1-117
L.....	1-118
M .....	1-130
N.....	1-141
O.....	1-147
P.....	1-150
Q.....	1-168
R.....	1-168
S.....	1-179
T.....	1-200
U.....	1-215
V.....	1-218
W .....	1-221
X.....	1-222

Z..... 1-231

## Numeric

### 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 to set all inactive channels on that line to out\_of\_service state, as soon as the user saves the menu changes. When current calls on that line are ended, the associated channels will be put out of service. Selecting any other option after the Quiesced option restores all channels to in\_service state, as soon as the user saves the menu.
- Disabled to disable the line.
- Trunk (the default) to enable line 1 to exchange signaling information over the interface.
- T-Online-USER  
This setting indicates that the line connects to the switch, allowing the user to dial in.
- T-Online-ZGR  
This setting indicates that the line connects to the ZGR server.

**Example:** 1st Line=Trunk

**Dependencies:** If you specify Quiesced, 2nd line cannot be 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. It gives the MAX a logical interface on two networks or subnets on the same backbone, a feature 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 whether it will support trunk calls or drop-and-insert applications only. Drop-and-insert applications are used to accept calls on line #1 and drop them through to line #2. It 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 to set all inactive channels on that line to out\_of\_service state, as soon as the user saves the menu changes. When current calls on that line are ended, the associated channels will be put out of service. Selecting any other option after the Quiesced option restores all channels to in\_service state, as soon as the user saves the menu.
- Disabled to disable the line.
- Trunk (the default) to enable line 2 to exchange signaling information over the interface.
- D&I to use the second line for Drop-and-Insert applications only.
- T-Online-USER  
This setting indicates that the line connects to the switch, allowing the user to dial in.
- T-Online-ZGR  
This setting indicates that the line connects to the ZGR server.

**Example:** 2nd Line=Trunk

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

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

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

## 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 this example setting, the terminal server displays these prompts:

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

**Dependencies:** This parameter is not applicable when 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 3rd 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 Ascend unit sends the user's input to the additional prompt to RADIUS as a part of the authentication request. The user's input 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 in the Third Prompt parameter appears when the user connects and the user's input is echoed. After the user enters a Login name and Password, the input in response to the third prompt is passed to RADIUS as part of the authentication request.

**Example:** 3rd Prompt Seq=Last

**Dependencies:** This parameter is not applicable when 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 specify the address of the server using the Acct Host parameter.

**Usage:** Specify one of the following values:

- None (the default) specifies that no accounting takes place.
- RADIUS enables RADIUS accounting.
- TACACS+ enables TACACS+ accounting.

**Example:** Acct=RADIUS

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

**Location:** Ethernet > Mod Config > Accounting

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

### Acct Checkpoint

**Description:** Specifies the interval, in minutes, that 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 the RADIUS Accounting is not used.

**Location:** Ethernet > Mod Config > Accounting

### 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

## MAX Alphabetic Parameter Reference

### Acct Host #N (N=1–3)

---

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

**Location:** Ethernet > Connections > Accounting

**See Also:** Acct Type

### Acct Host #N (N=1–3)

**Description:** Each of these parameters 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 connects to a server other than the server #1, it 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 in 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 indicates that no authentication server exists.

**Dependencies:** The Acct Host #N parameter does not apply when Acct=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. See the MAX *RADIUS Configuration Guide* for more information.

**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) specifies that the numeric base is 10. This is the default.
- 16 (hexadecimal) specifies that the numeric base is 16.

**Example:** Acct-ID Base=10

**Dependencies:** This parameter is 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 > 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=Ascend

**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 > Accounting

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

## Acct Max Retry

**Description:** The Acct Max Retry parameter addresses the situation where the RADIUS accounting server is not responding to the MAX unit's Accounting Request packets. This parameter sets the number of times the MAX sends an Accounting Request before it gives up. If the RADIUS accounting backoff queue overflows, the MAX discards Accounting Requests whether or not they have reached the maximum number of retries.

**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 when the Acct parameter = RADIUS and the other required RADIUS accounting parameters have been configured.

**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 Ascend 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 > Accounting

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

## Acct Reset Timeout

**Description:** This parameter forces the MAX to try to return to the primary RADIUS accounting server; specifically, the server defined by the parameter Acct Host #1.

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

**Usage:** Enter the 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 Profile: 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 between 0 and 65535. The default value is 0 (zero); if you accept this value, the MAX can use any port number between 1024 and 2000.

**Location:** Ethernet > Mod Config > Accounting

**See Also:** Auth Src Port

## Acct Timeout

**Description:** 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.

**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 > 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 in this 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 > Accounting

## ACK Suppression

**Description:** For DTE-initiated calls, this 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)  
Specifies that the PAD acknowledges the DTE's opening frame and the establishment of a call with the host.
- On  
Specifies that the PAD does not acknowledge either the DTE's opening frame or the establishment of a call with the host.

**Dependencies:** Keep the following information in mind.

- ACK Suppression only applies to DTE-initiated calls using Transparent or Blind mode.

**Location:** Ethernet > Connections > *any Connection profile* > Encaps options  
Etherne > 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 to activate the time period. This is the default for Time Period 1.

- Disabled to ignore the time period. This is the default for Time Periods 2, 3, and 4.
- Shutdown to clear the dynamic call during the time period and redial it at the end of the time period. The MAX can use a shutdown port for answering and dialing calls, but the MAX 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/6) > PortN Menu > Directory > Time Period N

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

## Activation

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

**Usage:** Specify one of the following values:

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

**Example:** Activation=Static

**Location:** Serial WAN > Mod Config

## Active

**Description:** Activates a profile (making it available for use) or a route (adding it to the routing table). A dash appears before each deactivated profile or route.

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

- Yes activates the profile or feature, making it available for use.
- No disables the profile or feature, making it unavailable for use.

**Example:** Active=Yes

**Location:** Ethernet > Connections, Ethernet > Frame Relay, Ethernet > Names / Passwords, Ethernet > Static Rtes, Ethernet > X.25

## Add Number

**Description:** Specifies a series of digits to add to the beginning of the dialout phone number after removing the digits specified by Delete Digits. The device connected to line #2 (typically a PBX) dials this phone number.

**Usage:** Specify the digits you want the MAX to add to the beginning of the phone 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 in the Inc Ch Count parameter.

**Usage:** Specify a number between 1 and 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.

**Location:** Ethernet > Answer > PPP Options, Host/Dual (Host/6) > Port/*N* Menu > Directory, Ethernet > Connections > 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 Ascend units on the same network are configured with redundant profiles and routes. It solves a problem that occurred when two or more Ascend 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) to always advertise IP routes. Use this setting unless you have redundant MAX units or do not use dialout routes.
- Trunks Up to stop advertising (“poison”) its 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-PDU (Protocol Data Units) to the SNMP manager. The following alarm events defined in the Ascend Enterprise MIB. (See the Ascend Enterprise MIB for the most up-to-date information.)

- coldStart (RFC-1215 trap-type 0)  
A coldStart trap signifies that the MAX sending the trap is reinitializing itself so that the configuration of the SNMP manager or the unit might be altered.
- warmStart (RFC-1215 trap-type 1)  
A warmStart trap signifies that the MAX sending the trap is reinitializing itself so that neither the configuration of SNMP manager or the unit is altered.
- linkDown (RFC-1215 trap-type 2)  
A linkDown trap signifies that the MAX sending the trap recognizes a failure in one of the communication links represented in the SNMP manager's configuration.
- linkUp (RFC-1215 trap-type 3)  
A linkUp trap signifies that the MAX sending the trap recognizes that one of the communication links represented in the SNMP manager's configuration has come up.
- frDLCIStatusChange (RFC-1315 trap-type 1)  
A DLCIStatusChange trap signifies that the MAX sending the trap 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, invalidated, or it has toggled between the active and inactive states.
- eventTableOverwrite (ascend trap-type 16)  
A new event has overwritten an unread event. This trap is sent only for systems that support Ascend's accounting MIB. Once sent, additional overwrites will not cause another trap to be sent until at least one table's worth of new events have occurred.

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

- Yes causes the MAX to generate alarm-event traps and send the trap-PDU to the SNMP host.
- No means 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 the administrator 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

## All Port Diag

**Description:** Enables or disables a permission that allows an operator to perform all port diagnostic commands listed in the Port Diag menu.

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

- Yes means the operator can perform all diagnostic commands in the Port Diag menu.
- No means the operator cannot use those commands.

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

**Example:** All Port Diag=No

**Location:** System > Security

**See Also:** Own Port Diag

## 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 all client DNS servers are not defined or available.

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

- Yes allows clients to use the local DNS servers.
- No prevent 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 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 one of the following values:

- Yes means that the MAX can send Stop Accounting Packets to RADIUS that do not contain a username.
- No means that you are not restricting 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 configured.

**Location:** Ethernet > Mod Config > Accounting

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

## Analog Encoding

**Description:** Specifies the encoding standard for digitized analog data. Its value is used for all codecs on the MAX.

If an encoding standard other than the default is selected, modem dialout does not work; choosing a non-default encoding method works only for incoming analog data. To arrive at the proper default, you must clear NVRAM. If a System 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 is the default for T1.
- a-Law (A-Law encoding). This is the default for E1.

**Example:** Analog Encoding=u-Law

**Location:** System > Sys Config



---

## Ans #

**Description:** Specifies a phone number to be used for routing calls received on the first T1 line to the second line. This may be an add-on number.

**Usage:** Specify a phone number. The default is null. You can enter up to 18 characters, and you must limit your specification to these 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 phone number to be used for call-routing purposes. It 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 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 phone number for each Ans N# parameter. You can enter up to 24 characters, which may 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 DNIS (Dialed Number Information Service). Under most circumstances, the Answer number 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 Answer number with EAZ service in Europe requires that you include the EAZ subaddress in the parameter.

**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/6) > 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 specifies that the MAX can initiate calls to the destination specified in the Connection profile, and that the MAX can receive calls from that destination as well.

Both is the default.

- Call Only specifies that the MAX can dial out to the destination specified in the Connection profile, but cannot answer calls from that destination.
- Ans Only specifies that 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 > 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. It provides an alternative way to indicate which calls received on line 1 should be forwarded to line 2. If you set both Ans # and Ans Service to null, the MAX 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 connects to MultiRate or GloBanD data services)
  - 1536K (Switched-1536 calls, which are supported only with ISDN NFAS signaling)
  - 1536KR (Switched-1536 calls, which are supported only with ISDN NFAS signaling, whose data is restricted)
  - 128K, 192K, 256K 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 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 RI (Ring Indicate) 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

**Dependencies:** The Answer parameter does not prevent you from answering manually.

**Location:** Host/Dual (Host/6) > PortN Menu > Port Config

## 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.

**Note:** This field cannot be left empty if Call Mode is set to Both or Incoming.

**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:** Answer X.121 Addr=031344159782111

**Dependencies:** This parameter applies only to X.25/IP connections.

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

**See Also:** Call Mode

## APP Host

**Description:** Specifies the IP address of the host that runs the 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 between 0 and 255, separated by periods. Separate the optional netmask from the address using a slash. The default value is 0.0.0.0/0. The default setting 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=PAP-Token and APP Server=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 network.

**Location:** Ethernet > Mod Config > Auth

**See Also:** APP Server, Send Auth

## APP Port

**Description:** Specifies the UDP port number monitored by the APP server identified in 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=PAP-Token and APP Server=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=PAP-Token and APP Server=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 ARA (AppleTalk Remote Access) 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 non-seed 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

Specifies that 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 zero (0) does not cause a conflict. Non-seed 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 network with this range. A router with the zero 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
- Specifies that the router is not an AppleTalk seed router. It will acquire a network number range value from a seed router on the network.
- Off (the default)

**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 ARA (AppleTalk Remote Access) 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 means 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:** At this release, we recommend that you configure the local and WAN interfaces in the same area.

**Location:** Ethernet > Connections > 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. An administrator 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 area-type 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

**Dependencies:** You must set the AreaType parameter consistently on all OSPF routers within the area.

**Location:** Ethernet > Connections > OSPF Options, Ethernet > Mod Config > OSPF Options

## Ascend-Shared-Profile-Enable

**Description:** Enables or disables sharing of a RADIUS user file for multiple incoming users.

**Note:** To apply Shared Profiles on a per RADIUS user profile basis, you have to disable profile sharing on a system-wide basis by setting Ethernet > Mod Config > Shared Prof = No on the MAX

**Usage:** You can specify one of the following settings:

- Ascend-Shared-Profile-Enable = Shared-Profile-Yes specifies that multiple incoming calls can share this RADIUS user profile.
- Ascend-Shared-Profile-Enable = Shared-Profile-No specifies that multiple incoming calls cannot share a local Connection Profile.

The default value is Shared-Profile-No

**Dependencies:** 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.

## 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 may 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 > OSPF Options, Ethernet > Mod Config > OSPF Options, Ethernet > Static Rtes

## 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

## **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 > Session Options

**See Also:** ATMP Mode, Password, Type, UDP Port

## **ATMP Mode**

**Description:** Specifies whether ATMP (Ascend Tunnel Management Protocol) is enabled and, if so, whether this unit is a home agent, a foreign agent, or both.

**Usage:** Specify one of the following values:

- Disabled (the default) specifies that ATMP is not enabled.
- Home specifies that this unit is a home agent.
- Foreign specifies that this unit is a foreign agent.
- Both specifies that 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=Disabled, all other fields in the ATMP Options menu are 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, then all four attributes must be sent. As another example, if a session has a user name, session id and session key, then 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 on RADIUS, see the *MAX RADIUS Configuration Guide*. See the *MAX Security Supplement* for details on other authentication servers.

**Usage:** Specify one of the following values:

- None (the default) to 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 and CHAP, and terminal server validation.
- RADIUS/LOGOUT  
This setting is 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 parameters of the TServ Options submenu for the Ethernet profile. There currently is no way to get user-specific configuration information from the SecurID ACE server, except by using RADIUS.

**Example:** Auth=RADIUS (for authentication using RADIUS), Auth=RADIUS/LOGOUT (for authentication using RADIUS and a SecurID server).

**Dependencies:** This parameter requires a server address in an Auth Host # parameter.

**Location:** Ethernet > Mod Config > Auth

**See Also:** Auth Host, Auth Key, Auth Port, Auth Timeout, Encaps

### Auth Boot Host #1

**Description:** Specifies the IP address of the first RADIUS bootup server the MAX contacts, at startup, to obtain ZGR subaddresses or answer numbers.

**Usage:** Specify an IP address in dotted decimal notation. The default value is 0.0.0.0. If you accept the default, the MAX does not use a RADIUS server for ZGR subaddresses or answer numbers.

**Dependencies:** You can use the ZGR subaddress and answer number feature without specifying a special bootup server. If you do not specify a special bootup server, the MAX uses the authentication server specified by Auth Host in the Ethernet > Mod Config menu to store the ZGR subaddresses and answer numbers.

If you set the Auth Boot Host #1 parameter, you must also specify a value for the Auth Key and Auth Src Port parameters in the Ethernet > Mod Config > Auth menu.

**Location:** Ethernet > Mod Config > Auth

**See Also:** Auth Boot Host #2, Auth Boot Port

### Auth Boot Host #2

**Description:** Specifies the IP address of the RADIUS server the MAX contacts if the server specified by Auth Boot Host #1 fails to respond.

**Usage:** Specify an IP address in dotted decimal notation. The default value is 0.0.0.0. If you accept the default, the MAX does not use a secondary RADIUS server for ZGR subaddresses or answer numbers.

**Dependencies:** You can use the ZGR subaddress and answer number feature without specifying a special bootup server. If you do not specify a special bootup server, the MAX uses the authentication server specified by Auth Host in the Ethernet > Mod Config menu to store the ZGR subaddresses and answer numbers.

If you set the Auth Boot Host #2 parameter, you must also specify a value for the Auth Key and Auth Src Port parameters in the Ethernet > Mod Config > Auth menu.

**Location:** Ethernet > Mod Config > Auth

**See Also:** Auth Boot Host #1, Auth Boot Port

## Auth Boot Port

**Description:** Specifies the port number to use when contacting the RADIUS server specified by Auth Boot Host #1 or Auth Boot Host #2.

**Usage:** Specify a value between 0 and 1024. The default value is 0 (zero), which disables the RADIUS bootup-server feature.

**Location:** Ethernet > Mod Config > Auth

Auth Boot Host #1, Auth Boot Host #2

## Auth Host #N (N=1–3)

**Description:** Each of these parameters specifies the IP address of an external authentication 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 connects to a server other than the server #1, it 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 in 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; this setting 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, which is typically a shared secret with the authentication server.

- For RADIUS, this is a string up to 22 characters. Because the MAX can act both as a client to external servers and as an on-board server responding to client commands, this parameter is configured in two places for RADIUS.
- If the MAX is acting as a TACACS or TACACS+ client, this is a password supplied by the MAX to the server.
- If the MAX is acting as a Defender client, this is a DES secret key shared between the MAX and the Defender authentication server. This key is also used for authentication by the MAX in its role as a Defender authentication agent.

- If the MAX is acting as a SecurID client, this parameter is not applicable. See SecurID DES Encryption and SecurID Node Secret for details.

**Usage:** Specify the authentication key.

**Example:** Auth Key=Ascend

**Dependencies:** This value of this parameter depends on the setting of the Auth parameter. If Auth is set to SECURID, this parameter is not applicable.

**Location:** Ethernet > Mod Config > Auth

**See Also:** Auth, Auth Host, Auth Port, Auth Timeout, SecurID DES Encryption, SecurID Node Secret

## 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. 0 is the default.

0 directs the MAX to send three requests to each configured external authentication server. You configure the time that the MAX waits before sending each retry in Auth Timeout.

**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 Ascend daemon. See the MAX *RADIUS Configuration Guide* for details.

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

- Yes means 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. It must match the port specified for use in the server's configuration.

- If the MAX is acting as a RADIUS client, this is 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, it specifies the UDP destination port to use for authentication (49 by default).
- If the MAX is acting as a RADIUS server, this is the UDP port to use for the on-board RADIUS server. (The on-board server is a mechanism that allows the MAX to respond to messages from the radius daemon, as described in the *MAX RADIUS Configuration Guide*.) It is set to 1700 by default.
- If the MAX is acting as a Defender client, this is 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 is 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 what is actually in use 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, Auth Key, Auth Timeout

## Auth Req

**Description:** Specifies how the MAX acts if an authentication request times out after a call has been CLID-authenticated. If set to Yes, calls that have passed CLID-authentication are dropped if the external authentication request times out. If set to No, CLID-authentication connections are allowed even if there is no response from the external server.

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

- Yes means the MAX drops a call if the authentication requests times out after the call has been CLID-authenticated.

- No means the MAX attempts external authentication, but if the request times out, it allows the session to be established based solely upon 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:** This parameter forces the MAX to try to return to the primary RADIUS authentication server; specifically, the server defined by the parameter Auth Host #1.

If a timeout occurs while the MAX was waiting for a reply to an authentication request to the primary RADIUS server; the MAX sends the authentication request to secondary RADIUS server defined by Auth Host #2 and if that fails, Auth Host #3. If either of the secondary servers acknowledges the request, the MAX continues to use that server instead of the primary. Auth Reset Timeout parameter sets the period of time the MAX uses the secondary RADIUS server. At the end of this period of time, the next authentication request the MAX sends to Auth Host #1.

**Usage:** Enter the 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.

**Dependencies:** This parameter will be N/A if Auth=None or Auth=TACACS+ in the this profile.

**Location:** Ethernet Profile: Ethernet > Mod Config > Auth

**See Also:** Auth Host #N

## Auth Send Attr 6,7

**Description:** Specifies whether the MAX sends values for RADIUS attributes 6 and 7. Typically, it 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, async PPP users that authenticate via 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 access to PPP and SLIP via the terminal server 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 a remote authentication requests. You can define 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 between 0 and 65535. The default value is 0 (zero); if you accept this value, the MAX can use any port number between 1024 and 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 Defender or SecurID client (which support only 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 set to No, the MAX 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 still high enough to permit the unit 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=20

**Dependencies:** This parameter applies only when using an external authentication server.

**Location:** Ethernet > Mod Config > Auth

**See Also:** Auth, Auth Host, Auth Key, Auth Port, SecurID Host Retires.

## Auth TS Secure

**Description:** Specifies whether remote dialin 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 means 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 means 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. It is used by OSPF routers to allow or exclude packets from an area. The default value for OSPF is *ascend0*.

**Usage:** Specify a string up to 9 characters for an OSPF auth-key.

**Example:** AuthKey=Ascend

**Dependencies:** This parameter is not used if AuthType is None.

**Location:** Ethernet > Connections > OSPF Options, Ethernet > Mod Config > OSPF Options

**See Also:** AuthType

## AuthType

**Description:** Specifies the type of authentication in use for validating OSPF packet exchanges: Simple (the default) or None. Simple authentication is designed to prevent configuration errors from affecting the OSPF routing database. It is not designed for firewall protection.

**Usage:** Specify one of the following values:

- None  
Routing exchanges are not authenticated. The 64-bit authentication field in the OSPF header may 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 field in 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.



**Example:** AuthType=Simple

**Location:** Ethernet > Connections > OSPF Options, Ethernet > Mod Config > OSPF Options

**See Also:** AuthKey

## Auto-BERT

**Description:** Specifies that an automatic byte-error 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 monitors the entire data stream between codecs. At the end of the time period, if any channels have failed, the MAX clears the bad channels, 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. These 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 reports the total number of errors for each channel during the current call, not the error rate.

The MAX resets the error display for the current call to 0 (zero) when the call disconnects, or if the MAX disconnects a channel during the Auto-BERT or during the call itself. You can abort the Auto-BERT at any time by choosing the command DO 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/6) > PortN Menu > Directory

## Auto-Call X.121 Addr

**Description:** Specifies the X.25 host to call immediately when an X.25/PAD session is established via 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, where the user can issue the “pad” command to begin a session.

**Usage:** Specify the information needed to call the X.25, up to 48 characters. Use this format:

<address> [ \*P | \*D | \*F <data> ] ]

- <address> is the X.121 address to which the call is made (up to 15 characters).

- \*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 > Encaps Options

**See Also:** Immed Service

## Auto Logout

**Description:** Specifies whether the MAX automatically logs a user out when a device disconnects from the MAX unit's control port or when the MAX loses power.

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

- Yes causes the MAX to log out the current user and go back to default privileges when a device disconnects from the MAX unit's control port or when the MAX loses power.
- No disables auto-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 NAS (network authentication server).

**Example:** Aux Send PW=Ascend

**Dependencies:** This parameter applies only to multichannel PPP calls.

**Location:** Ethernet > Connections > 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. The B&O Restore parameter specifies how long the MAX waits before reinstating the channels.

**Usage:** Specify the number of seconds you want the MAX to wait before restoring a nailed-up channel. You can enter a number between 30 and 30000. The default is 300.

**Example:** B&O Restore=50

**Location:** Host/Dual (Host/6) > Port/N Menu > Directory

**See Also:** Call Mgm, Call Type

### BN Prt/Grp (N=1–2)

**Description:** BN Prt/Grp has two meanings, 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 profiles 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 specify the slot number using B N Slot.

**Example:** B1 Prt/Grp=5

**Location:** Net/BRI > Line Config > Line *N*, *BRI/LT* > Line Config > Line *N*

**See Also:** BN Slot, Group

### BN Slot (N=1–2)

**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. 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). Zero means 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.

## MAX Alphabetic Parameter Reference

### *BN Trnk Grp(N=1–2)*

---

- 3 through 8 represent 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 represents 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:** BN Prt/Grp

### **BN Trnk Grp(N=1–2)**

**Description:** Assigns a B channel to a trunk group, making it available for outbound calls. Note that you cannot specify the same trunk group number for channels that belong to a BRI and PRI line.

**Usage:** Specify a number between 4 and 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 profile.

**Location:** Net/BRI > Line Config > Line *N*, *BRI/LT* > Line Config > Line *N*

**See Also:** B2 Trnk Grp, Ch *N* Trnk Grp, Dial #

### **BN Usage(N=1–2)**

**Description:** Specifies the B channel's usage.

**Usage:** Specify one of the following values:

- Switched (the default) specifies that the channel supports switched connectivity.
- Nailed specifies that the channel is used for a leased connection.
- Unused specifies that 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 whose signaling mode is DPNSS.

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

**See Also:** Sig Mode

## Backup

**Description:** Specifies the number of a backup Connection profile for a nailed connection. It is intended as a backup if the far-end device goes out of service, in which case the backup call is made. It is not intended to provide alternative lines for getting to a single destination.

**Note:** A Connection profile's number is the unique portion of the number preceding the profile's name in the Connections menu.

**Usage:** Specify the Connection profile number. The default value is null.

**Example:** Backup=22

**Location:** Ethernet > Connections > Session Options

**See Also:** Name

## BACP

**Description:** Enables or disables the Bandwidth Allocation Control Protocol (BACP). If 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 > 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 number of channels to use to set up a session initially. If it is 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 may 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 amount you specify cannot exceed the maximum channel count set 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/6) > PortN Menu > Directory, Ethernet > Connections > Encaps Options

**See Also:** Call Mgm, Data Svc, Max Ch Count, Parallel Dialing

## Beg Time

**Description:** Specifies the start-time of a dynamic AIM call's time period. You do not need to specify an ending time; the starting time specified by the Beg Time parameter of the next time period is the implicit ending time.

**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/6) > PortN 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 phone number it dials for the call.

For PRI lines, the MAX uses the billing-number parameter rather than the phone number ID to identify itself to the answering party.

If the calling party uses the billing-number parameter instead of its phone number as its ID, the CLID used by the answering side is not the true phone 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 billing-number parameter, there is no guarantee that the phone 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 and 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/6) > Port/N Menu > Directory, Ethernet > Connections > 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 and answering unit.

**Location:** Host/Dual (Host/6) > Port/N Menu > Directory

## Block calls after

**Description:** Specifies how many unsuccessful attempts the Ascend unit will make before beginning to block outgoing calls.

**Usage:** Enter the number of connection attempts permitted before the Ascend unit blocks calls for the connection. The maximum number you can enter is 65535 (65535 attempts). The default is 0.

**Location:** Session Options submenu of the Connection Profile.

**See Also:** Blocked duration

## Blocked duration

**Description:** Specifies the length of time in seconds during which the Ascend unit will block outgoing calls.

**Usage:** Enter the number of seconds for the Ascend unit to block all calls made to the connection. When this period has elapsed, the unit will again allow calls to this connection.

**Location:** Session Options submenu of the Connection Profile.

**See Also:** Block calls after

**See Also:**

## BOOTP Relay Enable

**Description:** Specifies whether Bootstrap Protocol (BOOTP) requests are relayed to other networks. If you enable BOOTP relay, you must also specify the address of at least one BOOTP server in the Server parameter.

**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

## 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 based on 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 profile. If you have a MAX running Multiband Simulation, Bridge is disabled.

**Location:** Ethernet > Answer > PPP Options, Ethernet > Connections

**See Also:** Bridging, Encaps, Route IP, Route IPX

## Bridging

**Description:** Enables or disables packet-bridging system-wide. It causes the MAX unit's Ethernet controller to run 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 based on 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 msec 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 T1 lines with an internal CSU (Channel Service Unit). The buildout value is the amount of attenuation the MAX should apply to the line's network interface in order to match the cable length from the MAX to the next repeater.

Attenuation is a measure of the power lost on a transmission line or on a portion of that line. When you specify a build-out value, the MAX applies an attenuator to the T1 line, causing the line to lose power when the received signal is too strong. Repeaters boost the signal on a T1 line. If the MAX is too close to a repeater, you need to add some attenuation.

**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 calls back the device at the remote end of the link using the Dial # specified in the Connection profile.

You can use the Callback parameter 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 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 both answer the call and call 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 > Telco Options

**See Also:** AnsOrig, Call Type, Dial #, Calling #

## Call-by-Call

**Description:** In a T1 Line profile, specifies the call-by-call signaling value to set for routing calls from a local device through the MAX to the network. When it is set in another profile, it specifies the PRI service to use when placing a call using that profile.

**Note:** The Call-by-Call setting in the Dial Plan profile overrides the Call-by-Call setting in the Call profile and the Connection profile.

These are the call-by-call services available if the service provider is AT&T:

- 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)

These are the VPN and GVPN call-by-call services available if the service provider is Sprint:

- 0 (Reserved)
- 1 (Private)
- 2 (Inwatts)
- 3 (Outwatts)
- 4 (FX)
- 5 (Tie Trunk)

These are the call-by-call services available if the service provider is MCI:

- 1 (VNET/Vision)
- 2 (800)
- 3 (PRISM1, PRISM II, WATS)
- 4 (900)
- 5 (DAL)

**Usage:** Specify a number between 0 and 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 > Telco Options, System > Dial Plan, Ethernet > Frame Relay, Net/T1 > Line Config > Line *N*, Ethernet > X.25

**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 placing a call using the associated Dial #. 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 the Call profile or Connection profile.

These are the call-by-call services available if the service provider is AT&T:

- 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)

These are the VPN and GVPN call-by-call services available if the service provider is Sprint:

- 0 (Reserved)
- 1 (Private)
- 2 (Inwatts)
- 3 (Outwatts)
- 4 (FX)
- 5 (Tie Trunk)

These are the call-by-call services available if the service provider is MCI:

- 1 (VNET/Vision)
- 2 (800)
- 3 (PRISM1, PRISM II, WATS)
- 4 (900)
- 5 (DAL)

**Usage:** Specify a number between 0 and 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 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 between 0 and 199. The number you enter depends on whether you are applying a filter you created using the vt100 interface, or a firewall you created using Secure Access Manager (SAM).

If you are applying a filter created using 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 SAM, 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. Refer to your SAM documentation for information on downloading firewalls to the MAX. 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 using the vt100 interface is being used
- 100-199 indicates that a filter created using SAM is being used.

**Example:** Call Filter=7

**Location:** Ethernet > Answer > Session Options, Ethernet > Connections > 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 means 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 address, the call is accepted.
- Outgoing means 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 means the MAX accepts both incoming and outgoing call requests if the CUD indicates encapsulation that are supported. The called address must match the Answer X.121 address. If no virtual circuit is established and IP packets show up, 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 in the Answer X.121 or Remote X.121 address parameters.

**Location:** Ethernet > Connections > 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:

- AIM, FT1-B&O, and FT1-AIM calls  
For these types of calls, call management consists of remote management, online error monitoring, remote loopbacks, and online bandwidth control between codecs.
- BONDING calls  
For this type of call, 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, enabling the MAX to place a call to itself over the WAN and to send a user-specified number of packets over the connection. The data loops at the AIM port interface of the remote MAX, and comes back to the local MAX. The loopback tests the MAX unit's ability to initiate and receive calls, and diagnoses whether the connection over the digital access line and the WAN is sound.

For the call management features available by command, see Chapter 1, "DO Command Reference."

**Usage:** Specify one of the following values:

- Manual (the default)  
This setting 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 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  
This setting differs from Manual in that (a) you cannot add or subtract bandwidth while the call is online, and (b) 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 get a clock synchronized to 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 56k access	Network bandwidth (in kbps) for 64k access
1536	24	1568	1600
1344	21	1400	1408
1024	16	1064	1088
768	12	784	832

<b>Host bandwidth (in kbps)</b>	<b>Base Ch Count</b>	<b>Network bandwidth (in kbps) for 56k access</b>	<b>Network bandwidth (in kbps) for 64k access</b>
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**

This setting uses dynamic bandwidth allocation algorithms to automatically add or removes 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 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 specify 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 gets 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 of 5 and the Switched-56 data service, the host device receives 280 kbps (5x56kbps).

- **Mode 0** is required when the remote device (a) uses the BONDING inverse-multiplexing protocol and (b) 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 phone number of the primary host port associated with the remote codec. The remote BONDING device must have the secondary host port’s phone 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 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; choose it 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/6 cards.

**Location:** Host/Dual (Host/6) > PortN 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 Port 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 may 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/6) > Port N Menu > Directory

**See Also:** Port Password

## Call Type

**Description:** Specifies a type of connection, or in the case of codecs, the architecture of the connection. These two different usages for this parameter are specified in two Usage sections below.

**Usage:** To specify the type of connection in a Frame Relay, Connection, or X.25 profile, specify one of these values:

- Nailed (a link that consists of nailed-up channels)



This is the default for Frame Relay and X.25 profiles. You must specify which nailed channels to use in the Group or Nailed Grp parameter.

- Switched (a link that consists of switched channels)

This is the default in a Connection profile.

- Nailed/MPP (nailed channels that may be augmented with switched channels if bandwidth is needed during an MP+ call)

A Nailed/MPP 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/MPP 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/MPP connection is either the Max Ch Count 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 permanent switched connection attempts to restore the link at 10-second intervals, which is similar to the way a nailed connection is maintained. A permanent switch connection conserves connection attempts but causes a long connection time, which may be cost effective for some customers. For the answering device at the remote end of the permanent switched connection, we recommend 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.

**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 TA (Terminal Adapter) or a DSU (Data Service Unit) 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**

This setting provides automatic backup and overflow protection of nailed-up circuits. For this setting to appear in the menu of a Host/6 module, the current host port must be the primary port of a dual-port pair.

- In providing backup bandwidth, the MAX 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 MAX 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. You must specify Call Mgm=Dynamic in order for the MAX 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**

This setting 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 (such as callback) inapplicable, and a call type of Switched makes parameters related to nailed connections (such as 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, 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, X.25 Max Pkt Size

**Location:** Host/Dual (Host/6) > PortN Menu > Directory, Ethernet > Connections > 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

## 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 DNIS (Dial Number Information Service) is in use. In some cases, the phone company may 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. See the *MAX Security Supplement* for details.

**Usage:** Specify the number to be used for Called Number authentication.

**Example:** Called #=5551234

**Location:** Ethernet > Connections, Ethernet > Answer

**See Also:** Id Auth

## Calling #

**Description:** Specifies the calling number (the far-end device's number). Many carriers include the calling number (the far-end device's number) in each call. Calling # is the caller ID number displayed on some phones and used by the MAX for CLID (Calling Line ID) authentication.

CLID authentication enables you to prevent the MAX from answering a connection unless it originates at the specified phone number. The number you specify in this parameter may also be used for callback security if you configure callback in the per-connection telco options.

Calling # is also used for callback security with CLID. See Callback.

**Usage:** Specify the called number to be used for authentication purposes.

**Example:** Calling #=555-6787

**Location:** Ethernet > Connections, Ethernet > Answer

**See Also:** Id Auth, Callback

## CBCP Enable

**Description:** Specifies how the MAX responds to caller requests to support CBCP.

**Usage:** Press Enter to cycle through the choices.

- Yes specifies the MAX will positively acknowledge, during LCP negotiations, support for CBCP.
- No specifies the MAX will reject any request to support CBCP.  
No is the default.

**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 the MAX will use the number in Ethernet > Connections > Any 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=PPP or MPP or MP.

**Location:** Ethernet > Connections > Any 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 phone number the MAX uses for the callback. The value in 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:** CBCP Trunk Group applies only if CBCP is negotiated for a connection. Encaps=PPP or MPP or MP.

**Location:** Ethernet > Connections > Any Connection Profile > Encaps Options

**See Also:** CBCP Enable, CBCP Mode

## 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 parameter that selects whether the modem negotiates land-based or cellular first, and Y is the modem gain used for cellular communication. For example, if Cell First=No and Cell Level=18 is set in the TServ options menu, the command would be:

`-sec=0,18`

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

- Yes means a cellular connection is attempted first, followed by a land-based connection.
- No means 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 may be different from the usage specified for the line itself. For example, the line may specify switched usage while individual channels within that line specify nailed.

**Usage:** Specify one of the following values for T1 channels:

- Switched (the default). A switched channel supports switched connections. It may be robbed-bit or a B channel, depending on the line's signal mode.
- Nailed (a clear-channel 64k circuit).
- D channel (the channel used for ISDN D channel signaling). This is assigned automatically to channel number 24 on T1 lines when ISDN signaling is in use.
- Unused (unavailable for use).
- D&I (drop-and-insert), the channel drops through to the second T1 line, which typically supports a PBX.
- NFAS-Prime (the primary D channel for two NFAS lines).
- NFAS-Second (the secondary D channel for two NFAS lines). This channel 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). A switched channel supports switched connections. It may be robbed-bit or a B channel, depending on the line's signal mode.
- Nailed (a clear-channel 64k circuit).
- D channel (the channel used for ISDN D channel signaling). This is 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:** You build multichannel calls (MP, MP+, AIM, BONDING) by specifying add-on numbers. A multichannel call begins as a single-channel connection to one phone number. The calling unit then requests additional phone numbers it can dial to connect those channels, and stores the add-on numbers it receives from the answering unit. The calling unit must integrate the add-on numbers with the phone number it dialed initially to add channels to the call. Three parameters specify add-on numbers: Ch N #, PRI Num and Sec Num.

**Note:** Do not enter phone numbers of the MAX you are calling in the Line Profile. The numbers you are calling belong in the Call and Connection profiles.

Typically, the phone numbers assigned to the channels share a group of leading (leftmost) digits. Enter only the rightmost digits identifying each phone number, excluding the digit(s) that are in common, as in the following example:

- If the add-on number in the called unit is shorter than the phone number dialed by the calling unit, only the rightmost digits are replaced.
  - For example, suppose you dial 777-3330 to reach channel 1 of line 1 and 777-3331, 777-3332, through 777-3348, reaches other channels and other lines. In this case, set Ch1#=30 and the other channels and lines 31, 32, and so forth.
- If the add-on number is longer than the phone number dialed, the extra digits are discarded. 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.
  - 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. The group of channels that make a multichannel call is called a bundle. A 10-channel bundle in which each channel is 64kbps, provides a 640 kbps connection.

**Note:** 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, you have two PRI lines from different service providers. You set the ChN Trnk Grp parameters for the first line to 9 and for the second line to 8. Also, enabling trunk groups on your MAX separates the two dial plans, and prevents the formation of bundles with channels from both PRI lines.

The phone numbers that you specify are the ones used to call this unit. There is a one-to-one correspondence between a phone number and a channel, except when you are using GloBanD lines. (When the switch type is GloBanD, the MAX pools the phone numbers and can apply them to any channel of the PRI line.)

**Usage:** Specify a phone number with a limit of 24 characters, which can include the following characters: 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:** Sub-Adr

**Ch N Prt/Grp (N=1–24, 1–32)**

**Description:** Ch N Prt/Grp has two meanings, 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 Call or Connection profiles 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 specify the slot number using Ch N Slot.

**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). Zero means 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 through 8 represent 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 represents the LAN. Calls are routed to the bridge/router module.

**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 phone number.

**Usage:** Specify a number between 4 and 9 for each trunk group. The default is 9.

**Dependencies:** This parameter applies only when trunk groups have been enabled in the System 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 endpoint. When combined as a circuit, the two DLCI endpoints act as a tunnel—data received on one DLCI bypasses the Ascend 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 for the circuit, up to 16 characters. The other end-point of the PVC must specify the same name in its Circuit configuration.

**Example:** Circuit=circuit-1

**Dependencies:** This parameter applies only to FR\_CIR-encapsulated calls.

**Location:** Ethernet > Connections > Encaps options

**See Also:** Encaps

## Clear

**Description:** Specifies whether the control-line state determines when the MAX clears a call.

**Usage:** Specify one of the following values:

- Terminal (clear the call manually by using DO 2). This 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/6) > PortN 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 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 means the MAX clears the call when a Telnet, Rlogin, or TCP session terminates.
- No means 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

## Client

**Description:** Enables the MAX to respond to multicast clients on the local Ethernet. Clients cannot be support on the MBONE interface, so this means that the multicast router resides across a WAN link.

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

- Yes means the MAX 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 means the MAX does not handle IGMP client requests and responses on the interface.

**Example:** Client=Yes

**Dependencies:** This parameter is not applicable if Multicast Forwarding is disabled or if the local Ethernet is the MBONE interface (supporting a multicast router).

**Location:** Ethernet > Mod Config > Multicast

**See Also:** Multicast 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 enables RADIUS requests from any hosts on the 125.65.5 subnet.
- Client #2= 125.5.0.0/16  
This enables RADIUS requests from any hosts on the 125.5 subnet.
- Client #3= 135.50.248.76/32

This enables requests from the host whose address is 138.50.248.76.

**Note:** If no mask bits are supplied, the software supplies a default netmask 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, MAX *RADIUS Configuration Guide*

## 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 > IP Options

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

## 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 Ascend 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 > 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 > 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 > IP Options

## Clock Source

**Description:** Specifies whether the T1 or E1 line may be used as the clock source for timing synchronous transmissions. If it is enabled, 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, selecting 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 means the line may be used as the clock source for timing synchronous transmissions.
- No means the line may not be used as the clock source. When this setting is disabled, the MAX uses another line for timing or uses its internal clock. This 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*

## 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 means the MAX clears the screen when a terminal server session begins.
- No means 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

## 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 means the MAX will answer inbound Combinet calls, provided that they meet all other connection criteria.
- No means 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 profile.

**Location:** Ethernet > Answer > Encaps

**See Also:** Bridge, Bridging, Encaps

## Comm

**Description:** Specifies the SNMP community name associated with the SNMP PDU (Protocol Data Units). 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

## 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 means the filter matches the packet when the specified value and the packet contents are equal. This is a default.
- NotEquals means the filter matches the packet when the specified value and the packet contents are equal.

**Dependencies:** This parameter does not apply if the filter is not Valid 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

## Compression

**Description:** Enables or disables data compression on or off 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 an Ascend 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 > Encaps Options

**See Also:** Link Comp

## Connection #

**Description:** Specifies the number of a Connection profile needed to bring up a bridged or routed connection. The MAX 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 it receives a packet whose destination MAC address is not on the local Ethernet, it looks in the bridging table for a matching MAC address and uses the specified Connection profile to bring up a bridged connection.

If it 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 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 port labeled Control on the back panel of the MAX.

**Usage:** Specify one of the following values:

- Standard means the standard set of edit menus comes up in the vt100 window at system startup. This is the default.
- MIF means MIF (Machine Interface Format) is accessible at system startup. From the MIF interface you can display the edit menus by pressing Ctrl-C, and return to MIF again by using the Use MIF command.
- Limited means a set of simplified menus comes up, 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

## 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 non-zero. A link with a cost of 0xFFFFFFFF (16777215) is considered non-operational.

In a static 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 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 > OSPF Options, Ethernet > Mod Config > OSPF Options

## 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 > *any 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 between 0 and 199. The number you enter depends on whether you are applying a filter you created using the vt100 interface, or a firewall you created using Secure Access Manager (SAM).

If you are applying a filter created using 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 SAM, 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. Refer to your SAM documentation for information on downloading firewalls to the MAX. 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 using the vt100 interface is being used
- 100-199 indicates that a filter created using SAM 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 > Session Options

**See Also:** Call Filter, Filter



## Data Format

**Description:** Specifies the data format and parity checking/generation behavior of the PAD when it validates opening frames as well as during Local mode data transfer.

**Usage:** Specify one of the following values:

- 7-E-1 (the default)  
Specifies that the PAD uses 7 data bits, even parity, and 1 stop bit during opening frame validation and local mode data transfer.
- 7-O-1  
Specifies that the PAD uses 7 data bits, odd parity, and 1 stop bit during opening frame validation and local mode data transfer.
- 7-M-1  
Specifies that the PAD uses 7 data bits, mark parity, and 1 stop bit during opening frame validation and local mode data transfer.
- 7-S-1  
Specifies that the PAD uses 7 data bits, space parity, and 1 stop bit during opening frame validation and local mode data transfer.
- 8-N-1  
Specifies that the PAD uses 8 data bits, no parity, and 1 stop bit during opening frame validation and local mode data transfer.

**Dependencies:** This parameter is always applicable.

**Location:** Ethernet > Connections > *any 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, 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 (digital voice call)**

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 may become unusable unless you meet these technical requirements:

- Use only digital end-to-end connectivity; no analog signals should be present anywhere in the link.
- Make sure that the phone 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 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 (digital modem call)**

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 (V.110 terminal adapter call)**

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 may be one of the following:

- 2.4
- 4.8
- 9.6
- 19.2
- 38.4

The data-service may be one of the following:

- 56K (switched-56)
- 56KR (restricted switched-56)
- 64K (switched-64)

If the MAX cannot sync up with the remote terminal adapter using the specified bit rate, it attempts to use one of the other four bit rates.

- **Inherit (use the data service requested by the local calling device)**

This setting is available only in Dial Plan profiles. The call connects with the data service as requested by the caller on the local Host/BRI line. 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 (switched-384)**

This setting is available only in Call profiles. It means that the call contains any type of data and connects to the Switched-384 data service. This AT&T data service does not require MultiRate or GloBanD. A Host/6 expansion module supports a maximum of four 384K/H0 calls.

- 384KR (restricted switched-384)  
This setting is available only in Call profiles. It means that the call contains restricted data and connects to MultiRate or GloBanD data services at 384 kbps.
- 1536K (switched-1536)  
This setting is available only in Call profiles. It means that the call contains any type of data and connects to the Switched-1536 data service at 1536 kbps. This setting is valid only for lines using NFAS signaling.
- 1536KR (restricted switched-1536)  
This setting is available only in Call profiles. It means that 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.
- 128K, 192K, 256K, and other multiples of 64K (multi-rate)  
This setting is available only in Call profiles. These values are available on a PRI line with MultiRate or GloBanD data services. If the MAX has the MultiRate option, these data services appear.

**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 indicates how much bandwidth the MAX routes to the host for each channel in the connection. When Call Type=FT1-B&O or Call Type=FT1-AIM, the Data Svc parameter refers to the switched channels.

**Location:** Host/Dual (Host/6) > Port/N Menu > Directory, Ethernet > Connections > 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  
This setting specifies that the MAX adds or subtracts bandwidth based on the amount of data it transmits.  
Transmit is the default.
- Transmit-Recv

This setting specifies that the MAX adds or subtracts bandwidth based on the amount of data it transmits *and* receives.

- None

This setting specifies that the MAX does not monitor traffic over the link.

**Dependencies:** DBA Monitor is only supported on MP+ calls.

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

**See Also:** DTE Addr, Encaps

## DCE N392

**Description:** Specifies the number of errors during DCE N393 monitored events which causes the network side to declare the user side procedures inactive.

**Usage:** Specify a value between 1 and 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 (between 1 and 10).

**Usage:** Specify a value between 1 and 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. In the Ethernet profile, the default is 40 seconds.

**Example:** DeadInterval=240

**Location:** Ethernet > Connections > 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 between 1 and 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 Call Mgm parameter is set to Manual, Dynamic, or Mode 2.

**Location:** Host/Dual (Host/6) > Port/N Menu > Directory, Ethernet > Connections > 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 an Ascend 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 Ascend 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 submenu

**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 typed 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 ten-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 phone number dialed by the device connected to line #2. Typically, a PBX (Private Branch Exchange) is

connected to line #2. A PBX is an internal telephone network in which one incoming number directs calls to various extensions and from one office to another.

Use this parameter when the PBX used to be connected to a switch that supplied a T1 line, 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 phone 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 Route profile, Dest specifies the route's target IP address. This is the destination address that will cause the MAX to bring up this route. In a Route 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

## 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. These 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) specifies that the MAX dials calls only when the user enters the DO 1 or Ctrl-D-1 (DO Dial) command.
- DTR Active specifies that 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 DTR (Data Transmit Ready). 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 on, DTR is asserted.

- RS-366 ext1 specifies that 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 specifies that 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 Ascend Communications, Inc.  
The port must support AIM functionality for this setting to have any effect. V.25bis does not appear if you have paired the port with another one using the Dual Ports parameter in the Host-Interface profile.
- V.25bis-C is identical to V.25bis, except that the CTS (Clear To Send) signal does not change its state during a call.
- X.21 ext1 specifies that 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/6) > PortN Menu > Port Config

**See Also:** RS-366 Esc

## **Dial #**

**Description:** Specifies the number used to dial out this connection. It can contain up to 24 characters, which may 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 phone numbers to total up to 49 characters. The two numbers must be separated by an exclamation mark, for example: 5551212!5551234

**Note:** The phone number may contain a subaddress or trunk-group number. If the use of trunk groups is enabled in the System profile, this parameter must specify a trunk group as the first digit.



**Usage:** Specify a phone number up to 24 characters. The MAX sends only the numeric characters to place a call. You must limit the number to these 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/6) > PortN Menu > Directory, Ethernet > Connections, Ethernet > Frame Relay, Ethernet > X.25

**See Also:** B1 Trnk Grp, B2 Trnk Grp, Call Type, Ch N Trnk Grp, Dial Plan, Encaps, Sub-Adr, Use Trunk Grps

## Dial N# (N=1–6)

**Description:** Specifies the phone numbers that reach the destination of the profile.

**Usage:** Specify a phone 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 containing up to 49 characters, or two phone numbers containing up to 24 characters each. The two phone numbers must be separated by an exclamation point, as in this specification:

5551212!5551234

The first digit of Dial N# must match a trunk group defined by Ch N Trnk Grp parameter in a Line profile. For example, suppose 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 specifies Trunk Grp, the digits following the first digit constitute an ordinary phone number. If the Dial Plan is Extended, the two digits that point to a Dial Plan profile come next, followed by an ordinary phone number.

**Dependencies:** This parameter is inapplicable unless trunk groups are enabled in the System profile.

**Location:** System > Destinations

**See Also:** B1 Trnk Grp, B2 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 dial-on-broadcast; 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 means 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

**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 the WAN using 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 specifies that the MAX uses the extended dial plan.  
When Dial Plan is Extended and the use of trunk groups is enabled in the System profile, the first digit of the 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 specifies that the digits following the first digit constitute an ordinary phone 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 service 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/6) > PortN Menu > Port Config, BRI/LT > Line Config > Line N

**See Also:** B1 Trnk Grp, B2 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 > 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 indicates that the Connection profile allows modem dialout.
- No indicates 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 > Telco Options

**See Also:** Imm. Modem Access

## Direct Call Addr

**Description:** For DTE-initiated calls, this 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:** This parameter is always applicable.

**Location:** Ethernet > Connections > *any Connection profile* > Encaps options  
Ethernet > Answer > T3POS options

## Disc on Auth Timeout

**Description:** Specifies whether the MAX gracefully shuts down the PPP connection on an external authentication server timeout.

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

- Yes causes the MAX to hang up a PPP connection when an external authentication server times out.
- No causes it 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 may 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 between 16 and 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 > 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 DM, but no digital modem is available, the MAX clears the 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:** Ans *N*#, Sub-Adr

## **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 download the configuration of the MAX using the Save Cfg parameter. 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 means the operator can 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 permission is disabled.

**Location:** System > Security

**See Also:** Chapter 1, “MAX Diag Command Reference.”

## DownMetric

**Description:** This parameter 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:** This parameter 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

Route type	Default value
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 System profile, the accumulated minutes apply to all ports on the MAX and to the Ethernet module. In a Port profile, the accumulated minutes apply only to the associated AIM port.

**Usage:** Specify one of the following values:

- Daily specifies that the MAX resets the accumulated DS0 minutes to 0 (zero) every day at 12 A.M.
- Monthly specifies that the MAX resets the accumulated DS0 minutes to 0 (zero) on the first day of every month at 12 A.M.
- Off (the default) specifies that the MAX disables the Max DS0 Mins parameter in the System profile or Port profile.

**Location:** System > Sys Config, Host/Dual (Host/6) > PortN 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 specified 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 Mask

**Description:** Specifies a mask to apply to the Dst Adrs before comparing it to the destination 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 destination addresses are matched. A mask of all ones (255.255.255.255) masks no bits, so the full destination address to a single host is matched.

**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=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 a value to compare with the destination port number in a packet. The default setting (zero) indicates that the MAX disregards the destination 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 Dst Port Cmp parameter specifies the type of comparison to be made.

**Usage:** Specify the number of the destination port the MAX should use for comparison when filtering packets. You can enter a number between 0 and 65535. The default setting is 0 (zero), which means the MAX does not compare destination ports

**Example:** Dst 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 Cmp, Src Port Cmp, Src Port #

## 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 specifies that the MAX does not compare the packet's destination port to the value specified by Dst Port #.  
None is the default.
- Less specifies that port numbers with a value less than the value specified by Dst Port # match the filter.
- Eql specifies that port numbers equal to the value specified by Dst Port # match the filter.
- Gtr specifies that port numbers with a value greater than the value specified by Dst Port # match the filter.
- Neq specifies that 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 #

## 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 > Encaps Options

**See Also:** DCE Addr, Encaps

## DTE init. mode

**Description:** For DTE-initiated calls, this specifies the default data transfer mode. Note that the DTE can override this setting with a opening frame.

**Usage:** Specify one of the following values:

- Local (the default)  
Specifies that 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 supervisor frames to the T3POS DTE.
- Transparent  
Specifies that 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  
The 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**

Specifies that there is no error recovery between the T3POS PAD and the host but that there is error recovery 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:** This parameter is always applicable.

**Location:** Ethernet > Connections > *any Connection profile* > Encaps options  
Ethernet > Answer > T3POS options

## DTE N392

**Description:** Specifies the number of errors during DTE N393 monitored events which cause the user side to declare the network side procedures inactive.

**Usage:** Specify a value between 1 and 10 that is less than DTE N393.

**Example:** DTE N392=3

**Dependencies:** This parameter is N/A when FR Type is DCE.

**Location:** Ethernet > Frame Relay

## DTE N393

**Description:** Specifies the DTE monitored event count (between 1 and 10). It is N/A when FR Type is DCE.

**Usage:** Specify a value between 1 and 10 that is greater than DTE N392.

**Example:** DTE N393=5

**Dependencies:** This parameter is N/A 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 use the pair two AIM ports to provide double the bandwidth for the 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) specifies that no host ports are paired for dialing or receiving dual-port calls.
- 1&2 Dual specifies that host ports 1 and 2 are paired for dialing and receiving dual-port calls.

**Example:** Dual Port=No Dual

**Location:** Host/Dual (Host/6) > 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/6) > Port/N Menu > Directory, Ethernet > Connections > 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 CD (Carrier Detect) 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) specifies that the MAX raises CD after the completion of handshaking and an additional short delay.
- Answer specifies that the MAX raises CD (Carrier Detect) 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 specifies that the MAX raises CD as soon as the remote end answers a call, rather than waiting for the completion of handshaking.
- Both specifies that 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/6) > PortN Menu > Port Config

## 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, it 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.

- X is the slot number  
The system itself is assigned slot number 0 (00-000).  
The built-in T1 or E1 lines are slot 1 and slot 2 (10-000 and 20-000).  
The six expansion slots are slots 3 through 8 (30-000 through 80-000).  
The Ethernet is slot 9 (90-000).  
EtherData is slot A (A0-000), which is not applicable for units with built-in Ethernet.  
The serial WAN port is slot B (B0-000).
- 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 operator is restricted to editing only the Dial # and Base Ch Count parameters in the current Call profile. The operator may access the profiles via Telnet, by local management, or by remote management.

**Note:** To restrict editing entirely, you must also disable the Edit Cur Call permission.

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

- Yes means the operator can edit all parameters in Call and Connection profiles.
- No means the operator can edit only the Dial # and Base Ch Count parameters in the current Call profile.

**Dependencies:** This parameter does not apply if the Operations permission is disabled.

**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 profiles. When the permission is disabled, the operator is restricted to editing only the current Port profile. The operator may access the profiles via Telnet, by local management, or by remote management.

**Note:** To restrict editing Port profiles entirely, you must also disable the Edit Own Port permission.

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

- Yes means the operator can edit all Port profiles.
- No means the operator can edit only the current Port 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 an operator 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 operator may access the profiles via Telnet, by local management, or by remote management.

**Note:** To restrict editing common Call profiles entirely, you must also disable the Edit All Calls permission.

**Usage:** Specify Yes or No. Yes is the default if Edit All Calls is set to No.

- Yes means the operator 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 permission is set to Yes.

**Location:** System > Security

**See Also:** Edit All Calls

## Edit Cur Call

**Description:** Specifies whether an operator can edit all the parameters in the current Call profile. When the permission is disabled, the operator is restricted to editing only the Dial #

and Base Ch Count parameters in the current Call profile. The operator may access the profiles via Telnet, by local management, or by remote management.

**Note:** To restrict editing entirely, you must also disable the Edit All Calls permission.

**Usage:** Specify Yes or No. Yes is the default if Edit All Calls is set to No.

- Yes means the operator 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 permission is set to Yes.

**Location:** System > Security

**See Also:** Edit All Calls

## Edit Line

**Description:** Specifies whether an operator can edit Line profiles. The operator may access the profiles via Telnet, by local management, or by remote management.

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

- Yes means the operator can edit all Port profiles.
- No means the operator can edit only the current Port profile.

**Dependencies:** This parameter does not apply if the Operations permission is disabled.

**Location:** System > Security

## Edit Own Call

**Description:** Specifies whether an operator can edit the Call profile for the port that has been called. The operator may access the profiles via Telnet, by local management, or by remote management.

**Note:** To restrict editing entirely, you must also disable the Edit All Calls permission.

**Usage:** Specify Yes or No. Yes is the default if Edit All Calls is set to No.

- Yes means the operator 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 permission is disabled or the Edit All Calls permission is set to Yes.

**Location:** System > Security

**See Also:** Edit All Calls

## Edit Own Port

**Description:** Enables or disables permission to edit the Port profile for the port that has been called.

**Note:** To restrict editing 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 means the operator can edit the Port profile for the port that has been called.
- No disables this permission.

**Dependencies:** This parameter does not apply if the Operations permission is disabled or the Edit All Ports permission 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 is the most powerful security permission, because it gives the operator the ability to modify his or her own permissions.

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

- Yes means the operator can edit Security profiles.
- No means the operator cannot edit Security profiles.

**Dependencies:** This parameter does not apply if the Operations permission is disabled.

**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 profile.

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

- Yes means the operator can edit the System profile and SNMP community strings.
- No disables this permission.

**Dependencies:** This parameter does not apply if the Operations permission is disabled.

**Location:** System > Security

## 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 means 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 host name successfully. The local DNS table provides the list of IP addresses only if the host name for the attempted connection matches a host name in the local DNS table.

**Usage:** Select Enable Local DNS Table=Yes to enable the local DNS table. No disables the feature. No is the default.

**Location:** Ethernet Profile: 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 submenu displays a group of parameters relevant to your selection; you must set the appropriate Encaps Options parameters.

**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 Ascend extensions for dynamic bandwidth allocation. This applies only to multi-channel links between two Ascend 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

**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 > Encaps Options

**See Also:** Encaps

## Encoding

**Description:** Specifies the type of T1 PRI line encoding that the MAX uses. Your carrier can tell you which type of encoding you require.

**Usage:** Specify one of the following values:

- AMI (the default) specifies that the MAX uses Alternate Mark Inversion encoding.
- None is identical to AMI, but without density enforcement.
- B8ZS specifies that the encoding is Bipolar with 8-Zero Substitution. This is often required for ISDN lines.



**Example:** Encoding=AMI

**Dependencies:** This parameter applies only to T1 lines.

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

## Enet Adrs

**Description:** In a Bridge profile, specifies the physical Ethernet address (MAC address) of a device at the remote end of the link. The Bridge profile correlates a remote MAC address with a Connection profile number, enabling the MAX to bring up that Connection 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)  
Specifies that 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  
Specifies that 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 > *any Connection profile* > Encaps options  
Ethernet > Answer > T3POS options

## EOC Address

**Description:** Specifies the Embedded Operations Channel (EOC) address from which the MAX rollbacks the signal.

**Usage:** Specify one of the following values:

- 0 (the default) specifies the remote ISDN TA device
- 1-6 specifies the number of an ISDN repeater between the MAX and the remote TA. 1 specifies the repeater nearest the MAX.

- 7 specifies that 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 submenu.

**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 means the MAX accepts EU-RAW encapsulated calls, provided that they meet all other connection criteria.
- No means 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 means the MAX accepts EU-UI encapsulated calls, provided that they meet all other connection criteria.
- No means 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, it is routed to the first available V.110 module. If the service is data, it is routed to the first available AIM port; or if no AIM ports are available, it is routed to the MAX unit's bridge/router. To prevent this service-based routing and instead reject the call, turn Excl Routing on.

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

- Yes means the MAX drops calls for which it has no explicit call-routing information (such as Answer numbers, ISDN subaddressing, and so forth).
- No means 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.

**Example:** Excl Routing=No

**Location:** System > Sys Config

## Exp Callback

**Description:** Specifies whether the MAX expects outgoing calls to result in a call back from the far-end device. Use this parameter when the remote device requires callback security.

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

- Yes means the MAX expects the connection to terminate and result in a call-back from the far-end device. This prevents problems that arise when CLID is set to Required on the device that is expected to callback. 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 the call the same number again if Exp Callback is set to Yes.
- No means the MAX does not expect call-back for this connection.

**Example:** Exp Callback=No

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

**See Also:** Callback

## Ext. Clock \* 1K

**Description:** Defines the maximum bandwidth that the MAX uses for the nailed portion of a Nailed/MPP call. The MAX cannot determine the bandwidth for the serial WAN line if it does not generate clocking for its serial WAN line. The MAX must know the bandwidth of the nailed line for a nailed/MPP 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 MPP 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 specifies that the MAX clears the call entirely.
- Reduce (the default) specifies that 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.  
Reduce is the default.

- Retry specifies that 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/6) > Port/N Menu > Directory

## FDL

**Description:** Specifies the FDL (Facilities Data Link) 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 Ascend-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 means the operator 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 permission is disabled.

**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 it.

**Usage:** Specify a number between 0 and 199. The number you enter depends on whether you are applying a filter you created using the vt100 interface, or a firewall you created using Secure Access Manager (SAM).

If you are applying a filter created using 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 SAM, 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. Refer to your SAM documentation for information on downloading firewalls to the MAX. 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 using the vt100 interface is being used
- 100-199 indicates that a filter created using SAM 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 should persist after the call has been disconnected.

Before Secure Access 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 Secure Access firewalls. Filter Persistence is needed to allow firewalls to persist across connection state changes, but it is not needed for filters. If you do set it for a static packet filter, the filter persists across connection state changes. See the *MAX Security Supplement* for details.

**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 > 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 into 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

## Flag Idle

**Description:** Specifies whether a dynamic call to an AIM port looks for a flag pattern (01111110) or a mark pattern (11111111) as the idle indicator.

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

- Yes means the MAX uses a flag pattern (01111110) as the idle indicator on an AIM dynamic call.
- No means it uses a mark pattern (11111111) as the idle indicator on an AIM dynamic call.

**Example:** Flag Idle=Yes

**Location:** Host/Dual (Host/6) > PortN Menu > Directory

## Force56

**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 feature 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 feature is not required if you are receiving calls only from North America.

**Note:** The MAX uses the Force56 value in a Connection profile only if the call authenticates by means of CLID/DNIS. The MAX uses the Force56 value in the Answer profile if a call authenticates by means of name and password, or for unauthenticated calls.

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

- Yes means the MAX uses 56K of a channel that may provide up to 64K bandwidth.
- No means the MAX uses the full 64K bandwidth if it is available.

**Dependencies:** This parameter should not be enabled for calls within North America.

**Example:** Force56=No

**Location:** Host/Dual (Host/6) > PortN Menu > Directory, Ethernet > Connections > 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 means the MAX forwards packets that match the filter.
- No means 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 directs the MAX to respond to directed broadcast ICMP echo requests.  
Yes is the default.
- No directs the MAX not to 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

## 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 profile and initiates the forwarding function. If you modify a multicast value in the Ethernet 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 means the MAX accepts calls that use frame relay encapsulation, provided that they meet all other connection criteria.
- No means the MAX will not accept inbound calls using frame relay encapsulation.

**Location:** Ethernet > Answer > Encaps

**See Also:** Encaps, FR Prof, DLCI

## FR Direct

**Description:** Specifies whether the MAX redirects incoming packets to the frame relay switch without processing. A 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:** A 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 they must contain the PPP caller's IP address to be routed correctly back across the WAN.

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

- Yes means this connection is a FR Direct connection.
- No means this is not a FR Direct connection.

**Example:** FR Direct=No

**Dependencies:** This parameter is not applicable for FR or FR\_CIR encapsulated calls.

**Location:** Ethernet > Connections > Session Options

**See Also:** FR DLCI, FR Prof

## FR DLCI

**Description:** Specifies a frame relay DLCI number to be used for FR Direct connections. A 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.

**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 > 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 > Encaps Options, Ethernet > Connections > 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 DTE 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 between 30 to 260. The default is 256. For an X.75 TA, specify a number between 128 and 2048. The default value is 2048.

**Example:** Frame Length=256

**Location:** Ethernet > Answer > V.120 Options, Ethernet > Answer > X.75 Options

**See Also:** K Window Size, N2 Retransmission Count, T1 Retransmission 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)  
Specifies that terminal server users connecting through this profile have unlimited access to the terminal server commands.
- Yes  
Specifies that terminal server users connecting through this profile only have access to the PPP, SLIP, CSLIP, and Quit terminal server commands.

**Dependencies:** Keep this additional information in mind:

- Framed Only has no affect if TS Enabled is set to No in the Ethernet > Mod Config > TServ Options submenu.
- PPP, SLIP, and CSLIP must be enabled in the Ethernet > Mod Config > TServ Options submenu before users can start a PPP, SLIP, or CSLIP session.

**Location:** Ethernet > Answer > Session Options  
Ethernet > Connections > *any Connection profile* > Session Options

## Framed Addr Start

**Description:** This parameter specifies whether the Ascend unit 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 one of these settings:

- Yes indicates that the Ascend unit sends a second accounting Start record.
- No indicates that the Ascend unit does not send a second accounting Start record.  
No is the default.

**Location:** Ethernet profile: Ethernet > Mod Config > Auth

## Frames/Packet

**Description:** Specifies the number of 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 of from 1 to 10. 4 is the default.

**Dependencies:** Frames/Packet only applies if you set Ethernet > VOIP Options > Pkt Audio Mode to G.729.

**Location:** Ethernet > VOIP Options

**See Also:** Pkt Audio 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 D4 on the other.

**Usage:** Specify one of the following values for a Net/T1 line:

- D4 specifies the D4 format, also known as the Superframe format.  
This format consists of 12 consecutive frames, separated by framing bits. Do not use this setting with ISDN D-channel signaling; false framing and Yellow Alarm emulation can result.
- ESF specifies the Extended Superframe Format.  
This format 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) specifies the standard framing mode used by most E1 ISDN providers and by DASS 2.
- 2DS specifies 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*

## 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 means the MAX can initiate FT1-AIM, FT1-B&O, or Nailed/MPP calls using this profile.
- No means 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 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/6) > Port/N Menu > Directory, Ethernet > Connections > 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 (on Ethernet) 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 how to route 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

### 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 profile.

**Example:** Group=3

**Location:** Host/Dual (Host/6) > Port/N Menu > Directory, Ethernet > Connections > Telco Options

**See Also:** Call Type, Ch N Prt/Grp, Ch N

## GRP Leave Delay

**Description:** Specifies the amount 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 a `igmp query` to the WAN interface from which it received the `leave group` message. If the MAX does not receive a response from an active multicast client from the same group from the WAN interface, it sends a `leave group` message when the time you specified in 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 between 10 and 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:** GRP Leave Delay 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, we strongly recommend 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 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 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 > IPX Options

**See Also:** Dial Brdcast, NetWare t/o

## Handle IPX Type 20

**Description:** Specifies whether the MAX will propagate IPX type 20 packets over all its interfaces. Some applications (like NETBIOS) use IPX Type 20 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, like NetBIOS over IPX, require these 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 means these broadcasts are not propagated.

**Dependencies:** This parameter does not apply if the MAX does not support IPX routing.

**Location:** Ethernet > Mod Config > Ether options

## HeartBeat Addr

**Description:** Specifies a multicast address. The MAX listens for packets to and from this group to perform the heartbeat-monitoring feature. When it is running as a multicast forwarder, the MAX is continually receiving multicast traffic. The heartbeat-monitoring feature enables the administrator 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 multicast address to use for heartbeat monitoring.

**Example:** HeartBeat Addr=224.1.1.1

**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 Udp Port, Source Addr, Source Mask, HeartBeat Slot Time, HeartBeat Slot Count, Alarm Threshold

## HeartBeat Udp Port

**Description:** Specifies a UDP port number. The MAX listens only to packets received on that port to perform the heartbeat-monitoring feature. When it is running as a multicast forwarder, the MAX is continually receiving multicast traffic. The heartbeat-monitoring feature enables the administrator 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 UDP port to use for heartbeat monitoring.

**Example:** HeartBeat Udp Port=16387

**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, 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 Alarm Threshold. The MAX polls for multicast traffic the specified number of times, waits for the interval specified in the HeartBeat Slot Time parameter, and then polls again.

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

**Usage:** Specify a number of seconds.

**Example:** HeartBeat Slot Count=10

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

**Usage:** Specify a number of seconds.

**Example:** HeartBeat Slot Time=10

**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 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 profile, the default is 10 seconds.

**Example:** HelloInterval=60

**Location:** Ethernet > Connections > OSPF Options, Ethernet > Mod Config > OSPF Options

**See Also:** DeadInterval

## 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 them, 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

## 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 init. mode

**Description:** For host-initiated calls, this specifies the default data transfer mode. Note that the host can override this setting with a control frame.

**Usage:** Specify one of the following values:

- Local (the default)  
Specifies that 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 supervisor frames to the T3POS DTE.
- Transparent  
Specifies that 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  
The 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  
Specifies that there is no error recovery between the T3POS PAD and the host but that there is error recovery 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:** This parameter is always applicable.

## MAX Alphabetic Parameter Reference

### Host #N Addr (N=1–4)

---

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

### Host #N Addr (N=1–4)

**Description:** Specifies 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 to if they are not allowed to enter command mode. Note that you can specify a longer list of hosts using RADIUS.

To specify hosts to 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 establish raw TCP sessions instead of Telnet or Rlogin, configure Host #N Addr using the following format:

```
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 # 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:** Specifies 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 # 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:** These parameters indicate the hunt group numbers associated with the T1 line in a specific Line Profile. An SNMP manager can retrieve these numbers from Ascend devices

and store them in a table that includes the devices from which information is retrieved and the hunt group numbers in their WAN Line Profiles.

**Usage:** Enter the phone number for the hunt group associated with current line in the Hunt-x # parameter.

**Example:** Hunt-1 #=847-4747

**Dependencies:** The numbers entered in the Hunt-n # parameters must be the same as the numbers that are assigned to T1 channels, creating the hunt group

**Location:** Net T1 Line Profile > Line Config

## /

### 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 route discovery methods on the Internet and one of the least secure, because it is possible to counterfeit ICMP redirects and change the way a device routes packets.

**Usage:** Specify one of the following values:

- Accept (to process ICMP redirects). This is the default.
- Ignore (to 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)  
Don't require a matching ID from incoming calls.
- Prefer  
Authenticate using the CLID if available, otherwise fall back to using PAP or CHAP authentication.
- Require  
The CLID must be valid and match the value in a configured profile. If the profile also requires password authentication, do that as well.
- Fallback  
Authenticate using the CLID when RADIUS is available, otherwise fall back to using password authentication.
- Called Require

The called number must be valid and match the Calling # value in a configured profile. If the profile also requires password authentication, do that as well.

- **Called Prefer**  
Authenticate using the Calling # value in a configured profile if available, otherwise fall back to using password authentication.

**Location:** Ethernet > Answer

**See Also:** AnsOrig, Calling #, Called #

## **ID Fail Busy (previously CLID Fail Busy)**

**Description:** Specifies whether to return User Busy or Normal Call Clearing as a Cause in ISDN DISCONNECT messages when authentication fails due to 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 due to 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 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:** 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 profile, it 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** specifies that the port waits for a user to establish a call. None is the default.
- **Call** specifies that 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 and remote ends must use the same combination of these parameters. Further, if you set Idle to None and Dial to DTR, the hosts at both ends of the connection must make DTR (Data Terminal Ready) active for the MAX to connect the switched channels.

**Location:** Ethernet > Answer > Session Options, Ethernet > Connections > Session Options, Host/Dual (Host/6) > Port/V 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 between 0 and 60. The default setting is 0; this setting 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 enters 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 sets this parameter 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 between 0 and 99. The default value is 0; this setting 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 > Encaps Options

**See Also:** Call Filter, Encaps, Idle

## IF Adrs

**Description:** Specifies a numbered interface IP address for the MAX. Interface-based routing allows the MAX to operate more nearly the way a multi-homed 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 in the IF Adrs parameter. The far-end numbered interface address is specified in 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.

**Parameter Location:** Ethernet > Connections > IP options

**See Also:** WAN Alias, Route IP

## Ignore Def Rt

**Description:** Specifies whether the MAX ignores the default route when updating its routing table via RIP updates. The default route specifies a static route to another IP router, which is often a local router such as a Cisco router or another 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 means the MAX ignore advertised default routes. This is recommended.
- No means the MAX may modify its default route based on 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:** Previously, you could set the Imm. Modem Pwd parameter to null to allow unlimited access to the Immediate Modem feature—now you should set Imm. Modem Access to None instead. However, for compatibility reasons, 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  
This indicates that call restriction is disabled, and that all users can place outgoing calls.
- Global  
This indicates that a single password is used to verify dialout. Anyone who knows that password can place outgoing calls. The Imm. Modem Pwd parameter specifies the password.
- User (the default)  
When per-user Immediate Modem access is enabled, the MAX requests a login name before allowing any user access to 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 request 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 dialout. It tells the MAX that all Telnet sessions initiated with that port number want 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 dialout 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 dialout service will be denied if the user does not enter the proper password.

**Usage:** Specify a password 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 PAD (Packet Assembler/Disassembler).

**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 zero indicates 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)  
This disables immediate mode.
- Telnet  
For telnet service, you can set the Telnet Host Auth parameter to bypass the terminal server authentication and go right to a Telnet login prompt.
- Raw-TCP
- Rlogin
- X.25/PAD  
With this setting, 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 in 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 to access the MAX unit's modems, so that they can place outgoing calls without going through 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 to control access to the modems. See Immediate Modem Access.

**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 zero disables the inactivity timer.

**Example:** Inactivity Timer=120

**Dependencies:** This parameter applies only to X.25/IP connections

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

## 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 all channels if the call type is Nailed. In a Call profile, this parameter applies only if the call type is AIM, FT1-AIM, FT1-B&O, or BONDING and the Call Mgm parameter is set to Manual, Dynamic, or Mode 2.

**Location:** Host/Dual (Host/6) > Port/N Menu > Directory, Ethernet > Connections > 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 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) to display the command-line interface (*terminal mode*).
- Menu to display the menu interface (*menu mode*).

**Location:** Ethernet > Mod Config > TServ Options

## Interval

**Description:** Specifies the number of 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 between 5 and 50. The default is 10.

**Example:** Interval=10

**Dependencies:** This parameter applies only to Combinet connections.

**Location:** Ethernet > Answer > COMB Options, Ethernet > Connections > 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 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 that 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 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 > 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 Gateway 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-Ascend 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 > 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. This causes the MAX to listen for its network number and acquire it from another router on that interface. If you enter a number other than zero, the MAX becomes a *seeding* router and other routers can learn their IPX network number from the MAX. 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 packet frame used by the majority of NetWare servers on Ethernet. The MAX routes and spoofs only one IPX frame type (IEEE 802.2 by default), which is specified in the IPX Frame parameter. If some NetWare software transmits IPX in a frame type other than the type specified here, 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)

This setting indicates that the IPX clients and servers on the local Ethernet cable follow the IEEE 802.2 protocol for the MAC header. The framer contains the LLC (Logical Link Control) header in addition to the MAC (Media Access Control) header. This is the default.

- 802.3 (for NetWare 3.11 or earlier)  
This setting indicates that IPX clients and servers on the local Ethernet cable follow the IEEE 802.3 protocol for the MAC header, also called Raw 802.3. The frame does not contain the LLC (Logical Link Control) header in addition to the MAC (Media Access Control) header.
- SNAP  
This setting indicates that the IPX clients and servers on the local Ethernet network follow the SNAP (SubNetwork Access Protocol) for the MAC header. This specification includes the IEEE 802.3 protocol format plus additional information in the MAC header.
- Enet II  
This setting indicates that IPX clients and servers on the local Ethernet network follow the Ethernet II protocol for the MAC header.
- None disables IPX-specific features.  
If you choose this setting, 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 Net #

**Description:** Specifies the network number of the remote-end router. If specified, it creates a static route to that device. It 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 > IPX Options

**See Also:** Route IPX

## IPX Pool #

**Description:** Specifies a virtual IPX network to be assigned to dial-in NetWare clients. Dial-in clients do not belong to an IPX network, so they must be assigned an IPX network number to establish a routing connection with the MAX. The MAX advertises the route to this virtual network and assigns it as the network address for dial-in clients.

The dial-in Netware client must accept the network number, although it can provide its own node number or accept a node number provided by the MAX. If the client does not have a unique node address, the MAX assigns the node address as well.

**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.

**Example:** IPX Pool #=FF0000037

**Dependencies:** This parameter is not applicable if the MAX does not route IPX.

**Location:** Ethernet > Mod Config > Ether Options

## IPX RIP

**Description:** IPX RIP in a Connection profile defines how RIP packets are handled across this WAN connection. IPX RIP is set to Both by default, indicating 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 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 > IPX options...

**See Also:** IPX SAP, Peer

## IPX Routing

**Description:** This enables IPX routing mode. When you turn on IPX routing in the MAX and close the Ethernet profile, the MAX 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 to acquire its IPX network number from other IPX routers on that segment.

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

- Yes enables IPX routing in the MAX.
- No disables IPX routing system-wide.

**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:** IPX SAP in a Connection profile defines how SAP packets are handled across this WAN connection. IPX SAP is also set to Both by default, indicating 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 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 > 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 zero means 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 > Session Options, Ethernet > Mod Config > Ether Options

**See Also:** IPX Enet #, IPX Routing, Server Name, Server Type, Type, Valid

## K

### K Window Size

**Description:** This parameter establishes the maximum number of data packets that can be outstanding in an X.75 connection before acknowledgment is required.

**Usage:** Specify a number between 2 and 7. The default is 7.

**Location:** Ethernet > Answer > X.75 Options

**See Also:** Frame Length, N2 Retransmission Count, T1 Retransmission Timer, X.75

## L

### L2 End

**Description:** Specifies CCITT Layer 2, which is used to determine the address to send when two PBX devices are connected back-to-back. In that case, one side must act as a PBX and the other side must act as an ET.

**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 E1 lines.

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

**See Also:** L3 End, Switch Type

### L2TP Mode

**Description:** Specifies the system-wide type of L2TP functionality the MAX supports.

**Usage:** Specify one of the following values:

- LAC specifies that the MAX can function as an LAC only.
- LNS specifies that the MAX can function as an LNS only.
- Both specifies that 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

### L3 End

**Description:** Specifies CCITT Layer 3, which must be set to its default value when a DPNSS or DASS2 switch type is in use.

**Usage:** Specify one of the following values:

- x-side (the default)  
This value specifies that layer 3 favors the outbound call when a call collision occurs.
- y-side

**Example:** L3 End=x-side

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



**See Also:** L2 End, Switch Type

## LAPB k

**Description:** Specifies the maximum number of sequentially numbered frames that a given DTE/DCE link may 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 between 1 and 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:** This parameter indicates the retry limit—the maximum number of times the MAX can resend a frame when the LAPB (Link Access Protocol–Balanced) T1 timer expires.

**Usage:** Specify a number between 0 and 255. The default is 20. 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 > 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 may 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 between 1 and 255. The default is 3. When you choose a value for this parameter, you must take into account any frame transmission and processing delays you may 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:** This parameter determines the maximum number of milliseconds LAPB (Link Access Protocol–Balanced) waits for outgoing I-frames (Information 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 between 0 and 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 is to set the Ans N# parameter in the Ethernet profile.

**Usage:** Specify a subaddress number between 0 and 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 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 LAN Adrs.

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

**See Also:** Encaps, IP Adrs, Route IP, Station

## LCN

**Description:** Specifies the LCN (logical channel number) to use for a PVC (Permanent Virtual Connection) 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 enter a number between 0 and 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 an SVC (Switched Virtual Connection).

**Dependencies:** This parameter applies only to X.25/PAD and X.25/IP connections.

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

## Length

**Description:** In a T1 line profile, specifies the cable length of the line from the CSU (Channel Service Unit) or other network interface unit to the MAX. The setting you indicate should reflect the longest line length you expect to encounter in your installation.

In a Firewall profile, it specifies the length of the firewall uploaded to the MAX from Secure Access Manager (SAM). In Firewall profiles, the parameter is read-only.

In a filter of type Generic, specifies the number of bytes to test in a frame, starting at the specified Offset. The MAX compares the contents of those bytes to the value specified in the filter's Value parameter. For example, with this 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 filter applies the mask only to the eight bytes following the two-byte offset.

- In a T1 profile, specifies the length of the cable.

**Usage:** In a Filter profile, specify a number between 0 and 8 that defines the number of bytes to use for comparison. The default zero means no bytes are compared.

In a T1 line 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

## Listen X.121 Addr

**Description:** Specifies a listen pattern for host-initiated calls. This is similar to typing the following command in the X.25 PAD:

```
* listen addr=pattern
```

The pattern is in the same format as an X.121 address, or sub address and can contain wild cards.

**Usage:** Specify an address. You can enter up to 15 characters.

**Dependencies:** This parameter is always applicable.

**Location:** Ethernet > Connections > *any Connection profile* > Encaps options  
Ethernet > Answer > T3POS options

## Line *n* tunnel type

**Description:** Indicates 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:** Line *n* tunnel type 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

## Link Access Type

**Description:** Specifies the type of the DTE connection.

**Usage:** Specify one of the following values:

- Dedicated (the default)  
Specifies that the DTE connection is a permanent, leased-line connection.
- Dial  
Specifies that the DTE connection is a dial-up connection.

**Dependencies:** This parameter is always applicable.

**Location:** Ethernet > Connections > *any Connection profile* > Encaps options  
Ethernet > Answer > T3POS options

## Link Comp

**Description:** Specifies the link compression method for a PPP, MP, and MP+ call. Both sides of the connection must set the same type of link compression or it will not be used.

**Usage:** Specify one of the following values:

- None (the default in the Answer profile)
- Stac (Use an Ascend 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.

**Example:** Link Comp=Stac

**Dependencies:** This parameter applies only to PPP and its multilink variants. Both sides of the link must support the same kind of compression or it is not used.

**Location:** Ethernet > Answer > PPP Options, Ethernet > Connections > 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 specifies 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 specifies the link management protocol defined in ANSI T1.617 Annex D.
- Q.933A the link management protocol defined Q.933 Annex A.

**Location:** Ethernet > Frame Relay

**See Also:** DLCI, FR DLCI

## 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 can set one channel to unused by setting B1 Usage or B2 Usage to Unused, and enter only one SPID. The device sharing the line must enter the other assigned SPID.

**Usage:** Check with your carrier to find out the setting you should specify for this parameter. You can specify one of the following values:

- P-T-P specifies point-to-point mode, in which the MAX requires one phone number and no SPIDs.
- Multi-P specifies multipoint mode, in which the MAX requires two phone numbers and two SPIDs. This is the default.

**Dependencies:** All switch types use multi-point except the AT&T 5ESS switch.

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

**See Also:** Pri SPID, Sec SPID, Switch Type

## List Attempt

**Description:** Enables or disables the DNS List Attempt feature. 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 fails. To avoid tearing down physical links when a host is unavailable, you can use the List Attempt parameter to enable the MAX to try one entry in the DNS list of hosts, and if that connection 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 enables a user to try the next host in the DNS list if the first Telnet login attempt fails, which may prevent the physical connection from being torn down.
- No means 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

## 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 entry in the local DNS table that matches the host name, up to the number of entries you specify in 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 with the dnstab entry terminal command depends upon the value you set in the List Size parameter.

**Usage:** Specify a number between 1 and 35. The default is 6.

**Example:** Following are three possible local DNS table situations:

- You have set List Size=4 and the remote DNS returns 3 addresses, the three addresses replace the entire list of four IP addresses in the local DNS table.

- You have set List Size= 35, and the remote DNS server returns only 4 addresses. The MAX places the four IP addresses in the table and sets the remaining 31 addresses in the list to zero.
- You have just changed the List Size =1. Previously, you had set List Size=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, all nine others will be set to zero.

**Dependencies:** This parameter is applicable only when the parameter List Attempt = Yes. A local DNS table is created only if the parameter Enable Local DNS Table= Yes.

**Location:** Ethernet > Mod Config > DNS

**See Also:** List Attempt, Enable Local DNS Table

## Local Echo

**Description:** Allows you to configure local echo mode on a terminal server session. Local echo mode is a line-by-line mode, where the line that appears as it is typed is not actually transmitted until a carriage return is entered. 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 non-standard Telnet ports and programs. If the remote server turns local echo on or off in its option negotiation for a Telnet session, this setting will override the setting made locally.

A terminal server user can override the Local Echo setting from the command line for the current session 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 using local profiles. If that fails, the MAX tries to authenticate the connection using an external authentication server.

If this parameter 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 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.)

- 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 the remote authentication is tried first if this parameter set to No, the MAX 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 still 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 Note above for related dependencies.

**Location:** Ethernet > Mod Config > Auth

**See Also:** Auth Timeout

## Location

**Description:** This is an SNMP-readable parameter that specifies the physical location of the MAX. 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. When 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:** Loc.DNS Tab Auto Update=Yes to enable automatic updating of the IP addresses in the local DNS table. No disables automatic updating. No is the default.

When 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 on the table.

**Dependencies:** The Enable Local DNS Table parameter must be set to Yes.

**Location:** Ethernet Profile: Ethernet > Mod Config > DNS



## 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 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 will be directed.

**Usage:** Specify the IP address or hostname of the device.

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

**See Also:** Login Port

## Login Port

**Description:** Specifies the TCP port the raw TCP connection will use to connect to the specified host.

**Usage:** Specify the TCP port number on the login host. You can specify a value between 1 and 65535. The default is 1.

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

**See Also:** Login Host

## Login Prompt

**Description:** Specifies the string used to prompt for a user name 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 “escape” it with another backslash. For example, you could enter this string:

```
Welcome to\n\t\\Ascend Remote Server\\\nEnter your user name:
```

to display the following text as a login prompt:

```
Welcome to
  \\Ascend Remote Server\\
Enter your user name:
```

**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 indicated in the Login Timeout field 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 between 0 and 300 seconds. The default is 300. A zero value 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 may be routed.

**Usage:** Specify a number between 1 and 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

## 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 > 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 between 0 and 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 > 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 between 0 and 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 > Encaps Options

**See Also:** LQM, LQM Max

## LSA-type

**Description:** This specifies the OSPF ASE 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). Type-1 is the default.
- 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  
This indicates that this static route should be advertised in an internal LSA.

**Dependencies:** Keep this additional information in mind.

- The MAX only advertises the static route if the Static Route gateway has a corresponding entry in a Connection profile.
- When you set LSA-type to Internal, the internal LSA static route appears as a stub area to external OSPF routers.

**Location:** Ethernet > Connections > OSPF Options, Ethernet > Mod Config > OSPF Option, Ethernet > Static Rtes

**See Also:** Ospf-Cost

## M

### Mask

**Description:** In a filter of type Generic, specifies a 16-bit mask to apply to the Value before comparing it to the packet contents at the specified offset. You can use it to fine-tune exactly which bits you want to compare.

The MAX applies the mask to the specified value using a logical AND after the mask and value are both translated into binary format. The mask hides the bits that appear behind each binary 0 (zero) in the mask. A mask of all ones (FF FF FF FF FF FF FF FF) masks no bits, so the full Compare To value must match the packet contents. 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 mask is applied as shown below, resulting in a value that matches the Value.

	2-byte Byte Offset	8-byte Comparison
	2A 31	97 FE 45 70 12 22 33 99
Mask	-----	0F FF FF FF 00 00 00 F0
Result of mask	-----	07 FE 45 70 00 00 00 90
Value to test	-----	07 FE 45 70 00 00 00 90

The packet matches this filter. Because the Filter Action is “Discard”, the packet will be dropped. The byte comparison works as follows:

- 2A and 31 are ignored due to the two-byte offset.
- 9 in the lower half of the third byte is ignored, because the mask has a 0 in its place. The 7 in the third byte matches the value parameter’s 7 in the upper half of that byte.
- F and E in the fourth byte match the value parameter for that byte.
- 4 and 5 in the fifth byte match the value parameter for that byte.
- 7 and 0 in the sixth byte match the value parameter for that byte.
- 12 and 22 and 33 in the seventh, eighth and ninth bytes are ignored because the mask has a 0 in those places.
- 9 in the tenth byte equals the matches the value parameter’s 9 in the lower half of that byte. The second 9 in the upper-half of the packet’s tenth byte is ignored because the mask has a 0 in its place.

**Usage:** Specify a 16-bit hexadecimal number. The default of all zeroes means the MAX uses the data in the packet as is for comparison purposes.

**Example:** Mask=0FFFFFFF000000F0

**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 units configured as an ATMP Home agent.

Changes take effect after the Connection Profile is saved, 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 profile* > Session Options menu.

**See Also:** ATMP Mode, ATMP Gateway

## 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 what you specify here.

**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 transmission (including the length of opening frame) in bytes that the PAD must be able to accept and process from the DTE or host. This only applies to processing opening frame and to both local modes of operation.

**Usage:** Specify one of the following values:

- 512 (the default)
- 1024

**Dependencies:** Keep the following information in mind.

- The Max. Block Size may apply even if both the host and DTE initiated call default mode are non-local. This is because the mode can be changed through an opening frame, in which case this parameter applies.

**Location:** Ethernet > Connections > *any 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:** Specify a value from 1-1440. The default is zero, which disables the timer.

**Example:** Max Call Duration=0

**Location:** Ethernet > Answer > Session Options, Ethernet > Connections > 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 between 0 and 2,142,270. The default is 0. Accepting the default disables the parameter.

**Location:** Port profile: Host/Dual (Host/6) > Port/V 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 MPP calls. In a Call profile, it applies only to dynamic AIM calls.

**Location:** Ethernet > Answer > PPP Options, Host/Dual (Host/6) > Port/V Menu > Directory > Time Period N, Ethernet > Connections > 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 profile, it applies to calls from the AIM port within the specified time period. In the System 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 56-kbps or 64-kbps switched channel for one minute. For example, a 5-minute, 6-channel call uses 30 DS0 minutes. When the usage

## MAX Alphabetic Parameter Reference

### Max. Time (min)

---

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 profile, specify a number from 1 to 2,142,720 (default 1).
- In a System 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/6) > PortN Menu > Port Config, System > Sys Config

**See Also:** DS0 Min Rst

### Max. Time (min)

**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 will find out 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:** Specify a number between 1 and the maximum number of minutes the connection should stay up. The default setting is 0 (zero); this setting indicates an unlimited connection time.

**Dependencies:** This parameter applies only to ARA connections.

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

**See Also:** Password, ARA, AppleTalk, Encaps

### Max Leases

**Description:** Specifies the number of dynamic addresses to assign to NAT (Network Address Translation) clients using this connection. When NAT is used, an initial dynamic address is automatically assigned via the PPP negotiations. This 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 > DHCP options

**See Also:** Reply Enabled

## 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 between 0 and 9999. The default is 10. A value of 0 (zero) indicates 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 > Encaps Options

## Mbone profile

**Description:** Specifies the name of a resident Connection profile 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 Mbone profile name is null and Multicast Forwarding is turned on, the MAX assumes that its Ethernet is the MBONE interface.

**Usage:** Specify the name of the Connection profile 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 Multicast Forwarding is set to No.

**See Also:** Multicast Forwarding, Multicast Client

## MDM Trn Level

**Description:** Specifies the default transmit level for a digital modem. When a modem calls the MAX, the unit attempts to connect at the transmit attenuate level you specify. This is the amount of attenuation in decibels the MAX should apply to the line, causing the line to lose power when the received signal is too strong. Generally, you do not need to change the transmit level. However, when the carrier is aware of line problems or irregularities, you may 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 connection. Transmitting at higher level helps certain modems with near-end-echo problems.

**Usage:** Specify a value between -13 db and -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

## Method of host notif

**Description:** For DTE-initiated calls, this specifies how the host is notified of the mode of the call.

**Usage:** Specify one of the following values:

- None (the default)  
Specifies that the host is not notified of the mode of the call and any data in the CUD is discarded.
- CRP  
Specifies that the host is informed of the mode of the call by the DTE sending a Call Request Packet (CRP) in the CUD field of a control frame.
- MSF  
Specifies that 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:** Keep the following information in mind.

- This parameter does not apply if the opening frame is a general frame. In this case the default DTE-initiated mode is not changed.

**Location:** Ethernet > Connections > *any Connection profile* > Encaps options  
Ethernet > Answer > T3POS options

## Metric

**Description:** In a Connection or Route profile, specifies a RIP metric (a virtual hop count) associated with the IP route. In the Answer profile, it specifies the RIP metric of the IP link when the MAX validates an incoming call using RADIUS or TACACS 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 lowest metric. If you enable RIP (Routing Information Protocol) 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 Route profile because the MAX always uses the lower hop count.

**Usage:** Press Specify a number between 1 and 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 > 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 between 1 and the maximum channel count. The default setting is 1.

**Example:** Min Ch Count=1

**Location:** Ethernet > Answer > PPP Options, Ethernet > Connections > Encaps Options, Host/Dual (Host/6) > Port/V Menu > Directory > Time Period *N*

**See Also:** Call Mgm, Max Ch Count

## Modem Dialout

**Description:** Specifies whether an operator 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 dialout connections, those connections are not affected. However, no new modem dialouts 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 dialout.

**Dependencies:** This parameter does not apply if terminal services are disabled.

**Location:** Ethernet > Mod Config > TServ Option

**See Also:** TS Enabled, Immediate Modem

## Modem Ringback

**Description:** 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 one of the following values:

- Yes specifies that the MAX generates a ringback tone.  
This is the default.
- No specifies that the MAX does not generate a ringback tone.

**Location:** Ethernet > Mod Config

## Modem:NumPlanID

**Description:** Modem:NumPlanID is used for outbound calls made by the MAX on PRI lines so that the switch can properly interpret the phone number dialed. Ask your PRI provider for

## MAX Alphabetic Parameter Reference

### Modem:PRI # Type

---

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 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 profile)

**See Also:** Modem:PRI # Type, NumPlanID (Call and Connection profiles), T1-PRI:NumPlanID (System profile)

### Modem:PRI # Type

**Description:** Modem:PRI # Type is used for outbound calls made by the MAX on PRI lines so that the switch can properly interpret the phone number dialed. Ask your PRI provider for details on when to use each of the following settings. This parameter specifies the TypeOfNumber field in the called party's information element.

**Note:** 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 specifies phone numbers within the U.S. (TypeOfNumber=2)
- Intl specifies phone numbers outside the U.S. (TypeOfNumber=1)
- Local specifies phone numbers within your Centrex group. (TypeOfNumber=4)
- Abbrev. specifies that the phone number is abbreviated. (TypeOfNumber=6)
- NetSpecific (currently not implemented) specifies that the network you are connected to understands the phone number (TypeOfNumber=3)
- Unknown (the default) specifies that the phone number is none of the above. (TypeOfNumber=0)

**Location:** Net/T1 > Line Config (Line profile)

**See Also:** Modem:NumPlanID, NumPlanID (Call and Connection profiles), T1-PRI:NumPlanID (System profile)

### Module Name

**Description:** In the Ethernet profile, this assigns an optional name to the Ethernet interface. In a Host-Interface profile, it assigns a name to an AIM port module, which is sent to the remote end of the connection.

**Usage:** Specify a name containing up to 16 characters. For the Ethernet interface, you can leave this parameter blank.

**Location:** Ethernet > Mod Config, Host/Dual (Host/6) > Mod Config, Serial WAN > Mod Config

## More

**Description:** In a filter of type Generic, specifies whether the MAX includes the next filter condition before determining whether the frame matches the filter. If checked, the current filter condition is linked to the one immediately following it, so the filter can examine multiple non-contiguous bytes within a packet. In effect, this parameter *marries* the current filter to the next one, so that the next filter is applied before the forwarding decision is made. The match occurs only if *both* non-contiguous bytes contain the specified values.

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

- Yes links the current filter rule 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 made based solely on this 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:** This enables incoming Multilink PPP (MP) connections, which use the encapsulation defined in RFC 1990. MP enables the MAX to interact with Multilink PPP-compliant equipment from other vendors to use multiple channels for a call. Both sides of the connection must support MP.

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

- Yes means the MAX answers MP calls, provided that they meet all other connection criteria.
- No means the MAX will not accept inbound MP calls.

**Location:** Ethernet > Answer > Encaps

**See Also:** Encaps

## MPP

**Description:** Enables incoming MP+ (Multilink Protocol Plus) connections, which use PPP encapsulation with Ascend extensions. MP+ enables the MAX to connect to another Ascend unit using multiple channels.

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

- Yes means the MAX answers MP+ calls, provided that they meet all other connection criteria.

- No means 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 right setting, unless the far end requires a lower number.

Third-party devices can calculate MRU differently. If you connect to a non-Ascend device, you might need to specify a different MRUs 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 or a Connection profile, specify a number between 1 and 1524.
- In a Frame Relay profile, specify a number between 128 and 1600.
- In an X.25 profile, specify a number between 1 and 1500.

**Example:** MRU=1524

**Location:** Ethernet > Answer > PPP Options, Ethernet > Connections > Encaps Options, Ethernet > Frame Relay

**See Also:** Encaps

## **Multicast Client**

**Description:** Enables the MAX to respond to multicast clients on the WAN link. Clients cannot be supported on the MBONE interface, so this means another WAN link or the local Ethernet 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 means the MAX does not respond to multicast clients on the interface.

**Example:** Multicast Client=Yes

**Dependencies:** This parameter is not applicable if Multicast Forwarding is disabled or if the Connection profile is the Mbone profile (linking to a remote multicast router). See Multicast Rate Limit for related dependencies.

**Location:** Ethernet > Connections > IP options

**See Also:** Multicast Rate Limit

## Multicast 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 t parameter is set to 100. *This 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 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 > Connections > IP Options

**See Also:** Multicast Client

## N

### N2 Retransmission Count

**Description:** Specifies the retry limit—the maximum number of times the MAX can resend a frame on an X.75 connection when the T1 Retransmission Timer expires.

**Usage:** Specify a number between 2 and 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 Retransmission 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 DCE.

**Location:** Ethernet > Frame Relay

**See Also:** Link Mgmt

## Nailed Grp

**Description:** Specifies a number assigned to a group of nailed channels or a serial WAN port. In a Frame Relay or X.25 profile, it 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 that will represent this port's bandwidth. It can be a number between 1 and 60 (default 1). In a Frame Relay or X.25 profile, specify the number assigned to nailed T1 or serial WAN bandwidth.

**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, 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, Ascend 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 contain up to 16 characters.
- In the X.25 profile, the name is limited to 15 characters.
- In the Names / Passwords profile, Route profile, and SNMP Traps profile, the name can contain up to 31 characters.

**Example:** Name=PacBell

**Location:** Host/Dual (Host/6) > 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,

## Net Adrs

**Description:** In a Bridge 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 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 Net Adrs parameter of a Bridge profile, the MAX responds to the ARP request with the Ethernet (physical) address specified in the Bridge profile and brings up the specified connection. In effect, the MAX 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 in to 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 may 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 > 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 > 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 > 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 the 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 NFAS (Non-Facility Associated Signaling). 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 this line. The default value is required when the line connects to a DPNSS or DASS2 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 DASS2 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 00000000000001.

**Dependencies:** This parameter does not apply if the IPX routing is not enabled.

**Location:** Ethernet > IPX Routes

**See Also:** Route IPX, Network

## 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 means the MAX closes the back panel alarm relay when all trunks go out of service.
- No means the MAX records the event in the log but does not close the alarm relay.

**Location:** System > Sys Config

## 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 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 > *any Connection profile* > Encaps options  
Ethernet > Answer > PAD options  
Ethernet > Answer > T3POS options

## NumPlanID

**Description:** NumPlanID is used for outbound calls made by the MAX on PRI lines so that the switch can properly interpret the phone number dialed. Ask your PRI provider for details on when to use each of the following settings. This parameter specifies 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/6) > PortN Menu > Directory (Call profiles), Ethernet > Connections (Connection profiles), 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 bytes 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 means the operator 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 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:** Keep this additional information in mind.

- 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 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-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

**See Also:** ASE-type, ASE-tag

## 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 operator'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 means the operator 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 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

## Palmtop

**Description:** Specifies whether the MAX enables or disables access to AIM ports through the Palmtop Controller. If it is restricted, the operator 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 operator 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 operator access to a Palmtop port.

**Location:** Host/Dual (Host/6) > 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/6) > 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/6) > Mod Config

**See Also:** Palmtop

## 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 > Encaps Options, Ethernet > Mod Config > ATMP Options

**See Also:** AppleTalk, ARA, ATMP Gateway, ATMP Mode, Encaps, Type, UDP Port

## Password Req

**Description:** Specifies that a password will be required to authenticate Combinet connections.

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

- Yes means the MAX requires a password from all incoming calls from a Combinet bridge.
- No means a password is not required for Combinet calls.

**Example:** Password Req=Yes

**Dependencies:** This parameter applies only to Combinet connections.

**Location:** Ethernet > Answer > COMB Options, Ethernet > Connections > Encaps Options

**See Also:** COMB, Encaps, Recv PW, Send PW, Station

## 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 phone 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 phone number matches the phone 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 > 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 Ascend 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 > AppleTalk Options

**See Also:** Net Start, Net End, AppleTalk, AppleTalk Router, Route AppleTalk, Zone Name

## 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 > *any Connection profile* > Encaps options  
Ethernet > Answer > T3POS options

## Pkt Audio Mode

**Description:** Specifies the type of voice compression and coding used with any MultiVoice call. MultiVoice calls are compressed before the MultiVoice Gateway sends them across an IP network.

**Usage:** Specify one of the following values:

- G.711 U Law  
Appropriate in T1 environments. The MultiVoice Gateway sends digitized voice at 64 Kbps and provides toll quality voice on managed IP networks with sufficient available bandwidth.  
This is the default for MAX T1 units.
- G.711 A Law  
Appropriate in E1 environments. The MultiVoice Gateway sends digitized voice at 64 Kbps and provides toll quality voice on managed IP networks with sufficient available bandwidth.  
This is the default for MAX E1 units.

- G.729

The MultiVoice Gateway sends digitized voice at 8 Kbps, is a low-complexity coding algorithm, and provides toll quality voice on managed IP networks.

**Example:** Pkt Audio Mode=G.729

**Dependencies:** Pkt Audio Mode only applies if the MAX acts as a MultiVoice Gateway.

**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 > 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 may 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 may 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 means the caller must accept dynamic assignment. This is recommended if Names/ Passwords profiles are in use.
- No means 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 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 > 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 must 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, with this configuration:

```
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 means the MAX traps AIM port state changes and send traps-PDS to the SNMP manager.
- No means 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/6 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/6) > 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 *Ascend* for AIM port #1, the menu called *21-000 Port1 Menu* becomes *21-100 Ascend*.

**Usage:** Specify the name. You can specify up to 16 alphanumeric characters.

**Example:** Port Name=Ascend

**Location:** Host/Dual (Host/6) > PortN 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 may 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=Ascend

**Location:** Host/Dual (or Host/6 > Port N Menu > Port Config

**See Also:** Call Password

## 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 means 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 means the MAX begins PPP/LCP negotiation immediately after a user enters PPP at the command line.
- No means 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 PPTP (Point-to-Point Tunneling Protocol) 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

## 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 > 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 > IP Options, Ethernet > Static Rtes

## 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 phone number dialed. Ask your PRI provider for details on when to use each of the following settings. This parameter specifies the TypeOfNumber field in the called party's information element.

**Usage:** Specify one of the following values:

- National (the default) specifies phone numbers within the U.S. (TypeOfNumber=2)
- Intl specifies phone numbers outside the U.S. (TypeOfNumber=1)
- Local specifies phone numbers within your Centrex group. (TypeOfNumber=4)
- Abbrev. specifies that the phone number is abbreviated. (TypeOfNumber=6)
- NetSpecific (currently not implemented) specifies that the network you are connected to understands the phone number (TypeOfNumber=3)
- Unknown specifies that the phone 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/6) > PortN Menu > Directory (Call profiles), Ethernet > Connections (Connection profiles), 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 phone 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)" for more detail on add-on numbers.)

**Usage:** Specify a phone 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

## 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 > 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:

01nnnnnnn0

01nnnnnnnn00

In the AT&T SPID formats, *nnnnnn* is the 7-digit phone number (not including the area code). For example, if the phone number is 555-1212, the SPID will be 0155512120 or 01555121200.

For a Northern Telecom switch, SPIDs have one of these formats:

aaannnnnnnSS

aaannnnnnnSS00

In the Northern Telecom SPID formats, *aaannnnnnn* is the 10-digit phone 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 phone numbers are 212-555-1212 and 212-555-1213, the SPIDs may 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 means the route is advertised via routing protocols.

**Dependencies:** This parameter does not apply if the IP routing is not enabled.

**Location:** Ethernet > Connections > IP Options, Ethernet > Static Rtes

**See Also:** LAN Adrs, Metric, RIP, Route IP

## 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

## Profile Req'd

**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 Req'd to Yes disables Guest access for ARA connections.

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

- Yes means a configured profile is required for all callers.
- No means 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

## 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 means 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. 0 is the default.

**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

### 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 16 characters. The default is Write.

**Location:** Ethernet > Mod Config > SNMP Options

**See Also:** Read Comm, R/W Comm Enable

## 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:** Multicast Forwarding, Mbone Profile, 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 > Encaps Options, Ethernet > Names / Passwords

**See Also:** Encaps, Password Req'd, Recv Auth, Send Auth, Send PW

## Remote Conf

**Description:** Specifies whether or not a RADIUS server remotely 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 means the MAX obtains the configuration for these items from RADIUS. The local configuration for these items is ignored.
- No means 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 operator 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 operator 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 > 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 > 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 > OSPF Options, Ethernet > Mod Config > OSPF Options

## 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 > *any Connection profile* > Encaps options  
Ethernet > Answer > T3POS options

## RIP

**Description:** Specifies how the MAX handles RIP update packets on the interface.

**Note:** Ascend 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 > IP Options,  
Ethernet > Mod Config > Ether Options

**See Also:** Route IP

## RipASETtype

**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. 50 is the default.

**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 means 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 means 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 (the default) means the calling device goes off-hook and waits for a 200 msec wink before dialing.  
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. Neither device sends a wink before answering a call.
- Idle-Start means neither device sends a wink before either dialing or answering, and that off-hook dialing alone initiates a call.
- Inc-W-400 means each device sends a 400 msec 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 means each device sends a 200 msec wink before dialing or answering a call.
- Loop-Start means 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, and the parameter in the AppleTalk options submenu for the profile.

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

- Yes enables AppleTalk routing.
- No means 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 means 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 Req'd

## 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 means 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 > *any 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/6) > Port/V 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 > OSPF Options, Ethernet > Mod Config > OSPF Options

## 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 > Any 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 > Any 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 means 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 keep 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 may 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 may 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/6) > Port/V Menu > Directory, Ethernet > Connections > 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 a add-on number and the calling MAX needs to add more channels, it redials the phone number it used to make the first connection. (See "Ch N # (N=1-24, 1-32)" for more detail on add-on numbers.)

**Usage:** Specify a phone 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 phone number for the Net BRI line. The carrier supplies both the phone 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 means the server uses standard DES encryption.
- No means 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 operator 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 where the parameter appears.

**Usage:** Specify one of the following values:

For SNMP address security, the default is No.

- Yes means the MAX compares the source IP address of packets containing SNMP commands against a list of qualified IP addresses specified in the RD Mgr1-5 and WR Mgr1-5 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 means the MAX does not compare IP addresses, so address-security is not used.

For SNMP traps, the default is No.

- Yes means the MAX will generate traps for Security events (such as failed login attempts) and send the trap-PDU to the SNMP manager.
- No means Security events will not generate traps.

For terminal-server security, the default is None.

- Full means users are prompted for a name and password upon initial login and when they switch between terminal mode and menu mode.
- Partial means they are prompted for a name and password only when entering terminal mode, not for menu mode.
- None means they are not prompted 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 Mgr1-5, Toggle Scrn, WR Mgr1-5

## **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 SAFWORD 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 > 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. 0 disables this parameter. 0 is the default.

**Dependencies:** Send Disc does not apply if the MAX does not support ISDN signalling.

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

**See Also:** Timeout Busy

## 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 Req'd=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 > Encaps Options

**See Also:** Encaps, Password Req'd, 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, MAX *RADIUS Configuration Guide*

## 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 an SAP service 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 or exclude 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, it 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 means session keys will be assigned to all new session entries.
- No means 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 means the MAX will allow more than one caller to share the same profile, provided that no IP address conflicts will result.
- No means 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 > any profile

**See Also:** Encaps, Name, Pool # Count, Pool # 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:

- Inband (the default)  
In this type of signaling, 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 of each channel used for signaling. T1 lines containing one or more switched channels, and Switched-56 lines use inband signaling.

If you specify inband signaling, you must specify a call control mechanism using the Rob Ctl parameter.

- **ISDN**

In this type of signaling, 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)**

NFAS is 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, 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 places and answers calls using the call control mechanism you specify for Rob Ctl. If you set Sig Mode=PBX T1, keep this additional information in mind:

- If Line #2 uses inband signaling and line #1 uses ISDN D-channel signaling, set PBX Type=Voice or PBX Type=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=Leased 1:1.
- The MAX connects calls received on line #1 to the corresponding nailed-up channels of line #2, or 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.

Specify one of the following values on an E1 line:

- **None** indicates a leased line.
- **ISDN** signaling using the D channel. The 32nd channel of the E1 line must be designated as the D channel.
- **DPNSS** indicates that the interface supports DPNSS or DASS 2 signaling.
- **R2** indicates R2 signaling.
- **Metered** indicates metered R2 signaling protocol, used in Brazil and South Africa.
- **Chinese** indicates a version of the R2 signaling protocol specified for use in China.

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

**See Also:** PBX Type, Rob Ctl, Switch Type



## 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 means 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 means 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 an SLIP (Serial Line IP) 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 Gateway 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.

**Location:** Ethernet > Mod Config > SNTP Server

**See Also:** 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 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 Mask, HeartBeat Slot Time, HeartBeat Slot Count, Alarm Threshold

## 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

## 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 #

## 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 may 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 may communicate with each other. You can create a new stack by specifying an 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.  
A virtual module (0–2) reflects a function of the base system. Virtual module 0 manipulates overall system functions. Virtual module 1 is the Net/T1 module, which manipulates the base system's two-line T1 PRI network interface. Virtual module 2 is the Host/Dual module, which manipulates the base system's two AIM ports.  
A real module (3–8) plugs into an expansion slot in the MAX.
- *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 phone 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 may or may not have a subaddress.

If a subaddress is present, it becomes part of the incoming phone 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/6) > Port/V Menu > Directory, Ethernet > Connections > Encaps Options

**See Also:** Add Pers, Dec Ch Count, Dyn Alg, Min Ch Count, Sec History, Target Util



## Switch Type

**Description:** Specifies the carrier switch type that services the T1 or BRI line.

**Usage:** In a Net/T1 profile, specify one of the following values:

- AT&T (the default)
- NT1 (Northern Telecommunications, Inc.)
- Japan
- GloBanD (Q.931W GloBanD data service)  
Although GloBanD can appear in the list of switch types available under 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 like GloBanD that allows data service bandwidths higher than 64 kbps. Contact your T1 PRI service provider for specific information.
- NI-2 (National ISDN-2)
- IDSL  
Identical to AT&T Point-to-Point, but has support for Q.931 en-bloc dialing.

In a Net/BRI Line profile, these North American switch types are supported:

- AT&T (the default)
- NI-1 (National ISDN-1)
- NT1 (Northern Telecommunications, Inc.)

In a Net/E1 profile, specify one of the following values:

- GloBanD (Q.931W GloBanD data service)
- NI-1 (National ISDN-1)
- Net 5 (Euro ISDN services in Belgium, the Netherlands, Switzerland, Sweden, Denmark, and Singapore)
- DASS 2 (U.K. only)
- ISLX (DPNSS switch type)
- ISDX (DPNSS switch type)
- Mercury (DPNSS switch type)
- Australian (Australia only)
- French (VN3 ISDN PRI)
- German (ITR6)
- CAS (New Zealand)

These international BRI switch types are supported:

- 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)
- SWISS (Switzerland: Swiss Net 2)
- GERMA (Germany ITR6 version: DBP Telecom)
- MP GERMAN (Germany: ITR6 multipoint)

- FRANC (France: FT Numeris)
- DUTCH (Netherlands ITR6 version: PTT Netherlands BRI)
- BELGI (Belgium: Pre-Euro ISDN Belgacom Aline)
- JAPAN (Japan: NTT INS-64)
- AUSTR (Australia and New Zealand)
- NET 3 (Same as U.K. NET 3 is also known as Euro-ISDN)
- NET3 PTP (A variation of EURO-ISDN signaling used in Germany)

**Note:** All international switch types except German operate in multipoint mode.

**Example:** Switch Type=AT& T

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

## Sys Diag

**Description:** Enables or disables permission to perform all system diagnostics.

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

- Yes means the operator can use the commands in the Sys Diag menu.
- No specifies that an operator cannot use any of those commands.

**Location:** System > Security

**See Also:** Chapter 1, “MAX Diag Command Reference.”

## 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:** You can specify either 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 Profile: 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 phone number dialed. Ask your PRI provider for details on when to use each of the following settings. This parameter specifies the TypeOfNumber field in the called party's information element.

**Note:** 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 phone numbers within the U.S. (TypeOfNumber=2)
- Intl specifies phone numbers outside the U.S. (TypeOfNumber=1)
- Local specifies phone numbers within your Centrex group. (TypeOfNumber=4)
- Abbrev. specifies that the phone number is abbreviated. (TypeOfNumber=6)
- NetSpecific (currently not implemented) specifies that the network you are connected to understands the phone number (TypeOfNumber=3)
- Unknown (the default) specifies that the phone 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 phone 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 Retransmission 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 Retransmission 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 30000 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

## 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 > *any 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 the following information in mind.

- The T2 timer only applies to the opening frame and to Local or Bin-Local mode.

**Location:** Ethernet > Connections > *any 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 the following information in mind.

- This is not applicable when you set ENQ Handling to Off.

**Location:** Ethernet > Connections > *any 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 > *any 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 only; 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 may apply even if the default modes for both the host- and DTE-initiated calls are Local or Bin-Local. This is because the mode can be changed through an opening frame, in which case this parameter applies.
- The T5 timer applies only to transparent and blind mode only; it is disabled in both Local mode and Bin-Local mode.

**Location:** Ethernet > Connections > *any 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 > *any Connection profile* > Encaps options  
Ethernet > Answer > T3POS options

## 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/6) > Port/V Menu > Directory > Time Period *N*, Ethernet > Connections > 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 means the MAX will answer TCP-Clear connections, provided they meet all other connection criteria.
- No means 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 means 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 may 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 Ascend unit 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 means operators 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 means rely on the Telnet host for authentication.
- No means 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. Some hosts

**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 via 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=Ascend

**Location:** Ethernet > Mod Config

## Template Connection #

**Description:** Specifies a Connection profile to use a *template* Connection profile rather than the Answer profile settings to build the session for this Name-password profile, 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 may 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 may 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 feet 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 means the MAX will use the Terminal Timing signal from the codec.
- No means the MAX uses its Send Timing signal to clock data it receives from the codec.

**Example:** Term Timing=No

**Location:** Host/Dual (Host/6) > Port/N Menu > Port Config

## Term Type

**Description:** Specifies the default terminal type for Telnet and Rlogin sessions.

**Usage:** Specify the a 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 may be configured with different bandwidth management settings.

**Dependencies:** The Time Period subprofile apply only to dynamic AIM calls.

**Location:** Host/Dual (Host/6) > 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

## MAX Alphabetic Parameter Reference

### *Time zone*

---

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, in Newfoundland the time is 1.5 hours ahead of UTC, which is represented as follows:

UTC+0130

For San Francisco, which is 8 hours ahead of UTC:

UTC+0800

For Frankfurt, which is 1 hour behind UTC:

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 means terminal-server users can switch between terminal mode and menu mode.
- No means 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

## 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/6) > Port/N Menu > Directory, Ethernet > Connections > 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 > OSPF Options, Ethernet > Mod Config > OSPF Options

## TS Enabled

**Description:** This enables or disables terminal services.

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

- Yes enable 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 > 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 > Session Options

**See Also:** Encaps, TS Idle

## 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 may want to 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 a UDP port number assigned to a particular function. Depending on where it is located, it may specify the UDP port on which the MAX listens when using ATMP, or the UDP port the MAX uses to communicate with members of a stack.

**Note:** Units that use UDP to communicate for a particular purpose must all agree on the assigned port number. For ATMP, both agents must specify the same UDP port number. For MAX stacks, all members of a stack must specify the same UDP port number.

**Usage:** Specify a valid UDP port number (0–65535). For ATMP, the default port number is 5150. For MAX stacks, the default is 5151.

**Example:** UDP Port=5150

**Dependencies:** This parameter must match the UDP port configured in other units that communicate with the MAX for the specified function.

**Location:** Ethernet > Mod Config > ATMP Options, Ethernet > Mod Config > Stack Options

**See Also:** ATMP Gateway, ATMP Mode, Password, Type, Stack Enabled, Stack Name

## Upload

**Description:** Enables or disables permission to upload the MAX configuration from another device.

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

- Yes means the operator 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 means the MAX uses the factory default Internet profile instead.  
When set to No, the MAX uses factory defaults for options not specified in a 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 means all channels must be assigned a trunk group number to be available for outbound calls.
- No means 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 means 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

## 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 > Encaps Options

**See Also:** Max Unsucc.Calls, VC Timer Val

## VCE Timer Val

**Description:** This 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 an 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

## 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 > Encaps 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

## 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/MPP 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 > IP Options

**See Also:** Route IP, IF Adrs

### WR MgrN (N=1–5)

**Description:** Specify up to five IP addresses of SNMP managers that have SNMP write permission. The MAX 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; this setting indicates no host.

**Example:** WR Mgr1= 10.5.6.7/29

**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 Mgr1-5

# 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 means 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 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 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 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 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. This is the only network type currently supported.

**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 an operator 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 > 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 means 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 means 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 may 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 ten-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 ten-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 ten-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 ten-second 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 means the MAX accepts X.25/PAD calls, provided that they meet all other connection criteria.
- No means 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 Ascend unit parses this string into X.3 profile parameters when an operator 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 Ascend unit 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:** Answer profile: Ethernet > Answer > X.25 Options

Connection profile: Ethernet > Connections > Any 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 > 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 Retransmission Count, T1 Retransmission Timer

# Z

## Zone Name #n

**Description:** Specifies the name of the AppleTalk zone to which the MAX is connected. 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

## MAX Alphabetic Parameter Reference

### Zone Name #n

---

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 an Ascend 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 Ascend 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

## Numerics

- 128K calls 65
- 1536K calls 65
- 1536KR calls 65
- 192K calls 65
- 1st Line 2
- 256K calls 65
- 2nd Adrs 2
- 2nd Line 2
- 384K/H0 calls 64
- 384KR calls 65
- 3rd Prompt 3
- 3rd Prompt Seq 3
- 56K calls 63
- 56KR calls 63
- 64K calls 63, 65
- 7-bit parity, specifying 4
- 7-Even 4

## A

- accounting
  - specifying connection-specific host 5
  - specifying connection-specific server 9
  - specifying multiple hosts 6
  - specifying service 5
  - specifying shared secret 7
  - specifying source port 8
- Acct 5
- Acct Checkpoint 5
- Acct Host 5
- Acct Host #n 6
- Acct Host #N (N=1-3) 6
- Acct Key 7
- Acct Max Retry 7
- Acct Src Port 8
- Acct Timeout 8
- Acct Type 9
- Acct-ID Base 6
- Activ 9

- Activation 10
- Active 10
- Add Number 10
- Add Pers 11
- add-on numbers 53
- address pool. *see* IP address
- addresses, assigning IP 21
- Adv Dialout Routes 11
- AIM calls
  - password for 46
  - remote management during 171
  - remote management of 171
  - specifying call management time period 9
  - specifying start of time period 36
- AIM ports
  - connecting to codec 68
  - dialing from 69
  - pairing for dual port calls 79
  - specifying flag pattern 92
  - specifying whether MAX raises CD 80
  - terminal-timing 209
- AIM setting 48
- Alarm 12
- alarm relay, exceeding bit-error rate 102
- Alarm Threshold 12
- All Port Diag 13
- Allow as Client DNS 13
- Allow Stop Only 14
- ALU
  - configuring 11
  - defined 181
- Analog Encoding 14
- Ans # 15
- Ans n# (n=1-4) 15
- Ans Service 16
- AnsOrig 15
- Answer 16
- Answer profile
  - building connection with RADIUS or TACACS 217
  - specifying time between packets 112
  - time clearing call in inactive session 106
- Answer X.121 Addr 17
- APP Host 17, 18

## Index

### B

---

- APP Port 18
- APP Server 18
- AppleTalk 19
- AppleTalk Router 19
- AppleTalk, Zone Name #n 231
- ARA 20
  - configuring MAX to accept incoming 19
  - disabling Guest access 165
  - specifying maximum connect time for call 134
  - specifying password 153
- ARA setting 86
- Area 20
- AreaType 20
- ARP requests, specifying how MAX responds 167
- Ascend-Shared-Profile-Enable 21
- ASE-tag 21
- Assign Adrs 21
- ATMP
  - ATMP Gateway 22
  - Password 153
  - SAP Reply 179
  - specifying password for 153
  - specifying port 216
  - Type 215
  - type of agent 215
- ATMP Gateway 22
- ATMP Mode 22
- attenuation, specifying for T1 line 40
- Attributes 22
- Attributes, RADIUS 28
- Auth 23
- Auth Boot Host #1 24
- Auth Boot Host #2 24
- Auth Boot Port 25
- Auth Host #n (n=1-3) 25
- Auth Key 25
- Auth Pool 26
- Auth Port 27
- Auth Req 27
- Auth Reset Timeout 28
- Auth Send Attr 6,7 28
- Auth Send PW 32
- Auth Src Port 29
- Auth Timeout 29
- Auth TS Secure 30
- Auth-BERT 31
- authentication
  - by called number 49
  - by calling number 49
  - for Telnet sessions 207
  - incoming for PPP 170
  - local before remote 125
  - outgoing for PPP 184
  - password for incoming PPP call 170
  - password for PPP call 185
  - SecureID DES Encryption 182
  - SecurID Host Retries 182
  - SecurID NodeSecret 183
  - specifying 23, 25
  - specifying disconnect on timeout 73
  - specifying external server 27
  - specifying key for OSPF 30
  - specifying source port 29
  - specifying timeout 29
  - specifying type for OSPF packet exchanges 30
  - timeouts 27
- AuthKey 30
- AuthType 30
- auto byte-error test, specifying 31
- Auto Logout 32
- Auto-Call X.121 Addr 31
- Aux Send PW 32
- Average Line Utilization, *see* ALU

### B

- B&O Restore 33
- B1 Prt/Grp 33
- B1 Slot 33
- B1 Trnk Grp 34
- B1 Usage 34
- back panel alarm relay, specifying no 146
- Back-to-back 34
- Backup 35
- BACP 35
- bandwidth
  - management time periods 211
  - specifying maximum number of channels 133
  - specifying minimum number of channels 137
- Banner 35
- Base Ch Count 36
- Beg Time 36
- Bill # 37
- billing, specifying phone number for 37
- Bit Inversion 37
- bit-error rate
  - exceeding specified value of 102
  - specifying maximum 102
- Block calls after 37
- Blocked duration 38

- 
- BONDING
    - calls, password for 46
    - defined 44
  - BOOTP Relay Enable 38
  - BOOTP, enabling/disabling server 186
  - BRI
    - enabling/disabling 85
    - routing outbound using PRI 72
    - secondary phone number for 181
    - secondary SPID for 182
    - specifying primary phone number for 163
    - specifying primary SPID for 164
  - Bridge 38
  - Bridging 39
  - bridging
    - enabling 38
    - enabling system-wide 39
    - Net Adrs 142
    - specifying broadcast packets to initiate call 71
    - specifying MAC address of remote device 87
    - table, how the MAX uses its 71
  - broadcast packets
    - specifying dial connection when receiving 71
  - Buffer Chars 39
  - Buildout 40
- C**
- calculating
  - Call Filter 42
  - Call Mgm 44
  - Call Mode 43
  - Call Password 46
  - call routing
    - from line #1 to #2 16
    - specifying answer number for 15
    - specifying phone number for 15
    - using B channel port groups 33
    - using B channel slots 33
    - using channel and port groups 54
    - using channel slot numbers 54
    - using exclusive port routing 88
  - Call Type 46
  - Callback 40
  - Call-by-Call 41
  - Call-by-Call n (n=1-6) 42
  - Called # 49
  - Calling # 49
  - calls
    - accepting PPP 160
    - accepting/rejecting Cominet encapsulation 59
    - action following failure to establish codec 89
    - Connection Profile shared by incoming 189
    - determining answer to 16
    - enabling incoming/outgoing 15
    - enabling MP 139
    - enabling MPP 139
    - enabling X.75 231
    - establishes time online before disconnected 133
    - FT1-AIM 44
    - FT-B&O 44
    - how MAX answers 191
    - maximum number of unsuccessful X.25 135
    - monitoring DBA 65
    - outbound PRI 72
    - remote management during AIM 171
    - specifying delay in dual-port 68
    - specifying idle time before disconnecting 106
    - specifying maximum duration for incoming 133
    - specifying maximum time for ARA 134
    - specifying number of channels on 133
    - specifying origin of port 69
    - specifying type of IPX 154
    - specifying when to clear 107
    - spoofing IPX watchdog packets 143
    - TCP-Clear 205
    - using channels of idle link for 162
    - verifying password for PPP 170
    - with no Connection profile 165
    - See also MP calls, MPP calls, phone numbers
  - calls, enabling MPP 139
  - CBCP Enable 50
  - CBCP Mode 50
  - CBCP Trunk Group 50
  - CD (Carrier Detect), raising 80
  - Cell First 51
  - Cell Level 51
  - cellular phone
    - MAX answering 51
    - specifying transmit and receive level 51
  - Ch n # 52
  - Ch n (Ch 1, Ch 2...) 52
  - Ch n (Ch1, ch2...) 52
  - Ch n Prt/Grp 54
  - Ch n Slot 54
  - Ch n Trnk Grp 54
  - channels
    - assigning to trunk groups 54
    - simultaneously connection/disconnecting 152
    - specifying usage 52
  - Circuit 55
  - circuits, specifying Frame Relay 55
  - Clear 55
  - Clear Call 56
  - Clid Auth 105
-

## Index

### D

---

- Client 56
  - Client #n 56
  - Client Assign DNS 57
  - Client Gateway 57
  - Client Pri DNS 57
  - Client Sec DNS 58
  - Clock Source 58
  - Clr Scrn 58
  - codec (COder/DECoder)
    - connecting to AIM ports 68
    - defined 17
    - terminal-timing 209
  - COMB 59
  - COMB setting 86
  - Combinet
    - calls, specifying whether to accept or reject 59
    - compression for 60
    - Interval 112
    - password 170
  - Comm 59
  - commands, DO
    - limiting access to 148
  - community name
    - enable read/write 168
    - read 169
    - read/write 168
  - Compare 59
  - Compression 60
  - compression
    - IP header 220
    - specifying PPP, MP, and MP+ 123
  - configuring
    - data service calls
      - for 384K/HO 64
      - for 56K calls 63
      - for 56KR 63
      - for 64K 63
    - data service calls for
      - 128K 65
      - 1536K 65
      - 1536KR 65
      - 192K 65
      - 256K 65
      - 384KR 65
      - 64K 65
      - multirate 65
  - Connection # 60
  - Connection profile
    - backing up nailed connection 35
    - requiring 165
    - sharing among users 189
    - specifying as multicast profile 135
  - connections
    - accepting PPP 160
    - bringing up for IPX query 72
    - bringing up when MAX receives broadcast packet 71
    - enabling raw-TCP 205
    - name of remote device 197
    - specifying an idle timeout 106
    - specifying compression for 123
    - specifying dial out number 70
    - specifying when to clear 107
    - specifying whether to accept Combinet 59
  - Console 61
  - Contact 61
  - control port, baud rate of 209
  - Cost 61
  - CUG Index 62
- ### D
- Data Filter 62
  - data filter, specifying number of 90
  - data service, defined 63
  - Data Svc 63
  - Date 65
  - DBA
    - configuring 11
    - monitoring calls 65
    - seconds below ALU 198
    - specifying algorithm 80
    - specifying number of channels to add 111
    - specifying number of channels to remove 67
    - specifying time period for calculating ALU 181
    - target utilization 205
  - DBA Monitor 65
  - DCE Addr 66
  - DCE N392 66
  - DCE N393 66
  - DeadInterval 66
  - Dec Ch Count 67
  - Def Telnet 68
  - default routes
    - specifying connection-specific 57
    - specifying whether MAX ignores 107
  - Default Zone 67
  - Delay Dual 68
  - Delete Digits 68
  - Dest 69
  - destination
    - network, identifying distance to 210
    - port, specifying 77
    - port, specifying comparison 77
    - specifying address for filtering 76

- hr/>
- destination, *continued*
    - specifying route 69
  - DHCP
    - Reply Enabled 172
    - specifying maximum lease time 134
  - diagnostics
    - setting permissions for port 13
  - Dial 69
  - Dial # 70
  - Dial Brdcast 71
  - Dial n# (n=1-6) 71
  - Dial Plan 72
  - Dial Query 72
  - dialin users, specifying whether to drop 30
  - Dialout OK 73
  - dialout, specifying modem 137
  - digital modems, subaddresses 74
  - Direct Call Addr 73
  - disabling lines, T1 or E1 2
  - Disc on Auth Timeout 73
  - DLCI 74
    - specifying endpoint 55
  - DM 74
  - DNS
    - Allow as Client DNS 13
    - Client Assign DNS 57
    - Client Pri DNS 57
    - Client Sec DNS 58
    - Domain Name 74
    - List Attempt 124
    - List Size 124
    - Pri DNS 163
    - Sec DNS 180
    - secondary domain Name 180
    - secondary domain name server 180
    - specifying connection-specific servers 57, 58
    - specifying domain name server 163
  - DO commands, limiting access to 148
  - Domain Name 74
  - domain name server 163, 180
  - Download 75
  - DownMetric 75
  - DownPreference 75
  - DPNSS lines, setting back-to-back 34
  - Drop-and-Insert
    - enabling/disabling 2
    - framing mode for 97
  - DS0 Min Rst 76
  - DS0 minutes 76
    - specifying maximum 133
  - Dst Adrs 76
  - Dst Mask 77
  - Dst Port # 77
  - Dst Port Cmp 77
  - DTE Addr 78
  - DTE init. mode 78
  - DTE N392 79
  - DTE N393 79
  - dual IP, configuring 2
  - Dual Ports 79
  - dual-port calls
    - specifying delay between first and second 68
    - specifying whether to pair ports 159
  - Dyn Alg 80
  - dynamic addresses
    - assigning 21
    - requiring for callers 156
    - specifying first address in pool 157
    - specifying number in address pool 156
    - specifying pool for RADIUS-authenticated calls 26
    - specifying pool to use for callers 156
  - dynamic bandwidth, using BACP 35
- E**
- E1 lines
    - enabling/disabling 2
    - setting back-to-back 34
    - specifying clock source 58
    - specifying retransmissions for 145
  - Early CD 80
  - Edit 81
  - Edit All Calls 81
  - Edit All Ports 82
  - Edit Com Call 82
  - Edit Cur Call 82
  - Edit Line 83
  - Edit Own Call 83
  - Edit Own Port 84
  - Edit Security 84
  - Edit System 84
  - Enable ASBR 84
  - Enable Local DNS Table 85
  - Enabled 85
  - enabling third-party routing for OSPF 210
  - Encaps 85
  - Encaps Type 86
  - encapsulation, specifying 85
  - Encoding 86
  - encoding, specifying 14

## Index

### F

---

encryption  
specifying type for SecureID 182

Ent Adrs 87

escape characters, for RS-366 178

EU-RAW 88

EU-UI 88

Excl Routing 88

Exp Callback 89

extended dial plan, specifying 72

Extended Superframe format 97

### F

Facilities Data Link, *see* FDL

Fail Action 89

FDL 89, 90

Field Service 90

field service operations, privileges to perform 90

Filter 90

Filter Persistence 91

filtering

- enabling/disabling filter 219
- including/excluding advertisements in IPX SAP 187
- source IP address 194
- source IP address mask 194
- source port 195
- specifying action of 215
- specifying an IPX SAP filter 117
- specifying call 42
- specifying comparison 59
- specifying destination port comparison 77
- specifying hex number to compare 219
- specifying number of data filter 90
- specifying type of comparison for source ports 195
- specifying whether should match established connections 205
- specifying whether to forward or drop packets 92
- specifying whether to include next filter 139
- watchdog packets 143

filters

- mask 77
- order applied 62
- persistence of 91
- protocol 166
- SAM numbering scheme in VT-100 interface 62
- specifying data filter 62
- specifying destination 77
- specifying destination address 76
- specifying mask 130
- specifying number of bytes to test in Generic 121
- specifying offset 147

Finger 91

firewalls

- numbers in Firewall menu 43
- SAM numbering scheme in VT-100 interface 62
- specifying number of 90

Flag Idle 92

flag pattern, specifying 92

Force56 92

Forward 92

Forwarding 93

FR 93

FR Direct 94

FR DLCI 94

FR Prof 94

FR setting 86

FR Type 95

Frame Length 95

Frame Relay

- DCE N392 66
- DCE N393 66
- DLCI 74
- DTE N392 79
- DTE N393 79
- FR 93
- FR Direct 94
- FR DLCI 94
- FR Prof 94
- FR Type 95
- Link Mgmt 123
- N391 141
- Nailed Grp 142
- NNI and UNI-DTE connections 95
- querying for DLCI status 95
- redirect connection 94
- specifying DLCI endpoint 55
- specifying DLCI for redirect connection 94

Framed Addr Start 96

Framed Only 96

FT1 Caller 97

FT1 setting 48

FT1-AIM setting 48

FT1-B&O setting 48

### G

Gateway 98

gateway, specifying connection-specific 57

Group 98



## **H**

Handle IPX 99  
Handle IPX Type 20 100  
HeartBeat Addr 100  
HeartBeat Slot Count 101  
HeartBeat Slot Time 101  
HeartBeat Udp Port 100  
heartbeat, setting alarm threshold 12  
HelloInterval 102  
High BER 102  
High BER Alarm 102  
Hop Count 103  
Host #n Addr (n=1-4) 103  
Host #n Text (n=1-4) 104  
Host init. mode 103  
Host/6 module, FT1-B&O calls on 159  
Host/BRI 72  
Hunt-n (N=1-3) 104

## **I**

ICMP Redirects 105  
ID Auth 105  
ID Fail Busy (previously CLID Fail Busy) 106  
Idle 106  
idle channels, specifying when to reuse 162  
Idle Logout 106  
Idle Pct 107  
idle timer, resetting 42  
IF Adrs 107  
Ignore Def Rt 107  
Imm. Modem Access 108  
Imm. Modem Port 108  
Imm. Modem Pwd 109  
Immed Host 109  
Immed Port 109  
Immed Service 110  
Immediate Modem 110  
immediate service  
    specifying host 109  
    specifying port 109  
    specifying type of 110  
Inactivity Timer 111  
inband signaling, specifying 176  
inbound packets, specifying address for 113  
Inc Ch Count 111  
incoming call routing 198

    enabling/disabling trunk groups 217  
    Serial 186  
    specifying subaddress 120  
    subaddress for V.110 modem 218  
Inherit setting (Dial Plan Profile only) 64  
Initial Scrn 112  
Input Sample Count 111  
interfaces, specifying address for 107  
Interval 112  
inverse multiplexing, defined 45  
IP (Internet Protocol)  
    assigning two interface addresses 2  
    dynamic address assignment 157  
IP Addr Msg 112  
IP address  
    of device used in Telnet or raw TCP 109  
    of primary domain name server 163  
    of remote interface to WAN 221  
    of secondary domain name server 180  
    remote device address 221  
    requiring dynamic 156  
    secondary domain name server 180  
    specified for remote end station/router 120  
    specifying address pool to use for callers 156  
    specifying first address in pool 157  
    specifying for remote device 120  
    specifying interface address 107  
    specifying maximum time for DHCP address 134  
    specifying number in address pool 156  
    specifying router 98  
    specifying which to use for NAT clients  
IP Adrs 112  
IP dialout routes, poisoning 11  
IP Direct 113  
IP Gateway Addr Msg 113  
IP Netmask Msg 113  
IP routing, enabling 177  
IPX  
    assigning network number to point-to-point link 114  
    Dial Query 72  
    enabling routing 177  
    filtering watchdog packets 143  
    Handle IPX Type 20 100  
    Hop Count 103  
    IPX Alias 114  
    IPX Enet# 114  
    IPX Frame 114  
    IPX Net# 115  
    IPX Pool # 115  
    IPX RIP 116  
    IPX SAP 116  
    IPX SAP Filter 117  
    NetWare t/o 143  
    Network 144

## Index

### K

---

#### IPX, *continued*

- Node 145
- Peer 154
- SAP Reply 179
- SAP service type 187
- Server Name 187
- Server Type 187
- specifying a virtual network address 115
- specifying how SAP packets are handled 116
- specifying internal network number of server 144
- specifying IPX address for 114
- specifying network number for remote router 115
- specifying node address of server 145
- specifying type of bridging 99

IPX Enet# 114

IPX Frame 114

IPX Net# 115

IPX network, specifying distance to destination 103

IPX Pool# 115

IPX RIP 116

IPX Routing 116

IPX routing, enabling 116

IPX SAP 116

#### ISDN

- secondary phone number for BRI 181
- secondary SPID for BRI 182
- specifying BRI mode 123
- specifying primary phone number for BRI 163
- specifying primary SPID for BRI 164
- specifying subaddress 120
- subaddressing 198
- subaddressing 186

### K

K Window Size 117

### L

L2 End 118

L2TP Mode 118

L3 End 118

LAN 120

LAN Adrs 120

LAPB k 119

LAPB N2 119

LAPB T1 119

LAPB T2 119

LCN 120

Length 121

Line n tunnel type 122

lines, enabling/disabling T1 or E1 2

Link Access Type 122

Link Comp 123

Link Mgmt 123

Link Quality Monitoring *see* LQM

link quality reports, specifying duration between 129

Link Type 123

List Attempt 124

List Size 124

Listen X.121 Addr 122

Loc. DNS Tab Auto Update 126

Local Echo 125

Local Profiles First 125

Location 126

Log Facility 127

Log Host 127

login

- defining sequence of prompts 3

- whether RADIUS configures banner 171

Login Host 127

Login Port 128

Login Prompt 128

login prompts 3

Login Timeout 128

logout, specifying timeout 106

loop start 176

LoopAvoidance 129

LQM 129

LQM Max 129

LQM Min 129

LQM, defined 129

LSA-type 130

LSUs, delay 214

### M

Mask 130

#### MAX

- assigning to stack 196

- enabling stacks 196

- how it answers calls 191

- ringback tone generated by 137

- setting date 65

- specifying administrative logout 106

- specifying IP address of 112

- specifying IPX address for Ethernet interface 114

- specifying Location 126

- uploading/downloading configuration 75

- using interface-based routing 107

Max ATMP Tunnels 132  
 Max Baud 132  
 Max Call Duration 133  
 Max Call Mins 133  
 Max Ch Count 133  
 Max DS0 Mins 133  
 Max Leases 134  
 Max Unsucc. Calls 135  
 Max. Block Size 132  
 Max. Time 134  
 Mbone profile 135  
 Method of host notif 136  
 Metric 136  
 Min Ch Count 137  
 Modem  
     NumPlanID 137  
     PRI # Type 138  
 modem calls, configuring data service for 64  
 Modem Dialout 137  
 modem dial-out 138  
 modem dialout,enabling 73  
 Modem Ringback 137  
 Modem Ringback, setting 137  
 Modem setting 64  
 modem strings, for cellular phones 51  
 modems  
     enabling dialout 137  
     specifying highest baud rate for V.34 132  
     specifying immediate 108  
     specifying immediate service 110  
     specifying transmit level for digital 135  
     V42/MNP  
         error control 218  
 Module Name 138  
 More 139  
 MP 139  
 MP calls, using BACP 35  
 MP+ calls, specifying how to monitor 65  
 MPP 139  
 MPP setting 86  
 MRU 140  
 Multicast  
     Alarm Threshold 12  
     Client 56  
     excluding address from heartbeat monitoring 194  
     Forwarding 93  
     HeartBeat Addr 100  
     HeartBeat Slot Count 101  
     HeartBeat Slot Time 101  
     HeartBeat Udp Port 100  
     Mbone profile 135

Multicast Client 140  
 Multicast Rate Limit 141  
     Rate Limit 169  
     Source Addr 193  
     Source Mask 194  
 Multicast Client 140  
 Multicast forwarding  
     changing a configuration 93  
     enabling multicast traffic 141, 169  
 Multicast Rate Limit 141  
 multichannel calls  
     specifying algorithm for monitoring usage 80  
     specifying how many channels to add 111  
     specifying how many channels to remove 67  
     specifying password for 32  
 Multilink calls, enabling 139  
 multipoint link, specifying 123  
 multirate calls 65

## **N**

N2 Retransmission Count 141  
 N391 141  
 nailed channels  
     assigning to group 98  
     MAX dropping 33  
 nailed connection, specifying backup 35  
 Nailed Grp 142  
 Nailed setting 46  
 Nailed/MPP setting 47  
 Name 142  
 Name/Password profile  
     building a connection profile 209  
 NAT  
     Max Leases 134  
     Pool Number 157  
     Reply Enabled 172  
     whether MAX acts as DHCP server for 172  
 Net Adrs 142  
 Net End 143  
 Net Start 144  
 NetWare t/o 143  
 Network 144  
 network summarization, using 158  
 New NASPort ID 145  
 NFAS ID Num 145  
 NFAS, ID for line using 145  
 NL Value 145  
 NNI Frame Relay connection, specifying 95  
 No Trunk Alarm 146

## Index

### O

Node 145  
NSSA-Type 146  
NUI 146  
NumPlanID 147

### O

Offset 147  
Operations 148  
Option 148  
OSPF  
    Area 20  
    AreaType 20  
    assigning tag to RIP routes 175  
    Auth Key 30  
    Auth Type 30  
    Cost 61  
    DeadInterval 66  
    designated router election 164  
    Enable ASBR 84  
    enabling third-party routing 210  
    enabling/disabling 178  
    Hello Interval 102  
    metrics and costs 149  
    OSPF Preference 149  
    Ospf-Cost 149  
    Priority 164  
    Retransmit Interval 172  
    RIP Preference 174  
    RipASETtype 174  
    RunOSPF 178  
    specifying cost of link 61  
    specifying retransmission interval 172  
    stub areas 20  
    Third-Party 210  
    Transit Delay 214  
OSPF ASE Preference 149  
OSPF Preference 149  
Ospf-Cost 149  
outgoing call routing  
    specifying trunk group to use 148  
out-of-band signaling 190  
Own Port Diag 150

### P

Packet Characters 150  
Packet Wait time 151  
packets  
    masked bytes from start of 147  
    passed to next filter specification 139  
    specifying whether to forward or drop 92

Palmtop 151  
Palmtop Menus 151  
Palmtop Port # 151  
Parallel Dial 152  
parameters, alphabetic listing 1  
parity, specifying 7-bit even 4  
Passwd 152  
Passwd Prompt 152  
Password 153  
Password Req'd 153  
passwords  
    Combinet 170  
    for AIM or BONDING calls 46, 160  
    for incoming PPP 170  
    for PPP 185  
    Imm Modem Pwd and Imm Modem Access 108  
    not saved when you save configuration 75  
    specifying ARA 153  
    specifying ATMP 153  
    specifying for multichannel calls 32  
    Telnet 208  
    terminal server 152  
PBX Type 153  
PBX, configuring 68  
Peer 154  
Peer (AppleTalk Options) 154  
Perm/Switched setting 47  
permanent virtual circuit, *see* PVC 55  
phone numbers  
    assigning to switched channels 52  
    specifying answer number 15  
    specifying number used to dial out 70  
    specifying number used to route T1 15  
PID selection 155  
Pool 156  
Pool #n Count 156  
Pool #N name (N=1-10) 157  
Pool #n Start 157  
Pool Number 157  
Pool Only 156  
Pool OSPF Adv Type 158  
Pool Summary 158  
Port 159  
Port 1/2 Dual 159  
port diagnostics, performing 150  
Port Name 159  
Port Password 160  
ports  
    authentication 27  
    specifying accounting source 8  
    specifying destination in filter 77

PPP 160  
PPP calls, accepting 160  
PPP Delay 160  
PPP Direct 161  
PPP Info 161  
PPP setting 86  
PPP, specifying whether to start immediately 161  
PPTP Enabled 161  
Preempt 162  
Preference 162  
preference  
    default values for 149  
    for static route 196  
    RIP 174  
Preferences, *see* Routing  
PRI # Type 162  
Pri DNS 163  
PRI lines, specifying maximum bit-error rate 102  
Pri Num 163  
PRI service, specifying 42  
Pri SPID 164  
Pri WINS 124, 165  
primary domain name server, IP address of 163  
primary port, defined 45  
Priority 164  
PRI-T1 conversion 111  
Private 165  
Profile Req'd 165  
Prompt 166  
Prompt Format 166  
prompts  
    defining sequence of login 3  
    login 3  
    multiple line 166  
    specifying multiple line 128  
Protocol 166  
protocols, type to filter 166  
Proxy Mode 167  
PVC  
    defined 55  
    specifying logical channel for X.25 120

## Q

Queue Depth 168

## R

R/W Comm 168

R/W Comm Enable 168

### RADIUS

    accounting timer 188  
    Acct Host #N (N=1-3) 6  
    Acct Key 7  
    Acct Port 7  
    Acct Src Port 8  
    Acct Timeout 8  
    Acct-ID Base 6  
    Attributes 22  
    Auth 23  
    Auth Pool 26  
    Auth Send Attr 6,7 28  
    Auth TS Secure 30  
    Client #n 56  
    enabling/disabling onboard 186  
    port for onboard server 187  
    Server Key 186  
    Server Port 187  
    Sess Timer 188  
    Session Key 188  
    session keys 188  
    sharing profiles 189  
    specifying clients 56  
    Use Answer as Default 217  
    whether it configure login banner 171

RADIUS accounting 7, 14

RADIUS server  
    remote configuration by 171

Rate Limit 169

### raw TCP

    directing raw sessions to host 127  
    directing raw sessions to port 128

RD Mgr1-5 169

Read Comm 169

recovered loop timing mode 58

Recv Auth 170

Recv PW 170

Red Alarm mode 58

Remote Conf 171

remote loopback 44

remote management  
    during AIM call 171

Remote Mgmt 171

Remote X.121 Addr 171

Reply Enabled 172

retransmissions, specifying number for E1 lines 145

Retransmit Interval 172

Retry limit 172

Reverse Charge 173

ringback tone, specifying 137

## Index

### S

- RIP 173, 175
    - assigning tag to routes propagated into OSPF 175
    - how MAX handles updates 173
    - how routes are propagated 174
    - how routes are propagated into OSPF 174
    - summarizing routes 175
  - RIP Policy 174
  - Rip Preference 174
  - Rip Queue Depth 175
  - RIP Summary 175
  - RIP tag 175
  - RipASETtype 174
  - Rlogin 175
  - Rlogin, default terminal type for 210
  - Rob Ctl 176
  - robbed-bit
    - call control mechanism 176
    - signaling 189
  - Route AppleTalk 177
  - Route IP 177
  - Route IPX 177
  - Route line n 178
  - route preferences, default values of 149
  - routes 210
    - how MAX handles RIP updates 173
    - how RIP are propagated 174
    - how RIP are propagated into OSPF 174
    - poisoning dialout 11
    - preference for RIP 174
    - preference for static 196
    - specifying destination 69
    - specifying preference for 162
    - specifying whether MAX ignores default 107
    - specifying whether private 165
    - summarizing 158
    - summarizing RIP 175
  - routing
    - enabling IP 177
    - enabling IPX 177
    - how the MAX places entries in table 149
    - specifying preference for OSPF 149
  - routing outbound using PRI 72
  - RPOA 178
  - RS-366 Esc 178
  - RunOSPF 178
- S**
- SAM
    - firewall numbering scheme in VT-100 interface 62
    - version number of 220
  - SAP
    - specifying a filter for 117
    - tables, exchanged by both ends of connection 116
  - SAP HS Proxy 179
  - SAP HS Proxy Net#n (n=1-6) 179
  - SAP Reply 179
  - Sealing Current 180
  - Sec DNS 180
  - Sec Domain Name 180
  - Sec History 181
  - Sec Num 181
  - Sec SPID 182
  - Sec WINS 184
  - secondary domain name server, IP address of 180
  - secondary port, defined 45
  - SecureID
    - SecureID DES Encryption 182
    - SecurID Host Retries 182
    - SecurID NodeSecret 183
  - SecurID DES Encryption 182
  - SecurID Host Retries 182
  - SecurID NodeSecret 183
  - Security 183
  - security 105
    - APP Host 17
    - APP Port 18
    - APP Server 18
    - enabling/disabling 183
    - incoming PPP call authentication 170
    - incoming PPP call password 170
    - local authentication before remote 125
    - password for terminal server or Security profile 152
    - passwords for AIM or BONDING calls 160
    - PPP call authentication 184
    - PPP call password 185
    - required Connection profile 165
    - requiring password for Combinet connection 153
    - requiring password for Combinet connections 153
    - setting permissions for diagnostics 200
    - setting permissions for uploading configuration 216
    - specifying number of firewall 90
    - specifying permission for field service 90
    - specifying permissions for configuration 148
    - specifying permissions for configuring port 150
    - specifying permissions to edit Call profiles 82
    - specifying permissions to edit Call/Connection profiles 81
    - specifying permissions to edit own Call profile 83
    - specifying permissions to edit own Port profiles 84
    - specifying permissions to edit Port profiles 82
    - specifying permissions to edit Security profiles 84
    - specifying permissions to edit System profile 84
    - specifying permissions to Read Comm/R/W Comm strings 84
    - turning off ICMP redirects 105

- 
- security, *continued*
    - using callback 89
  - Send Auth 184
  - Send Disc 185
  - Send PW 185
  - Serial 186
  - serial port
    - baud rate of 209
    - specifying when to logout user 32
  - Serial WAN
    - Activation 10
    - Nailed Grp 142
  - Server 186
  - Server Key 186
  - Server Name 187
  - Server Port 187
  - Server Type 187
  - Sess Timer 188
  - Session Key 188
  - settings
    - FT1 48
    - FT1-AIM 48
    - FT1-B&O 48
    - Nailed 46
    - Nailed/MPP 47
    - Perm/Switched 47
    - Switched 47
  - Shared Prof 189
  - shared secret, defined 7
  - Sig Mode 189
  - signaling
    - conversion 153
    - E1 and T1 189
    - robbed-bit 189
    - specifying 189
  - Silent 191
  - Single Answer 191
  - SLIP 191
  - SLIP BOOTP 191, 192
  - SLIP Info 192
  - SNMP 168
    - Comm 59
    - community name 59
    - enable read/write (set commands) 168
    - enabling/disabling security 183
    - manager's IP addresses 169
    - managers 221
    - read community name 169
    - read/write community name 168
    - sending traps 12
  - SNMP traps
    - multicast heartbeat 12
    - specifying destination for 69
    - specifying whether to send AIM 159
  - SNTP
    - Enabled 192
    - enabling 192
    - Host #n 193
    - servers 193
  - Socket 193
  - socket 175
  - Source Addr 193
  - Source Mask 194
  - SPID
    - secondary for BRI 182
    - specifying primary for BRI 164
  - Src Adrs 194
  - Src Mask 194
  - Src Port # 195
  - Src Port Cmp 195
  - Stack Name 196
  - Stacking Enabled 196
  - stacks
    - enabling 196
    - maximum number of channels in 196
    - naming 196
    - specifying port 216
  - Static Preference 196
  - static routes
    - enabling OSPF third-party routing 210
    - specifying preference for 196
  - Station 197
  - Status 1-8 197
  - Status Enquiry messages, timing between 202
  - status windows
    - specifying how they appear 197
    - specifying which are displayed 81
  - stub area, defined 20
  - Sub Pers 198
  - subaddress
    - digital modem 74
    - for V.110 modem 218
    - specifying ISDN 120
  - Sub-Adr 198
  - subaddressing 198
  - Superframe format 97
  - Switch Type 199
  - Switched setting 47
  - Sys Diag 200
  - Syslog
    - specifying how logs are sorted 127
    - specifying IP address of host 127
    - specifying the types of messages MAX sends 200
-

**T**

## T1 lines

- enabling/disabling 2
- inband signaling 176
- retransmission timer 202
- signaling 189
- signaling conversion for PBX 153
- specifying attenuation for 40
- specifying cable length 121
- specifying clock source 58
- specifying encoding 86
- specifying FDL 89
- specifying no alarm 146
- specifying number of channels 152

## T1 Retransmission Timer 202

## T1-PRI

- conversion 201
- NumPlanID 201
- PRI # Type 201

## T302 Timer 202

## T391 202

## T392 203

## T3POS T1 203

## T3POS T2 203

## T3POS T3 204

## T3POS T4 204

## T3POS T5 204

## T3POS T6 204

## TACACS+

- Acct Host #N (N=1-3) 6
- Acct Key 7
- Acct Port 7
- Acct Src Port 8
- Auth 23

## TACACS, Use Answer as Default 217

## Target Util 205

## TCP

- directing raw sessions to host 127
- directing raw sessions to port 128

## TCP connections, matching filter to 205

## TCP Estab 205

## TCP Modem Enabled 206

## TCP Modem Port 206

## TCP timeout 206

## TCP-Clear 205

## TCP-CLEAR setting 86

## TEI 207

## Telnet 207

- authentication for 207
- connecting to non-standard ports 125
- default terminal type for 210

- enabling/disabling 207

- passwords 208

- setting default mode 207

- specifying what MAX interprets as hostnames 68

## Telnet Host Auth 207

## Telnet mode 207

## Telnet PW 208

## Template Connection # 209

## Term Rate 209

## Term Timing 209

## Term Type 210

## terminal server 112

- default terminal type 210

- enabling 214

- enabling SLIP calls 191

- enabling/disabling security 183

- Host #n Addr (n=1-4) 103

- Host #n Text (n=1-4) 104

- idle time before disconnect 214

- if MAX uses 214

- IP Addr Msg 112

- Local Echo 125

- Login Host 127

- Login Port 128

- Login Prompt 128

- Login Timeout 128

- Packet Characters 150

- Packet Wait time 151

- Passwd 152

- Passwd Prompt 152

- PPP delay 160

- PPP Direct 161

- PPP Info 161

- Prompt 166

- Prompt Format 166

- Rlogin 175

- Silent 191

- SLIP 191

- SLIP BOOTP 191

- specifying banner 35

- specifying how MAX interprets hostnames 68

- specifying IP address message string 112

- specifying message to display at beginning of PPP session 161

- specifying toggling between menus and command line mode 213

- specifying when to clear session 56

- specifying whether to clear screen 58

- suppressing status messages 191

- Telnet 207

- Telnet Mode 207

- Telnet mode 207

- Telnet PW 208

- Toggle Scrn 213

- TS Enabled 214



terminal server, *continued*  
    TS Idle 214  
    TS Idle Mode 214  
    whether RADIUS configure login banner 171  
Terminal Timing signal, using 209  
terminal type, specifying 210  
Third-Party 210  
Tick Count 210  
Time 211  
Time Period 1-4 211  
Time Zone 211  
time, setting 211  
timeout  
    authentication 29  
    specifying disconnect on failed authentication 73  
    specifying login timeout 128  
Timeout Busy (previously CLID Timeout Busy) 211  
Toggle Scrn 213  
T-Online 200  
Transit # 213  
TransitDelay 214  
traps  
    multicast 12  
    sending 12  
trunk groups  
    assigning B channel to 34  
    assigning channel to 54  
    enabling/disabling 217  
    specifying how MAX selects 148  
TS Enabled 214  
TS Idle 214  
TS Idle Mode 214  
tunnelling  
    enabling PPTP 161  
Type 215

## U

UDP Cksum 215  
UDP Port 216  
Upload 216  
Use Answer as Default 217  
Use Trunk Grps 217

## V

V.110 218  
    calls, configuring data service for 64  
V.120 218

V.120 calls  
    accepting 218  
    specifying maximum length of information field 95  
V.34 modems, specifying highest baud rate for 132  
V42/MNP 218  
V42/MNP error control, enabling 218  
Valid 219  
Value 219  
VC Timer enable 219  
VCE Timer Val 219  
Version 220  
VJ Comp 220  
Voice calls  
    configuring data service for 64  
    notes on using 64  
Voice setting 16, 64  
VT-100 port, specifying control interface at 61

## W

WAN alias 221  
watchdog spoofing 143  
window  
    K Window Size 117  
WINS  
    secondary server 184  
    specifying primary WINS server 165  
WR Mgr 1-5 221

## X

X.121 Source Address 222  
X.25  
    Call Mode 43  
    Encaps Type 86  
    LCN 120  
    Max Unsucc. Calls 135  
    Nailed Grp 142  
    Remote X.121 Addr 171  
    specifying inactivity timer 111  
    specifying logical channels 120  
    VC Timer enable 219  
    VCE Timer Val 219  
X.25 Clear/Diag 222  
X.25 Default Packet Size 226  
X.25 Highest PVC 222  
X.25 Highest SVC 223  
X.25 Link Setup Mode 223  
X.25 Lowest PVC 223  
X.25 Lowest SVC 224

## Index

### Z

---

- X.25 Max Packet Size 224
- X.25 Min Packet Size 224
- X.25 Network Type 225
- X.25 Node Type 225
- X.25 Options 225
- X.25 PAD, specifying address for immediate service 31
- X.25 Prof 226
- X.25 R20 226
- X.25 R22 226
- X.25 R23 227
- X.25 Reset/Diag 227
- X.25 Restart/Diag 228
- X.25 Seq Number Mode 228
- X.25 T20 228
- X.25 T21 229
- X.25 T22 229
- X.25 T23 229
- X.25 Window Size 229
- X.3 Custom 230
- X.3 Param Prof 231
- X.75 231
  - calls, specifying maximum length of information field 95
  - EU-RAW 88
  - EU-UI 88
  - K Window Size 117
  - N2 Retransmission Count 141
- X25/PAD 230

### Z

- Zone Name #n 231