MAX 1800
Reference Guide

Ascend Communications, Inc.

Part Number 7820-0409-002 July 18, 1997

Ascend Customer Service

When you contact Ascend Customer Service, make sure you have this information:

- The product name and model
- The software and hardware options
- The software version
- Whether you are routing or bridging with your Ascend product
- The type of computer you are using
- A description of the problem

How to contact Ascend Customer Service

If you need Technical Assistance, contact Ascend in one of the following ways:

Telephone in the United States	800-ASCEND-4 (800-272-3634)
Telephone outside the United States	510-769-8027 (800-697-4772)
- UK	(+33) 492 96 5671
- Germany/Austria/Switzerland	(+33) 492 96 5672
- France	(+33) 492 96 5673
- Benelux	(+33) 492 96 5674
- Spain/Portugal	(+33) 492 96 5675
- Italy	(+33) 492 96 5676
- Scandinavia	(+33) 492 96 5677
- Middle East and Africa	(+33) 492 96 5679
E-mail	support@ascend.com
E-mail (outside US)	EMEAsupport@ascend.com
Facsimile (FAX)	510-814-2312
Customer Support BBS by modem	510-814-2302

You can also contact the Ascend main office by dialing 510-769-6001, or you can write to Ascend at the following address:

Ascend Communications
One Ascend Plaza
1701 Harbor Bay Parkway
Alameda, CA 94502-3002

Need information on new features and products?

We are committed to constantly improving our products. You can find out about new features and product improvement as follows:

- For the latest information on the Ascend product line, visit our site on the World Wide Web:
  `http://www.ascend.com/`
- For software upgrades, release notes, and addenda to this manual, visit our FTP site:
  `ftp.ascend.com`

Contents

Figures

Tables

DO Command Reference

1

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

Using DO commands

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

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

To type a DO command, press and release the Palmtop's DO key or the vt100 interface Ctrl-D combination, and then press and release the next key in the sequence; for example, press 1 to invoke the DO 1 (Dial) command. The PF1 function key on a vt100 monitor is equivalent to the DO key or Ctrl-D.

List of supported commands

Table 1-1 lists the DO commands. Different commands are available in the DO menu depending on your location in the vt100 menus and your permission level.

Table 1-1. DO commands

Command	Description
Answer (DO 3)	Answer an incoming call.
Beg/End BERT (DO 7)	Begin/End a byte-error test.
Beg/End Rem LB (DO 6)	Begin/End a remote loopback.
Beg/End Rem Mgm (DO 8)	Begin/End remote management.
Close TELNET (DO C)	Close the current Telnet session.
Contract BW (DO 5)	Decrease bandwidth.
Diagnostics (DO D)	Access the diagnostic interface.
Dial (DO 1)	Dial the selected or current profile.
ESC (DO 0)	Abort and exit the DO menu.
Extend BW (DO 4)	Increase bandwidth.
Hang Up (DO 2)	Hang up from a call in progress.
Load (DO L)	Load parameter values into the current profile.
Menu Save (DO M) 8	Save the vt100 interface menu layout.

Table 1-1. DO commands (continued)

Command	Description
Password (DO P) 9	Log into or out of the MAX.
Resynchronize (DO R)	Resynchronize a call in progress.
Save (DO S)	Save parameter values into the specified profile.
Termserv (DO E)	Access the terminal server interface.

Example use of DO commands to place and clear a call

To manually place a call, the Connection profile for that call must be open or selected in the list of profiles. To clear a call, you can either open the Connection profile for the active connection, or tab over to the status window in which that connection is listed. (See Chapter 2, "Status Window Reference.") For example:

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

2 Press Ctrl-D to invoke the DO menu.

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

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

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

To manually clear a call:

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

2 Press Ctrl-D to open the DO menu.

When you open the DO menu for an active session, it looks similar to this:

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

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

The status window will indicate when the call has been terminated.

DO command reference in alphabetic order

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

Answer (DO 3)

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

Beg/End BERT (DO 7)

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

When you select DO Beg/End BERT, these events take place:

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

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

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

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

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

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

Keep this additional information in mind:

- No user data transfer takes place in either direction during a BERT.
- All commands that affect the call are disabled, except the command that ends the BERT.
- You must be in a port-specific edit menu or status window to use the DO Beg/End BERT command.
- You can run the BERT in only one direction at a time; that is, only one side can be the requester.
- To allow the MAX time to complete handshaking, you must wait at least 20 seconds between toggling the BERT on and off.
- The DO Beg/End BERT command does not appear if you are not logged in with operational privileges.

For related information, see the Operations parameter in Chapter 3, “MAX Alphabetic Parameter Reference,” and the Line Errors, Session Err, Port Info, Call Status, and Statistics sections in Chapter 2, “Status Window Reference.”

Beg/End Rem LB (DO 6)

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

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

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

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

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

Keep this additional information in mind:

- A remote loopback disables data flow from the remote host, but the call remains online.
- A remote loopback disables Dynamic Bandwidth Allocation.
- Only switched and nailed-up channels active during the current call are looped back.
- Drop-and-Insert channels are not looped back.
- You must be in a port-specific edit menu or status window to use the DO Beg/End LB command.
- To allow the MAX time to complete handshaking, you must wait at least 20 seconds between toggling the remote loopback on or off.
- There are no remote loopback limitations when the remote end of the call is connected by a current Ascend inverse multiplexer, but some limitations exist when the remote end of the call is connected by other equipment.

  When the remote device is a not an Ascend inverse multiplexer, you cannot set up a remote loopback if the network connection occurs over an ISDN line and any of these settings appears in the Call profile:

  - Call Type=1 Chnl or 2 Chnl
  - Call Type=AIM or BONDING and Call Mgm=Static or Mode 1

  If the remote device is an ISDN TA (Terminal Adapter), the MAX cannot usually perform a remote loopback. ISDN TAs cannot recognize the loopback signal. However, most switching CSU/DSUs (Channel Service Units/Data Service Units) recognize the remote loopback signal that the MAX sends, and remote loopbacks are usually possible with these types of equipment.
- The MAX uses a proprietary loopback message when the AIM management subchannel is present (Call Mgm=Manual, Dynamic, or Delta in a Call profile).
- The MAX uses the CCITT V.54 loopback pattern when no management subchannel is present (Call Type=1 Chnl or 2 Chnl and Call Mgm=Static in a Call profile).
- If the MAX fails to set up a remote loopback, it establishes a loopback at the local host interface calling for the loopback.
- The DO Beg/End LB command does not appear if you are not logged in with operational privileges.

For related information, see the Call Mgm, Call Type, and Operations in Chapter 3, "MAX Alphabetic Parameter Reference."

Beg/End Rem Mgm (DO 8)

The DO Beg/End Rem Mgm command begins and ends remote management of the device at the remote end of an AIM call. When you enter this command, the vt100 interface displays the following message at the top of its screen:

```
REMOTE MANAGEMENT VIA <port>
```

In this message, <port> specifies the serial host port through which you are conducting remote management. To end an AIM remote management session, enter DO 8 or Ctrl-D 8. You cannot exit remote management from a port other than the port from which you began remote management. When the message at the top of the vt100 screen disappears, you are viewing the screens associated with the local MAX.

Note: Ascend strongly recommends that you perform remote management using only the vt100 interface. The Palmtop Controller provides no indication as to whether you are in remote management or local management.

Keep this additional information in mind:

- During an AIM call, remote management adds 20 kbps to the 0.2% overhead of the call, and to that small extent reduces the bandwidth provided to serial host devices using the connection.
- The DO Beg/End Rem Mgm command is available for connections with Call profile settings of Call Type=FT1-AIM, FT1-B&O, or AIM (but not Call Mgm=Static).
- This error message indicates you have tried to control a MAX that is not configured to allow remote management:

  ```
  Remote Mgmt Denied
  ```

  You cannot remotely manage a device configured with the value No for the Remote Mgmt parameter in the System profile.
- You cannot begin remote management if you do not have an online call to the remote device; furthermore, you must select the DO Beg/End Rem Mgm command from a menu specific to that call.
- The DO Beg/End Rem Mgm command does not appear if you are not logged in with operational privileges.

For related information, see the Call Mgm, Call Type, Operations, and Remote Mgmt parameters in Chapter 3, "MAX Alphabetic Parameter Reference."

Close TELNET (DO C)

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

Contract BW (DO 5)

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

Keep this additional information in mind:

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

For related information, see the Dec Ch Count and Operations parameters in Chapter 3, "MAX Alphabetic Parameter Reference."

Diagnostics (DO D)

The DO D command invokes diagnostics mode. The user must have sufficient privileges in the active Security profile. In diagnostics mode, the vt100 interface displays a command-line prompt:

```
>
```

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

```
> help ascend
```

To exit diagnostics mode and return to the vt100 interface, type quit.

```
> quit
```

Dial (DO 1)

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

- In front of a Call profile in the Directory menu.
- At any parameter within a Call profile.
- In front of or within any port-specific menu, but not at any specific Call profile.

  Because the current Call profile contains the parameters of the last call made from a port, this option redials that call.

Dial automatically performs a DO Load of the selected profile, overwriting the current Call profile, including any Call profile parameters you might have edited. However, edited parameters are not overwritten if the current Call profile is protected by Security profiles.

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

Keep this additional information in mind:

- Dial is not available when the link is busy.
- You cannot place a call from the secondary port of a dual-port pair.

- The DO Dial command does not appear if you are not logged in with operational privileges.
- You cannot dial if you have not selected the correct profile, if Dial # does not appear in the profile, or if no IP address is set for the profile when IP routing is enabled.

For related information, see the Operations parameter in Chapter 3, “MAX Alphabetic Parameter Reference.”

Esc (DO 0)

The DO ESC command exits the DO menu.

Extend BW (DO 4)

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

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

Keep this additional information in mind:

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

For related information, see the Inc Ch Count and Operations parameters in Chapter 3, “MAX Alphabetic Parameter Reference.”

Hang Up (DO 2)

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

Keep this additional information in mind:

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

For related information, see the Call Type and Operations parameters in Chapter 3, “MAX Alphabetic Parameter Reference.”

Load (DO L)

The DO Load command loads a saved or edited profile onto the current profile. Loading a selected profile overwrites the values of the current profile. For example, suppose you have saved a profile named Memphis in the Directory location 21-102:

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

When you execute DO Load, this screen appears:

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

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

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

The Directory menu shows the results of the load operation:

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

The DO Load command does not appear if you are not logged in with operational privileges. For more information, see the Operations parameter in Chapter 3, "MAX Alphabetic Parameter Reference."

Menu Save (DO M)

The DO Menu Save command saves the entire current vt100 interface layout. The current layout replaces the default layout.

Keep this additional information in mind:

- The DO Menu Save command appears only if the cursor is in front of the Sys Config menu.
- The command always places Sys Config in the default Edit display.

  To change the default Edit display, you must configure the Edit parameter in the System profile after using the DO Menu Save command.
- Menu Save does not apply to Palmtop Controllers, nor does it apply when your vt100 is plugged into an RPM or Palmtop port.

For related information, see the Edit parameter in Chapter 3, "MAX Alphabetic Parameter Reference."

Password (DO P)

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

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

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

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

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

The MAX logs you out to the default Security profile if any one of these situations occurs:

- You end a console session.
- You exceed the time set by the Idle Logout parameter in the System profile.
- You are connected to a Palmtop control port and you disconnect your terminal.
- Auto Logout=Yes in the System profile and you are connected to the vt100 control port.

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

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

For related information, see the Auto Logout and Idle Logout parameters in Chapter 3, “MAX Alphabetic Parameter Reference.”

Resynchronize (DO R)

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

Keep this additional information in mind:

- You must be in a serial host port edit menu or status window to use this command.

- Resynchronize is not available for all call management types specified by the Call Mgm parameter in the Call profile.
- Resynchronize is not available when the host port is idle or when the host port is the secondary port of a dual-port pair.
- Resynchronize does not appear if you are not logged in with operational privileges.

For related information, see the Call Mgm and Operations parameters in Chapter 3, "MAX Alphabetic Parameter Reference."

Save (DO S)

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

Keep this additional information in mind:

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

For more information, see the Operations parameter in Chapter 3, "MAX Alphabetic Parameter Reference."

Termserv (DO E)

The DO E command invokes the terminal-server command-line interface. The user must have sufficient privileges in the active Security profile. In terminal server mode, the vt100 interface displays a command-line prompt, by default the prompt is:

```
ascend%
```

Use the Help command to display a list of terminal-server commands.

```
ascend% help
```

For examples that use terminal-server commands, see the *MAX ISP & Telecommuting Configuration Guide*. To exit terminal server mode and return to the vt100 interface, use the Quit command:

```
ascend% quit
```

Status Window Reference

2

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

Using the MAX status windows

Eight status windows are displayed on the right side of the screen in the MAX configuration interface (Figure 2-1). These status windows provide a great deal of read-only information about what is currently happening in the MAX.

This section gives an overview of the information contained in the eight windows that are displayed by default, and shows you how to swap out a default window and replace it with status windows of your choice. These are the parameters used to customize the display:

```
System
   Sys Config
      Status 1=10-100
      Status 2=50-300
      Status 3=50-100
      Status 4=00-200
      Status 5=50-500
      Status 6=50-400
      Status 7=00-100
      Status 8=00-000
```

The Status numbers 1 through 8 refer to the status window positions, which start with 1 in the upper left, 2 in the upper right, and so forth. For details on each parameter, see Chapter 3, "MAX Alphabetic Parameter Reference."

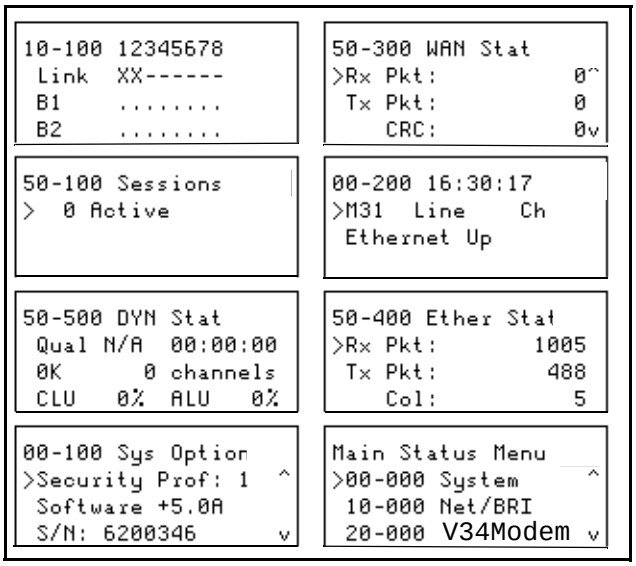


Figure 2-1. Status windows

Navigating the status windows

To scroll the information in a status window or execute a context-specific DO command, you must make the status window active by pressing the TAB key until that window is highlighted by a thick border. The TAB key moves the active window in sequence from left to right, top to bottom, and then returns to the Edit window (the menu).

Some of the status windows contain more information than can be displayed in the small window. If a lowercase v appears in the lower-right corner of a window, it means there is more information available. To scroll through additional information in a window, use the TAB key to move to that window.

Default status window displays

You can use the Status parameters in the System profile to change which status windows are displayed when the MAX powers up. For details on all of the codes and information that can be displayed in each window, see Status window reference in alphabetic order.

Line status window

Slot 1 contains the two leftmost lines when you look at the unit's back panel. By default, the status of the lines in Slot 1 are shown in the top left status window:

```
10-100 12345678
 Link  PPP-----
 B1    *** .....
 B2    *** .....
```

This window displays four lines.

- The first line shows the menu number and column numbers for channels 1—8.
- The second line identifies the line.
- The third and fourth lines show the state of the B channels.

Session and message log windows

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

```
50-100 Sessions
>  1 Active
   0 slc-lab-234
```

```
00-200 16:30:17
>M31  Line    Ch
 Ethernet Up
```

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

The system message log provides a log of up to 32 of the most recent system events. Use the arrow key to scroll up (previous messages) or down (later ones). The Delete key clears all the messages in the log. The message log window is organized as follows:

- The first line shows the menu number and the time the most recent logged event occurred.
- The second line identifies the log entry number (M00-M31) and, if applicable, the line and channel on which the event occurred.

- The third line contains the text of the message.

  For example:

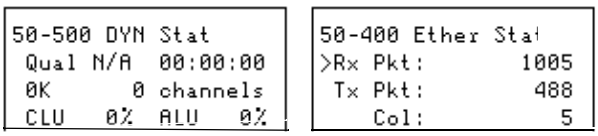
  Call Terminated means an active call disconnected normally.

  LAN session up means that an incoming connection has been established.

  No Connection means the remote device did not answer the call.
- The fourth line contains a message qualifier, such as a name or phone number that qualifies the message displayed.

Dyn and Ethernet status windows

By default, the next two status windows show statistics on the Dynamic Bandwidth Allocation status or Dyn interface and on the Ethernet interface:

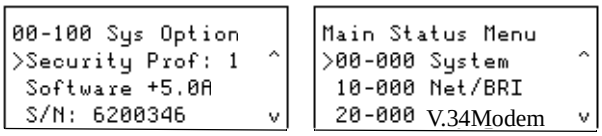


The Dyn Stat window shows the name, quality, bandwidth, and bandwidth utilization of each online multi-channel PPP connection with dynamic bandwidth management.

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

Sys Option and Main Status Menu windows

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



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

```
Up: 12:17:18:26
```

When the Sys Options window is active, you can use the arrow keys to scroll down and view the list of system options. For example, you see the software load name, various installed software options (such as frame relay, AIM, BONDING, and so forth), and the AuthServer and AcctServer options, which specify the IP addresses of the RADIUS (or TACACS) authentication server and the RADIUS accounting server.

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

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

Customizing which status windows appear

You can change which status windows are displayed in the vt100 interface. The total number of status windows displayed is eight when the MAX starts up. For details on the windows you can choose to display in these eight locations and the information in each one, see Status window reference in alphabetic order.

For example, to instruct the MAX to display the MAX line status window for the BRI lines location in status window number 2:

1 Open the System profile>Sys Config.

2 Arrow down to Status 2.

3 Type the menu number identifying the BRI line status window.

```
Status 2=10-100
```

4 Close the System profile.

5 Back arrow to select from:

- ESC (Don’t exit): (Your changes are not made.)
- Exit and discard: (Your changes are not saved.)
- Exit and accept: (Your changes are saved and appear after you restart the MAX.)

For more details about slot, line, and port numbers, see the *MAX ISP & Telecommuting Configuration Guide*.

Status window reference in alphabetic order

This section describes the contents of each status window in detail. The windows are listed in alphabetic order.

BRI/LT window

BRI/LT is a branch of the Main Status Menu that lists windows indicating the status of the ISDN BRI interfaces. The BRI/LT window appears only if a BRI/LT module is installed. To display the BRI/LT window, select BRI/LT from the Main Status Menu.

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

The Line BRI/LT status window shows the condition of the electrical link to the carrier and the status of the B1 and B2 channels. See Line Status (BRI) window.

The Line Errors status window displays the errors recorded on all current channels in a channel-by-channel, line-by-line list. See Line Errors window.

The Block Errors status display shows the errors for near-end block errors (NEBE) and far-end block errors (FEBE). The numbers displayed are totals accumulated since the last time the block error buffers were cleared. The FEBE and NEBE error buffers can be cleared per line and per counter (you can clear the FEBE buffer for a line without clearing the NEBE buffer). The totals for each buffer wrap back to zero after they reach 65535. Restarting the MAX clears the buffers.

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

The Loopback counters status display shows the number of test frames sent and received since the Loopback command was issued. The numbers displayed are cumulative totals since the Line loopback command was issued; when the loopback command is started or restarted the LB counters are reset to 0.

```
X0-XXX XMIT      RECV
 1:      0         0
 2:      0         0
 3:      0         0
 4:      0         0
 5:      0         0
 6:      0         0
 7:      0         0
 8:      0         0
```

Net Options for the BRI/LT lists the interface features with which your MAX has been equipped. See Net Options window.

Call Status window

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

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

```
21-000 Port1 Stat
>21-100 Call Status
   21-200 Message Log
   21-300 Statistics
   21-400 Port Opts
   21-500 Session Err
   21-600 Port Leads
```

For example, this screen shows the four-line Call Status display for the first AIM port on the base system:

```
21-100 Albuquerqu+ C
CALLING/ONLINE
336K      6 channels
 Albq. NM
```

The first line of the Call Status window shows the status window number, the name of the current Call profile, and a call status character (see Table 2-1).

The second line shows the call status message corresponding to the current state. It can change dynamically as you dial, modify, or receive calls. These are the call status characters and messages that can appear:

Table 2-1. Call status characters and messages

Status indicator	Status message	Description
Blank	IDLE	No calls exist and no other MAX operations are being performed.
A	ANSWERING	An incoming call is being answered.
R	RINGING	An incoming call is on the line, ready to be answered.
C	CALLING	An outgoing call is being dialed.
O	ONLINE	A call is up on the line.
H	CLEARING	The current call is being cleared.
D	LOCAL LOOP	Local loopback diagnostic tests are in progress.
!	HANDSHAK	The MAX is exchanging information with the inverse multiplexer at the remote end and verifying that the call is transmitting reliably.
!	SETUP ADD	The MAX is preparing to add channels while a call is online and passing data.
!	SETUP REM	The MAX is preparing to remove channels while a call is online and passing data.
!	SETUP HND	The MAX is preparing to handshake for resynchronization while a call is online and passing data.
L	LOOP MAST	You have selected DO 6 or Control-D 6 to begin a remote loopback test. While the loopback test is in progress, the remote end displays the status message LOOP SLAV.
T	BERT MAST	The MAX has connected with the remote-end AIM-compatible product and is performing an automatic BERT (byte error test). Or, you are performing a manual BERT from the local MAX.
T	BERT SLAVE	Your MAX has received a call and the calling AIM-compatible product is performing an automatic BERT. Or, someone using the remote MAX is performing a manual BERT test.

Note: When the MAX is adding or removing channels, it appends /ONLINE to another status word. For example, if you issue a DO 4 command to increase the bandwidth of an active call, the status changes to CALLING/ONLINE. When the remote end responds, the status ANSWERING/ONLINE appears at the remote MAX unit.

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

```
21-100 Albuquerqu+ C
CALLING
336K  6/2  channels
 Albq. NM
```

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

The last line of the Call Status window contains the name of the AIM port of the remote end AIM-compatible product that has been connected. If the remote end Port profile is not named, the MAX uses the remote end module name taken from the host-module profile. If both the module and the port are not named, the MAX uses the remote end system name.

CDR window

The CDR (call detail reporting) display provides detailed calling information. Like the MAX message logs, CDR shows the most recent session event; the MAX generates new CDRs as events occur. However, unlike a log, the MAX does not store CDR events that have passed. CDR is primarily a source of data captured by external devices.

You can view CDR status displays in real time through the vt100 interface or Palmtop Controller. This screen shows the four-line CDR display:

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

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

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

<year>:<month>:<day>:<hour>:<minute>:<second>

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

- CDR event description

  The event description uses these abbreviations:

  - OR for Originated (outgoing call)
  - AN for Answered (incoming call)
  - AP for Assigned to Port or module (incoming call)
  - CL for Cleared
  - OF for Overflowed

  All events except OF are associated with calls. OF indicates that the CDR buffer overflowed because events occurred faster than the MAX could report them.

- CDR event ID

  The MAX creates a new event ID for every DS0 channel originating a connection. The event ID ranges from 0 to 255; events after 255 start the count again at 0. In addition, CDR creates a new event ID for every change in a channel's status. Because a MAX call can consist of several channels, the MAX can generate multiple CDRs for every change in call status.

- The data service in use

  Indicates the data service, using values nearly identical to those available to the Data Svc parameter in the Call profile. The only difference is that the Data Svc values 384K/H0 and 1536K correspond to the CDR data service values 384K and 1536KR, respectively.

- The slot-port address on which the event occurred

  For example, if the event occurred on the first port of a Host/6 card installed in slot 3, the slot-port address is 03-01.

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

For related information, see the Data Svc parameter in Chapter 3, "MAX Alphabetic Parameter Reference."

Dyn Stat window

The Dyn Stat window shows the name, quality, bandwidth, and bandwidth utilization of each online multi-channel PPP connection with dynamic bandwidth management. This screen shows the Dyn Stat display for the Ethernet module in slot 9:

```
90-500 Dyn Stat
 Qual Good 00:02:03
 56K     1 channels
 CLU  12%  ALU  23%
```

Note: Press the Down Arrow key to see additional online multi-channel PPP connections.

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

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

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

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

The last line displays these values:

- CLU (Current Line Utilization)

  CLU is the percentage of bandwidth currently being used by the call for transmitted data, divided by the total amount of bandwidth available.

- ALU (Average Line Utilization)

  ALU is the average amount of available bandwidth used by the call for transmitted data during the current history period as specified by the Sec History and Dyn Alg parameters.

Ether Opt window

The Ether Opt window lists the type of Ethernet interface specified in the Ethernet I/F parameter, and its MAC address. The following illustration shows the Ether Opt display for the Ethernet module in slot 5:

```
50-600 Ether Opt
>Enet I/F: UTP
 Adrs: 00c07b637bf9
```

The interface type may be AUI, UTP, or COAX. The MAC address is a 6-byte hexadecimal address assigned to the Ethernet controller by the manufacturer. For related information, see the Ethernet I/F parameter in Chapter 3, “MAX Alphabetic Parameter Reference.”

Ether Stat window

The Ether Stat window shows the number of Ethernet frames received and transmitted and the number of collisions at the Ethernet interface. For example, this screen shows the Ether Stat display for the Ethernet module in slot 5:

```
50-400 Ether Stat
>Rx Pkt:      106
    Col:        0
 Tx Pkt:      118
```

This screen shows the following fields:

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

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

Ethernet window

The Ethernet window is a branch of the Main Status Menu. It lists those windows that display the status of the Ethernet interface. This screen shows the Ethernet window:

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

FR Stat window

The FR Stat (Frame Relay Status) window shows the status of each online link defined in a Frame Relay profile. For example, this screen shows the FR profile display when the link uses a serial WAN module is installed in slot B:

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

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

Host/6 (Host/Dual) window

The Host/6 (or Host/Dual) status window is a branch of the Main Status Menu. It holds a list of windows that give the status of the MAX unit's AIM host interface, and the status of calls to and from the AIM ports of that interface. For example, this screen shows a Host/Dual status window for a module installed in slot 2:

```
20-000 Host/Dual
   21-000 Port1 Menu
   22-000 Port2 Menu
   20-100 Mod Config
```

Line Errors window

The Line Errors status window shows errors recorded on all current channels in a channel-by-channel, line-by-line list. The Line Errors window displays the status of lines even if the interface is disabled in the Line profile. This section describes the Line Errors windows for BRI lines.

To open the Line Errors window, you can choose Line Errors in the Net/T1 or Net/BRI status window. For example:

```
10-000 Net/BRI
 10-100 Line Status
```

```
10-200 Line Errors
10-300 Net Options
```

The Line Errors window displays the channel-by-channel errors accumulated during all current calls. The window is divided into three columns:

```
10-200   B1 B2
 1:      0   -
 2:      33  -
 3:     0   -
```

The first column displays the line number (1 through 8) for a BRI line.

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

If a channel is not associated with a current call, a dash (-) appears in place of errors. Any channel in the Line Errors display that would show dashes in both columns is omitted.

Line Status (BRI) window

The Line Status window shows the dynamic status of each BRI line, the condition of its electrical link to the carrier, and the status of each line's individual channels. For example, when a Net/BRI module is installed in slot 3:

```
30-100 12345678    O
Link   PPP-----
B1     ***.....
B2     ***.....
```

The first line of the Line Status window shows the window number and the column headers for each of the 8 BRI lines in an expansion module. The second line of the window uses the following one-character abbreviations to characterize the overall state of the line (see Table 2-2). The third and fourth lines show a single-character abbreviations that indicate B1 and B2 channel status, respectively (see Table 2-2).

Table 2-2. BRI line status indicators

Line status	Mnemonic	Description
.	Not available	The line is not active at this time, but it is physically connected.
-	Idle	The line is disabled. The channel usage parameter in the Line profile is set to Unused.
P	Point-to-point	The line is in a point-to-point active state and is physically connected.
D	Dual-terminal	The line is in a multipoint active state, initialized in dual-terminal mode, and is physically connected.

Table 2-2. BRI line status indicators (continued)

Line status	Mnemonic	Description
M	Multipoint	The line is in a multipoint active state, initialized in single-terminal mode, and is physically connected.
X	Not connected	The line is not physically connected and cannot pass data. In some countries outside the U.S., the character X might appear even though the line is physically connected.

The third and fourth lines describe the state of the B1 and B2 channels, respectively, using the indicators shown in Table 2-3.

Table 2-3. B1 and B2 channel status indicators

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

Message Log windows

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

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

AIM port message logs

The Message Log for an AIM port provides a log of events that occurred at each AIM port during call dialing and transmission. It is listed in the Port N Stat menu. This example shows a Message Log record generated by an incoming call on an AIM port installed in slot 7:

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

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

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

System message logs

The Message Log for the system provides a log of system events. It is listed in the System status window. This example shows a Message Log (System) record generated by an incoming call not yet assigned to an AIM port:

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

The first line of the window shows the status window number and the time the event occurred. The second line identifies the log entry number (M00-M31) and, if applicable, the line and channel on which the event occurred. The third line contains the text of the message. See "Log messages." The fourth line contains connection-specific messages. See Table 2-6.

Log messages

Table 2-4 shows the informational messages that can appear in the Message Log windows:

Table 2-4. Informational log messages

Message	Description
Added Bandwidth	The MAX has added bandwidth to an active call.
Assigned to port	The MAX has determined the assignment of an incoming call to an AIM port, a digital modem, the packet-handling module, or the terminal server.
Call Terminated	An active call was disconnected normally, although not necessarily by operator command.
Callback Pending	The MAX is waiting for callback from the remote end.
Ethernet up	The Ethernet interface has been initialized and is running.

Table 2-4. Informational log messages (continued)

Message	Description
Handshake Complete	The handshake completed, but no channels were added. Either an operator entered the DO R command to resynchronize channels, or an attempt to add channels to an inverse-multiplexing call failed.
Incoming Call	The MAX has answered an incoming call at the T1 PRI network interface, but has not yet assigned the call to an AIM port or to the IP router.
Incomplete Add	An attempt to add channels to an inverse-multiplexing call failed; the MAX added some channels, but fewer than the number requested. This situation can occur when placing a call; the first channel connects, but the requested base channel count fails.
LAN session down	This message appears before Call Terminated if a PPP, MP+, or Combinet session is terminated
LAN session up	This message appears after Incoming Call if a PPP, MP+, or Combinet session is established
Moved to primary	Some nailed-up channels that the MAX removed from an FT1-B&O call have been restored because their quality was no longer poor. The fourth line of the Message Log window indicates the number of channels restored.
Moved to secondary	The MAX has detected some poor quality nailed-up channels in an FT1-B&O call, and has backed up the call on switched channels. The fourth line of the Message Log window indicates the number of channels removed.
Outgoing Call	The MAX has dialed a call.
Port use exceeded	Call usage for a AIM port has exceeded the maximum specified by either the Max DS0 Mins or Max Call Mins parameter in the Port profile.
Removed Bandwidth	The MAX has removed bandwidth from an active call.
Sys use exceeded	Call usage for the entire system has exceeded the maximum specified by the Max DS0 Mins parameter in the System profile.
RADIUS config error	The MAX has detected an error in the configuration of a RADIUS user entry.
Requested Service Not Authorized	This message appears in the terminal server interface if the user requests a service not authorized by the RADIUS server.

Table 2-5 shows the warning messages that can appear in the Message Log windows:

Table 2-5. Warning log messages

Message	Description
Busy	The phone number was busy when the call was dialed.
Call Disconnected	The call has ended unexpectedly.
Call Refused	An incoming call could not be connected to the specified AIM port, digital modem, packet-handling module, or terminal server because the resource was busy or otherwise unavailable.
Dual Port req'd	The call could not be placed because both ports of the dual-port pair were not available.
Far End Hung Up	The remote end terminated the call normally.
Incoming Glare	The MAX could not place a call because it saw an incoming "glare" signal from the switch. Glare occurs when you attempt to place an outgoing call and answer an incoming call simultaneously. If you receive this error message, you have probably selected incorrect Line profile parameters.
Internal Error	Call setup failed because of a lack of system resources. If this type of error occurs, notify Ascend customer support.
LAN security error	This warning appears after Incoming Call but before Call Terminated if a PPP, MP+, terminal server, or Combinet session has failed authentication, another session by the same name already exists, or the timeout period for RADIUS/TACACS authentication has been exceeded. For details, see the Auth Timeout parameter in Chapter 3, "MAX Alphabetic Parameter Reference."
Network Problem	The call setup was faulty because of problems within the WAN or in the Line profile configuration. The D channel might be getting an error message from the switch, or the telco might be experiencing a problem.
No Chan Other End	No channel was available on the remote end to establish the call.
No Channel Avail	No channel was available to dial the initial call.
No Connection	The remote end did not answer when the call was dialed.
No Phone Number	No phone number exists in the Call profile being dialed.
No port DSO Mins	No maximum has been specified for the Max DS0 Mins or Max Call Mins parameter in the Port profile.
No System DSO Mins	No maximum has been specified for the Max DS0 Mins parameter in the System profile.

Table 2-5. Warning log messages (continued)

Message	Description
Not Enough Chans	A request to dial multiple channels or to increase bandwidth could not be completed because there were not enough channels available.
Not FT1-B&O	The local MAX attempted to connect an FT1-B&O call to the remote end, but the call failed because the call type at the remote end was not FT1-B&O.
Remote Mgmt Denied	The MAX rejected a request to run the remote MAX by AIM remote management because the Remote Mgmt parameter in the System profile at the remote end is set to No.
Request Ignored	The MAX denied a request to manually change bandwidth during a call because the Call Mgm parameter in the Call profile has the value Dynamic. With this value, the MAX allows only automatic bandwidth changes.
Wrong Sys Version	The remote-end product version was incompatible with the version of the local MAX. The software version appears on the Sys Options status window.

Table 2-6 shows connection messages that can appear on the fourth line of the Message Log windows:

Table 2-6. Message indicators

Indicator	Description
MBID	The MBID parameter appears with either the Incoming Call or Assigned to Port (line 3) messages. The first message means an incoming call has been received and the second message means it has been routed to a MAX port. If you cannot match the MBID value of an incoming call log to the MBID value in an assigned-to-port log, the call disconnected, often because the intended port was busy. MBID also appears in the System log.
Channels	This parameter specifies the number of channels added to or removed from a call. It appears with the Added Bandwidth, Removed Bandwidth, Moved to Primary, and Moved to Secondary messages. When line 3 is an Outgoing Call, line 4 displays the Phone Number dialed. In multichannel calls, line 4 displays the phone number for the first connection. Only the phone number appears; the parameter name Phone Number does not.
Cause Code	This parameter indicates a signaling error or event. The code number was sent by the ISDN network equipment and received by the MAX.

Table 2-6. Message indicators (continued)

Indicator	Description
Name	When the message in line 3 is either LAN session up or LAN session down, line 4 displays the remote end's Name. If the session is a Combinet bridging link, the MAC address is displayed. If the session is a PPP link, either the remote end's system name (as specified by the Name parameter in the System profile) or IP address (as specified by the IP Adrs parameter in the Ethernet profile) is displayed. The IP address is displayed only if the system's name is not known.
CLID	When an incoming call is answered and the calling party number is known, line 4 specifies the CLID (calling line ID). When the CLID appears, the MBID does not.

Modem window

The Main Status Menu contains a V.34 Modem entry for each modem card. When you select the V.34 Modem entry for a card, the Modem Status menu displays. On this menu, each modem is correlated with a display character. For example, this is a Modem Stats window for an 8 modem card:

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

The first line shows the window name. The second line lists the modems by number, and the third contains a status indicator. The status indicators are described in Table 2-7.

Table 2-7. Modem status characters

Indicator	Mnemonic	Description
.	Nothing	This modem is non-existent.
f	Failed	This modem failed the POST (Power-On Self Test). The modem is unavailable for use.
-	Not used	The modem is not in use.
a	Waiting to go active	The modem has been instructed to dial or answer a call, and the unit is waiting for RLSD (Received Line Signal Detector) to go active.
A	Active	RLSD has already gone active and the unit is waiting for result codes to be decoded. This state is entered only if RLSD precedes the codes.
*	Connected	A call is connected, and the unit is monitoring RLSD.
i	Initializing	The modem is re-initializing after being reset.

Table 2-7. Modem status characters (continued)

Indicator	Mnemonic	Description
q	Open request	The modem is re-initializing after being reset and an open request is waiting to be processed when re-initialization completes.
Q	Open request for virtual connection	The modem is re-initializing after being reset and an open request for Virtual Connection is waiting to be processed when re-initialization completes.
d	Dialing	The first part of the dial string has been sent. This unit is pausing for the modem to read and process the second part before sending it.
v	Virtual connection	A virtual connection session is active on modem. No call is active yet.
o	out of service in interface	The user has disabled the modem from the MAX configuration interface. The modem is unavailable for calls.
O	Out of service	The user has disabled the modem from the MAX configuration interface. The modem is unavailable for calls and a B-channel is set to OutOfService.

Net BRI windows

Net/BRI windows are branches of the Main Status Menu that enable you to open windows related to those lines. The Net/BRI window appears only if a Net/BRI module is installed.

This screen shows the Net/BRI window:

```
10-000 Net/BRI
>10-100 Line Status
   10-200 Line Errors
   10-300 Net Options
```

Net Options window

The Net Options window lists the WAN interface features with which your MAX has been equipped. This screen shows the Net Options window:

```
10-300 Net Options
>BRI U Interface
```

The first line defines the physical interface to the WAN or (in the case of Host BRI modules) to the local BRI lines.

Port Info window

The Port Info window displays the status of active calls, and indicates the bandwidth that current calls are not using. This screen shows a Port Info window:

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

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

The fourth line and each line that follows it display the AIM host-interface status. It includes these fields, in the order shown:

- Module and port number
- Call status indicator (see Table 2-8)
- Call quality indicator (the quality of the link for an active call)

  This value can be G (good), F (fair), M (marginal), N (not applicable), or P (poor). Not applicable (N) appears before the call is connected end-to-end.
- Bandwidth (the approximate bandwidth given to the codec)

  If the call is an FT1-B&O call, these values specify the offline bandwidth as well as the online bandwidth of the call. This screen shows statistics for an FT1-B&O call on the base system's AIM port 2:

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

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

Table 2-8 shows call status indicators for AIM port calls.

Table 2-8. Call status characters for AIM ports

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

Table 2-8. Call status characters for AIM ports (continued)

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

Port Leads window

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

For example, this screen shows the Port Leads window for the serial WAN port:

```
21-600 Port Leads
 DSR+ DCD+ RI + DTR+
```

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

The first line of the window shows the slot-port address of the AIM port. The remaining lines show the state of the control leads going into and out of the serial port. The plus symbol (+) indicates an active control lead, while the minus symbol (-) indicates that the lead is inactive. For RS-366 dialing output and input signals, the MAX uses the abbreviations in Table 2-9.

Table 2-9. RS-366 abbreviations

Output	Input
acr (Abandon Call and Retry)	dp (Digit Present)
pnd (Present Next Digit)	crq (Call Request)
dlo (Data Line Occupied)	

The digit field in the lower right-hand corner displays the last digit dialed if the port is an RS-366 dialing interface.

Table 2-10 lists the abbreviations for dialing output and input signals at the AIM port. The Clear to Send (CTS) output signal is not monitored in this window. The standard cables supplied with the MAX tie CD and CTS together.

Table 2-10.Serial host port abbreviations

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

Table 2-11 lists the abbreviations used for dialing output and input signals at the serial WAN port.

Table 2-11.Serial WAN port abbreviations

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

Port Opts window

The Port Opts window is a read-only window that displays information about the configuration options of the MAX unit's AIM ports. A Port Opts status window exists for each AIM port. This screen shows the Port Opts window for the fourth AIM port on a Host/6 card in slot 7:

```
21-400 Port Opts
>V.35 Host I/F
```

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

Table 2-12.Port Opts information

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

PortN Stat window

The PortN Stat window appears in the Host/6 or Host/Dual branch of the Main Edit Menu. It consists of a list of windows that show the status of an AIM port. This screen shows the Port1 Stat window of the first port of an AIM card installed in slot 2:

```
21-000 Port1 Stat
  21-100 Call Status
  21-200 Message Log
  21-300 Statistics
  21-400 Port Opts
   21-500 Session Err
   21-600 Port Leads
```

Routes window

The Routes window displays the current routing table. This screen shows a Routes window:

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

Note: Press Down-arrow to view the next route, or Up-arrow to view the previous one.

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

The third line shows the address of the router.

The fourth line can have one of the values listed in Table 2-13.

Table 2-13.Routes window values

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

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

Serial WAN window

The Serial WAN status window is a branch of the Main Status Menu. It displays the status of the serial WAN interface.

```
40-000 Serial WAN
   40-100 Port Leads

    DSR-- DCD-- RI-- DTR--
```

From this window, you can show the Port Leads status display, which indicates the status of the serial WAN port's control signals.

Session Err window

The Session Err status window displays the errors encountered during the current call on a channel-by-channel, line-by-line basis. A Session Err window exists for each host port. Each row of this window reports the accumulated errors on one of the channels active in the call. Four columns are separated from each other by colons (:).

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

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

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

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

For related information, see the Line Errors window.

Sessions window

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

```
50-100 Sessions
>0 Active
```

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

<status> <remote device>

where <status> is a status indicator and <remote device> is the name, address, or CLID of the remote device. Table 2-14 lists the session status characters that can appear.

Table 2-14.Session status characters

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

Note: For remote terminal server sessions, the third and following lines of the Sessions window appear in the format Modem <slot>:<position>, where <slot> specifies the slot of the active digital modem, and <position> indicates the position of the modem in that slot.

Statistics window

The Statistics window is an AIM port-specific window that provides information about line utilization and synchronization delay while a call is up. A Statistics window exists for each AIM port. This screen shows the Statistics display for the first port of an AIM card installed in slot 2:

```
21-300 Albuquerqu+ O
 Qual Good 01:23:44
 Max Rel Delay 10
 CLU  80%  ALU  77%
```

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

The second line lists the quality of the call and the call duration. When a call lasts more than 96 hours, the window displays the call duration in number of days. The call quality, or Qual, can be Good, Fair, Marg (Marginal), or Poor.

- Good means that no errors have been detected during the transmission of the call.
- Fair means that some errors have been detected in transmission.
- Marg means that a significant number of errors have been detected; in this case, reliable transmission is not guaranteed and resynchronization is recommended.
- Poor means that the MAX may drop individual channels from the call, or clear the call automatically.

For FT1-B&O calls, the second line of the Statistics window might not show the call duration. When an FT1-B&O call has no bad channels, the call duration appears as usual. Otherwise, the

number of offline nailed-up channels appears after the call quality. The following screen shows the Statistics window of an FT1-B&O call with two channels offline:

```
21-300 Albuquerqu+ O
 Qual Good 2=Poor
 Max Rel Delay 10
 CLU  80%  ALU  77%
```

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

The last line displays these values:

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

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

For related information, see the Call Mgm, Call Type, Dyn Alg, and Sec History parameters in Chapter 3, “MAX Alphabetic Parameter Reference.”

Syslog window

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

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

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

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

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

  The device address (slot, port or line, and channel) is followed by two lines of text, which are displayed on lines 3 and 4 of the Message Log window.

  The device address is suppressed when it is not applicable or unknown.

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

- Level 5 (notice) syslog messages

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

  ASCEND: *call-event-ID event-description slot-n port-n data-svc*K *phone-n*

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

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

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

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

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

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

- Disconnect cause codes and progress codes

  If the syslog option is set, a call-close (CL) message is sent to the syslog daemon whenever a connection is closed. Additional information about the user name, disconnect reason, progress code, and login host is appended to each CL message. The disconnect cause code uses this format:

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

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

  Xxxx is the disconnect cause code.

  Yyyy is the connection progress code.

  Ip-addr is the login host’s IP address for Telnet and raw TCP connections (if applicable).

Table 2-15 list the Ascend Disconnect codes.

Table 2-15.Ascend Disconnect Cause codes

Code	Description
0	No reason.
1	The event was not a disconnect.
2	The reason for the disconnect is unknown. This code can appear when the remote connection goes down.
3	The call has disconnected.
4	ID authentication has failed.
5	RADIUS timeout during ID authentication.

Table 2-15.Ascend Disconnect Cause codes(continued)

Code	Description
6	The MAX disconnected because callback is configured.
7	The Send Disconnect timer in the Line profile has been triggered.
These codes can appear if a disconnect occurs during the initial modem connection.	
9	No modems available.
10	The modem never detected DCD.
11	The modem detected DCD, but became inactive.
12	The result codes could not be parsed.
These codes are related to immediate Telnet and raw TCP disconnects during a terminal server session.	
20	The user exited normally from the terminal server.
21	The user exited from the terminal server because the idle timer expired.
22	The user exited normally from a Telnet session.
23	The user could not switch to SLIP or PPP because the remote host had no IP address or because the dynamic pool could not assign one.
24	The user exited normally from a raw TCP session.
25	The login process ended because the user failed to enter a correct password after three attempts.
26	The raw TCP option is not enabled.
27	The login process ended because the user typed Ctrl-C.
28	The terminal server session has ended.
29	The user closed the virtual connection
30	The modem outdial virtual connection has ended.
31	The user exited normally from an Rlogin session
32	The user selected an invalid Rlogin option.
33	The MAX has insufficient resources for the terminal server session.
35	The MAX did not receive an MPP keepalive packet and closed down the session.

Table 2-15.Ascend Disconnect Cause codes(continued)

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

Table 2-15.Ascend Disconnect Cause codes(continued)

Code	Description
65	The TCP host was unreachable.
66	The TCP network was administratively unreachable.
67	The TCP host was administratively unreachable.
68	The TCP port was unreachable.
These are additional disconnect codes.	
100	The session timed out because there was no activity on a PPP link.
101	The session failed for security reasons, such as an invalid incoming user.
102	The session ended for callback.
115	Far-end device has hung up.
120	One end refused the call because the protocol was disabled or unsupported.
150	RADIUS requested the disconnect.

Table 2-16 lists the Ascend Connect codes.

Table 2-16.Ascend Connect codes

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

Table 2-16.Ascend Connect codes(continued)

Code	Explanation
43	The MAX has established a raw TCP session with the host. This code does not imply that the user has logged into the host.
44	The MAX has established an immediate Telnet connection with the host. This code does not imply that the user has logged into the host.
45	The MAX is establishing an Rlogin session.
46	The MAX has established an Rlogin session with the host. This code does not imply that the user has logged into the host.
50	Active modem outdial call.
60	The LAN session is up.
61	LCP negotiations are allowed.
62	CCP negotiations are allowed.
63	IPNCP negotiations are allowed.
64	Bridging NCP negotiations are allowed.
65	LCP is in the Open state.
66	CCP is in the Open state.
67	IPNCP is in the Open state.
68	Bridging NCP is in the Open state.
Codes 69 through 77 are LCP progress codes. Refer to the RFC 1331 state transition table.	
69	LCP is in the Initial state.
70	LCP is in the Starting state.
71	LCP is in the Closed state.
72	LCP is in the Stopped state.
73	LCP is in the Closing state.
74	LCP is in the Stopping state.
75	LCP is in the Request Sent state.
76	LCP is in the ACK Received state.
77	LCP is in the ACK Sent state.

Table 2-16.Ascend Connect codes(continued)

Code	Explanation
80	IPXNCP is in the Open state.
81	AT NCP is in the Open state.
82	BACP session is being opened.
83	BACP is opened.

- The backoff queue error message in the syslog file

  Accounting records are kept until they are acknowledged by the accounting server. Up to 100 unacknowledged records are stored in the backoff queue. If the unit never receives an acknowledgment to an accounting request, it will eventually run out of memory. In order to keep this situation from the occurring, the unit deletes the accounting records and displays this error message in the syslog file:

  `Backoff Q full, discarding user <username>`

  This error generally occurs for one of the following reasons:

  – You enabled RADIUS accounting on the MAX, but not on the RADIUS server.

  – The Accounting Port or Accounting Key are incorrect. The Accounting Key must match the value assigned in the RADIUS clients file or the TACACS+ configuration file.

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

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

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

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

  – <date> indicates the date the message was logged by syslog.

  – <time> indicates the time the message was logged by syslog.

  – <router name> indicates the router this message was sent from.

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

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

  The message fields appear in this order:

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

  – <protocol> is the 4 hexadecimal digit Ether Type, or one of the following network protocol names: arp, rarp, ipx, appletalk. For IP protocols, it is either the IP protocol number (up to 3 decimal digits) or one of the following names: ip-in-ip, tcp, icmp, udp, esp, ah. In the special case of icmp, it will also include the ICMP Code and Type ([Code]/[Type]/icmp).

- For non-IP packets, <local> is the source Ethernet MAC address of transmitted packets and the destination Ethernet MAC address of received packets. On a non-bridged WAN connection, the two MAC addresses will be all zeros.

  For IP protocols, it is the IP source address of transmitted packets and the IP destination address of received packets. In the case of TCP or UDP, it will also include the TCP or UDP port number ([IP-address];[port]).

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

- For non-IP protocols, <remote> has the same format as <local> non-IP packets but shows the destination Ethernet MAC destination address of transmitted packets and the source Ethernet MAC address of received packets. For IP protocols, it has the same format as <local> but shows the IP destination address of transmitted packets and the IP source address of received packets.

- <length> is the length of the packet in octets (8-bit bytes).

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

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

  corrupt—the packet is internally inconsistent

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

  !pass—the packet was blocked by the data firewall

  bringup—the packet matches the call firewall

  !bringup—the packet did not match the call firewall

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

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

- <tag> contains any user defined tags specified in the filter template used by SAM.

Sys Options window

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

```
00-100 Sys Options
>Security Prof:1   ^
 Software +5.0A+
 S/N:6200346
```

The Sys Options window can contain the following information:

Table 2-17.Sys Options information

Option	Description
Security Prof: 1, Security Prof: 2...	Indicates which of the nine Security profiles is active.
Software	Defines the version and revision of the system ROM code.
S/N	Displays the serial number of the MAX. The serial number of your MAX can also be found on the model number/serial number label on the MAX unit's bottom panel.
Up *uptime*	Indicates the system uptime in this format: Up: *days*:*hours*:*minutes*:*seconds* For example: `Up: 13:12:18:26` The Days value "turns over" every 999 days. If the unit stays up continuously for 1000 days, the initial field will contain a 0 and will begin incrementing again.
Load	Indicates the software load name. Ascend software releases are distributed in software loads, which vary according to the functionality and target platform for the binary.
Switched Installed or Switched Not Inst	Indicates if the MAX can place calls over switched circuits.
Frm Rel Installed or Frm Rel Not Inst	Indicates if the frame relay option is installed.
Sec Acc Installed or Sec Acc Not Installed	Indicates if the Secure Access Firewalls option is installed.
MAX Link Installed or MAX Link Not Inst	Indicates if the MAX Link option is installed.
PRI <-> T1 Installed or PRI <-> T1 Not Inst	Indicates if the PRI to T1 signalling option is installed. This is used for PBX support.
MRate Installed or MRate Not Installed	Indicates if the unit supports MultiRate and GloBanD ISDN data services. Currently, T1 PRI providers in the U.S. do not support GloBanD.
RS-366 Installed or RS-366 Not Inst	Indicates if the EIA RS-366 dialing protocol has been installed.
Dyn Bnd Installed or Dyn Bnd Not Inst	Indicates if Dynamic Bandwidth Allocation functionality is available.

Table 2-17.Sys Options information(continued)

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

Note: Although GloBanD (Q.931W) does not appear in this window, its presence can be verified by checking the value of the Switch Type parameter. For more information, see Chapter 3, “MAX Alphabetic Parameter Reference.”

System Status window

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

The System Status window contains the following selections:

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

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

WAN Stat window

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

This screen shows WAN statistics:

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

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

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

MAX Alphabetic Parameter Reference

3

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

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

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 Host

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

Usage: Specify the IP address of an accounting server.

Example: Acct Host=10.2.3.4/24

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

Location: Ethernet>Connections>Accounting, Ethernet>Mod Config>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 Port

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

Usage: Specify e 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 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

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)>Port*N* 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>IPX Routes

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

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 MAXs or don’t 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-PDF to the SNMP host.
- No means alarm-events traps are not generated.

Example: Alarm=Yes

Location: Ethernet>SNMP Traps

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

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.

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

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)>Port*N* Menu>Port Config

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 a minimal AppleTalk stack to support ARA (AppleTalk Remote Access) connections.

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

- Yes enables AppleTalk to support ARA connections.
- No disables AppleTalk

Example: AppleTalk=Yes

Location: Ethernet>Mod Config

See Also: ARA, Encaps

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

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, than all four attributes must be sent. As another example, if a session has a user name, session id and session key, than 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.

- 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

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 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 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 form 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 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

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)>Port*N* Menu>Directory

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: B*N* Slot, Group

BN Slot (N=1–2)

Description: This parameter routes incoming calls on a switched BN channel to one of the expansion slot modules or to the Max's internal bridge router. This parameter specifies the slot number.

Usage: Specify one of the following values for processing incoming calls:

- 2 and 3 represent expansion slots.

  The modules in these expansion slots can be:

  – digital modem - processes incoming voice encoded calls

  - V.110 - processes incoming V.110 calls
  - AIM/BONDING - processes incoming unpacketized inverse MUX calls and outputs calls to one of its ports (video conference)
  - Host/BRI and IDSL - does not process the call, but switches it to a local line on one of its ports
- 5 represents the bridge/ router. Calls processed contain pockets to be bridged or routed, but do not require pre-processing as above.

Dependencies:

- This parameter is applicable only for switched channels.
- You cannot determine whether an incoming call will ring on line #1 or line #2; therefore set these parameters to identical values, (i.e., B1 Usage=switched, B2 Usage =switched) and set the BN Prt/Grp parameters similarly.

Example: B1 Slot=7

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

See Also: B*N* 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

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

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>TServ Options

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 of channels to be used as the base channels of a session. The default is 1.

Example: Base Ch Count=2

Dependencies: This parameter does not apply for leased connections.

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

See Also: Time Period

Bill

Description: Specifies a telephone number to be used for billing purposes. If a number is specified, it is used either as a billing suffix or the calling party number. For robbed-bit lines, the MAX uses the billing-number as a suffix that is appended to each 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.

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

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

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, 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.

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

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 msecs 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

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 call-back must be configured to both dial calls and answer them.

Location: Ethernet>Connections>Telco Options

See Also: AnsOrig, Call Type, Dial #

Call-by-Call

Description: This parameter currently does not apply to the Max 1800.

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 the 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 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 BRI 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. Table 6 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.

Table 6. Delta clock values

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
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 BRI 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 BRI 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. See Table 6 for a list of the host bandwidths available and the corresponding bandwidth that the network provides.

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 doesn't 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, or Connection profile, specify one of these values:

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

  This is the default for Frame Relay 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.

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.

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 nailed-up BRI circuits.

- 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.

Location: Host/Dual (Host/6)>PortN Menu>Directory, Ethernet>Connections>Telco Options, Ethernet>Frame Relay

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

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.

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

Example: Calling #=555-6787

Location: Ethernet>Connections

See Also: Id Auth

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

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)>Port*N* Menu>Port Config

See Also: Answer, Dial

Clear Call

Description: Specifies whether the dial-in connection is cleared when an interactive Telnet, Rlogin, or TCP session terminates. If 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

CLID Fail Busy

Description: Specifies whether to return Busy when Caller ID authentication fails for reasons other than a RADIUS timeout. This parameter is not RADIUS-specific.

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

- Yes means the Cause Element in the DISCONNECT message specifies User Busy.
- No means the DISCONNECT message specifies Normal Call Clearing.

Location: Ethernet>Mod Config>Auth

See Also: CLID Fail Busy, Auth

CLID Timeout Busy

Description: When Caller ID authentication times out on an ISDN connection, the MAX sends a DISCONNECT message. CLID Timeout Busy specifies whether to return User Busy when Caller ID authentication fails due to a RADIUS timeout.

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

- Yes means the Cause Element in the DISCONNECT message specifies User Busy.
- No means the DISCONNECT message specifies Normal Call Clearing.

Example: CLID Timeout Busy=Yes

Dependencies: This field applies only to RADIUS-authenticated calls.

Location: Ethernet>Mod Config>Auth

See Also: CLID Fail Busy, Auth

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

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 doesn't 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

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

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 the 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 infomation 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 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, or Frame Relay profile, Data Svc specifies the type of data service the link uses.

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.
- 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.
- 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, or PPP. 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.
- 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, Ethernet>Frame Relay

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

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

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

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)>Port*N* 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; 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)>Port*N* Menu>Directory, Ethernet>Connections, Ethernet>Frame Relay

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.

Example: Dial Plan=Trunk Grp

Location: Ethernet>Mod Config>WAN Options, Host/BRI>Line Config>Line *N*, Host/Dual (Host/6)>Port*N* 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*#

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 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

Disc on Auth Timeout

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

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

- Yes causes the MAX to hang up a PPP connection on RADIUS timeout.
- No causes it to shut down cleanly when RADIUS 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 4, "MAX Diag Command Reference."

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)>Port*N* Menu>Port Config

See Also: Max Call Mins, Max DS0 Mins

Dst Adrs

Description: Specifies a destination IP address. After this value has been modified by applying the 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 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

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)>Port*N* 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

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*

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)

Example: Encaps=MPP

Dependencies: The encapsulation type must be enabled in the Answer profile.

Location: Ethernet>Connections

See Also: MPP, MP, PPP, COMB, FR, V.120, TCP-CLEAR, ARA

See Also: Encaps

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

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 Call-back 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

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

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 the 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 infomation 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

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)>Port*N* 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 place calls to European or Pacific Rim countries from within North America and the complete path cannot distinguish between the Switched-56 and Switched-64 data services. This feature is not required if you are placing calls only within North America.

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)>Port*N* 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, Ethernet>Filters>Input filters>In filter *N*>Generic, Ethernet>Filters>Output filters>Out filter *N*>Generic

See Also: Call Filter, Data Filter, Filter, More

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 redirect 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 redirect mode, and is not commonly used.

Note: A frame relay redirect 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 frame relay redirect connection.
- No means this is not a redirect 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 redirect connections. A redirect 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 redirect mode, and is not commonly used.

Note: More than one redirected PPP connection can share a frame relay DLCI.

Usage: Specify the DLCI obtained from the frame relay administrator for redirect 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>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 Count, X.75

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

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

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

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 #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.

Usage: Specify the IP address of the host. The default value is 0.0.0.0/0.

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

/

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 #

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*N* Menu>Port Config

See Also: Call Type, Dial, Dual Ports, Profile Reqd

Idle Logout

Description: Specifies the number of minutes an administrative login can remain inactive before the MAX logs out and hangs up.

Usage: Specify a number 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 doesn't 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 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").

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

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

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

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

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 MAXnot 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, Ethernet>Answer>Session 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, X.75

L

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

Length

Description: 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.

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.

Location: Ethernet>Filters>Input filters>In filter *N*>Generic, Ethernet>Filters>Output filters>Out filter *N*>Generic, Ethernet>Firewalls

See Also: Offset, Mask, Value

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 doesn't 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

LinkUp

Description: Specifies whether the Frame Relay link comes up automatically and stays up even when the last DLCI has been removed or does not come up unless a Connection profile (DLCI) brings it up, and it shuts down after the last DLCI has been removed.

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

- Yes causes the MAX bring the link up and keep it up even if there are no active DLCIs.
- No means the link does not come up unless a Connection profile (DLCI) brings it up, and it shuts down after the last DLCI has been removed.

Dependencies: You can start and drop frame relay datalink connections by using the DO Dial and DO Hangup commands. If LinkUp is set to Yes, DO Dial brings the link down, but it will be automatically restarted. A restart will also occur if there is a Connection or Frame Relay profile invoking the datalink.

Location: Ethernet>Frame Relay

See Also: FR Prof, DLCI, Circuit

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 user 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.

Example: List Attempt=Yes

Location: Ethernet>Mod Config>DNS

See Also: List Size

List Size

Description: Specifies the number of DNS addresses that will be made accessible to terminal server users in response to a DNS query. The maximum is 35 because BSD has a limit of 35.

Usage: Specify a number between 0 and 35. The default is 6.

Dependencies: This parameter is not applicable if the List Attempt feature is disabled.

Location: Ethernet>Mod Config>DNS

See Also: List Attempt

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

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>Log

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 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

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

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.

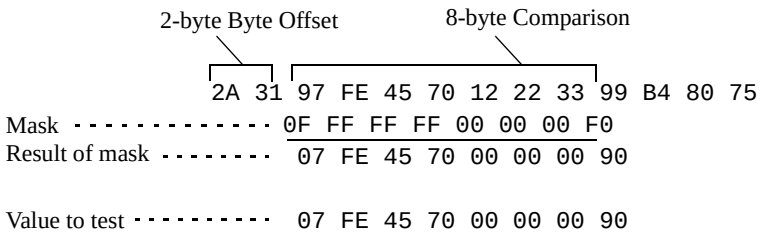
The MAX applies the mask to the specified value using a logical AND after the mask and value are both translated into binary format. The mask hides the bits that appear behind each binary 0 (zero) in the mask. A mask of all ones (FF FF FF FF FF FF FF FF) masks no bits, so the full Compare To value must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



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 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 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>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*N* Menu>Port Config

See Also: Max DS0 Mins

Max Ch Count

Description: Specifies the maximum number of channels that can be allocated to a multilink connection. For optimum performance, both sides of the connection should specify the same maximum channel count.

Usage: Specify a number between 1 and the maximum number of channels your system supports. 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*N* 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

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)>Port*N* Menu>Port Config, System>Sys Config

See Also: DS0 Min Rst

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

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*N* 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

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 packet. Usually the default is the right setting, unless the far end requires a lower number.

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.

Example: MRU=1524

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

See Also: Encaps

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 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 profile, specify the number assigned to serial WAN bandwidth.

Example: Nailed Grp=5

Location: Ethernet>Frame Relay, Serial WAN>Mod Config

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 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, BRI/LT>Line Config, System>Destinations, Ethernet>Filters, Ethernet>Firewalls, Ethernet>Frame Relay, Ethernet>IPX SAP Filters, Ethernet>Static Rtes, System>Security, Ethernet>SNMP Traps, System>Sys Config, Ethernet>Names / Passwords, System>Dial Plan

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

Network

Description: Specifies 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 NetWare server's internal 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

Node

Description: Specifies the node address on the internal network number of the server that will be reached through this static IPX route. If you are not familiar with internal network numbers, see the Novell documentation.

Usage: Specify the server's node address on its own internal network. Typically, a server running NetWare 3.11 or later has a node number of 0000000000001.

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

Location: Ethernet>IPX Routes

See Also: Route IPX, Network

No Trunk Alarm

Description: This parameter currently does not apply to the Max 1800.

O

Offset

Description: In a filter of type Generic, specifies a byte-offset from the start of a frame to the data in the packet to be tested against this filter. For example, with this filter specification:

```
Filters
   Name=filter-name
   Input filters...
      In filter 01
         Generic...
            Forward=No
            Offset=2
            Length=8
            Mask=0F FF FF FF 00 00 00 F0
            Value=07 FE 45 70 00 00 00 90
            Compare=Equals
            More=No
```

and the following packet contents:

```
2A 31 97 FE 45 70 12 22 33 99 B4 80 75
```

The first two byes in the packet (2A and 31) are ignored due to the two-byte offset.

Note: If the current filter is linked to the previous one (if More=Yes in the previous filter), the offset starts at the endpoint of the previous segment.

Usage: Specify a number indicating a byte-offset.

Example: Offset=2

Location: Ethernet>Filters>Input filters>In filter *N*>Generic, Ethernet>Filters>Output filters>Out filter *N*>Generic

See Also: Length, Mask, More

Operations

Description: Enables or disables permission to view MAX profiles and to change the value of any parameter. When it is disabled, users can view MAX profiles, but cannot change the value of any parameter (read-only security). In addition, when this permission is disabled, users cannot access most DO commands. Only DO Esc, DO Close Telnet, and DO password are available.

Note: If this permission is disabled, all other permissions are disabled as well.

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

- Yes 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

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 BRI 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 Reqd

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 Reqd=Yes

Dependencies: This parameter applies only to Combinet connections.

Location: Ethernet>Answer>COMB Options

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

Peer

Description: Specifies whether the remote IPX caller is a router or a dialin client.

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#

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 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 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 "Port*N* 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)>Port*N* Menu>Port Config

Port Password

Description: Specifies the password for incoming AIM or BONDING calls. Authentication is used only if the calling unit has a password defined in the Call profile. If the Call profile in the calling unit doesn't 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

Location: Ethernet > Mod Config >PPTP 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>Connections>Session Options

See Also: Call Type

Preference

Description: Specifies the preference value for a route. Routes come from a variety of sources. These sources have different metric systems. Whenever the Max uses multiple sources for routes, the Preference parameter allows these incompatible metrics to be compared to each other.

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
- 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 “Don't use this route;” this value is meaningful only for Connection profiles.

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

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 phone number for the ISDN BRI line. When the MAX receives a multichannel AIM, BONDING, or MP+ call, it reports the primary phone number (Pri Num) and the secondary phone number (Sec Num) to the calling party. The calling MAX can then add more channels. If you do not specify a phone 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.

Usage: Specify up to 16 characters; you must limit those characters to numbers, hyphens, and parentheses.

Example: Pri Num=30

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

See Also: Sec Num, Sub-Adr

Pri SPID

Description: Specifies the primary Service profile Identifier (SPID) for the ISDN BRI line. The SPIDs assigned to a BRI line operating in multipoint mode are numbers used at the central switch to identify services provisioned for your ISDN line. A SPID is derived from a telephone number and should be supplied by your carrier.

Note: Not all telephone companies include a suffix on their SPIDs. When receiving SPIDs from your telephone company, ask them to verify whether or not suffixes are included. The SPID formats described in the next sections have been agreed upon by most telephone companies.

For example, for an AT&T switch in multipoint mode, SPIDs have one of these formats:

01*nnnnnnn*0

01*nnnnnnn*00

In the AT&T SPID formats, *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

*aaannnnnnnSS*00

In the Northern Telecom SPID formats, *aaannnnnn* 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 Reqd

Description: Specifies whether the MAX rejects incoming calls for which it could find no Connection profile and no entry on a remote authentication server. If you don't require a configured profile for all callers, the MAX builds a temporary profile for unknown callers. Many sites consider this a security breach.

Note: Setting Profile Reqd to Yes disables Guest access for ARA connections.

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

- Yes 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. f 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 that have been assigned an address dynamically. It responds to the ARP request with its own MAC address while bringing up the connection to the remote device. This feature is referred to as Proxy ARP.

Description: Specify one of the following values:

- Off (the default) disables proxy ARP.
- Always specifies that the MAX responds to an ARP request regardless of whether a connection to the remote site is up.
- Inactive specifies that the MAX responds to an ARP request only for a remote IP address specified in a Connection profile, and only if there is no connection to the remote site.
- Active specifies that the MAX responds to an ARP request only if a connection to the remote site is up, regardless of whether a Connection profile exists for the link.

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

Location: Ethernet>Mod Config>Ether Options

See Also: Net Adrs, Route IP

R

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

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

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.

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 Reqd, 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

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

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 “Don't use this route.”

Dependencies: These are the default values for other types of routes:

- 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 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

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

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).

Location: Ethernet>Answer>PPP Option, Ethernet>Connections

See Also: Encaps, Profile Reqd

Route IPX

Description: This parameter enables or disables the routing of IPX data packets on the interface. IPX routing must be enabled on both sides of the connection, and the MAX unit must be configured with an IPX network address and frame type in the Ethernet profile. Note that the MAX will route and spoof only one IPX frame type. Other frame types will be bridged if bridging is enabled.

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

- Yes enables IPX routing.
- No 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).

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

See Also: Bridge, IPX Frame, IPX Net

Route Line N (N=1–8)

Description: There are eight Route Line parameters, one for each of the MAX unit's WAN BRI lines. If you specify the IP address of a PPTP Network Server (PNS) in one of these parameters, that WAN line is dedicated to receiving PPTP connections and forwarding them to that destination address.

The IP address you specify must be accessible via IP, but there are no other restrictions on it. It can be across the WAN or on the local network. If you leave the default null address, that WAN line handles calls normally.

Usage: Specify the IP address of a remote PNS.

Example: Route Line 1=10.1.2.3

Dependencies: These parameters do not apply if PPTP is not enabled.

See Also: PPTP Enabled

Location: Ethernet profile>Mod Config>PPTP 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*N* Menu>Port Config

See Also: Dial

S

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

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*N* Menu>Directory

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 phone number for the Net BRI line. When the MAX receives a multichannel AIM, BONDING, or MP+ call, it reports the primary phone number (Pri Num) and the secondary phone number (Sec Num) to the calling party. The calling MAX can then add more channels. If you do not specify a phone number and the calling MAX needs to add more channels, it redials the phone number it used to make the first connection.

Usage: Specify up to 16 characters; you must limit those characters to numbers, hyphens, and parentheses.

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: 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 SAFEWORD or ACE entry in the NAS's RADIUS users file with the caller's name. See the *MAX Security Supplement* for details.

Location: Ethernet>Connections>Encaps Options

See Also: APP Host, APP Port, APP Server, Call Type, Dial Brdcast, Encaps, Recv Auth, Recv PW, Send PW

Send PW

Description: Specifies the password that the MAX sends to the far-end while the connection is being authenticated. If this password is not received by the far-end device, authentication fails. If the link uses Combinet bridging and the far-end Answer profile specifies that a password is required (Password Reqd=Yes), you must enter a password using all lowercase letters.

Usage: Specify a password, up to 20 characters. The password is case sensitive. The default is null.

Dependencies: This parameter does not apply if Send Auth is set to None.

Location: Ethernet>Connections>Encaps Options

See Also: Encaps, Password Reqd, Recv Auth, Recv PW, Send Auth

Serial

Description: Specifies an ISDN subaddress associated with the MAX unit's AIM ports. ISDN subaddressing is used for routing inbound calls to the appropriate destination in the MAX unit.

Usage: Specify a number between 0 and 99. The default is 0.

Location: System>Sys Config

See Also: Ans *N*#

Server

Description: Enables or disables the on-board RADIUS server, or specifies the IP address of a BOOTP server, depending on where the parameter appears.

In the RADIUS Server submenu of the Ethernet profile, it enables or disables the on-board RADIUS server, which enables the MAX to appear as a server to some client requests.

In the BOOTP Relay submenu of the Ethernet profile, it specifies the IP address of a BOOTP server for handling BOOTP requests. If a server is on the same local-area network as the , 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 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: 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.

Dependencies: This parameter does not apply to Combinet links or connections that have hard-coded IP addresses.

Location: Ethernet>Mod Config

See Also: Encaps, Name, Pool # Count, Pool # Start, Recv PW

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

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.

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. 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

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 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/BRI module, which manipulates the base system's eight-line BRI 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.

  This applies only to AIM/BONDING cards and y indicates the port on the card.

- 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 the 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*N* 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 network switch type that provides ISDN BRI service to the MAX.

A network switch is the central office switch or PBX that terminates the ISDN BRI line at the MAX and connects the MAX to the circuit-switched WAN. The connection is a switched circuit consisting of one or more channels.

Usage: Press Enter to cycle through the choices. Your choices differ depending on the profile and enabled options.

You can select one of the switch types listed in the following table:.

Configure Profile switch types

Switch type	Explanation
AT&T/P-T-P	AT&T Point-to-Point is the default.
AT&T/Multi-P	ATT&T Multipoint.
NTI	Northern Telecommunications, Inc. Use this setting if your switch is DMS-100 Custom.
NI-1	National ISDN 1.
NI-2	National ISDN-2
U.K.	United Kingdom: ISDN-2 Hong Kong: HKT Switchline BRI Singapore: ST BRI Euro ISDN countries: Austria, Belgium, Denmark, Germany, Finland, Italy, Netherlands, Portugal, Spain, Sweden This is identical to NET 3.
SWISS	Switzerland: Swiss Net 2
NET 3	This is identical to U.K.
GERMAN	Germany 1TR6 version: DBP Telecom
MP GERMAN	Germany: 1TR6 multipoint
FRANC	France: FT Numeris
DUTCH	Netherlands 1TR6 version: PTT Netherlands BRI
BELGIUM	Belgium: Pre-Euro ISDN Belgacom Aline
JAPAN	Japan: NTT INS-64
AUSTRALIA	Australia and New Zealand

Dependencies: Keep this additional information in mind:

- The Switch Type parameter does not apply to a link using inband signaling (Call Type=56K or 56KR) or consisting entirely of nailed-up channels (Call Type=Nailed).

  For inband signaling, a line uses 8 kbps of each 64-kbps channel for WAN synchronization and signaling. The remaining 56 kbps handle the transmission of user data.

  Switched-56 lines use inband signaling.
- All international switch types except German operate in Point-to-Point mode.

Location: Net/BRI>Line Config

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 4, "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>Log

See Also: Log Facility, Log Host

T

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

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 non-zero 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

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*N* Menu>Directory>Time Period *N*

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

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.

Example: Telnet mode=ASCII

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

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 fee and a serial data rate of 2 mbps
- With a maximum cable length of 150 feet and a serial data rate of 512 kbps

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

- Yes 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

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

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 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

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 Limit

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 Limit=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 Limit 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 Limit 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 Limit

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, 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

  Don't 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

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 is the default.

- Yes enables VJ compression for TCP packets.
- No disables VJ compression.

Location: Ethernet>Answer>PPP Options

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.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

Description: Specifies the name of the AppleTalk zone in which the MAX resides. If the local Ethernet network supports an AppleTalk router with configured zones, you can place the MAX in one of those zones.

Usage: Specify the name of a zone that has been configured on the local Ethernet network. If you do not specify a name and AppleTalk=Yes, the MAX is placed in the default zone.

Dependencies: If AppleTalk is disabled, the Zone Name parameter does not apply.

Location: Ethernet>Mod Config>AppleTalk

MAX Diag Command Reference

4

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

This reference covers these topics:

Sys Diag commands

These commands appear in the System>Sys Diag menu. To use a command, highlight the command in the Sys Diag menu and press Enter.

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

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

Restore Cfg

This command restores a MAX configuration that was saved using the Save Cfg parameter, or transfers the profiles to another MAX. Because the Save Cfg command does not save passwords, the Restore Cfg command does not restore them.

You cannot save or restore a configuration using a Palmtop Controller. A Palmtop Controller is a hand-held unit for configuring, managing, and monitoring the MAX. Follow these instructions to restore your configuration from backup:

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

   The restore process is complete when the message "Upload complete--type any key to return to menu" appears on your emulator's display.

Save Cfg

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

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

You cannot save or restore a configuration using a Palmtop Controller. A Palmtop Controller is a hand-held unit for configuring, managing, and monitoring the MAX. Follow these instructions to save your configuration:

1. Verify that the Download permission is enabled in the active Security profile.
2. Verify that the Term Rate parameter in the System profile is set to 9600.
3. Verify that your terminal emulation program has a disk capture feature and an autotype feature, and that is data rate is set to 9600 baud or lower.
4. Connect the backup device to the MAX unit's Control port.
5. Turn on the autotype function on your emulator, and start the save process by typing any key on the emulator.
6. Highlight Save Cfg and press Enter.
7. Verify that configuration data is being echoed to the terminal emulation screen and that the captured data is being written to a file on your disk.

   The save process is complete when the message "Download complete--type any key to return to menu" appears on your emulator's display. The backup file is an ASCII file.
8. Turn off the autotype feature.

Use MIF

This command switches to the MIF (Machine Interface Format) interface instead of the standard vt100 interface. If you attempt to run MIF from the Palmtop Controller, the MAX displays an error message. You can also access MIF during a Telnet session or by setting Console to MIF in the System profile.

To return to the standard vt100 interface, press Ctrl-C.

Note: This command runs MIF only at the control port that makes the request (not system-wide). Similarly, Ctrl-C restores the standard vt100 interface only at the control port that makes the request.

Sys Reset

This command restarts the MAX and clears all calls without disconnecting the device from its power source. The MAX logs off all users, and returns user security to its default state. In addition, the MAX performs power-on self tests (POSTs) when it restarts. These POSTs are diagnostic tests. A system reset of a MAX causes momentary loss of T1 framing, and the T1 line might shut down. T1 framing is the way that data is encapsulated on a T1 line; if T1 framing is lost, the feedback from the MAX to the switch will be incorrect.

To perform a system reset, follow these steps:

1. Highlight System Reset and press Enter.

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

   In addition to clearing calls, the MAX performs a series of POSTs. The POST display appears. If you do not see the POST display, press Ctrl-L. If you are using the Palmtop Controller, unplug it, wait 5 seconds, and plug it back in to refresh the screen. These messages may be displayed:

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

While the yellow FAULT LED on the front panel remains solidly lit, the MAX checks system memory, configuration, installed modules, and T1 connections. If the MAX fails any of these tests, the FAULT LED remains lit or blinks. The alarm relay remains closed while the POST is running and opens when the POST completes successfully. When you see this message:

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

3 Press any key to display the Main Edit menu.

Term Serv

This command starts a terminal server session. The system displays the terminal-server command-line prompt (by default, “ascend%”). For information about the terminal server commands, type a question mark at the prompt. See the *MAX ISP & Telecommuting Configuration Guide* for more details about the terminal-server interface.

Upd Rem Cfg

This command (Upload Remote Configuration) opens a connection to a RADIUS server to upload the MAX terminal server banner, list of Telnet hosts, IP static routes, IP address pool, and other configuration information from the RADIUS user file. The MAX retrieves configuration from RADIUS at system startup or use of this command.

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

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

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

BRI/LT Line Diag commands

These commands appear in the BRI/LT>Line Diag>Line N menu. To use one of these commands, highlight the command and press Enter.

```
BRI/LT
   Line Diag
      Line N...
         Line LoopBack
         Corrupt CRC
```

```
UnCorrupt CRC
Rq Corrupt CRC
UnRq Corrupt CRC
Clr NEBE
Clr FEBE
```

Note: Maintenance functions supported by the BRI/LT driver use the BRI-U interface's embedded operations channel (EOC). The EOC transfers data from the exchange to the terminal side and vice versa without occupying either the B- or the D-channel. It is used to transmit diagnostic function and signaling information, for example:

- obtaining the block errors in close to real time.
- diagnostic functions to diagnose a line (for example, loopback, corrupt CRC)

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

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

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

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

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

Line LoopBack

This command puts the line into loopback mode. When you highlight the Line Loopback command and press Enter, this screen appears:

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

Select 1 to use the loopback command. The Line loopback command is issued and test frames are sent continuously in the D channel until the command is cancelled. Frames transmitted have a length of 24 bytes. The frames differ in content and should cover every possible bit pattern.

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

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

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

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

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

```
Line loopback terminated.
```

Corrupt CRC

This command causes the BRI-U interface to permanently transmit inverted CRCs until cancelled. When this command is issued, the far-end block error should be viewed from the remote TA. It is used to test the NEBE and FEBE counters—transmission errors are simulated with artificially corrupted CRCs.

Uncorrupt CRC

This command cancels a previous Corrupt CRC command.

Rq Corrupt CRC

This command requests NT1 to corrupt the CRC to artificially simulate transmission errors. It is used to verify that the block error counters are working, or providing the right information. When issued, check the near-end block error.

Rq Uncorrupt CRC

This command requests NT1 to return to normal.

Clr NEBE

This command clears the near-end block error (NEBE) counter.

Clr FEBE

This command clears the far-end block error (FEBE) counter.

Host/Dual (Host/6) Port Diag commands

This command appears in the Host/Dual (Host/6)>Port N Menu>Port Diag menu. To use it, highlight the command and press Enter.

```
Host/6 (or Host/Dual)
   PortN Menu
      Port Diag
         Local LB
```

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

Local LB

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

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

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

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

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

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

Modem Diag commands

These commands appear in the V.34 (V.42) Modem>Modem Diag menu. To use one of these commands, highlight the command and press Enter.

```
V.34 Modem (or V.42 Modem)
   Modem Diag
      ModemSlot=enable slot
      Modem #1=enable modem
      Modem #2=enable modem
      Modem #3=enable modem
      Modem #4=enable modem
      Modem #5=enable modem
      Modem #6=enable modem
      Modem #7=enable modem
      Modem #8=enable modem
```

Modem #N (N=1–8, 1–12)

This command temporarily disables a digital modem. A digital modem that has been temporarily disabled without disrupting existing connections is "quiesced." Active calls are not torn down. When an active call drops, that modem is added to the disabled modem list and is not available for use. If all modems are on the disabled list, incoming callers receive a busy signal until the modems have been restored for service. When you re-enable the quiesced modem, a delay of up to 20 seconds may occur before the modem becomes available for service.

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

You can specify one of the following values:

- enable modem

  This enables any modems that were on the disabled list, entering them on the enabled modem list and making them available for service.

  The default value is en modem.

- disable modem

  This places the modem on the disabled modem list, indicating that it is not available for use. When the active connection drops, the card becomes available for maintenance.

- enable modem+chan

  This enables the modem for use. The MAX removes it from the disabled modem list and enters it onto the available modem list. In addition, the MAX removes the disabled B channel from the disabled-channel map and restores it to service.

- disable modem+chan

  An arbitrary B channel is taken out of service along with the disabled modem. The B channel appears on a disabled-channel map, and the MAX polls all channels on the map with Out-Of-Service messages until the associated modem is re-enabled.

To quiesce a digital modem:

1 Open the Modem Diag submenu in the Modem profile and select a modem.

The modem ports on a slot card are numbered starting with #1 for the leftmost port on the card. Select ModemSlot to quiesce all available modems on that slot card.

2 Press Enter to disable (quiesce) the modem, or to re-enable it, depending on its current setting.

For example,

```
V.34 Modem
   Modem Diag
      ModemSlot=en slot
      Modem #1=dis modem
```

Note: To quiesce or re-enable all modems in the slot, select ModemSlot instead.

3 Close the Modem profile.

ModemSlot

This command temporarily disables a digital modem slot in the MAX without disrupting existing connections. A digital modem slot card that has been temporarily disabled without disrupting existing connections is "quiesced." Active calls are not torn down. When an active call drops, that modem is added to the disabled modem list and is not available for use. If all modems are on the disabled list, incoming callers receive a busy signal until the modems have been restored for service. When you re-enable the quiesced modem slot, a delay of up to 20 seconds may occur before the modems become available for service.

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

You can specify one of the following values:

- enable slot

  This enables any modems on the selected slot that were on the disabled list, making them available for service. The default value is en slot.

- disable slot

  All modems that are not active appear in a disabled modem list, indicating that they are not available for use.

- enable slot+chan

  This restores the slot card and channels to use. Any modems on the selected slot that appear on the disabled list are enabled and made available. For each modem enabled, an out-of-service B channel returns to service.

- disable slot+chan

  All modems on the selected slot are disabled, along with an equal number of B channels. The B channels appear on a disabled-channel map; the MAX polls all channels on the map with Out-Of-Service messages until the modems on the associated slot card return to service

MAX Profile Reference

5

This chapter shows the configuration profiles in the vt100 interface and example values for each parameter contained in those profiles. For details on the parameters listed here, see Chapter 3, “MAX Alphabetic Parameter Reference.” For details on the diagnostic commands, see Chapter 4, “MAX Diag Command Reference.”

Note: The MAX supports a variety of software loads that are customized to particular purposes. The software load you have installed may not support all of the profiles listed in this reference.

How the MAX profiles are organized

The MAX comes with eight BRI lines and a V.35 serial port for WAN access. It also has two expansion slots, which can support additional bandwidth (BRI lines), AIM ports modules to support videoconferencing, or digital modems to support analog modem connections over digital lines.

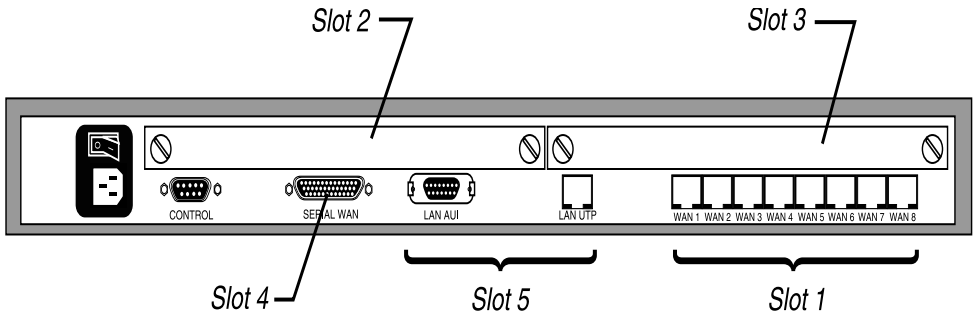


Figure 5-1. Slot and port numbering in the MAX 1800

The numbers in the vt100 menus relate to slot numbers in the MAX unit, which may be an actual expansion slot or a “virtual” slot on the unit’s motherboard.

- The system itself is assigned slot number 0 (menu 00-000).

  The System menu contains these profiles and submenus, which are all related to system-wide configuration and maintenance:

  ```
  00-000 System
     00-100 Sys Config
     00-200 Sys Diag
     00-300 Security
     00-400 Destinations
     00-500 Dial Plan
  ```

- The two expansion slots are slots 2 and 3 (menus 20-000 and 30-000), with the numbering shown in Figure 5-1.

- The Ethernet is slot 5 (menu 50-000). The Ethernet menu contains submenus and profiles related to the local network, routing and bridging, and WAN connections.
- The serial WAN port is slot 4 (menu 40-000).

This is an example Main Edit Menu at the top level, which shows expansion modules installed in slots 2 and 3.

```
Main Edit Menu
   00-000 System
   10-000 Net/BRI
   20-000 V.34
   30-000 V110
   40-000 Serial WAN
   50-000 Ethernet
```

System profiles

These profiles reside below the System menu at the top level of the vt100 menus. The settings in these profiles affect how the MAX functions system-wide.

System profile (Sys Config)

```
System
   Sys Config
      Name=gateway-1
      Location=east-bay
      Contact=mas
      Date=6/30/97
      Time=10:00:29
      Term Rate=9600
      Console=Standard
      Remote Mgmt=Yes
      Parallel Dial=5
      Single Answer=Yes
      Sub-Adr=None
      Serial=0
      LAN=0
      DM=0
      V.110=0
      Use Trunk Grps=No
      Excl Routing=No
      Auto Logout=No
      Idle Logout=0
      DS0 Min Rst=Off
      Max DS0 Mins=N/A
      High BER=10 ** -3
      High BER Alarm=No
      No Trunk Alarm=No
      Delay Dual=No
      Edit=00-000
```

```
      Status 1=10-100
      Status 2=50-300
      Status 3=50-100
      Status 4=00-200
      Status 5=50-500
      Status 6=50-400
      Status 7=00-100
      Status 8=00-000
```

System diagnostics (Sys Diag)

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

Security profiles

```
System
   Security
      Name=Default
      Passwd=Ascend
      Operations=No
      Edit Security=N/A
      Edit System=N/A
      Edit Line=N/A
      Edit All Ports=N/A
      Edit Own Port=N/A
      Edit All Calls=N/A
      Edit Com Call=N/A
      Edit Own Call=N/A
      Edit Cur Call=N/A
      Sys Diag=N/A
      All Port Diag=N/A
      Own Port Diag=N/A
      Download=N/A
      Upload=N/A
      Field Service=N/A
```

Destination profiles

```
System
   Destinations
      Name=outdial-1
      Option=1st Avail
      Dial 1#=4-212-555-1212
      Dial 2#=5-212-555-1212
      Dial 3#=
```

```
      Dial 4#=
      Dial 5#=
      Dial 6#=
```

Dial Plan profiles

```
System
   Dial Plan
      Name=host1
      Call-by-Call=8
      Data Svc=56KR
      PRI # Type=National
      Transit #=222
      Bill #=
```

Profiles for WAN lines and ports

Serial WAN port

```
Serial WAN
   Mod Config
      Module Name=serial
      Nailed Grp=3
      Activation=Static
```

Host/Dual (Host/6) AIM ports

```
Host/6
   Mod Config
      Module Name=dualport
      Port 1/2 Dual=Yes
      Port 3/4 Dual=Yes
      Port 5/6 Dual=No
      Palmtop=Full
      Palmtop Port #=N/A
      Palmtop Menus=Standard

Host/Dual
   Mod Config
      Module Name=nodual
      Dual Ports=No Dual
      Palmtop=Full
      Palmtop Port #=N/A
      Palmtop Menus=Standard

Host/6 (or Host/Dual)
   PortN Menu
      Port Config
         Port Name=Port1
         Dial Plan=Trunk Grp
         Ans 1#=1212
```

```
            Ans 2#=1213
            Ans 3#=
            Ans 4#=
            Idle=None
            Dial=Terminal
            Answer=Auto
            Clear=Terminal
            Term Timing=No
            RS-366 Esc=N/A
            Early CD=None
            DS0 Min Rst=Off
            Max DS0 Mins=N/A
            Max Call Mins=0
            Port Password=Ascend

Host/6 (or Host/Dual)
   PortN Menu
      Directory
         Name=bonding
         Dial #=212-555-1212
         Call Type=BONDING
         Call Mgm=Mode 1
         Data Svc=56K
         Force 56=No
         Base Ch Count=3
         Inc Ch Count=2
         Dec Ch Count=1
         Bill #=212-555-1213
         Auto-BERT=120
         Bit Inversion=No
         Fail Action=Disc
         Group=N/A
         FT1 Caller=N/A
         B&O Restore=N/A
         Flag Idle=Yes
         Dyn Alg=N/A
         Sec History=N/A
         Add Pers=N/A
         Sub Pers=N/A
         Time Period N...
            Activ=N/A
            Beg Time=N/A
            Min Ch Cnt=2
            Max Ch Cnt=12
            Target Util=N/A
         Call Password=Ascend

Host/6 (or Host/Dual)
   PortN Menu
      Port Diag
         Local LB
```

Net BRI lines

```
Net/BRI
   Line Config
      Name=bri-net
      Switch Type=AT&T
      Line N...
         Enabled=Yes
         Link Type=P_T_P
         B1 Usage=Switched
         B1 Slot=3
         B1 Prt/Grp=1
         B1 Trnk Grp=5
         B2 Usage=Switched
         B2 Slot=3
         B2 Prt/Grp=2
         B2 Trnk Grp=5
         Pri Num=555-1212
         Pri SPID=01555121200
         Sec Num=555-1213
         Sec SPID=01555121300
```

Host BRI lines

```
Host BRI
   Line Config
      Name=local
      Line N...
         Enabled=Yes
         Dial Plan=Extended
         Ans 1#=1212
         Ans 2#=
```

BRI/LT lines

```
BRI/LT
   Line Config
      Name=idsl
      Line N...
         Enabled=Yes
         Dial Plan=N/A
         B1 Usage=Switched
         B1 Prt/Grp=N/A
         B1 Trnk Grp=0
         B2 Usage=Switched
         B2 Prt/Grp=N/A
         B2 Trnk Grp=0
         Ans 1#=1212
         Ans 2#=

BRI/LT
   Line Diag
      Line N...
```

```
      Line LoopBack
      Corrupt CRC
      UnCorrupt CRC
      Rq Corrupt CRC
      UnRq Corrupt CRC
      Clr NEBE
      Clr FEBE
```

V.110 modems

```
V.110
   Mod Config
      Ans 1#=12
      Ans 2#=13
      Ans 3#=14
      Ans 4#=15
```

V.34 (V.42) modems

```
V.34 Modem (or V.42 Modem)
   Mod Config
      Ans 1#=12
      Ans 2#=13
      Ans 3#=14
      Ans 4#=15

V.34 Modem (or V.42 Modem)
   Modem Diag
      ModemSlot=enable slot
      Modem #1=enable modem
      Modem #2=enable modem
      Modem #3=enable modem
      Modem #4=enable modem
      Modem #5=enable modem
      Modem #6=enable modem
      Modem #7=enable modem
      Modem #8=enable modem
```

Network profiles

Answer profile

```
Ethernet
   Answer
      Use Answer as Default=No
      Force 56=No
      Profile Reqd=Yes
      Id Auth=None
      Assign Adrs=No
```

```
Encaps...
   MPP=Yes
   MP=Yes
   PPP=Yes
   COMB=Yes
   FR=Yes
   EU-RAW=Yes
   EU-UI=Yes
   V.120=Yes
   X.75=Yes
   TCP-CLEAR=Yes
   ARA=Yes

IP options...
   Metric=7
IPX options...
   Peer=N/A

PPP options...
   Route IP=Yes
   Route IPX=Yes
   Bridge=Yes
   Recv Auth=Either
   MRU=1524
   LQM=No
   LQM Min=600
   LQM Max=600
   Link Comp=Stac
   VJ Comp=Yes
   BACP=No
   Dyn Alg=Quadratic
   Sec History=15
   Add Pers=5
   Sub Pers=10
   Min Ch Count=1
   Max Ch Count=1
   Target Util=70
   Idle Pct=0
  Disc on Auth Timeout=Yes

COMB options...
   Password Reqd=Yes
   Interval=10
   Compression=Yes

V.120 options...
   Frame Length=260

X.75 options...
   K Window Size=7
   N2 Retran Count=10
   T1 Retran Timer=1000
   Frame Length=2048

Session options...
   RIP=Off
```

```
   Data Filter=5
   Call Filter=3
   Filter Persistence=No
   Idle=120
   TS Idle Mode=N/A
   IPX SAP Filter=1
```

Bridge Adrs profile

```
Ethernet
   Bridge Adrs
      Enet Adrs=CFD012367
      Net Adrs=10.1.1.12
      Connection #=7
```

Connection profile

```
Ethernet
   Connections
      Station=device-name
      Active=Yes
      Encaps=MPP
      Dial #=555-1212
      Calling #=555-2323
      Called #=555-1212
      Route IP=Yes
      Route IPX=No
      Bridge=No
      Dial brdcast=N/A
     Encaps=MPP
     Encaps options...
        Send Auth=None
        Send PW=N/A
        Aux Send PW
        Recv PW=
        DBA Monitor=Transmit
        Base Ch Count=1
        Min Ch Count=1
        Max Ch Count=2
        Inc Ch Count=1
        Dec Ch Count=1
        MRU=1524
        LQM=No
        LQM Min=600
        LQM Max=600
        Link Comp=Stac
        VJ Comp=Yes
        Dyn Alg=Quadratic
        Sec History=15
        Add Pers=5
        Sub Pers=10
        Target Util=70
       Idle Pct=0
```

```
Encaps=MP
Encaps options...
   Send Auth=None
   Send PW=N/A
   Aux Send PW
   Recv PW=
   Base Ch Count=1
   Min Ch Count=1
   Max Ch Count=2
   Inc Ch Count=1
   Dec Ch Count=1
   MRU=1524
   LQM=No
   LQM Min=600
   LQM Max=600
   Link Comp=Stac
   VJ Comp=Yes
   BACP=No
   Dyn Alg=Quadratic
   Sec History=15
   Add Pers=5
   Sub Pers=10
   Target Util=70

Encaps=PPP
Encaps options...
   Send Auth=None
   Send PW=N/A
   Recv PW=
   MRU=1524
   LQM=No
   LQM Min=600
   LQM Max=600
   Link Comp=Stac
   VJ Comp=Yes

Encaps=COMB
Encaps options...
   Password Reqd=No
   Send PW=N/A
   Recv PW=
   Interval=10
   Base Ch Count=1
   Compression=Stac

Encaps=FR
Encaps options...
   FR Prof=
   DLCI=16

Encaps=FR_CIR
Encaps options...
   FR Prof=
   DLCI=16

Encaps=X25/IP
Encaps options...
   X.25 Prof=ATT
   LCN=0
```

```
   Encaps Type=RFC877
   Reverse Charge=No
   Max Unsucc. calls=0
   Inactivity Timer=0
   MRU=1500
   Call Mode=Both
   Answer X.121 Addr=
   Remote X.121 addr=

Encaps=X25/PAD
Encaps options...
   X.25 Prof=ATT
   Recv PW=localpw
   LCN=0
   X.3 Param Prof=CRT
   Max Unsucc. calls=0
   VC Timer enable=DISABLE
   Auto-Call X.121 addr=
   Reverse Charge=No

Encaps=ARA
Encaps options...
   Password=*SECURE*
   Max. Time (min)=0

Encaps=TCP-CLEAR
Encaps options...
   Recv PW=localpw
   Login Host=techpubs
   Login Port=23

Encaps=EU-RAW
Encaps options...
   MRU=1524

Encaps=EU-UI
Encaps options...
   DCE Addr=1
   DTE Addr=3
   MRU=1524

 IP options...
    LAN Adrs=0.0.0.0/0
    WAN Alias=0.0.0.0/0
    IF Adrs=0.0.0.0/0
    Preference=100
    Metric=7
    Private=No
    RIP=Off
    Pool=0
    Client Pri DNS=0.0.0.0
    Client Sec DNS=0.0.0.0
    Client Assign DNS=Yes
    Client Gateway=0.0.0.0

 IPX options...
    Peer=Router
    IPX RIP=None
    IPX SAP=Send
    Dial Query=No
```

```
      IPX Net#=cfff0003
      IPX Alias#=00000000
      Handle IPX=None
      Netware t/o=30

   Session options...
      Data Filter=5
      Call Filter=3
      Filter Persistence=No
      Idle=120
      TS Idle Mode=N/A
      TS Idle =N/A
      Max Call Duration=0
      Preempt=N/A
      IPX SAP Filter=0
      BackUp=
      IP Direct=0.0.0.0
      ATMP Gateway=N/A
      FR Direct=No
      FR Prof=N/A
      FR DLCI=N/A

   Telco options...
      AnsOrig=Both
      Callback=Yes
      Exp Callback=No
      Call Type=Switched
      Group=N/A
      FT1 Caller=N/A
      Data Svc=56KR
      Force 56=N/A
      Bill #=555-1212
      Dialout OK=No

   Accounting...
      Acct Type=None
      Acct Host=N/A
      Acct Port=N/A
      Acct Timeout=N/A
      Acct Key=N/A
      Acct-ID Base=N/A
```

Ethernet profile (Mod Config)

```
Ethernet
   Mod Config
      Module Name=

      Ether options...
         IP Adrs=10.65.212.100/24
         2nd Adrs=0.0.0.0/0
         RIP=Both-v1
         Ignore Def Rt=Yes
```

```
   Proxy Mode=Off
   Filter=5
   IPX Frame=None
   IPX Enet#=N/A
   IPX Pool#=N/A
   IPX SAP Filter=N/A
   Handle IPX Type20=N/A

WAN options...
   Dial Plan=Trunk
   Ans 1#=1212
   Ans 2#=1213
   Ans 3#=1214
   Ans 4#=1215
   Pool#1 start=100.1.2.3
   Pool#1 count=128
   Pool#2 start=0.0.0.0
   Pool#2 count=0
   Pool#3 start=10.2.3.4
   Pool#3 count=254
   Pool#4 start=0.0.0.0
   Pool#4 count=0
   Pool#5 start=0.0.0.0
   Pool#5 count=0
   Pool#6 start=0.0.0.0
   Pool#6 count=0
   Pool#7 start=0.0.0.0
   Pool#7 count=0
   Pool#8 start=0.0.0.0
   Pool#8 count=0
   Pool#9 start=0.0.0.0
   Pool#9 count=0
   Pool#A start=0.0.0.0
   Pool#A count=0
   Pool only=No
   Pool Summary=No

SNMP options...
   Read Comm=Public
   R/W Comm=write
   Security=No
   RD Mgr1=10.0.0.1
   RD Mgr2=10.0.0.2
   RD Mgr3=10.0.0.3
   RD Mgr4=10.0.0.4
   RD Mgr5=10.0.0.5
   WR Mgr1=10.0.0.11
   WR Mgr2=10.0.0.12
   WR Mgr3=10.0.0.13
   WR Mgr4=10.0.0.14
   WR Mgr5=10.0.0.15

Route Pref…
   Static Preference=100
```

```
   Rip Preference-100
TServ options...
   TS Enabled=Yes
   Passwd=Ascend
   Banner=** Ascend Terminal Server **
   Login Prompt=Login:
   Passwd Prompt=Password:
   Prompt=ascend%
   Prompt Format=No
   Term Type=vt100
   PPP=Yes
   SLIP=Yes
   SLIP BOOTP=No
   V42/MNP=Will
   Max Baud=33600
   MDM Trn Level=-13
   Cell First=No
   Cell Level=18
   Telnet =Yes
   Rlogin=Yes
   Def Telnet=Yes
   Clear Call=Yes
   Telnet mode=ASCII
   Local Echo=No
   Buffer chars=No
   Initial Scrn=Cmd
   Toggle Scrn=No
   Security=Full
   3rd Prompt=
   3rd Prompt Seq=N/A
   IP Addr Msg=IP address is
   Remote Conf=No
   Host #1 Addr=0.0.0.0
   Host #1 Text=
   Host #2 Addr=0.0.0.0
   Host #2 Text=
   Host #3 Addr=0.0.0.0
   Host #3 Text=
   Host #4 Addr=0.0.0.0
   Host #4 Text=
   Immed Service=None
   Immed Host=N/A
   Immed Port=N/A
   Telnet Host Auth=No
   PPP Delay=5
   PPP Direct=No
   7-Even=No
   Ppp Info=mode
   Clr Scrn=Yes
   Silent=No
   Modem Dialout=Yes
   Immediate Modem=No
```

```
   Imm. Modem port=N/A
   Imm. Modem Access=None
   Immm. Modem Pwd=N/A
   Packet Wait time=0
   Packet characters=0
   Login Timeout=300

Bridging=Yes
IPX Routing = No
AppleTalk=Yes
Shared Prof=No
Telnet PW=Ascend
RIP Policy=Split Horzn
RIP Summary = Yes
ICMP Redirects = Ignore

BOOTP Relay...
   BOOTP Relay Enable=No
   Server=N/A
   Server=N/A

DNS...
   Domain Name=abc.com
   Sec Domain Name=
   Pri DNS=10.65.212.10
   Sec DNS=12.20 7.23.51
   Allow As Client DNS=Yes
   Pri WINS=0.0.0.0
   Sec WINS=0.0.0.0
   List Attempt=No
   List Size=N/A
   Client Pri DNS=0.0.0.0
   Client Sec DNS=0.0.0.0

Auth...
   Auth=RADIUS
   Auth Host #1=10.6.212.178
   Auth Host #2=10.6.212.178
   Auth Host #3=10.6.212.178
   Auth Port=1645
   Auth Src Port=0
   Auth Timeout=20
   Auth Key=Ascend
   Auth Pool=No
   Auth TS Secure=Yes
   Auth Send Attr. 6,7=No
   Local Profiles First=Yes
   Auth Req=Yes
   CLID Timeout Busy=No
   CLID Fail Busy=No
   APP Server=No
   APP Host=N/A
   APP Port=N/A
   SecureID DES encryption=N/A
   SecurID host retries=N/A
```

```
   SecureID NodeSecret=N/A
   Sess Timer=N/A

Accounting...
   Acct=RADIUS
   Acct Host #1=10.6.212.140
   Acct Host #2=0.0.0.0
   Acct Host #3=0.0.0.0
   Acct Port=1646
   Acct Src Port=0
   Acct Timeout=10
   Acct Key=Ascend
   Sess Timer=0
   Acct-ID Base=10

RADIUS Server...
   Server=No
   Client #1=N/A
   Server Key#1=N/A
   Client #2=N/A
   Server Key#2=N/A
   Client #3=N/A
   Server Key#3=N/A
   Client #4=N/A
   Server Key#4=N/A
   Client #5=N/A
   Server Key#5=N/A
   Client #6=N/A
   Server Key#6=N/A
   Client #7=N/A
   Server Key#7=N/A
   Client #8=N/A
   Server Key#8=N/A
   Client #9=N/A
   Server Key#9=N/A
   Server Port=N/A
   Session Key=N/A
   Attributes=N/A

Log...
   Syslog=Yes
   Log Host=10.65.212.12
   Log Facility=Local0

ATMP...
   ATMP Mode=Home
   Type=Gateway
   Passwd=Ascend
   SAP Reply=No
   UDP Port=5150

PPTP options...
   PPTP Enabled=Yes
   Route line 1=10.65.212.11
   Route line 2=0.0.0.0
```

```
      Route line 3=0.0.0.0
      Route line 4=0.0.0.0
   Modem Ringback=No
   AppleTalk...
      Zone Name=engnet
   SNTP Server...
      SNTP Enabled=Yes
      Time zone-UTC+0000
      SNTP host#1=0.0.0.0
      SNTP host#2=0.0.0.0
      SNTP host#3=0.0.0.0
   Stack options...
      Stacking Enabled=No
      Stack Name=maxstack-1
      UDP Port=6000
   UDP Cksum=No
   Adv Dialout Routes=Always
```

Filter profiles

```
Ethernet
   Filters
      Name=filter-name
      Input filters...
         In filter 01–12
            Valid=Yes
            Type=GENERIC
            Generic...
               Forward=No
               Offset=14
               Length=8
               Mask=ffffffffffffffff
               Value=aaaa0300000080f3
               Compare=Equals
               More=No
            Ip...
               Forward=No
               Src Mask=255.255.255.192
               Src Adrs=192.100.50.128
               Dst Mask=0.0.0.0
               Dst Adrs=0.0.0.0
               Protocol=0
               Src Port Cmp=None
               Src Port #=N/A
               Dst Port Cmp=None
               Dst Port #=N/A
               TCP Estab=N/A
      Output filters...
         Out filter 01–12
            Valid=Yes
            Type=GENERIC
            Generic...
               Forward=No
```

```
      Offset=14
      Length=8
      Mask=ffffffffffffffff
      Value=aaaa0300000080f3
      Compare=Equals
      More=No
   Ip...
      Forward=No
      Src Mask=255.255.255.192
      Src Adrs=192.100.50.128
      Dst Mask=0.0.0.0
      Dst Adrs=0.0.0.0
      Protocol=0
      Src Port Cmp=None
      Src Port #=N/A
      Dst Port Cmp=None
      Dst Port #=N/A
      TCP Estab=N/A
```

Firewall profiles

```
Ethernet
   Firewalls
      Name=my-firewall
      Version=2056
      Length=2.0b
```

Frame Relay profile

```
Ethernet
   Frame Relay
      Name=NNI
      Active=Yes
      Call Type=Nailed
      FR Type=NNI
      LinkUp=Yes
      Nailed Grp=1
      Data Svc=64k
      Dial #=N/A
      Link Mgmt=Q.933A
      N391=6
      DTE N392=3
      DTE N393=4
      DCE N392=3
      DCE N393=4
      T391=10
      T392=15
      MRU=1532
```

IPX Routes profile

```
Ethernet
   IPX Routes
```

```
IPX Routes A01-A16
Server Name=server-name
Active=Yes
Network=CC1234FF
Node=000000000001
Socket=0000
Server Type=0004
Hop Count=2
Tick Count=12
Connection #=0
```

IPX SAP Filter profile

```
Ethernet
   IPX SAP Filters
      IPX SAP Filters B01-B08
      Name=optional
      Input SAP filters...
         In SAP filter 01–08
            Valid=Yes
            Type=Exclude
            Server Type=0004
            Server Name=SERVER-1
      Output SAP filters
         Out SAP filter 01–08
            Valid=Yes
            Type=Exclude
            Server Type=0004
            Server Name=SERVER-1
```

Names / Passwords profile

```
Ethernet
   Names / Passwords
      Name=Brian
      Active=Yes
      Recv PW=brianpw
      Template Connection #=0
```

SNMP Traps profile

```
Ethernet
   SNMP Traps
      Name=
      Alarm=Yes
      Port=Yes
      Security=Yes
      Comm=
      Dest=10.2.3.4
```

Static Rtes profile (IP routes)

```
Ethernet
  Static Rtes
    Name=SITEBGW
    Active=Yes
    Dest=10.2.3.0/24
    Gateway=10.2.3.4
    Metric=2
    Preference=100
    Private=No
```

Index

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

X

Z