Pipeline 130 Reference Guide

Ascend Communications, Inc.
Part Number: 7820-0279-003
For software version 6.0
January 30, 1998

Contacting Ascend Customer Service

You can request assistance or additional information by telephone, email, fax, or modem, or over the Internet.

Obtaining Technical Assistance

If you need technical assistance, first gather the information that Ascend Customer Service will need for diagnosing your problem. Then select the most convenient method of contacting Ascend Customer Service.

Information you will need

Before contacting Ascend Customer Service, gather the following information:

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

How to contact Ascend Customer Service

After you gather the necessary information, 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)
Austria/Germany/Switzerland	(+33) 492 96 5672
Benelux	(+33) 492 96 5674

France	(+33) 492 96 5673
Italy	(+33) 492 96 5676
Japan	(+81) 3 5325 7397
Middle East/Africa	(+33) 492 96 5679
Scandinavia	(+33) 492 96 5677
Spain/Portugal	(+33) 492 96 5675
UK	(+33) 492 96 5671
Email	support@ascend.com
Email (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
1701 Harbor Bay Parkway
Alameda, CA 94502

Need information about new features and products?

Ascend is committed to constant product improvement. You can find out about new features and other improvements as follows:

- For the latest information about 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

Tables

About This Guide

How to use this guide

This manual is part of a set that describes all the standard features of a Pipeline running software version 6.0. Some features might not be available with older versions or specialty loads of the software. Features that are available only with specialty loads are documented in separate publications.

Use this manual in conjunction with the *Start Here* manual and the *User's Guide* to configure the Pipeline and monitor the status menus.

- DO commands give you a way to manually dial or hang up calls, plus gives you access to the diagnostic tools included in the Pipeline.
- The alphabetical parameter listing can help you quickly access the information you need to configure the Pipeline.
- The status menu reference gives you information about every field on the status screens seen in the on-board software.

What you should know

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

- Internet or telecommuting concepts
- Wide area network (WAN) concepts
- Local area network (LAN) concepts

Documentation conventions

This section explains all the special characters and typographical conventions in this manual.

Convention	Meaning
`Monospace text`	Represents text that appears on your computer's screen, or that could appear on your computer's screen.
>	Points to the next level in the path to a parameter. The parameter that follows the angle bracket is one of the options that appears when you select the parameter that precedes the angle bracket.
Press Enter	Means press the Enter, or Return, key or its equivalent on your computer.
Note:	Introduces important additional information.
 **Caution:**	Warns that a failure to follow the recommended procedure could result in loss of data or damage to equipment.
 **Warning:**	Warns that a failure to take appropriate safety precautions could result in physical injury.

Manual set

This manual is part of a set which includes the following publications:

- *Pipeline Start Here*

  The *Start Here* manual explains how to install the Pipeline and describes how to use the on-board software.

- *Pipeline User's Guide*

  The *User's Guide* explains how to configure the Pipeline as a router or bridge, and how to manage the inbound and outbound traffic over the unit.

- *Pipeline Reference Guide*

  The *Reference Guide* contains an alphabetical listing of all the parameters, fields in the status menus, and how to use the DO commands.

DO Command Reference

1

This chapter includes the following topics:

Using DO commands

The DO menu is a context-sensitive list of commands that appears when you press Ctrl-D if you are connected to the Pipeline in VT100 terminal emulation mode. If your connection to the Pipeline is via Ethernet, Telnet into the unit to use the DO commands. Otherwise, connect a serial cable from your computer to the serial connector on the back of the unit and connect to the Pipeline using the VT100 terminal emulator in your communications software.

The commands in the DO menu vary depending on your security privileges and 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, 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.

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
Close TELNET (DO C)	Close the current Telnet session.
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.
Hang Up (DO 2)	Hang up from a call in progress.
Save (DO S)	Save parameter values into the specified profile.
Password (DO P) 9	Log into or out of the Pipeline.
Termserv (DO E)	Access the terminal server interface.

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. 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.

Close TELNET (DO C)

Description: Closes the current Telnet session. You must be running a Telnet session from the Pipeline unit's terminal server interface.

Diagnostics (DO D)

Invokes diagnostics mode. You 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 establishes a session defined in the selected Connection profile. Before you can establish a session, the selector (>) must be in one of the following positions:

- In front of a Connection profile in the Connections menu.
- At any parameter within a Connection profile.

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

Keep this additional information in mind:

- Dial is not available when the link is busy.
- 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 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, “Parameter Reference.”

Esc (DO 0)

Exits the DO menu.

Hang Up (DO 2)

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).
- The DO Hangup command does not appear if you are not logged in with operational privileges.

Password (DO P)

Enables you to log into the Pipeline.

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 Pipeline automatically logs you out. The Pipeline 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 Pipeline, 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 Pipeline 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 Pipeline locally and you want to secure the Pipeline 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 Pipeline 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.

Save (DO S)

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.

Termserv (DO E)

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 *User's Guide*. To exit terminal server mode and return to the VT100 interface, use the Quit command:

```
ascend% quit
```

Terminal Server Commands

2

This chapter lists the commands available at the ascend% prompt in the terminal interface of the on-board software.

To invoke the terminal server command-line interface, you must have administrative privileges, as described in the "Pipeline System Administration" chapter of the *User's Guide*.

To open the terminal server command-line interface:

1 Open the Sys Diag > Term Serv menu and press Enter or, from the DO Command menu, select E=Termsrv.

The command-line prompt is displayed at the bottom of the VT100 window:

```
ascend%
```

2 To close the terminal server command-line interface, use the Quit command at the prompt.

For example:

```
ascend% quit
```

The terminal server command-line interface closes and the cursor is returned to the VT100 menus.

Alphabetical listing of commands

?

Displays help information.

Dnstab Edit

Starts editor for local DNS table. See the Show Dnstab Edit command for information about the output of this command.

Dnstab Entry

Displays local DNS table entry. See Dnstab Entry command for information about the output of this command.

Dnstab Show

Displays local DNS table. See Dnstab Show command for information about the output of this command.

Hangup

Closes the connection. Same as quit.

Help

Help on any named command. Use the syntax “help *command name*”. Alternatively, you can enter “*command name* ?” for information about a command.

Iproute Add

To add a static route to the Pipeline unit’s routing table, enter the Iproute Add command in this format:

```
iproute add <destination/size><gateway>[pref]
[metric][proto]
```

iproute add command arguments

The arguments to the Iproute Add command are as follows:

- destination/size

  The destination network address and the subnet mask in Ascend netmask (slash) notation.

- gateway

  The IP address of the router that can forward packets to that network.

- pref

  The preference value for the route. When choosing which routes should be put in the routing table, the router first compares the Preference value, preferring the lower number. If the Preference values are equal, the router then compares the Metric field, using the route with the lower Metric.

- metric

  The virtual hop count to the destination network (default 7).

- proto

  The protocol of the route.

For example, enter this command:

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

to add a route to the 10.1.2.0 network and all of its subnets through the IP router located at 10.0.0.3/24. The metric to the route is 1 (it is one hop away).

If you try to add a route to a destination that already exists in the routing table, the Pipeline replaces the existing route, but only if the existing route has a higher metric. If you get the message “Warning: a better route appears to exist”, the Pipeline rejected your attempt to add a route because the routing table already contained the same route with a lower metric. Note that RIP updates can change the metric for the route.

Note: The Iproute Add command adds a static route that is lost whenever the Pipeline is reset.

Iproute Delete

To remove a route from the Pipeline unit's routing table, enter the Iproute Delete command in this format:

```
iproute delete <destination/size><gateway>[proto]
```

For example:

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

Note: RIP updates can add back any route you remove with Iproute Delete. Also, the Pipeline restores all routes listed in the Static Route profile after a system reset.

iproute delete command arguments

The arguments to the Iproute Delete command are as follows:

- destination/size
  The destination network address.
- gateway
  The IP address of the router that can forward packets to that network.
- proto
  The protocol of the route.

Iproute Show

Displays IP routes. See Show IP Routes for information about the output of this command.

IPXping

The IPXping command enables you to verify the transmission path to NetWare stations at the network layer. It works on the same LAN as the Pipeline or across a WAN connection that has IPX Routing enabled.

Enter the IPXping command in this format:

ipxping [-c count] [-i delay] [-s packetsize] <[servername] [net#:node#]>

where <servername> is either the IPX address of the NetWare workstation or the advertised name of a server.

The IPX address consists of the IPX network and node numbers for a station; for example:

```
ascend% ipxping CFFF1234:000000000001
```

If you are using IPXping to verify connectivity with an advertised NetWare server, you can simply enter the symbolic name of the server; for example:

```
ascend% ipxping server-1
```

You can terminate the IPXping at any time by typing Ctrl-C.

During the IPXping exchange, the Pipeline calculates and reports this information:

```
PING server-1 (EE000001:000000000001): 12 data bytes
52 bytes from (EE000001:000000000001): ping_id=0 time=0ms
52 bytes from (EE000001:000000000001): ping_id=1 time=0ms
52 bytes from (EE000001:000000000001): ping_id=2 time=0ms
?
--- novl1 Ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0/0/0 ms
```

These statistics include the following information:

- The IPX address of the source and destination nodes.
- The byte counts of the request and response packets.
- The Ping ID of the command. (The Ping Request # replied to by target host.)
- The number of milliseconds required to send the IPXping and receive a response.
- The number of packets transmitted and received.
- Duplicate or damaged packets, if applicable.
- Average round-trip times for the Ping request and reply.

  In some cases, round-trip times cannot be calculated.

IPXping command arguments

The arguments to the IPXping command are:

- servername

  The advertised name of the IPX server.

- [-c count]

  (Optional.) Stop the test after sending and receiving the number of packets specified by count.

- [-i delay]

  (Optional.) Wait the number of seconds specified by wait before sending the next packet. The default is one second.

- [-s packet-size]

  (Optional.) Send the number of data bytes specified by packet-size. The default is 56 bytes. Packet-size does not include the 8-byte ICMP header.

- [net#:node#]

  The IPX network and node number of an IPX host.

  – The network number can be 0x00000000 (the local network) to 0xfffffffe.

  – The node number can be 0x0000000001 to 0xfffffffffe.

Local

Puts the terminal server in local mode.When a dial-in user enters the Local command, it begins a Telnet session to the Pipeline.

Ping

The Ping command sends an ICMP mandatory echo_request datagram, which asks the remote station “Are you there?” If the echo_request reaches the remote station, the station sends back an ICMP echo_response datagram, which tells the sender “Yes, I am alive.” This exchange verifies that the transmission path is open between the Pipeline and a remote station.

The Ping command uses this format:

```
ping [-qv] [-c count] [-i delay] [-s packetsize]
hostname
```

For example:

```
ascend% ping -c 256 10.1.2.3
```

You can terminate the Ping exchange at any time by typing Ctrl-C. During the Ping exchange, the Pipeline displays information about the packet exchange that looks similar to this:

```
PING 10.1.2.3 (10.1.2.3): 56 data bytes
64 bytes from 10.1.2.3: icmp_seq=0 ttl=255 time=30 ms
64 bytes from 10.1.2.3: icmp_seq=1 ttl=255 time=0 ms
64 bytes from 10.1.2.3: icmp_seq=2 ttl=255 time=0 ms
64 bytes from 10.1.2.3: icmp_seq=3 ttl=255 time=10 ms
64 bytes from 10.1.2.3: icmp_seq=4 ttl=255 time=0 ms
^ C
--- 10.1.2.3 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0/1/30 ms
```

The output contains this information:

- The TTL (Time-To-Live) of each ICMP echo_response datagram.

  The maximum TTL for ICMP Ping is 255 and the maximum TTL for TCP is often 60 or lower, so you might be able to ping a host but not be able to run a TCP application (such as Telnet or FTP) to that station.

  If you Ping a host running a version of Berkeley UNIX before 4.3BSD-Tahoe, the TTL report is 255 minus the number of routers in the round-trip path. If you Ping a host running the current version of Berkeley UNIX, the TTL report is 255 minus the number of routers in the path from the remote system to the station performing the Ping.
- Duplicate or damaged echo_response packets.
- Round-trip and packet-loss statistics.

  In some cases, round-trip times cannot be calculated.

Ping command arguments

The arguments to the Ping command are:

- hostname
  The IP address or name of the host.
- [-q]
  (Optional.) Use quiet input. Do not display any informational messages, except the summary lines at the beginning and end of the command.
- [-v]
  (Optional.) Use verbose output. The Pipeline lists all ICMP packets received, except echo_response packets.
- [-c count]
  (Optional.) Stop the test after sending and receiving the number of packets specified by count.
- [-i delay]
  (Optional.) Wait the number of seconds specified by wait before sending the next packet. The default is one second.
- [-s packet-size]
  (Optional.) Send the number of data bytes specified by packet-size. The default is 56 bytes. packet-size does not include the 8-byte ICMP header.

Quit

Closes the terminal server session.

Remote

After an MP+ connection has been established with a remote station (for example, by using the DO Dial command), you can start a remote management session with that station by entering the Remote command in this format:

```
remote <station>
```

For example:

```
ascend% remote lab17gw
```

During the remote management session, the user interface of the remote device replaces your local user interface, as if you had opened a Telnet connection to the device.You can enter Ctrl-\ at any time to terminate the Remote session. Note that

either end of an MP+ link can terminate the session by hanging up all channels of the connection.

The argument to the Remote command is the name of the remote station, which must match the value of a Station parameter in a Connection profile that allows outgoing MP+ calls.

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

Remote management privileges

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

Remote error messages

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

Table 2-1. REMOTE error messages

`not authorized`	Your current security privileges are insufficient for beginning a remote management session. To assign yourself the required privileges, log in with the DO Password command to a Security profile whose Edit System parameter is set to Yes.
`can’t find profile for <station>`	The Pipeline could not locate a local Connection profile containing a Station parameter whose value matched <station>.
`profile for <station> doesn’t specify MPP`	The local Connection profile containing a Station value equal to <station> did not contain Encaps=MPP.

Table 2-1. REMOTE error messages (continued)

`can't establish connection for <station>`	The Pipeline located a local Connection profile containing the proper Station and Encaps settings, but it could not complete the connection to the remote station.
`<station> didn't negotiate MPP`	The remote station did not negotiate an MP+ connection. This error occurs most often when the remote station does not support MP+, but does support PPP.
`far end doesn't support remote management`	The remote station is running a version of MP+ that does not support remote management.
`management session failed`	A temporary condition, such as premature termination of the connection, caused the management session to fail.
`far end rejected session`	The remote station was configured to reject remote management; its Remote Mgmt parameter was set to No in the System profile.

Set

Sets various items. Type 'set ?' for help. See the following Set commands.

Set All

The SET command can be used to specify a terminal type or to enable dynamic password serving. The SET ALL command displays current settings, for example:

```
ascend% set all

term = VT100
dynamic password serving = disabled
```

Set ARP Clear

To clear ARP cache, type

```
set arp clear
```

This deletes all dynamic entries to the ARP table.

Set FR

Sets Frame Relay datalink control.

Set Password

The Set Password command puts the terminal server in password mode, where a third-party ACE or SAFEWORD server at a secure site can display password challenges dynamically in the terminal server interface. This command applies only when using security card authentication. To enter password mode, type:

```
ascend% set password
```

It puts the terminal server in password mode, where it passively waits for password challenges from a remote ACE or SAFEWORD server. To return to normal terminal server operations and thereby disable password mode, press Ctrl-C.

Note: Note that each channel of a connection to a secure site requires a separate password challenge, so for multichannel connections to a secure site, you must leave the terminal server in password mode until all channels have been established. The APP Server utility is an alternative way to allow users to respond to dynamic password challenges obtained from hand-held security cards.

Set Sessid [val]

Sets and stores [val] or current ID.

Set Term

Sets the telnet/rlogin terminal type.

Show ARP

To display the ARP (Address Resolution Protocol) cache that associates IP addresses with physical network addresses, type:

```
ascend% show arp
```

The output looks similar to this:

```
IP Address    Hardware Address    Type     Interface  RefCount
10.2.3.4      00:40:c7:5a:64:6c   Static   ie0        65
100.5.6.7     00:ab:77:cf:12:47   Dynamic  wan0       39
```

The output contains these fields:

Table 2-2. ARP cache table columns

IP Address	The IP address in an ARP request.
Hardware Address	The MAC address in an ARP request.
Type	Dynamic or static, indicating how the address was obtained.
Interface	The interface on which the Pipeline received the ARP packet. ie0 is the Ethernet interface, wan *n* represents an active WAN interface.
Ref Count	The number of times the address was used.

Show DHCP

To display the supported DHCP commands, enter the Show DHCP command with a question mark:

```
ascend% show dhcp ?
```

Show DHCP Address

The Pipeline displays different output when you enter Show DHCP Address, on the basis of how you have set the Ethernet > Mod Config > DHCP Spoofing > Always Spoof parameter and the Ethernet > DHCP Spoofing > DHCP PNP Enabled parameter.

Displaying addresses when Always Spoof is Yes

Following is sample output the Pipeline displays when you enter the Show DHCP Address command, and you have set the Always Spoof parameter to Yes and the DHCP PNP Enabled parameter to either Yes or No:

```
ascend% show dhcp address


DHCP PNP Enabled = Yes
Renewal Time = 1440 seconds
Become Def. Router = Yes
Dial if Link Down = No
Always Spoof = Yes
Validate IP = Yes
Maximum no reply wait = 10 seconds

   IP Address      Hardware Address    Netmask       In Use
   10.10.10.20     00:80:C7:30:00:00   255.255.0.0       Y
   10.10.10.21     00:80:C7:12:34:50   255.255.0.0       Y
   10.10.10.22     ????????????????    255.255.0.0       N
   10.10.10.23     ????????????????    255.255.0.0       N
   10.10.10.24     ????????????????    255.255.0.0       N
   10.10.10.25     ????????????????    255.255.0.0       N
   10.10.10.201    ????????????????    255.255.0.0       N
   10.10.10.202    ????????????????    255.255.0.0       N
   10.10.10.203    ????????????????    255.255.0.0       N
   12.178.179.101  00:00:78:00:91:20   255.255.255.0     Y
   12.100.123.15   00:80:C7:5B:11:11   255.255.255.0     N
   12.100.123.16   00:80:C7:4C:11:11   255.255.255.0     Y
```

In the output:

- `IP Address` is the address supplied to the host by the Pipeline, via DHCP.
- `Hardware Address` is the Ethernet (MAC) address of the client configured with the DHCP-supplied address.

  Because the Pipeline learns hardware addresses from either ARP entries or DHCP messages, it is normal for you to see an entry with a hardware address that currently does not have an address assigned to it.

If the Pipeline requests a hardware address and does not receive a response, the Show DHCP Address command displays `??????????????????` for `Hardware Address`.

- `Netmask` indicates the configured subnet mask for the IP address.
- `In use` indicates whether or not the IP address is currently assigned to a host.

Displaying addresses when Always Spoof is No and DHCP PNP Enabled is Yes

Following is sample output the Pipeline displays when you enter the Show DHCP Address command, and you have set the Always Spoof parameter to No and the DHCP PNP Enabled parameter to Yes:

```
ascend% show dhcp address

DHCP PNP Enabled = Yes
Renewal Time = 1440 seconds
Become Def. Router = Yes
Dial if Link Down = No
Always Spoof = No
Validate IP = Yes
Maximum no reply wait = 10 seconds


IP Address       Hardware Address    Netmask          In Use
10.10.10.20      ??????????????????  255.255.0.0      N
```

In the output:

- `IP Address` is the address the Pipeline assigns to PNP clients.

  In the example, 10.10.10.20 is derived from the IP address of the Pipeline unit's Ethernet interface, 10.10.10.19. The displayed IP address is always one greater than that of the Pipeline.

- `Hardware Address` is the Ethernet (MAC) address of the client configured with the DHCP-supplied address.

  Because the Pipeline learns hardware addresses from either ARP entries or DHCP messages, it is normal for you to see an entry with a hardware address that currently does not have an address assigned to it.

If the Pipeline requests a hardware address and does not receive a response, the Show DHCP Address command displays ??????????????????.

- `Netmask` indicates the configured subnet mask for the IP address.
- `In use` indicates whether or not the IP address is currently assigned to a host.

Displaying addresses when Always Spoof and DHCP PNP Enabled are No

Following is sample output the Pipeline displays when you enter the Show DHCP Address command, and you have set the Always Spoof parameter to No and the DHCP PNP Enabled parameter to No:

```
ascend% show dhcp address

DHCP PNP Enabled = No
Renewal Time = 1440 seconds
Become Def. Router = Yes
Dial if Link Down = No
Always Spoof = No
Validate IP = Yes
Maximum no reply wait = 10 seconds

IP Address       Hardware Address    Netmask          In Use
10.10.10.17      ??????????????????  255.255.0.0      N
```

In the output:

- `IP Address` is address set in the Ethernet > Mod Config > DHCP Spoof > IP Group 1 parameter.
- `Hardware Address` is the Ethernet (MAC) address of the client configured with the DHCP-supplied address.

  Because the Pipeline learns hardware addresses from either ARP entries or DHCP messages, it is normal for you to see an entry with a hardware address that currently does not have an address assigned to it.

  If the Pipeline requests a hardware address and does not receive a response, the Show DHCP Address command displays ??????????????????.
- `Netmask` indicates the configured subnet mask for the IP address.

- `In use` indicates whether or not the IP address is currently assigned to a host.

Show DHCP Lease

To display the users currently assigned addresses via DHCP, enter the Show DHCP Lease command. For example:

```
ascend% show dhcp lease

IP Address    Hardware Address   Netmask         Renew in
10.10.10.2    0080C7300000        255.255.0.0    1130
10.10.10.202  0080C7123450        255.255.0.0    78
12.0.0.101    000078009120        255.255.255.0  12
```

In the output:

- `IP Address` is the address supplied to the client by the Pipeline, via DHCP.
- `Hardware Address` is the Ethernet (MAC) address of the client configured with the DHCP-supplied address.
- `Netmask` indicates the configured subnet mask for the IP address.
- `Renew in` indicates the number of seconds remaining until the DHCP lease expires for the supplied address. When the lease expires, the client must request another IP address.

Show Dnstab

Displays local DNS table.

Show Dnstab entry

Displays local DNS table entry when you specify the entry number.

Show FR DLCI [name]

To display the status of each DLCI (Data Link Connection Identifier) that uses a frame relay interface, use the Show FR DLCI command using this format:

```
show fr dlci <profile-name>
```

where <profile-name> specifies a Frame Relay profile. For example:

```
ascend% show fr dlci PacBell
```

This command prints the name of the Frame Relay profile followed by a list of all Connection Profiles that use the specific DLCIs and statistics about those DLCIs. For each Connection profile, DLCI information is reported using these fields:

Table 2-3. Show Frame Relay DLCI output columns

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

Show FR LMI

To display LMI (Link Management Information) for each link activated by a Frame Relay profile, enter this command:

```
ascend% show fr lmi
```

The output looks similar to this:

```
LMI for name:
   Invalid Unnumbered info      0    Invalid Prot Disc        0
   Invalid dummy call Ref       0    Invalid Msg Type         0
   Invalid Status Message       0    Invalid Lock Shift       0
   Invalid Information ID       0    Invalid Report Type      0
   Num Status Enq. Sent         0    Num Status msgs Rcvd     0
   Num Update Status Rcvd       0    Num Status Timeouts      0
```

This information is based on the ANSI T1.617 Annex D local in-channel signaling protocol. (See Annex D for a full definition of each of the fields reported.)

Show FR Stats

To display the status of each frame relay interface, enter this command:

```
ascend% show fr stats
```

The output looks similar to this:

```
Name          Status       Speed         MTU   InFrame      OutFrame
framerelay       Down      56000        1532         0            0
```

The output contains these fields:

Table 2-4. Show Frame Relay output columns

Name	The name of the Frame Relay profile associated with the interface.
Status	The status of the interface. “Up” means the interface is functional, but is not necessarily handling an active call. “Down” means the interface is not functional.
Speed	The data rate in bits per second.
MTU	The maximum packet size allowed on the interface.

Table 2-4. Show Frame Relay output columns (continued)

InFrame	The number of frames the interface has received.
OutFrame	The number of frames the interface has transmitted.

Show ICMP

To view the number of ICMP (Internet Control Message Protocol) packets received intact, received with errors, and transmitted, type:

```
ascend% show icmp
```

The output looks similar to this:

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

The Input and Output histograms show the number of ICMP packets received and transmitted in each category.

Show If Stats

To display the status and packet count of each active WAN link as well as local and loopback interfaces, type:

```
ascend% show if stats
```

The output looks similar to this:

```
Interface  Name     Status  Type   Speed     MTU   InPackets   Outpacket
ie0        ethernet Up      6      10000000  1500       7385       85384
wan0                Down    1             0  1500          0           0
wan1                Down    1             0  1500          0           0
wan2                Down    1             0  1500          0           0
wanidle0            Up      6      10000000  1500          0           0
```

```
lo0        loopback  Up     24      10000000  1500          0           0
```

The output contains these fields:

Table 2-5. Interface statistics table columns

Interface	ie0 is the Ethernet interface, lo0 is the loopback interface, “wan *n*” represents each of the active WAN interfaces in the order in which they became active, and wanidle0 is the inactive interface. The inactive interface is the special interface where all routes point when their WAN connections are down.
Name	The name of the profile associated with the interface, or a text name for the interface
Status	The interface status.Up means the interface is functional, but is not necessarily handling an active call. Down means the interface is not functional.
Type	The type of application being used on the interface, as specified in RFC 1213 (MIB-2). For example, 23 indicates PPP and 28 indicates SLIP.
Speed	The data rate in bits per second.
MTU	The maximum packet size allowed on the interface. MTU stands for Maximum Transmission Unit.
InPackets	The number of packets the interface has received.
OutPackets	The number of packets the interface has transmitted.

Show If Totals

To display the packet count at each interface broken down by type of packet, enter this command:

```
ascend% show if totals
```

The output looks similar to this:

```
Name        --Octets-- --Ucast---NonUcast-Discard -Error-Unknown-Same IF-
ie0      i:   7813606   85121      22383       0      0       0        0
         o: 101529978   85306        149       0      0       0        0
```

```
wan0      i:        0       0       0       0       0       0       0
          o:        0       0       0       0       0       0       0
wan1      i:        0       0       0       0       0       0       0
          o:        0       0       0       0       0       0       0
wan2      i:        0       0       0       0       0       0       0
          o:        0       0       0       0       0       0       0
wanidle0  i:        0       0       0       0       0       0       0
          o:        0       0       0       0       0       0       0
lo0       i:        0       0       0       0       0       0       0
          o:        0       0       0       0       0       0       0
```

The output contains these fields:

Table 2-6. Packet count statistics table columns

Name	The interface name (same as described immediately above).
Octets	The total number of bytes processed by the interface.
Ucast	Packets with a unicast destination address.
NonUcast	Packets with a multicast address or a broadcast address.
Discard	The number of packets that the interface could not process.
Error	The number of packets with CRC errors, header errors, or collisions.
Unknown	The number of packets the Pipeline forwarded across all bridged interfaces because of unknown or unlearned destinations.
Same IF	The number of bridged packets whose destination is the same as the source.

Show IGMP Clients

Displays IGMP clients.

Show IGMP Groups

To display all the active multicast group addresses and the clients(interfaces) registered for that group, type:

```
ascend% show igmp groups
```

The output is similar to this:

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

Where:

- Hash is an index to a hash table (displayed for diagnostics purposes only).
- Group address is the IP multicast address used in this packet.
- Members is the interface ID on which the membership resides. 0 represents the Ethernet interface. Other numbers represent WAN interfaces, numbered according to when they became active. The interface labeled Mbone is the interface on which the multicast router resides.
- Expire time indicates when this membership expires. The Pipeline sends out IGMP queries every 60 seconds, so the expiration time is usually renewed. If the expiration time is reached, the entry is removed from the table. When this field contains periods, it means that this membership never expires.
- Counts shows the number of packets forwarded to the client, the number of packets dropped due to lack of resources, and the state of the membership (the state is displayed for diagnostics purposes).

To list all IGMP multicast clients, enter:

```
ascend% show igmp clients
```

The output is similar to this:

```
IGMP Clients

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

Where:

- Client indicates the interface ID on which the client resides. 0 represents the Ethernet interface. Other numbers represent WAN interfaces, numbered according to when they became active. The interface labeled Mbone is the interface on which the multicast router resides.
- Version is the version of IGMP being used.
- RecvCount is the number of IGMP messages received on that interface.
- CLU (current line utilization) and ALU (average line utilization) show the percentage of bandwidth utilized across this interface. If bandwidth utilization is high, some IGMP packet types will not be forwarded.

Show IGMP Stats

To display IGMP activity statistics, type:

```
ascend% show igmp stats
```

The output shows the number of IGMP packet types sent and received, in the format below:

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

```
4 response packets sent.
 0 leave packets sent.
```

Show IP Address

To view the source and destination IP addresses for active IP routing connections, enter this command:

```
ascend% show ip address
```

The output looks similar to this:

```
Interface   IP Address    Dest IP Address   Netmask          MTU  Status
ie0           10.2.3.4    N/A               255.255.255.224  1500    Up
wan0          0.0.0.0     N/A               0.0.0.0          1500    Down
wan1          0.0.0.0     N/A               0.0.0.0          1500    Down
wan2          0.0.0.0     N/A               0.0.0.0          1500    Down
wanidle0      10.5.7.9    N/A               255.255.255.224  1500    Up
lo0           127.0.0.1   N/A               255.255.255.224  1500    Up
```

The output contains these fields:

Table 2-7. IP address output columns

Interface	ie0 is the Ethernet interface, lo0 for the loopback interface, “wan *n*” represents each of the active WAN interfaces in the order in which they became active, and wanidle0 is the inactive interface (the special interface where all routes point when their WAN connections are down).
IP Address	The IP address of the interface.
Dest IP Address	The IP address of the remote router. (This field applies only to an interface with an active link that is routing IP.)
Netmask	The netmask in use on the interface.
MTU	The maximum packet size allowed on the interface.
Status	The status of the interface. Up means the interface is functional, but is not necessarily handling an active call. Down means the interface is nonfunctional.

Show IP Routes

To display the Pipeline unit's entire IP routing table, enter this command:

```
ascend% show ip routes
```

Or, to view the route to a specific address, you can enter the command using this format:

```
show ip routes <hostname>
```

where <hostname> is a hostname or IP address.

The output looks similar to this:

```
Destination         Gateway         IF       Flg Pref  Met   Use   Age
0.0.0.0/0           10.0.0.100      wan0     SG   1     1     0     20887
10.207.76.0/24      10.207.76.1     wanidle0 SG   100   7     0     20887
10.207.76.1/32      10.207.76.1     wanidle0 S    100   7     2     20887
10.207.77.0/24      10.207.76.1     wanidle0 SG   100   8     0     20887
127.0.0.1/32        -               lo0      CP   0     0     0     20887
10.0.0.0/24         10.0.0.100      wan0     SG   100   1     21387 20887
10.0.0.100/32       10.0.0.100      wan0     S    100   1     153   20887
10.1.2.0/24         -               ie0      C    0     0     19775 20887
10.1.2.1/32         -               lo0      CP   0     0     389   20887
255.255.255.255/32  -               ie0      CP   0     0     0     20887
```

The output contains these fields:

Table 2-8. IP routes output columns

Destination	The target address of a route. To send a packet to this address, the Pipeline will use this route. Note that the router will use the most specific route (having the largest netmask) that matches a given destination.
Gateway	The address of the next hop router that can forward packets to the given destination. Direct routes (without a gateway) do not show a gateway address in the gateway column.

Table 2-8. IP routes output columns (continued)

IF	ie0 is the Ethernet interface, lo0 is the loopback interface, "wan *n*" specifies each of the active WAN interfaces, and wanidle0 is the inactive interface (the special interface where all routes point when their WAN connections are down).
Flg	One of the following characters: • C=Connected (A directly connected route, for example, the Ethernet.) • I=ICMP (ICMP Redirect dynamic route.) • N=NetMgt (Placed in the table via SNMP MIB II.) • R (A RIP dynamic route.) • S=Static (A local IP Route profile or Connection profile route.) • ?=Unknown (A route of unknown error, which indicates an error.) • G=Gateway (A gateway is required in order to reach this route.) • P=Private (This route will not be advertised via RIP.) • T=Temporary (This route will be destroyed when its interface goes down. • *=Hidden (A hidden route means that there is a better route in the table, so this route is hidden "behind" the better route. If the better route should go away, then this route may be used.)
Pref	The preference value of the route. Note that all routes that come from RIP will have a preference value of 100, while the preference value of each individual static route may be set independently.
Met	The RIP-style metric for the route, with a valid range of 0-16.
Use	This is a count of the number of times the route was referenced since it was created. (Many of these references are internal, so this is not a count of the number of packets sent using this route.)
Age	This is the age of the route in seconds. It is used for troubleshooting, to determine when routes are changing rapidly or flapping.

Show IP Stats

To display statistics on IP activity, including the number of IP packets the Pipeline has received and transmitted, enter this command:

```
ascend% show ip stats
```

The output looks similar to this:

```
107408 packets received.
     0 packets received with header errors.
     0 packets received with address errors.
     0 packets forwarded.
     0 packets received with unknown protocols.
     0 inbound packets discarded.
107408 packets delivered to upper layers.
 85421 transmit requests.
     0 discarded transmit packets.
     1 outbound packets with no route.
     0 reassembly timeouts.
     0 reassemblies required.
     0 reassemblies that went OK.
     0 reassemblies that Failed.
     0 packets fragmented OK.
     0 fragmentations that failed.
     0 fragment packets created.
     0 route discards due to lack of memory.
     64 default ttl.
```

Show ISDN

The Show ISDN command enables the Pipeline to display the last 20 events that have occurred on the specified ISDN line. Enter the command in this format:

```
show isdn <line-number>
```

where <line-number> is the number of the ISDN line. For example, to display information about the leftmost built-in WAN port, type:

```
ascend% show isdn 0
```

The Pipeline responds with one or more of these messages:

PH: ACTIVATED
PH: DEACTIVATED
DL: TEI ASSIGNED (BRI interfaces only)
DL: TEI REMOVED (BRI interfaces only)
NL: CALL REQUEST
NL: CLEAR REQUEST
NL: ANSWER REQUEST
NL: CALL CONNECTED
NL: CALL FAILED/T303 EXPIRY
NL: CALL CLEARED/L1 CHANGE
NL: CALL REJECTED/OTHER DEST
NL: CALL REJECTED/BAD CALL REF
NL: CALL REJECTED/NO VOICE CALLS
NL: CALL REJECTED/INVALID CONTENTS
NL: CALL REJECTED/BAD CHANNEL ID
NL: CALL FAILED/BAD PROGRESS IE
NL: CALL CLEARED WITH CAUSE

In some cases, the message can include a phone number (prefixed by #), a data service (suffixed by K for kbps), a channel number, TEI assignment, and cause code. For example, this information might display:

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

See Chapter 5, “ISDN Cause Codes.” Also refer to ITU-T Q.931 or other ISDN specifications.

Show Netw Networks

To display the IPX routing table, enter this command:

```
ascend% show netware networks
```

The output looks similar to this:

```
network     next router        hops        ticks   origin
CFFF0001    00000000000         0          1       Ethernet         S
```

The output contains these fields:

Table 2-9. Show Netware networks output columns

network	The IPX network number.
next router	The address of the next router, or 0 (zero) for a direct or WAN connection.
hops	The hop count to the network.
ticks	The tick count to the network.
origin	The name of the profile used to reach the network.

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

Show Netw Pings

To display statistics related to the IPXping command, type:

```
ascend% show netware pings
```

The output looks similar to this:

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

The output shows how many NetWare stations have pinged the Pipeline (InPing requests and replies) and how many times the IPXping command has been executed in the Pipeline.

Show Netw Servers

To display the IPX service table, enter this command:

```
ascend% show netware servers
```

The output looks similar to this:

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

The output contains these fields:

Table 2-10.Show Netware servers output columns

IPX address	The IPX address of the server. The address uses this format: <network number>:<node number>:<socket number>
type	The type of service available (in hexadecimal format). For example, 0451 designates a file server.
server name	The first 35 characters of the server name.

Show Netw Stats

To display IPX packet statistics, enter this command:

```
ascend% show netware stats
```

The output looks similar to this:

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

The Pipeline drops packets that exceed the maximum hop count (that have already passed through too many routers).

Show Revisions

The `show revision` command displays system type and version information for the system currently running on the Pipeline, including:

- system name
- build name
- release number of the loaded software

For example, typing

```
show revision
```

at the command line prompt would display information similar to:

```
Pipeline system revision: b2.p75 5.1A
```

Show Sessid

Displays current and base session ID.

Show TCP Connection

To display the current TCP sessions connected to or connecting to the Pipeline, enter this command:

```
ascend% show tcp connection
```

The output looks similar to this:

```
Socket      Local              Remote                   State
0           *.23               *.*                    LISTEN
1           10.2.3.23          15.5.248.121.15003  ESTABLISHED
```

The output contains these fields:

Table 2-11.TCP connection output columns

Socket	The socket associated with the port.

Table 2-11.TCP connection output columns (continued)

Local	The local IP address and port associated with the connection. For example, if the Pipeline has a connection on port 23 and to a local host at 10.0.0.2, the Local field would contain 10.0.0.2.23.
Remote	The IP address and port from which the connection originated. For example, if the connection originated at 200.5.248.210 on port 18929, the Remote field would contain 200.5.248.210.18929.
State	LISTEN if the Pipeline is listening for a connection, or ESTABLISHED if it has already established one.

Show TCP Stats

To display the number of TCP (Transmission Control Protocol) packets received and transmitted, enter this command:

```
ascend% show tcp stats
```

The output looks similar to this:

```
      0 active opens.
     11 passive opens.
      1 connect attempts failed.
      1 connections were reset.
      3 connections currently established.
  85262 segments received.
  85598 segments transmitted.
    559 segments re-transmitted.
```

An active open is an open TCP session that the Pipeline initiated. A passive open is an open TCP session that the Pipeline did not initiate.

Show UDP Listen

To view information about the socket number, UDP port number and the number of packets queued for each UDP port on which the Pipeline is currently listening, enter this command:

```
ascend% show udp listen

udp:
Socket  Local Port  InQLen  InQMax    InQDrops    Total Rx
     0        1023       0       1           0           0
     1         520       0      50           0         532
     2           7       0      32           0           0
     3         123       0      32           0           0
     4        1022       0     128           0           0
     5         161       0      64           0           0
```

The output contains these fields:

Table 2-12.UDP listen output columns

Socket	The socket number associated with the port.
Local Port	The UDP port on which the Pipeline is listening.
InQLen	The input queue length for the port.
InQMax	The maximum number of queued UDP packets on the socket. (These are set by Queue Depth and Rip Queue Depth parameters.)
InQDrops	The number of packets discarded so that InQLen would not exceed InQMax
Total Rx	The total number of packets received on the socket, including the InQDrops

Show UDP Stats

To display the number of UDP (User Datagram Protocol) packets received and transmitted, enter this command:

```
ascend% show udp stats
```

The output looks similar to this:

```
22386 packets received.
    0 packets received with no ports.
    0 packets received with errors.
    0 packets dropped
```

```
9 packets transmitted.
```

Show Uptime

To see how long the Pipeline has been running, type:

```
ascend% show uptime
```

The output looks similar to this:

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

If the Pipeline stays up 1000 consecutive days with no power cycles, the number of days displayed “turns over” to 0 and begins to increment again.

TCP

The TCP command initiates a login session to a remote host. It uses this format:

```
tcp <hostname> <port-number>
```

There are a number of settings in the Ethernet profile that affect how a TCP connection works. For example, if DNS is configured in the Pipeline Ethernet profile, you can specify a hostname such as:

```
ascend% tcp myhost
```

TCP command arguments

The arguments to the TCP command are as follows:

- <hostname>

  If DNS is configured in the Pipeline Ethernet profile, you can specify the remote system’s hostname. Otherwise, hostname must be the IP address of the remote station.

- [<port-number>]

  (Optional.) You can specifies the port to use for the session. The port number typically indicates a custom application that runs on top of the TCP session.

For example, port number 23 starts a Telnet session. However, terminating the Telnet session does not terminate the raw TCP session.

When the raw TCP session starts running, the Pipeline displays the word "connected." You can now use the TCP session to transport data by running an application on top of TCP.

You can hang up the device at either end to terminate the raw TCP session. If you are using a remote terminal server session, ending the connection also terminates raw TCP.

TCP error messages

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

Table 2-13.TCP error messages

`Can't open session: <hostname> <port-number>`	You entered an invalid or unknown value for <hostname>, you entered an invalid value for <port-number>, or you failed to enter a port number.
`no connection: host reset`	The destination host reset the connection.
`no connection: host unreachable`	The destination host is unreachable.
`no connection: net unreachable`	The destination network is unreachable.

Telnet

The Telnet command initiates a login session to a remote host. It uses this format:

```
telnet [-a|-b] <hostname> [<port-number>]
```

There are a number of settings in the Ethernet profile that affect how Telnet works. For example, if DNS is configured, you can specify a hostname such as:

```
ascend% telnet myhost
```

If DNS has not been configured, you must specify the host's IP address instead.

Another way to open a session is to invoke Telnet first, followed by the OPEN command at the Telnet prompt, for example:

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

In the example commands in this section, the Telnet prompt is the word `telnet` followed by a greater-than sign (`telnet>`). When you see that prompt, you can enter any of the Telnet commands.

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

You can quit the Telnet session at any time by typing quit at the Telnet prompt:

```
telnet> quit
```

Telnet command arguments

The arguments to the Telnet command are as follows:

- <hostname>

  If DNS is configured, you can specify the remote system's hostname. Otherwise, hostname must be the IP address of the remote station.

- [–a]

  (Optional.) This flag specifies standard 7-bit mode, in which bit 8 is set to 0 (zero). 7-bit Telnet is also known as NVT (Network Virtual Terminal) ASCII. If you do not enter –a or –b, the Binary Mode setting applies.

- [–b]

  (Optional.) This flag specifies the Telnet 8-bit binary option. X-Modem and other 8-bit file transfer protocols require this mode. If you do not enter –a or –b, the Binary Mode setting applies.

  Note: Note that the Telnet escape sequence does not operate in 8-bit binary mode. The Telnet session can close only if one end of the connection quits the session. Therefore, a local user not connected through a dial-up

connection cannot quit the session; he or she must wait for the remote user to close the session.

- [<port-number>]

  (Optional.) You can specify the port to use for the session. The default is 23, the well-known port for Telnet.

Telnet session commands

The commands in this section can be typed at the Telnet prompt during an open session. To display the Telnet prompt during an active login to the specified host, press Ctrl-] (hold down the Control key and type a right-bracket).

To display information about Telnet session commands, use the Help or ? command. For example:

```
telnet> ?
```

or

```
telnet> help
```

To open a Telnet connection after invoking Telnet, use the OPEN command. The arguments you specify are exactly the same as those for opening a connection from the Telnet command-line, except for that the OPEN command does not support the -a and -b options. For example:

```
telnet> open myhost
```

To send standard Telnet commands such as “Are You There” or “Suspend Process,” use the Send command. For example:

```
telnet> send susp
```

For a list of Send commands and their syntax, type:

```
telnet> send ?
```

To set special characters for use during the Telnet session, use the Set command. For example:

```
telnet> set eof ^D
```

To display current settings, type:

```
telnet> set all
```

To see a list of Set commands, type:

```
telnet> set ?
```

To quit the Telnet session and close the connection, use the Close or Quit command. For example:

```
telnet> close
```

or:

```
telnet> quit
```

Telnet error messages

The Pipeline generates an error message for any condition that causes the Telnet session to fail or terminate abnormally. These error messages may appear:

Table 2-14.Telnet session failure reasons

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

Test

To run a self-test in which the Pipeline calls itself, the Pipeline must have two open channels: one for the placing the call, and the other for receiving it. The TEST command has this format:

```
test <phonenumber> [<frame-count>] [<optional
fields>]
```

The number you enter depends on how your line is provisioned:

- Enter the value for My Num A (in the Configure profile) if your ISDN line is provisioned for only one phone number
- Enter the value for My Num B (in the Configure profile) if your ISDN line is provisioned for two phone numbers

For example:

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

You can enter Ctrl-C at any time to terminate the test. While the test is running, the Pipeline displays the status, for example:

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

Test command arguments

The arguments to the TEST command are as follows:

- <phonenumber>

  The phone number of the channel receiving the test call. Your specification can include the numbers 0 through 9 and the characters `()[]-, but cannot` include spaces. If you have two phone numbers associated with your ISDN line, you must specify the second number; otherwise, you can specify the single phone number for the line. The test calls out on channel 1 and calls back in on channel 2.

- [<frame-count>]

  (Optional.) The number of frames to send during the test. You can specify a number from 1 to 65535. The default is 100.

- [data-svc=<data-svc>]

  For data-svc, enter a data service identical to any of the values available for the Data Svc parameter of the Connection profile. For a list of valid values, see the *Reference Guide*. If you do not specify a value, the default value is the one specified for the Data Svc parameter.

Test error messages

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

Table 2-15.Test error messages

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

Table 2-15.Test error messages (continued)

`wrong phone number`	A device other than the Pipeline answered the call; therefore, the phone number you specified was incorrect.

Traceroute

Use Traceroute to diagnose IP routing and network performance. It is useful to locate slow routers and to find IP routing problems.

The Internet is a large and complex aggregation of network hardware, connected together by gateways. Tracking the route packets follow or finding the gateway that is discarding your packets can be difficult. The Traceroute command utilizes the IP protocol "time to live" field and attempts to elicit an ICMP Time Exceeded response from each gateway along the path to some host.

The Traceroute command syntax is:

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

The supported Traceroute options are:

host	This mandatory parameter specifies the destination host by name or IP address.
-n	Prints hop addresses numerically rather than symbolically and numerically (this eliminates a nameserver address-to-name lookup for each gateway found on the path).
-v	Verbose output. Received ICMP packets other than Time Exceeded and ICMP Port Unreachable are listed.
-m *max_ttl*	This sets the maximum time-to-live (maximum number of hops) used in outgoing probe packets. The default is 30 hops.

-p *port*	Sets the base UDP port number used in probes. Traceroute hopes that nothing is listening on any of the UDP ports from the source to the destination host (so an ICMP Port Unreachable message will be returned to terminate the route tracing). If something is listening on a port in the default range, this option can be used to pick an unused port range. The default is 33434.
-q *nqueries*	Sets the maximum number of queries for each hop. The default is 3.
-w *waittime*	Sets the time to wait for a response to a query. The default is 3 seconds.
datasize	Sets the size of the data field of the UDP probe datagram sent by Traceroute. The default is 0. This results in a datagram size of 38 bytes (a UDP packet carrying no data).

Note: The -r and -s options (present in the UNIX version of Traceroute) are not supported.

The Traceroute command attempts to trace the route an IP packet would follow to some Internet host by launching UDP probe packets with a small TTL (time to live) and then listening for an ICMP "time exceeded" reply from a gateway. Probes start with a TTL of one and increase by one until an ICMP "port unreachable" message is received, meaning the host could not be reached, or the packet expired.

Three probes are sent at each TTL setting and a line is printed showing the TTL, address of the gateway and round trip time of each probe. If the probe answers come from different gateways, the address of each responding system is printed. If there is no response within a 3 second timeout interval, a asterisk (*) is printed for that probe.

Possible annotations after the time field are as follows:

!H	Host reached.

!N	Network unreachable.
!P	Protocol unreachable.
!S	Source route failed. This should not occur and may indicate that there is a problem with the associated device.
!F	Fragmentation needed. This should not occur and may indicate that there is a problem with the associated device.
!h	Communication with the host is prohibited by filtering.
!n	Communication with the network is prohibited by filtering.
!c	Communication is otherwise prohibited by filtering.
!?	Indicates an ICMP sub-code. This should not occur.
!??	Reply received with inappropriate type. This should not occur.

Parameter Reference

3

This chapter lists the Pipeline parameters in alphabetical order. Each listing provides information in the following format:

Parameter Name

Description: Explains what the parameter is intended to do, or why you need it.

Usage: Explains when and how to use the parameter.

Example: Shows you an example entry or setting.

Dependencies: Tells you what other information you need to know or other parameters you need to set in order to configure and use the current parameter.

Location: Shows you where to find the parameter in the LCD interface (seen in a VT100 terminal emulation window). The location is described as a sequence of menu (or profile) selections.

The greater than symbol (>) means continue to the next menu, and press Enter. For example, Ethernet > Mod Config > Ether Options means open the Ethernet menu, then open the Mod Config menu, then open the Ether Options menu.

If a parameter occurs in more than one location, all locations are listed, separated by a semicolon (;).

See Also: Lists related parameters.

Alphabetical parameter listing

2nd Adrs

Description: Gives the Pipeline an IP address on a remote subnet. When you set the 2nd Adrs parameter, the Pipeline has a second IP address in addition to the IP Adrs value on its local Ethernet interface. Both IP addresses are treated equally, except that IP Adrs is the only one used for authentication over the WAN. Setting a second address doubles the number of entries in the Pipeline routing table. The Pipeline advertises a route from 2nd Adrs to IP Adrs and a route from IP Adrs to 2nd Adrs.

One use of 2nd Adrs is to advertise routes that would not otherwise be advertised. For example, suppose both the Pipeline and Router2 have a route to the network 200.0.2.0. Both are on the same subnet. The device with the lower hop count to the destination network sends all the traffic destined for that network.

Now, suppose the Pipeline has 2nd Adrs=200.0.2.9/28 and Router2 has 2nd Adrs=200.0.2.10/28 on the same subnet. The Pipeline assumes that all subnets in the 200.0.2.0 network have the same subnet mask (/28). In addition, the Pipeline has an address for a router at 200.0.2.129/28 and Router2 has an address for a router at 200.0.2.65/28. Because the Pipeline and Router2 assume that /28 is the subnet mask, the Pipeline routes traffic only to the 200.0.2.129/28 subnet and Router2 routes traffic only to the 200.0.2.65/28 subnet. The traffic to the 200.0.2.0 network is thereby shared.

Using the 2nd Adrs parameter also provides an easy way to change the IP address of the Pipeline. When all routers know the Pipeline by both its IP Adrs value and its 2nd Adrs value, you can safely turn off 2nd Adrs and put the new address in IP Adrs.

Usage: Press Enter to open a text field. Then, type the IP address of the Pipeline on the remote subnet.

The address consists of four numbers between 0 and 255, separated by periods. Use a slash to separate the optional netmask from the address. The IP address must be a valid address on the remote subnet.

The default value is 0.0.0.0/0.

Press Enter to close the text field.

Dependencies: Keep this additional information in mind:

- If you do not know the right IP address to enter, you must obtain it from the network administrator.

  Do not attempt to configure an IP address by guesswork!
- Do not use 2nd Adrs to force interface-based routing; it is not designed as a second WAN address.

Location: Ethernet > Mod Config > Ether Options

See Also: IP Adrs

Activation

Description: This parameter selects the signals at the serial WAN port that indicate that the Data Circuit-Terminating Equipment (DCE) is ready to connect.

Flow control is always handled by the Clear To Send (CTS) signal.

Usage: Press Enter to cycle through the choices.

- Static specifies that the Pipeline does not use flow control signals because the DCE is always connected.
- DPR (Call Digit or Tone) specifies that the DCE raises the DPR signal when it is ready.
- CRQ (Call Request) specifies that the DCE raises the CRQ signal when it is ready.
- RTS (Request to Send) specifies that the DCE raises the RTS signal when it is ready.
- CRQ+RTS specifies that the DCE raises the CRQ and RTS signals when it is ready.
- DPR+CRQ+RTS specifies that the DCE raises the DPR, CRQ and RTS signals when it is ready.
- Disabled specifies that the V.35 serial WAN port is disabled. This setting will terminate an active session and prevent further attempts to establish a connection.
- Serial WAN profile: Serial WAN/Mod Config

Location: V.35 > Serial WAN > Mod Config

Activation

Description: Enables or disables your nailed T1 line.

Usage: Press Enter to cycle through the choices.

- Enabled specifies that the Pipeline T1 line is enabled.
  Enabled is the default.
- Disabled specifies that the Pipeline T1 line is disabled.

Location: Nailed T1 > Mod Config

Active

Description: Appears in a Connection profile, a Frame Relay profile, and a Static Rtes profile. Its functionality differs depending on the profile:

- In a Connection profile or a Frame Relay profile, the Active parameter activates or deactivates the profile.
  If you activate a profile, it is available for use. If you deactivate a profile, it is not available for use.
- In a Static Rtes profile, the Active parameter determines whether the route defined in the profile appears in the Pipeline static routing table.

Usage: Press Enter to toggle between Yes and No.

- Yes activates the profile or specifies that the route can appear in the static routing table.
- No deactivates the profile, keeps the route from appearing in the static routing table, or removes the route if it is already in the table.
  A dash appears before each deactivated profile or route.
  No is the default.

Location: Ethernet > Connections > *any profile*; Ethernet > Frame Relay > *any profile*; Ethernet > Static Rtes > *any profile*

Add Pers

Description: Specifies the number of seconds that average line utilization (ALU) for transmitted data must exceed the threshold indicated by the Target Util parameter before the Pipeline begins adding bandwidth to a session. The Pipeline determines the ALU for a session by using the algorithm specified by the Dyn Alg parameter.

When utilization exceeds the threshold for a period of time greater than the value of the Add Pers parameter, the Pipeline attempts to add a channel. Using 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.

Usage: Press Enter to open a text field. Then, type a number between 1 and 300. Press Enter again to close the text field.

When the Pipeline is using MP+ (Encaps=MPP), the default value is 5.

Dependencies: Keep this additional information in mind:

- Additional channels must be available, and the number of channels added cannot exceed the amount specified by the Max Ch Count parameter.
- Add Pers in the Answer profile applies to incoming calls for which no Connection profile exists; if a Connection profile exists, the setting of its Add Pers parameter takes precedence.
- If Profile Reqd=Yes in the Answer profile, Add Pers does not apply (Add Pers=N/A) in the Answer profile.
- Add Pers and Sub Pers have little or no effect on a system with a high Sec History value.

  If the value of Sec History is low, the Add Pers and Sub Pers parameters provide an alternative way to ensure that spikes must persist for a certain period of time before the system responds.

Location: Ethernet > Answer profile > PPP Options; Ethernet > Connections > *any profile* > Encaps Options

See Also: Dyn Alg, Max Ch Count, Base Ch Count, Sec History, Sub Pers, Target Util

Adv Dialout Routes

Description: Specifies whether the Pipeline should continue to advertise dialout routes for which it is currently unable to establish a WAN connection. The default behavior of the Pipeline is to advertise routes regardless of the condition of its lines.

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 is not necessary to use this feature if you have a single Pipeline unit.

Usage: Press Enter to toggle between the choices.

- Always
  This setting causes the Pipeline to always advertise its IP routes. Use this setting unless you have redundant Ascend units or don't use dialout routes.
  Always is the default.
- Trunks Up
  This setting causes the Pipeline to stop advertising ("poison") its IP dialout routes if it temporarily loses the ability to dial out.

Location: Ethernet > Mod Config

Alarm

Description: Specifies whether the Pipeline sends a traps-PDU (Protocol Data Unit) to the SNMP manager when an alarm event occurs.

A trap is a mechanism in SNMP for reporting system change in real time. To report system change, the Pipeline sends a traps-PDU across the Ethernet interface to the SNMP manager.

Alarm events are defined in RFC 1215 and include the following:

- coldStart
  This event indicates that the Pipeline started up from a power-off condition.
- warmStart
  This event indicates that the Pipeline started up from a power-on condition, typically by a system reset.
- linkDown

This event indicates that a WAN link or Ethernet interface has gone offline.

- linkUp
  This event indicates that a WAN link or Ethernet interface has come online.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that the Pipeline traps alarm events.
- Yes is the default.
- No specifies that the Pipeline does not trap alarm events.

Location: Ethernet > SNMP Traps

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 Pipeline 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 prevents clients from using the local DNS servers.

Location: Ethernet > Mod Config > DNS

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

Alt Dial#n

Description: Up to three alternate dial numbers may be entered for the Pipeline 130 connection profiles. Use the alternate dial number fields in sequence. A blank field indicates the end of alternate numbers. (If Alt Dial#2 is blank, Alt Dial#3 will not be used, even if it contains data.)

Usage: Press Enter to open a text field and enter a phone number. Press Enter to close the text field. The field accepts up to 37 characters, which are limited to the following set:

```
1234567890()[]!z-*#|
```

Only the numerical characters are sent.

The default value is null.

Example: Alt Dial#1=5551112

Dependencies: An alternate number is used only if the number in Dial# does not connect, and only if a preceding alternate number field is not blank.

Location: Ethernet > Connections > *profile*.

Always Spoof

Description: Determines how the Pipeline responds to DHCP requests:

- It can be a DHCP server for up to 43 hosts and assign addresses from its own address pools.
- It can perform DHCP spoofing for a single host by providing a temporary IP address just long enough for a DHCP server on the remote network to provide an official address.

When a Pipeline performs DHCP spoofing, it responds to DHCP requests from only one host. It ignores requests from any host other than the first one to send a request.

Usage: Press Enter to cycle through the choices:

- Yes causes the Pipeline to be a DHCP server.
- No enables DHCP spoofing. No is the default.

Dependencies: If DHCP Spoofing is No, this parameter is N/A.

Note: If DHCP server functionality is enabled (when Always Spoof is Yes), BOOTP relay cannot function at the same time.

Location: Ethernet > Mod Config > DHCP Spoofing

See Also: DHCP Spoofing

Ans Voice Call

Description: Enables or disables incoming voice calls to a Pipeline with ISDN.

Usage: Enter Yes to enable or No to disable incoming voice calls. Yes is the default.

- For the Pipeline units without POTS, set the Ans Voice Call parameter to Yes to specify that a unit answer voice calls. Incoming calls are treated as Data Over Voice (DOV) calls.
- For the Pipeline units with POTS, if you set Ans Voice Call to Yes, the unit functions as usual, directing incoming voice calls to the POTS ports.
- For any model, if you set Ans Voice Call to No, incoming voice calls are rejected. You can list the phone numbers of rejected calls by entering the Show ISDN command at the terminal server prompt. For example:

  ```
  ascend% show isdn
  NL: CALL REJECTED/OTHER DEST: 5551010
  ```

  The phone number listed, 5551010, originated a call that was not answered by the Pipeline.

Dependencies: None.

Location: Configure

See Also: Phone 1 Usage, Phone 2 Usage, Data Usage

AnsOrig

Description: Specifies whether the Pipeline can initiate calls, receive them, or both. The setting you choose affects calls to or from the destination specified by the Station and LAN Adrs parameters in the Connection profile.

Usage: Press Enter to cycle through the choices.

- Both specifies that the Pipeline can initiate calls to the destination specified in the Connection profile, and that it can receive calls from that destination as well.

  Both is the default.
- Call Only specifies that the Pipeline can dial out to the destination specified in the Connection profile, but cannot answer calls from that destination.
- Ans Only specifies that the Pipeline can receive calls from the destination specified in the Connection profile, but cannot initiate calls to that destination.

Dependencies: The AnsOrig parameter does not apply (AnsOrig=N/A) when all channels of the link are nailed up (Call Type=Nailed).

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

See Also: LAN Adrs, Station

APP Host

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

Usage: Press Enter to open a text field. Then, type 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.

Press Enter again to close the text field.

Example: `200.65.207.63/29`

Dependencies: Keep this additional information in mind:

- APP Host 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: Press Enter to open a text field. Then, type 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. Press Enter again to close the text field.

Example: `35`

Dependencies: Keep this additional information in mind:

- The APP Port 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: Lets you enable responses to security card password challenges by using the APP Server utility on a UNIX or Windows workstation.

Usage: Press Enter to toggle between Yes and No.

- Yes enables the Pipeline to respond to password challenges by using the APP Server utility.

- No disables responses from the APP Server utility.

  Select No to authenticate calls through the terminal server. No is the default.

Dependencies: Keep this additional information in mind:

- You must set Send Auth=PAP-Token for the APP Server 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

Auto Logout

Description: Specifies whether the Pipeline automatically logs out when a device disconnects from its control port or when the Pipeline loses power. The disconnected device can be a terminal, a VT-100, a terminal emulator, or a modem.

Usage: Press Enter to toggle between Yes and No.

- Yes enables automatic logout.
- No disables automatic logout.

  No is the default.

Location: System > Sys Config

Aux Send PW

Description: Specifies the password that the Pipeline sends when it adds channels to a security-card MP+ call that uses PAP-TOKEN-CHAP authentication. The Pipeline obtains authentication of the first channel of this MP+ call from the hand-held security card.

Usage: Press Enter to open a text field. Then, type a password. This password must match the one set up for your Pipeline in the RADIUS users file on the NAS (Network Access Server). Press Enter again to close the text field.

Dependencies: Aux Send PW applies only to outgoing MP+ calls in which Send Auth=PAP-TOKEN-CHAP.

Location: Configure; Ethernet > Connections > *any profile* > Encaps Options

See Also: Send Auth

Backup

Description: Specifies the profile name of a backup connection.

If the primary connection is unavailable, the Pipeline automatically diverts traffic to the backup connection. A connection can fail if, for example, a frame relay connection loses a Permanent Virtual Circuit, the physical link fails, or if a T1 line is in a red alarm condition. When the primary connection is restored, traffic again uses the primary connection.

When you use the backup connection, the Pipeline does not move routes to the backup profile. Therefore, the IP routes shown in the terminal server display may be incorrect, although statistical counts reflect the change.

Usage: Press Enter to open a text field. Then, type the name of the profile that you want to act as the backup. The name you specify must match the value of the Name parameter in a local Connection profile. The backup connection can be switched or nailed up.

Dependencies: Keep this additional information in mind:

- Do not create nested backup connections.
- The Backup parameter applies only to nailed-up connections (for which Call Type=Nailed or Nailed/MPP); otherwise, Backup=N/A.
- Parameters that you define in the primary Connection profile do not automatically apply to the backup Connection profile.

  For example, if you set the primary Connection profile to filter Telnet packets, you must set the backup profile to filter Telnet packets as well. Outgoing Frame Relay packets are the only packets that follow the primary Connection profile definitions. All other packets follow the backup Connection profile definitions.
- Backup is intended for situations in which the remote device (such as a data center) goes out of service; the backup call is made to a backup data center.

Backup is not intended to provide alternative lines for getting to a single destination.

- Do not confuse the Backup parameter with the Secondary parameter. A Backup Connection profile is used to re-establish an existing connection that has terminated; a Secondary Connection profile is used to establish a new connection if the primary Connection profile cannot. That is, the Secondary Connection provides an alternative line for a single destination, which the Backup Connection profile does not.

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

See Also: Name, Secondary

BACP

Description: Used to send or receive data using the Bandwidth Allocation Control Protocol.

Usage: Select the parameter and use the up or down arrow to cycle through the choices of Yes or No. Press Enter to make a selection.

- In the Ethernet > Answer > PPP Options menu, set BACP to Yes to use BACP when receiving calls.

  No is the default.
- To use BACP when sending data, in Ethernet > Connections > *any profile*, set Encaps to MP. In the Encaps option submenu, set BACP to Yes.

  No is the default.

  Note: The Idle Percent parameter does not appear in the Encaps Options menu when Encaps is set to MP, as it does not apply to MP or BACP.

Location: Ethernet > Answer > PPP Options; Ethernet > Connections > *any profile* > Encaps Options

Base Ch Count

Description: Specifies the initial number of channels the Pipeline sets up when originating calls for a PPP, MP+, or MP multichannel link.

Usage: Press Enter to open a text field. Then, type a number.

The maximum value of the Base Ch Count parameter depends on the encapsulation method that both ends of the link use.

- For an PPP link (where Encaps=PPP), the Base Ch Count is always 1.
- For an MP+ or MP link (where Encaps=MPP), the amount you specify is limited by the number of channels available, but the device at the remote end of the link must also support MP+ or MP.

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.

Press Enter to close the text field.

Dependencies: Keep this additional information in mind:

- You can determine the base bandwidth of a call by multiplying the value of the Base Ch Count parameter by the value of the Data Svc parameter.
- The Base Ch Count parameter does not apply (Base Ch Count=N/A) when all channels of the link are nailed up (Call Type=Nailed).
- For optimum MP+ performance, both sides of a connection must set these parameters to the same values:
  - Base Ch Count (in the Connection profile)
  - Min Ch Count (in the Answer profile)
  - Max Ch Count (in the Answer profile and the Connection profile)

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

See Also: Data Svc, Max Ch Count, Min Ch Count

Become Default Router

Description: Determines whether the Pipeline should advertise itself as the default router in DHCP responses.D

Usage: Press Enter to toggle between choices.

- Yes indicates that the Pipeline performing DHCP responses is the default router.
- No does not advertise the Pipeline as the default. No is the default.

Location: Ethernet > Mod Config > DHCP Spoofing

See Also: BOOTP Relay Enable

Bill

Description: Specifies a billing number for charges incurred on the line. If you do not enter a billing number, the telephone company bills charges to the telephone number assigned to the line.

Your carrier determines the billing number, and uses it to sort your bill. If you have several departments, and each department has its own Bill #, your carrier can separate and tally each department's usage.

Usage: Press Enter to open a text field. Then, type a telephone number. You can specify up to ten characters, and you must limit those characters to the following:

```
1234567890()[]!z-*# |
```

The Pipeline uses the Bill # parameter differently depending on the type of line you use:

- For a T1 line, the Pipeline appends the value specified in the Bill # parameter to the end of each phone number it dials for the call.
- Bill # for outgoing calls on an ISDN BRI line applies only to installations in Australia.

Press Enter to close the text field.

Example: These specifications are valid for Bill #:

```
5105551972
510-555-1972
```

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

See Also: Calling #, Id Auth

Block calls after

Description: Specifies how many unsuccessful attempts the Pipeline will make before beginning to block calls (discard packets).

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

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

See Also: Blocked duration

Blocked duration

Description: Specifies the number of seconds the Pipeline will block calls (discard packets).

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

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

See Also: Block calls after

BOOTP Relay Enable

Description: Controls whether Bootstrap Protocol (BOOTP) requests are relayed to other networks.

Usage: Press Enter to cycle through the choices.

- Yes specifies that BOOTP requests are relayed.
- No specifies that BOOTP requests are not relayed.

  No is the default.

Dependencies: You must use the Server parameter to specify the address of at least one BOOTP server. The BOOTP Relay menu also includes a second Server parameter for specifying a second BOOTP server. If you specify two BOOTP servers, the Pipeline 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.

Location: Ethernet > Mod Config > BOOTP Relay

See Also: Server, DHCP Spoofing

Bridge

Description: Enables or disables protocol-independent bridging for a call. If you disable bridging, you must enable routing by setting Route IP=Yes or Route IPX=Yes in the Connection profile.

Usage: Press Enter to cycle through the choices.

- Yes enables bridging.
- No disables bridging.
  No is the default.

Dependencies: The effect of the Bridge parameter depends upon how you set the Route IP and Route IPX parameters.

Bridge and Route IP

- If Bridge=Yes and Route IP=Yes, the Pipeline routes IP packets, and bridges all other packets.
- If Bridge=Yes and Route IP=No, the Pipeline bridges all packets.
- If Bridge=No and Route IP=Yes, the Pipeline routes only IP packets.
- If Bridge=No and Route IP=No, an error occurs and you cannot save the profile
  You must enable bridging or routing, or both.

Bridge and Route IPX

- If Bridge=Yes and Route IPX=Yes, the Pipeline routes IPX packets, and bridges all other packets.
- If Bridge=Yes and Route IPX=No, the Pipeline bridges all packets.
- If Bridge=No and Route IPX=Yes, the Pipeline routes only IPX packets.
- If Bridge=No and Route IPX=No, an error occurs and you cannot save the profile.
  You must enable bridging or routing, or both.

Additional Dependencies

- Bridging must be enabled on both the dialing and answering sides of the link.

  The Connection profile on the dialing side and the Answer profile on the answering side must both set the Bridge parameter to Yes. Otherwise, the Pipeline does not bridge the packets.

- The Bridge parameter does not apply (Bridge=N/A) if you turn off bridging in the Ethernet profile (Bridging=No).
- Bridge in the Answer profile applies to incoming calls for which no Connection profile exists; if a Connection profile exists, the setting of its Bridge parameter takes precedence.
- If Profile Reqd=Yes in the Answer profile, Bridge does not apply (Bridge=N/A) in the Answer profile.
- If Profile Reqd=Yes in the Answer profile, you must set Bridge=Yes in the answering Connection profile.
- Do not confuse the Bridge parameter with the Bridging parameter.
  - The Bridge parameter in the Answer profile applies only to connections that the Pipeline answers.
  - The Bridge parameter in the Connection profile applies only to a specific connection.
  - The Bridging parameter globally enables or disables bridging.

Location: Configure; Ethernet > Connections > *any profile*; Ethernet > Answer profile > PPP Options

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

Bridging

Description: Allows you to globally enable or disable bridging for all connections that the Pipeline answers or dials.

Usage: Press Enter to toggle between Yes and No.

- Yes globally enables bridging.

When you choose this setting, the Pipeline operates in promiscuous mode. The Ethernet controller in the Pipeline accepts all packets and passes them up the protocol stack for a higher-level decision on whether to route, bridge, or reject them. This mode is appropriate if you are using the Pipeline as a bridge.

- No globally disables bridging.

  When you choose this setting, the Ethernet controller filters out all packets except broadcast packets and those explicitly addressed to the Pipeline. The Bridge parameter in the Connection and Answer profiles, and all parameters exclusively associated with bridging, are set to N/A.

  This mode significantly reduces processor and memory overhead when the Pipeline is routing, and can result in much better performance, especially in moderate to heavily loaded networks.

  No is the default.

Dependencies: Do not confuse the Bridge parameter in the Answer and Connection profiles with the Bridging parameter in the Ethernet profile.

- The Bridge parameter in the Answer profile applies only to connections that the Pipeline answers.
- The Bridge parameter in the Connection profile applies only to a specific connection.
- The Bridging parameter in the Ethernet profile globally enables or disables bridging.

Location: Ethernet > Mod Config

See Also: Bridge

Buildout

Description: Specifies the amount of attenuation that the Pipeline should apply to the line's network interface in order to match the cable length from the Pipeline to the next repeater.

Attenuation is a measure of the power lost on a transmission line or on a portion of that line. When you specify a value for Buildout, the Pipeline applies an attenuator to the T1 line, causing the line to lose power when the received signal

is too strong. Repeaters boost the signal on a T1 line. If the Pipeline is too close to a repeater, you need to add some attenuation.

Usage: Press Enter to cycle through the choices.

- 0db
  db stands for decibels. 0db is the default.
- 0.6db
- 1.2db
- 1.8db
- 2.4db
- 3.0db
- 7.5db
- 15db
- 22.5db

Check with your carrier to determine the correct value.

Dependencies: The Buildout parameter applies only if the Pipeline has an internal CSU (Channel Service Unit) or other network interface unit at the line. You use a CSU to connect your Pipeline to the local digital telephone system.

Location: Nailed T1 Group > Mod Config

Call Filter

Description: Enables you to specify a call filter to plug into an Answer profile or a Connection profile.

By default, any packet destined for the WAN causes the Pipeline to place a call. In addition, by default, every packet resets the idle timer, the indicator that the Pipeline uses to know when to clear a call. When you set up a call filter, only those packets that the call filter forwards can initiate a call or reset the Preempt or Idle parameters.

Usage: Press Enter to open a text field. Then, type a number between 0 and 16. The number corresponds to a call filter you created in the Filters menu. Press Enter again to close the text field.

When you set Call Filter to 0 (zero), the Pipeline forwards all packets. Zero is the default.

Dependencies: Keep this additional information in mind:

- If all channels of a link are nailed up (Call Type=Nailed in the Connection profile), the Call Filter parameter does not apply (Call Filter=N/A) in both the Answer and Connection profiles.
- The Pipeline applies a call filter after applying a data filter; only those packets that the data filter forwards can reach the call filter.
- If IPX client bridging is in use (Handle IPX=Client), set the Call Filter parameter to 0 (zero).
- Call Filter in the Answer profile applies to incoming calls for which no Connection profile exists; if a Connection profile exists, the setting of its Call Filter parameter takes precedence.
- If Profile Reqd=Yes in the Answer profile, Call Filter does not apply (Call Filter=N/A) in the Answer profile.

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

See Also: Call Type, Data Filter, Forward, More, Profile Reqd

Call Type

Description: Appears in a Connection profile and a Frame Relay profile. Its functionality differs depending on the profile:

- In a Connection profile, specifies a type of link.
- In a Frame Relay profile, specifies the type of connection to a frame relay switch

  Frame Relay is an HDLC-based packet protocol that enables you to send data to a destination using one or more frame relay switches within a private network or a public carrier's network. HDLC stands for High Level Data Link Control.

  From the viewpoint of the Pipeline, a frame relay switch is an endpoint for all DLCIs (Data Link Connection Indicators) connecting to it. A DLCI identifies a Connection profile as a logical link; because more than one Connection profile can connect to a frame relay switch, a physical circuit can

carry more than one logical link. The DLCI parameter enables the frame relay switch to identify each Connection profile.

The frame relay switch connects the endpoints of the DLCIs to each other to make a virtual permanent circuit to which users can connect. The circuit acts like a wire between two endpoints with a fixed maximum bandwidth.

Usage: The settings you can choose for the Call Type parameter differ depending on the profile. In a Connection profile or a Frame Relay profile, you can specify Nailed, Switched, Nailed/MPP, Perm/Switched. Each selection is discussed below:

Nailed

This setting specifies a link that consists entirely of nailed-up channels.

- In a Connection profile, you must use the Group parameter to specify which channels are in the connection.
- In a Frame Relay profile, you must use the Nailed Grp parameter to specify which channels are in the connection.

  The Nailed setting is the default in a Frame Relay profile.

Switched

This setting specifies a link that consists entirely of switched channels.

- In a Connection profile, the Telco Options parameters specify the bandwidth of the connection, as well as other features of the switched link.

  The maximum number of channels on the link is the number set by Max Ch Count.

  The Switched setting is the default in a Connection profile.
- In a Frame Relay profile, you must specify the Switched setting if the Pipeline always initiates the connection to the frame relay switch; if a device at the remote end of the link initiates bridging or routing sessions, do not choose Switched.

  If you choose Switched, you must specify the bandwidth of the switched connection in the Data Svc parameter of the Frame Relay profile.

Nailed/MPP (Connection profile only)

This setting specifies a link that consists of both nailed-up and switched channels. The Pipeline establishes this connection whenever any of its nailed-up

or switched channels are connected end-to-end. If a Nailed/MPP link is down and the nailed-up channels are down, the link cannot re-establish itself until the Pipeline brings up one or more of the nailed-up channels, or dials one or more switched channels.

Typically, the switched channels are dialed when the Pipeline receives a packet whose destination is the unit at the remote end of the Nailed/MPP connection. The packet initiating the switched call must come from the caller side of the connection.

If a channel in a call fails for any reason, and the total number of channels in the Nailed/MPP connection falls below the value of the Min Ch Count parameter, the Pipeline tries to add a switched channel to bring the connection back up to the minimum.

If a failed channel is in the group specified by the Group parameter, that channel is replaced with a switched channel, even if the call is online with more than the minimum number of channels. Failed nailed-up channels are replaced by switched channels, regardless of the Min Ch Count setting.

Perm/Switched (Connection profile only)

This setting specifies a permanent switched connection.

A permanent switched connection is an outbound 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 ten-second intervals.

Use this setting if your telephone company charges for each incoming and outgoing connection attempt, but does not charge for connection time on local calls. Ascend's regular bandwidth-on-demand feature conserves connection time but causes many connection attempts. A permanent switched connection performs the opposite function—it conserves connection attempts but causes a long connection time.

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 Pipeline 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=Ans Only for that device.

Dependencies: Keep this additional information in mind:

- The Pipeline determines the minimum number of channels by the value of the Min Ch Count parameter or the number of nailed-up channels in the group, whichever is greater.

  The Pipeline does not count a nailed-up channel that is unused.
- The Pipeline determines the maximum number of channels by the value of the Max Ch Count parameter or the number of nailed-up channels in the group, whichever is greater.

  The Pipeline does not count a nailed-up channel that is unused.
- The Pipeline adds or subtracts switched channels on a Nailed/MPP connection as required by the parameters on either side of the connection.

  Each side makes its calculations based on the traffic received at that side. If the two sides of the connection disagree on the number of channels needed, the side requesting the greater number prevails.
- The DO Hangup parameter works only from the caller side of the connection when you choose Nailed/MPP.
- The Idle parameter works for both sides of the connection when you choose Nailed/MPP.

  However, if the answering side of the connection brings the link down because of an Idle timeout, the calling side can bring it back up.

Dependencies: Keep this information in mind concerning the Call Type parameter in a Connection profile or a Frame Relay profile:

- If the link consists entirely of nailed channels (Call Type=Nailed), the Callback feature does not apply (Callback=N/A).
- If the link consists entirely of switched channels (Call Type=Switched), the Group parameter does not apply (Group=N/A).
- In a Connection profile, the encapsulation must be MPP (Encaps=MPP) in order to select Call Type=Nailed/MPP.
- When you set Call Type=Perm/Switched in a Connection profile, the following parameters do not apply and are set to N/A:
  - AnsOrig=N/A because permanent switched connections are always outbound.

  - Callback=N/A because the device will not answer calls for a permanent switched connection.
  - Idle=N/A because a permanent switched connection is up permanently.
  - Backup=N/A because permanent switched connections do not support backup calls.
- The Idle and Backup parameters in the Session Options submenu are also set to N/A when Call Type=Perm/Switched.

Location: Ethernet > Connections > *any profile* > Telco Options; Ethernet > Frame Relay > *any profile*

See Also: Callback, Data Svc, DLCI, Group (Connection), Idle, Max Ch Count, Min Ch Count, Nailed Grp parameters, and DO Hangup in Chapter 1, "DO Command Reference."

Callback

Description: Enables or disables the callback feature. When you enable the callback feature, the Pipeline hangs up after receiving an incoming call that matches the one specified in the Connection profile. The Pipeline then calls back the device at the remote end of the link using the Dial # specified in the Connection profile.

You can use this parameter to tighten security, as it ensures that the Pipeline always makes a connection with a known destination.

Usage: Press Enter to toggle between Yes and No.

- Yes enables the callback feature.
- No disables the callback feature.

  No is the default.

Dependencies: Keep this additional information in mind:

- The Callback parameter does not apply (Callback=N/A) if all channels of the link are nailed up (Call Type=Nailed).
- If you set Callback=Yes, you must also set AnsOrig=Both, because the Connection profile must both answer the call and call back the device requesting access.

By the same token, any device calling into a Connection profile set for callback must be configured to both dial calls and answer them.

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

See Also: AnsOrig, Call Type, Dial #, Exp Callback

Called

Description: Adds authentication by Called Number using the number (ID) of the unit being called instead of the number of the calling unit. Called # is the same as Dial #, but without the trunk group or dialing prefix prepended.

Usage: Select the parameter and cycle through the possible choices.

- Ignore. Ignore calling number or called number.
- Prefer. Use Calling number ID authentication, but if it's not available, use name/password authentication.
- Require. Use Calling number ID authentication.
- Fallback does not apply to the Pipeline.
- Called Require. Same as Require, except uses the called number rather than the calling number ID.
- Called Prefer. Same as Prefer, except use the called number rather than the calling number ID.

Dependencies: You should also supply all the information to use PAP or CHAP authentication in case the called number is blocked (using Caller ID blocking from the phone company). Both types of authentication are not performed for the same connection.

Location: Ethernet > Connections > *any profile*

See Also: Id Auth

Caller ID

Description: Specifies if the ISDN phone number data associated with the POTS port should be included in, or blocked from, the ISDN BRI data stream

when outgoing analog calls are placed. The parameter setting applies to both ports. You cannot set each port separately.

Usage: Select the parameter and cycle through the possible values of Yes or No by pressing Enter. Yes is the default.

Example: Caller ID = Yes

Location: Configure menu

Calling

Description: Specifies the calling party's phone number (also called CLID or ID). If authentication by CLID is enabled by the Id Auth parameter, the Pipeline compares the CLID of incoming calls to the value of the Calling # parameter.

Usage: Press Enter to open a text field. Then, enter the calling party's phone number. You can enter up to 20 characters. Press Enter again to close the text field.

Location: Ethernet > Connections > *any profile*

See Also: Id Auth

Chan Usage

Description: Specifies how the B channels are used on an ISDN line. Typically, both channels are switched. The first setting in each pair represents B1 channel usage, and the second represents the B2 channel usage.

Switched means that the channel uses dial-in switched service at either 64 kbps (the default) or 56 kbps per B channel. The B channels can be used singly or together for one or more simultaneous dial-ups on the same line, depending on active sessions and bandwidth demands.

Unused means that the channel is not used for dial-in connections. The Pipeline will have access only to the other channel, which limits the bandwidth to 64 kbps.

Leased means that the channel is leased (dedicated to a permanent "nailed" connection to one remote network).

Super Dig 128 supports ISDN connections in Japan. It concatenates the two B channels into a single 128 kbps pipe on a nailed-up connection, delivering unrestricted 128 kbps bandwidth. Super Digital 128 uses a single group number with both nailed lines connected to a single PPP/MPP interface. Only one dial-up phone number is assigned, and only one call can be supported at one time. The switch type must be set to JAPAN.

Alternatively, you can specify Leased/Leased to configure two separate B channels, with separate group numbers to be nailed to the same or different destinations. This method works inter-lata, similarly to any switched service.

Usage: Press Enter to cycle through the choices.

- Switch/Switch (default)
- Unused/Switch
- Switch/Unused
- Super Dig 128
- Leased/Unused
- Unused/Leased
- Switch/Leased
- Leased/Switch
- Leased/Leased

Location: Configure

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 > *any profile* > IP Options

See Also: Client Pri DNS, Client Sec DNS

Client Gateway

Description: Specifies the default route for IP packets coming from the user on this connection.

Usage: Specify the IP address of the next hop router in dotted decimal notation. The default value is 0.0.0.0; if you accept this value, the Pipeline routes packets as specified in the routing table, using the system-wide default route if it cannot find a more specific route.

The Pipeline must have a direct route to the address you specify. The direct route can take place via a profile or an Ethernet connection. If the Pipeline does not have a direct route, it drops the packets on the connection. When you diagnose routing problems with a profile using this feature, an error in a per-user gateway address is not apparent from inspection of the global routing table.

Example: If you specify Client Gateway=10.0.0.3 in a profile, IP packets from the user with destinations through the default route will be routed through the gateway at 10.0.0.3.

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

Client Pri DNS

Description: Specifies a primary DNS server address to be sent to any client connecting to the Pipeline. 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 > *any profile* > IP Options

Client Sec DNS

Description: Specifies a secondary DNS server address to be sent to any client connecting to the Pipeline. 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 > *any profile* > IP Options

Clock Source

Description: Specifies whether or not the Pipeline should use its own internal oscillator to generate the T1 transmit clock. If not, the unit synchronizes to the network (telco) using the receive clock.

Usage: Select the field and cycle through the possible choices of Yes or No.

- Yes means the unit provides its own clocking.
  When connecting two Pipeline 130 units back-to-back on a private, twin shielded, twisted-pair connection, set Clock Source on one Pipeline to Yes, and set the other to No.
- When set to No, the unit takes its clocking from the telco line.
  No is the default.

Location: Nailed T1 > Mod Config

Comm

Description: Specifies an SNMP (Simple Network Management Protocol) community name. The string you specify becomes a password that the Pipeline sends to the SNMP manager when an SNMP trap event occurs. The password authenticates the sender identified by the IP address in the IP Adrs parameter.

SNMP provides a way for computers to share networking information. In SNMP, two types of communicating devices exist: agents and managers. An agent (such as the Pipeline) provides networking information to a manager application running on another computer. The agents and managers share a database of information, called the Management Information Base (MIB).

A trap is a mechanism in SNMP for reporting system change in real time. To report system change, the Pipeline, sends a traps-PDU across the Ethernet interface to the SNMP manager. A complete list specifying the events that cause the Pipeline to send a traps-PDU appears in the Ascend Enterprise Traps MIB.

Usage: Press Enter to open a text field. Then, type the community name. You can enter an alphanumeric string containing up to 31 characters. The default is [ ]. Press Enter again to close the text field.

Dependencies: To turn off SNMP traps, leave the Comm parameter blank and set Dest=0.0.0.0.

Location: Ethernet > SNMP Traps

See Also: Dest

Compare

Description: Specifies how a packet's contents are compared to the value specified in the filter.

After applying the Offset, Mask, and Length values to reach the appropriate location in a packet, the Pipeline compares the packet's contents to the Value parameter. If Compare is set to Equals (the default), the Pipeline applies the filter if the packet data is identical to the setting of the Value parameter. If Compare is set to NotEquals, the Pipeline applies the filter if the packet data is not identical to the setting of the Value parameter.

Usage: Press Enter to cycle through the choices.

- Equals indicates that a match occurs when data in the packet equals the conditions specified in the filter.

  Equals is the default
- NotEquals indicates that a match occurs when data in the packet does not equal the conditions specified in the filter.

Dependencies: Keep this additional information in mind:

- Compare=N/A if the filter is not Valid or if the filter type is IP.

Location: Ethernet > Filters > *any type* > *any filter* > Generic

See Also: Length (Filter), Mask, Offset, Value

Connection

Description: Appears in a Bridging profile or an IPX Route profile. Its functionality differs depending on the profile:

- In a Bridging profile, specifies the number of a Connection profile through which you can reach the node specified by the Enet Adrs parameter of the Bridging profile.

  The IP address contained in the Connection profile's LAN Adrs parameter corresponds to the MAC address contained in the Bridging profile's Enet Adrs parameter. The Pipeline dials the Connection profile when a node on its LAN sends a packet whose destination matches the Enet Adrs value in the profile.
- In an IPX Route profile, identifies the number of the Connection profile through which you can reach the NetWare server connected by the static route and is required.

Usage: Press Enter to open a text field. Your usage depends on the profile.

Bridging profile

Type the last two digits of the menu number of a Connection profile in which Bridging=Yes. You can type a number from 1 to 31. Zero (0) is the default; this setting disables the profile.

Press Enter again to close the text field.

IPX Route profile

Type the last two digits of the menu number of a Connection profile. You can type a number from 1 to 31. Zero (0) is the default; this setting specifies that no Connection profile can reach the destination.

You must enter a value in this parameter, because you should only advertise static routes that you can reach.

Press Enter again to close the text field.

Dependencies: Keep this additional information in mind for each type of profile.

Bridging profile

You must set Dial Brdcast=No if you want the Pipeline to use a static bridge entry. Any Connection profile that dials on broadcast does not need a Bridging profile.

IPX Route profile

In an IPX Route profile, you must carry out these tasks if you want static IPX routes to appear in the route table:

- Enable IPX routing in the Connection profile by setting Route IPX=Yes.
- Configure IPX on the local Ethernet network by specifying a setting for one or more of these parameters: Active, Connection #, Hop Count, IPX Alias, IPX Frame, IPX Net#, Network, Node, Server Name, Server Type, Socket, and Tick Count.

Location: Ethernet > Bridge Adrs > *any profile*; Ethernet > IPX Route > *any profile*

See Also: Active, Hop Count, IPX Alias, IPX Frame, IPX Net#, Network, Node, Route IPX, Server Name, Server Type, Socket, Tick Count

Console

Description: Specifies the type of control interface established at the VT-100 port labeled Control on the back panel of the Pipeline.

Usage: Standard enables you to use the standard set of menus. Standard is the default and cannot be changed on the Pipeline.

The Control Monitor is a menu-based user interface for configuring, managing, and monitoring the Pipeline. It consists of nine windows—eight status windows and a single edit window.

Location: System > Sys Config

Contact

Description: Specifies the person or department to contact if you experience problems using the Pipeline.

Usage: Press Enter to open a text field. Then, type the name of the contact person or department. You can enter up to 60 characters. An SNMP management application can read this field, but the value you enter does not affect the operation of the Pipeline.

Press Enter again to close the text field.

Location: System > Sys Config

See Also: Location

Data Filter

Description: Specifies a data filter to plug into an Answer profile or a Connection profile. This data filter examines each incoming or outgoing packet on a WAN, and either forwards or discards it.

Usage: Press Enter to open a text field. Then, type a number between 0 and 16. The number corresponds to a data filter you created in the Filters menu. Press Enter again to close the text field.

When you set Data Filter to 0 (zero), the Pipeline forwards all data packets. Zero is the default.

Dependencies: Keep this additional information in mind:

- The Pipeline applies a call filter after applying a data filter; only those packets that the data filter forwards can reach the call filter.
- If IPX client bridging is in use (Handle IPX=Client), set the Data Filter parameter to 0 (zero).

- Do not confuse the Filter parameter with the Data Filter parameter.
  The Filter parameter filters data packets on the Pipeline unit's local LAN interface; the Data Filter parameter filters data packets on the Pipeline unit's WAN interface. The WAN interface is the port on the Pipeline that is connected to a WAN line.
- Data Filter in the Answer profile applies to incoming calls for which no Connection profile exists; if a Connection profile exists, the setting of its Data Filter parameter takes precedence.
- If Profile Reqd=Yes in the Answer profile, Data Filter does not apply (Data Filter=N/A) in the Answer profile.

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

See Also: Call Filter, Call Type, Forward, More, Profile Reqd

Data Svc

Description: Specifies the type of data service the link uses for outgoing calls.

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.

Usage: Press Enter to cycle through the choices. You can specify one of the settings listed in Table 3-1.

Table 3-1. Data Svc settings

Setting	Description
56K	The call contains any type of data and connects to the Switched-56 data service. The only services available to lines using inband signaling (such as Switched-56 lines) are 56K and 56KR. The only services available to lines using inband signaling (T1 access lines containing one or more switched channels, and Switched-56 lines) are 56K and 56KR. For most T1 lines, select 56K.

Table 3-1. Data Svc settings (continued)

Setting	Description
56KR	The call contains restricted data, guaranteeing that the data the Pipeline transmits meets the density restrictions of D4-framed T1 lines. D4 specifies the D4 format, also known as the Superframe format, for framing data at the physical layer. This format consists of 12 consecutive frames, separated by framing bits. The only services available to lines using inband signaling (T1 access lines containing one or more switched channels, and Switched-56 lines) are 56K and 56KR.
64K	The call contains any type of data and connects to the Switched-64 data service.
Voice	This value applies only to calls made over an ISDN BRI or T1 line. The voice setting enables the Pipeline to instruct the network to place 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 might become corrupted or 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.

Dependencies: Keep this additional information in mind:

- The Voice setting only applies to switched channels.
- You can determine the base bandwidth of a call by multiplying the value of the Base Ch Count parameter by the value of the Data Svc parameter.
- Either party can request a data service that is unavailable; in this case, the Pipeline cannot connect the call.

Location: Ethernet > Connections > *any profile* > Telco Options; Ethernet > Frame Relay > *any profile*

See Also: Call Type

DBA Monitor

Description: Specifies how the Pipeline monitors the traffic over a Multilink Protocol Plus (MPP) call.

Usage: Press Enter to cycle through the choices:

- Transmit

  This specifies that the Ascend unit will add or subtract bandwidth based on the amount of data it transmits.
- Transmit-Recv

  This specifies that the Ascend unit will add or subtract bandwidth based on the amount of data it transmits *or* receives.
- None

  This specifies that the Ascend unit will not monitor traffic over the link and will not use DBA.

Dependencies: DBA-Monitor is only supported on MPP calls (Encaps=MPP).

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

See Also: Encaps, Dyn Alg, Target Util, Idle Pct

DCE N392

Description: Specifies the maximum number of error events that can occur in the sliding window defined by DCE N393. The error events can include link reliability errors, protocol errors, and sequence number errors. If the Pipeline exceeds the threshold defined by N392, the Frame Relay switch declares the Pipeline inactive.

Usage: Press Enter to open a text field. Then, type a number between 1 and 10. The default is 3. Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- The DCE N392 parameter applies only if Link Mgmt=T1.617D and the FR Type is DCE.
- If you turn off the Pipeline, disconnect its WAN connection, or set Active=No in the Frame Relay profile, the setting of N392 multiplied by the setting of N391 indicates the time it takes the frame relay switch to declare an inactive state.

Location: Ethernet > Frame Relay > *any profile*

See Also: Link Mgmt, N391, DTE N393, FR Type

DCE N393

Description: Specifies the width of the sliding window used by the DCE N392 parameter. For example, if DCE N393=5, the sliding window begins five monitored events ago and extends to the present. A monitored event occurs when the Pipeline makes a Status Enquiry.

Usage: Press Enter to open a text field. Then, type a number between 1 and 10. The default is 4. Press Enter again to close the text field.

Dependencies: The DCE N393 parameter applies only if Link Mgmt=T1.617D and the FR Type is DCE.

Location: Ethernet > Frame Relay > *any profile*

See Also: Link Mgmt, DTE N392, FR Type

Def Server

Description: Defines the server to which the Pipeline routes incoming packets when their destination port number does not match an entry in Static Mappings nor does it match a port number dynamically assigned when a local host initiates a TCP / UDP session. The default server is used only when the Pipeline is running network address translation (NAT) in single-address mode.

Note: If you change the value of this parameter, the change does not take effect until the next time a connection is made to the remote network specified in the NAT profile. To make the change immediately, you must terminate the connection to the remote network and then reopen it.

Usage: Press Enter to open a text field and then type the IP address.

The address consists of four numbers between 0 and 255, separated by periods. Enter 0.0.0.0 to disable routing of packets to a default server.

The default value is 0.0.0.0.

Press Enter again to close the text field, press Esc to exit the menu, and then confirm the change when prompted.

Note: The change does not take effect until the next time the link is brought up. To make the change immediately, bring the link down and back up.

Dependencies: Keep this additional information in mind:

- For routing of packets from a remote network to occur, the Routing parameter in the NAT menu must be set to Yes and the Lan parameter in the NAT menu must be set to Single IP Addr. Parameters in Static Mapping nn menus (where nn is a number between 01 and 10) control whether the Pipeline routes packets from a remote network for up to 10 different TCP or UDP ports to specific servers and ports on the local network.
  - The Dst Port# and Loc Port# parameters must be set to values other than 0.
  - The address cannot be 0.
- If your local network has only one server that handles all incoming packets, you can specify the server by
  - setting this parameter to the address of the server.
  - setting the Valid parameter in each of the Static Mapping nn menus to No, which disables routing of incoming packets by their destination ports.
- If the Routing parameter in the NAT menu is set to No or the Lan parameter in the NAT menu is set to Multi IP Addr, this parameter is N/A.

Location: Ethernet > NAT > NAT

See Also: Dst Port # (Static Mapping), Loc Adrs, Loc Port#, Lan, Routing, Protocol (Static Mapping), Validate IP

See Also:

Dest

Description: Appears in a Static Rtes profile and in an SNMP Traps profile. Its functionality differs depending on the profile:

- In a Static Rtes profile, specifies the IP address of the route's destination.
- In an SNMP Traps profile, specifies the IP address of the SNMP manager to which the Pipeline sends traps-PDUs (Protocol Data Units).

Usage: Press Enter to open a text field. Then, type the IP address of the destination.

An IP address consists of four numbers between 0 and 255, separated by periods. If a netmask is in use, you must specify it. Separate a netmask from the IP address with a slash.

The Pipeline ignores any digits in the IP address hidden by a netmask. For example, the address 200.207.23.1/24 becomes 200.207.23.0. To specify a route to a specific host, use a mask of 32.

The default value is 0.0.0.0/0. This value has a different meaning depending on the profile:

- In a Static Rtes profile, the first route is the default route, and the Dest parameter is set to 0.0.0.0/0; this default specifies all destinations for which no other route exists.
- In an SNMP Traps profile, you turn off traps by setting Dest=0.0.0.0 and deleting the value for the Comm parameter.

Press Enter to close the text field.

Example: `200.207.23.1`

Dependencies: Keep this additional information in mind:

- If you do not know the right IP address to enter, you must obtain it from the network administrator.
- Do not attempt to configure an IP address by guesswork!
- The Dest parameter does not apply (Dest=N/A) if the Pipeline does not support IP (Route IP=No).

Location: Ethernet > Static Rtes > *any profile*; Ethernet > SNMP Traps > *any profile*

See Also: Comm, Encaps, Route IP

DHCP PNP Enabled

Description: Determines whether the Pipeline enables Plug and Play when running in DHCP server mode. In Plug and Play, the Pipeline assigns an IP address, and returns it along with the Default Gateway and Domain Name Server IP addresses to the requesting device on a remote network. The default is Yes.

Usage: Press Enter to toggle between Yes (the default) and No.

Location: Ethernet > Mod Config > DHCP Spoofing

See also: BOOTP Relay Enable

DHCP Spoofing

Description: Enables or disables all of the DHCP features.

Usage: Press Enter to cycle through the choices.

- Yes enables all DHCP features.
- No disables all DHCP features.
  Yes is the default.

Location: Ethernet > Mod Config > DHCP Spoofing

See Also: Always Spoof

Dial

Description: Appears in the Configure menu, a Connection profile, and a Frame Relay profile. Its functionality differs depending on the profile:

- In the Configure or Connection profile, specifies the phone number the Pipeline dials to reach the bridge, router, or node at the remote end of the link.

- In a Frame Relay profile, specifies the phone number that the Pipeline dials to reach a frame relay switch.

  Frame Relay is an HDLC-based packet protocol that enables you to send data to a destination using one or more frame relay switches within a private network or a public carrier's network. HDLC stands for High Level Data Link Control.

  From the viewpoint of the Pipeline, a frame relay switch is an endpoint for all DLCIs (Data Link Connection Indicators) connecting to it. A DLCI identifies a Connection profile as a logical link. The frame relay switch connects the endpoints of the DLCIs to each other to make a virtual permanent circuit to which users can connect. The circuit acts like a wire between two endpoints with a fixed maximum bandwidth.

Usage: Press Enter to open a text field. Then, type a telephone number. You can enter up to 37 characters, and you must limit those characters to the following:

```
1234567890()[]!z-*#|
```

The Pipeline sends only the numerical characters to place a call.

The default value is null.

Press Enter to close the text field.

Dependencies: Keep this additional information in mind:

- Dial # does not apply (Dial #=N/A) when all channels are nailed up (Call Type=Nailed) or if you are using frame relay encapsulation (Encaps=FR).
- If Sub-Adr=Termsel (in the System, Sys Config menu) include the ISDN subaddress in the Dial #, separating it from the phone number with a comma. The characters before the comma comprise the phone number; the one or two numeric characters after the comma comprise the subaddress. Consider this example:

  555-1212,23

  The Pipeline dials the phone number 555-1212, and conveys the subaddress 23 to the answering party.

Location: Configure; Ethernet > Connections > *any profile*; Ethernet > Frame Relay > *any profile*

See Also: Call Type, Encaps, Nailed T1 Group, Group (Connection), Sub-Adr

Dial Brdcast

Description: Specifies whether broadcast packets initiate dialing.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that the Pipeline dials a link if (a) the link is not online and (b) the Pipeline receives a frame whose MAC address is set to broadcast.

  When a device on the local Ethernet interface sends out broadcast packets that the Pipeline must bridge to another network, the Pipeline starts up a session for each Connection profile in which Dial Brdcast=Yes. Gradually, it builds an internal bridge table based on experience; this table helps to limit the number of calls by recording the appropriate destination network for various addresses.

- No specifies that broadcast packets do not initiate dialing.

  If you choose this setting, the Pipeline relies on its Bridging Profiles, which contain remote physical addresses you have manually entered.

  The IP address contained in the Connection profile's LAN Adrs parameter corresponds to the MAC address contained in the Bridging profile's Enet Adrs parameter. The Pipeline dials the Connection profile when a node on its LAN sends a packet whose destination matches the Enet Adrs value.

  No is the default.

Dependencies: The Dial Brdcast parameter applies only if the Connection profile enables bridging (Bridge=Yes) and allows outgoing calls (AnsOrig=Call Only or AnsOrig=Both).

Location: Ethernet > Connections > *any profile*

See Also: Connection #

Dial If Link Down

Description: Dial If Link Down applies when both DHCP spoofing and BOOTP relay are enabled. If no wide area network links are active, the Pipeline performs DHCP spoofing. When set to Yes, as soon as the dialed link is established, the Pipeline stops DHCP spoofing and acts as a BOOTP relay agent.

Usage: Press Enter to toggle between choices.

- Yes forces the Pipeline to dial the first Connection profile whenever a it responds to a DHCP client request. Be sure the first Connection profile accesses the DHCP server for which the Pipeline is spoofing.
- No lets the Pipeline connect according to settings already in place in the environment, such as according to the current TCP/IP settings, or settings for any other network management software in use.
  No is the default.

Location: Ethernet > Mod Config > DHCP Spoofing

See Also: BOOTP Relay Enable

Dial Query

Description: Specifies whether the Pipeline 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: Press Enter to toggle between Yes and No.

- Yes specifies that the Pipeline 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 Pipeline establishes any connections with the Dial Query mechanism.
- No specifies that the Pipeline does not place a call to the location specified in the Connection profile when a workstation looks for the nearest server.

  No is the default.

Dependencies: If there is an entry in the Pipeline unit's routing table for the location specified by the Connection profile, Dial Query has no effect.

Location: Ethernet > Connections > *any profile* > IPX Options

Disc on Auth Timeout

Description: Enables you to specify whether the Pipeline gracefully shuts down the PPP connection after an authentication timeout.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that the Pipeline does not shut down cleanly, but simply hangs up a PPP connection on an authentication timeout.
- No specifies that the Pipeline shuts down a call gracefully on a authentication timeout.

  No is the default.

Location: Ethernet > Answer > PPP Options

DLCI

Description: Specifies the Data Link Connection Indicator that identifies the Connection profile to the frame relay switch as a logical link on a physical circuit.

Frame Relay is an HDLC-based packet protocol that enables you to send data to a destination using one or more frame relay switches within a private network or a public carrier's network. HDLC stands for High Level Data Link Control.

From the viewpoint of the Pipeline, a Frame Relay switch is an endpoint for all DLCIs (Data Link Connection Indicators) connecting to it. A DLCI identifies a Connection profile as a logical link. The frame relay switch connects the endpoints of the DLCIs to each other to make a virtual permanent circuit to which users can connect. The circuit acts like a wire between two endpoints with a fixed maximum bandwidth.

Each Frame Relay profile can include more than one Connection profile, all sharing the total bandwidth of the Frame Relay link.

Usage: Press Enter to open a text field. Then, enter a number between 16 and 991. The default is 16. Ask your Frame Relay network administrator for the value you should enter. Press Enter to close the text field.

Dependencies: Keep this additional information in mind:

- DLCI only appears in a Connection profile when Encaps=FR
- Each Connection profile that contains the setting Encaps=FR represents a separate logical link; you must assign it a unique setting for DLCI.

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

See Also: Encaps, FR Prof

Domain Name

Description: Specifies the name of domain the Pipeline is located in. This name is used by the Domain Name System (DNS) to associate IP addresses with symbolic names.

DNS is a TCP/IP service that enables you to specify a symbolic name instead of an IP address. A symbolic name consists of a username and a domain name in the format *username@domain name*. The *username* corresponds to the host number in the IP address. The *domain name* corresponds to the network number in the IP address. A symbolic name might be steve@abc.com or joanne@xyz.edu.

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

Usage: Press Enter to open a text field. Then, type the domain name of the Pipeline. Press Enter again to close the text field.

Location: Ethernet > Mod Config > DNS

See Also: Pri DNS, Sec DNS

Dst Adrs

Description: In a filter of type IP, specifies the destination address to which the Pipeline compares a packet's destination address.

Usage: Press Enter to open a text field. Then, type the destination address the Pipeline should use for comparison when filtering a packet. The address consists of four numbers between 0 and 255, separated by periods.

The null address 0.0.0.0 is the default. If you accept the default, the Pipeline does not use the destination address as a filtering criterion.

Press Enter to close the text field.

Example: `200.62.201.56`

Dependencies: Dst Adrs does not apply (Dst Adrs=N/A) if you are using a generic filter (Type=Generic) or if you have not activated the IP filter (Valid=No).

Location: Ethernet > Filters > *any type of filter* > *any input or output filter* > *any numbered filter* > Ip Options

See Also: Dst Mask

Dst Mask

Description: In a filter of type IP, specifies the bits that the Pipeline should mask when comparing a packet's destination address to the value of the Dst Adrs parameter. The masked part of an address is hidden; the Pipeline does not use it for comparison with Dst Adrs. A mask hides the part of a number that appears behind each binary 0 (zero) in the mask; the Pipeline uses only the part of a number that appears behind each binary 1 for comparison.

The Pipeline applies the mask to the address using a logical AND after the mask and address are both translated into binary format.

Usage: Press Enter to open a text field. Then, type the IP mask in dotted decimal format. The value 0 (zero) hides all bits, because the decimal value 0 is the binary value 00000000; the value 255 does not mask any bits, because the decimal value 255 is the binary value 11111111.

The null address 0.0.0.0 is the default; this setting indicates that the Pipeline 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 Pipeline uses for comparison.

Press Enter to close the text field.

Example: Suppose a packet has the destination address 10.2.1.1. If Dst Adrs=10.2.1.3 and Dst Mask=255.255.255.0, the Pipeline masks the last digit and uses only 10.2.1, which matches the packet.

Dependencies: Dst Mask does not apply (Dst Mask=N/A) if you are using a generic filter (Type=Generic) or if you have not activated the IP filter (Valid=No).

Location: Ethernet > Filters > *any type of filter* > *any input or output filter* > *any numbered filter* > Ip Options

See Also: Dst Adrs

Dst Port # (Filters)

Description: In a filter of type IP, specifies the destination port number to which the Pipeline compares the packet's destination port number. The destination port number specifies the port on the remote device that must be "listening" for packets.

The Dst Port Cmp criterion determines how the Pipeline carries out the comparison.

Usage: Press Enter to open a text field. Then, type the number of the destination port the Pipeline should use for comparison when filtering packets. You can enter a number between 0 and 65535.

The default setting is 0 (zero). If you accept the default, the Pipeline does not use the destination port number as a filtering criterion. Press Enter to close the text field.

Note that 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 sessions.

Location: Ethernet > Filters > *any type of filter* > *any input or output filter* > *any numbered filter* > Ip Options

See Also: Dst Port # (Static Mapping), Src Port Cmp, Src Port #

Dst Port # (Static Mapping)

Description: The number of a TCP or UDP port to which users outside the local private network can send packets to access servers and services on the local LAN.

When the Pipeline is configured for single-address NAT, each Dst Port # corresponds to a service (Loc Port # parameter) provided by a server (Loc Adrs parameter) on the local network; however the actual port number of the service is given by the Loc Port # parameter for which Dst Port # is an alias.

Note: If you change the value of this parameter or of any of the other parameters in a Static Mapping nn menu, the change does not take effect until the next time a connection is made to the remote network specified in the NAT profile. To make the change immediately, you must terminate the connection to the remote network and then reopen it.

Usage: Press Enter to open a text field and then type the port number.

Enter a port number between 1 and 65535.

Press Enter again to close the text field, press Esc to exit the menu, and then confirm the change when prompted.

Dependencies: Keep this additional information in mind:

- For routing of incoming packets for a particular port to occur, the Routing parameter in the NAT menu must be set to Yes, the Lan parameter in the NAT menu must be set to Single IP Addr, the Valid parameter in the same Static Mapping nn menu must be set to Yes, and other parameters in the same Static Mapping nn menu must be set to non-null values:
  - The Loc Port# parameter must be set to a value other than 0.
  - The Loc Adrs parameter must be set to an address other than 0.0.0.0.

  If you enter 0 as the value of this parameter, you receive the message Invalid Input: Zero input is not Valid.
- The Protocol parameter in the same Static Mapping nn menu determines whether the port you specify is a TCP or UDP port.
- If the Routing parameter in the NAT menu is set to No or the Lan parameter in the NAT menu is set to Multi IP Addr, this parameter is N/A.

Location: Ethernet > NAT > Static Mapping > Static Mapping *nn* (where *nn* is a number between 01 and 10)

See Also: Def Server, Loc Adrs, Loc Port#, Lan, Routing, Protocol (Filter), Valid (Static Mapping)

Dst Port Cmp

Description: In a filter of type IP, specifies the type of comparison the Pipeline makes when using the Dst Port # parameter.

Usage: Press Enter to cycle through the choices.

- None specifies that the Pipeline 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: Keep this additional information in mind:

- This parameter works only for TCP and UDP packets.

  You must set Dst Port Cmp=None if the Protocol parameter is not set to 6 (TCP) or 17 (UDP).
- Dst Port Cmp does not apply (Dst Port Cmp=N/A) if you are using a generic filter (Type=Generic) or if you have not activated the IP filter (Valid=No).

Location: Ethernet > Filters > *any type of filter* > *any input or output filter* > *any numbered filter* > Ip Options

See Also: Dst Port # (Filters)

DTE N392

Description: Specifies the maximum number of error events that can occur in the sliding window defined by DTE N393. The error events can include link reliability errors, protocol errors, and sequence number errors. If the Pipeline exceeds the threshold defined by DTE N392, the frame relay switch declares the Pipeline inactive.

Usage: Press Enter to open a text field. Then, type a number between 1 and 10. The default is 3. Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- The DTE N392 parameter applies only if Link Mgmt=T1.617D and the FR Type is DTE.
- If you turn off the Pipeline, disconnect its WAN connection, or set Active=No in the Frame Relay profile, the setting of N392 multiplied by the setting of N391 indicates the time it takes the frame relay switch to declare an inactive state.

Location: Ethernet > Frame Relay > *any profile*

See Also: Link Mgmt, N391, DCE N393, FR Type

DTE N393

Description: Specifies the width of the sliding window used by the DTE N392 parameter. For example, if DTE N393=5, the sliding window begins five monitored events ago and extends to the present. A monitored event occurs when the Pipeline makes a Status Enquiry.

Usage: Press Enter to open a text field. Then, type a number between 1 and 10. The default is 4. Press Enter again to close the text field.

Dependencies: The DTE N393 parameter applies only if Link Mgmt=T1.617D and the FR Type is DTE.

Location: Ethernet > Frame Relay > *any profile*

Link Mgmt, DCE N392, FR Type

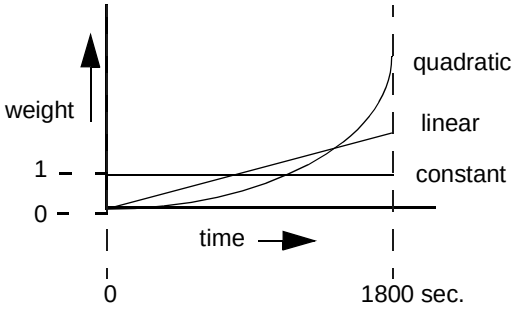
Dyn Alg

Description: Specifies which Dynamic Bandwidth Allocation (DBA) algorithm to use for calculating average line utilization (ALU) of transmitted data. DBA enables you to specify that the Pipeline uses ALU as the basis for automatically adding or subtracting bandwidth from a switched connection without terminating the link.

The Pipeline uses the historical time period specified by the Sec History parameter as the basis for calculating ALU. It then compares ALU to the amount specified in the Target Util parameter. When ALU exceeds the threshold defined by Target Util for a period of time greater than the value of the Add Pers parameter, the Pipeline attempts to add a channel. When ALU falls below the threshold defined by Target Util for a period of time greater than the value of the Sub Pers parameter, the Pipeline attempts to remove a channel.

MP+ supports Dynamic Bandwidth Allocation.

Usage: Press Enter to cycle through the choices. This graph illustrates the algorithms you can choose:



- Linear gives more weight to recent samples of bandwidth usage than to older samples taken during the historical period specified by the Sec History parameter; the weighting grows at a linear rate.
- Quadratic gives more weight to recent samples of bandwidth usage than to older samples taken during the historical period specified by the Sec History parameter; the weighting grows at a quadratic rate.

  Quadratic is the default for MP+ calls (Encaps=MPP).
- Constant gives equal weight to all samples taken during the historical time period specified by the Sec History parameter.

  When you select this option, older historical samples have as much impact on the decision to change bandwidth allocation as do more recent samples.

Dependencies: Keep this additional information in mind:

- To dynamically allocate bandwidth by tracking line usage, you must specify the Add Pers, Dyn Alg, Max Ch Count, Sec History, Sub Pers, and Target Util parameters.
- Dyn Alg in the Answer profile applies to incoming calls for which no Connection profile exists; if a Connection profile exists, the setting of its Dyn Alg parameter takes precedence.
- If Profile Reqd=Yes in the Answer profile, Dyn Alg does not apply (Dyn Alg=N/A) in the Answer profile.

Location: Ethernet > Answer > PPP Options; Ethernet > Connections > *any profile* > Encaps Options

See Also: Add Pers, DBA Monitor, Dyn Alg, Max Ch Count, Sec History, Sub Pers, Target Util

Edit Security

Description: Grants or restricts privileges to edit Security Profiles.

Usage: Press Enter to toggle between Yes and No.

- Yes grants privileges.

  Yes is the default. When you choose Yes, a user is permitted to edit Security Profiles, and can access all other operations by enabling them in his or her active Security profile.
- No restricts privileges.

Dependencies: Keep this additional information in mind:

- The Edit Security parameter does not apply (Edit Security=N/A) if Operations=No.
- Do not set the Edit Security parameter to No on all nine Security Profiles; if you do, you will be unable to edit any of them.

Location: System > Security > *any profile*

Edit System

Description: Grants or restricts privileges to edit the System profile and the Ethernet profile.

Usage: Press Enter to toggle between Yes and No.

- Yes grants privileges to edit the System profile, and to edit the Read Comm and R/W Comm parameters in the Ethernet profile.

  Yes is the default.
- No restricts privileges.

Dependencies: The Edit System parameter does not apply (Edit System=N/A) if Operations=No.

Location: System > Security > *any profile*

Enable Local DNS Table

Description: Enables the use of a local DNS table that can provide a list of IP addresses for a specific host when the remote DNS server fails to resolve the host name successfully. The Local DNS table will provide the list of IP addresses only if the host name for the attempted connection matches a host name in the local DNS table.

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

Location: Ethernet > Mod Config > DNS

See Also: Loc.DNS Tab Auto Update

Encaps

Description: Enables you to choose the encapsulation method to use when exchanging data with a remote network.

Usage: Press Enter to cycle through the choices. You can choose one of the settings listed below.

PPP

PPP (Point-to-Point Protocol) provides a standard means of encapsulating data packets over a single-channel WAN link that a Connection profile sets up. It ensures basic compatibility with non-Ascend devices.
For this setting to work, both the dialing side and the answering side of the link

must support PPP.

MP

MP supports multi-channel links, but not dynamic bandwidth allocation (DBA). The base-channel count is used to determine the number of calls to place, and the number of channels used for that connection does not change. In addition, MP requires that all channels in the connection share the same phone number (that is, the channels on the answering side of the connection must be in a hunt group).

MPP

Specifies MP+ (Multilink Protocol Plus), which extends the capabilities of MP (Multilink PPP) to support inverse multiplexing, session management, and bandwidth management. MP is an extension of PPP that supports the ordering of data packets across multiple channels.

MP+ consists of two components: a low-level channel identification, error monitoring, and error recovery mechanism, and a session management level for supporting bandwidth modifications and diagnostics. MP+ enables the Pipeline to perform Dynamic Bandwidth Allocation (DBA)—that is, MP+ enables the Pipeline to add or remove channels without disconnecting a link as the need for bandwidth increases or decreases.

Both the dialing side and the answering side of the link must support MP+. If only one side supports MP+, the connection then tries to use MP. If that fails, the connection uses standard single-channel PPP. Note that neither MP nor PPP support DBA.

MPP drops the most recently connected channel first.

Note: MP+ calls cannot combine an ISDN BRI channel with a channel on a T1 access line or a T1 PRI line.

FR

FR stands for Frame Relay.

Frame Relay is an HDLC-based packet protocol that enables you to send data to a destination using one or more frame relay switches within a private network or a public carrier’s network. HDLC stands for High Level Data Link Control.

From the viewpoint of the Pipeline, a frame relay switch is an endpoint for all DLCIs (Data Link Connection Indicators) connecting to it. A DLCI identifies a Connection profile as a logical link. The frame relay switch connects the endpoints of the DLCIs to each other to make a virtual permanent circuit to which users can connect. The circuit acts like a wire between two endpoints with a fixed maximum bandwidth.

If you set Encaps=FR, the Connection profile provides a bridge or route across the WAN over frame relay circuits. You must configure the FR Prof parameter in the Encaps submenu to send this connection to the frame relay switch. The FR Prof name must exist in a Frame Relay profile before you can save the Connection profile.

Dependencies: Keep this additional information in mind:

- When you select an encapsulation method, the Encaps Options submenu displays a group of parameters relevant to your selection; you must set the appropriate Encaps Options parameters.
- The Encaps parameter does not apply (Encaps=N/A) when the Pipeline answers a call, or if the link consists of only nailed-up channels (Call Type=Nailed).
- If Call Type=Nailed/MPP then Encaps must be set to MPP. In this case, or whenever Encaps=MPP, the Pipeline adds or subtracts switched channels on the connection as required by the DBA parameters on either side of the connection.

  DBA, or Dynamic Bandwidth Allocation, enables the Pipeline to use average line utilization (ALU) of transmitted data as the basis for adding or subtracting bandwidth from a switched connection without terminating the link. MP+ and AIM support Dynamic Bandwidth Allocation. Each side makes its calculations based on the traffic received at that side. If the two sides of the connection disagree on the number of channels needed, the side requesting the greater number prevails.
- If Encaps=MPP and Call Type=Nailed/MPP, the minimum number of channels in the link is the number set by Min Ch Count or the number of nailed-up channels in the group, whichever is greater.
- If Encaps=MPP and Call Type=Nailed/MPP, the maximum number of channels in the link is the number set by Max Ch Count or the number of nailed-up channels in the group, whichever is greater.

  The Pipeline does not count a nailed-up channel that is not online.

Location: Ethernet > Connections > *any profile*

Encoding

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

Encoding refers to the way in which data is represented by the digital signals on the line. Both sender and receiver must agree on the type on encoding in use in order to accurately interpret the value of a signal.

Usage: Press Enter to cycle through the choices.

- AMI specifies that the Pipeline uses Alternate Mark Inversion encoding. AMI is the default.
- B8ZS specifies that the encoding is Bipolar with 8-Zero Substitution. B8ZS is often required for ISDN lines.

Location: Nailed T1 > Mod Config

See Also: Framing Mode

Enet Adrs

Description: In a Bridging profile, specifies the physical Ethernet address (MAC address) of a device at the remote end of the link.

The Pipeline uses the Bridging profile to build a bridge table with corresponding MAC and IP addresses. The Enet Adrs parameter specifies the MAC address of each remote device; the Net Adrs parameter specifies the IP address of each remote device.

These parameters enable the Pipeline to respond to local ARP (Address Resolution Protocol) requests on behalf of a device at the remote end of the link. Whenever the Pipeline receives an ARP request for a MAC address corresponding to a specified IP address, it checks to see whether the IP address matches one in its bridge table. If it does, the Pipeline returns the MAC address corresponding to the IP address.

Usage: Press Enter to open a text field. Then, type the physical address of the device on the remote network. An Ethernet address is a 12-digit hexadecimal number.

The default setting is 000000000000.

Press Enter to close the text field.

Example: `0180C2000000`

Location: Ethernet > Bridge Adrs > *any profile*

See Also: Net Adrs

Exp Callback

Description: Used with Callback security, puts the number of *any* far end that does not connect (for any reason) on a list that disallows calls to that destination for 90 seconds. This gives the far end an opportunity to complete a callback.

Usage: Set Expect Callback to Yes by doing the following:

1 Open Ethernet > Connections > *any profile* > Telco Options.

2 Set Exp Callback to Yes.

Dependencies: Expect Callback should only be set to Yes in dialout profiles.

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

FDL

Description: This specifies the FDL (Facilities Data Link) protocol that the Pipeline uses. FDL is a protocol used by the telephone company to monitor the quality and performance of T1 lines. It provides information at regular intervals to your carrier's maintenance devices.

You continue to accumulate D4 and ESF performance statistics in the FDL Stats windows, even if you do not choose an FDL protocol. Your carrier can tell you which FDL protocol to specify.

Usage: Specify one of the following values:

- None (the default) disables FDL signaling.
- AT&T specifies AT&T FDL signaling.
- ANSI specifies ANSI FDL signaling.
- Sprint specifies Sprint FDL signaling.

Dependencies: This parameter does not apply to D4-framed T1 lines.

Location: Nailed T1> Mod Config

See Also: Framing Mode

Field Service

Description: Grants or restricts privileges to perform Ascend-provided field service operations, such as uploading new system software.

Usage: Press Enter to toggle between Yes and No.

- Yes grants privileges.

  Yes is the default.
- No restricts privileges.

  Selecting No does not disable access to any Pipeline operations. Field service operations are special diagnostic routines not available through Pipeline menus.

Dependencies: The Field Service parameter does not apply (Field Service=N/A) if Operations=No.

Location: System > Security > *any profile*

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: Press Enter to open a text field. Then, type a number between 0 and 16. The number corresponds to a data filter you created in the Filters menu. When you set Filter to 0 (zero), the Pipeline forwards all packets.

Zero is the default.

Press Enter again to close the text field.

Dependencies: Do not confuse the Filter parameter with the Data Filter parameter or the Call Filter parameter.

- The Filter parameter filters data packets on the Pipeline's local LAN interface.
- The Data Filter parameter filters data packets on the Pipeline's WAN interface.

  The WAN interface is the port on the Pipeline that is connected to a WAN line.
- The Call Filter parameter determines which packets can initiate a call or reset the idle timer.

  By default, any packet destined for the WAN causes the Pipeline to place a call. In addition, by default, every packet resets the idle timer, the indicator that the Pipeline uses to know when to clear a call. The Call Filter parameter limits the packets that can cause these events.

  The Pipeline applies the call filter specified by Call Filter only after applying the data filter specified by Filter or Data Filter. Only those packets that a data filter forwards reach a call filter.

Location: Ethernet > Mod Config > Ether Options

See Also: Forward, More

Filter Persistence

Description: Specifies whether the filter or firewall assigned to a Connection profile should persist after the call has been disconnected.

Usage: Press Enter to cycle through the choices:

- Yes specifies that the filter or firewall assigned to this Connection profile will persist after the connection has been torn down.

  Note: Typically a firewall will persist for about an hour after its associated connection has been torn down.

- No specifies that the filter or firewall assigned to this Connection profile will not persist after the connection has been torn down.

  No is the default.

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

See Also: Call Filter, Data Filter, Name, Version, Length (Filter)

Force56

Description: Specifies whether the Pipeline 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 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: Press Enter to toggle between Yes and No.

- Yes specifies that the Pipeline uses only 56 kbps.
- No specifies that the Pipeline can use 64 kbps, if available.

  No is the default.

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

Forward

Description: In a data filter or a call filter, specifies whether the Pipeline forwards or discards packets that match the filter. When you use Forward in a call filter, any forwarded data packet resets the idle timer and can initiate a call.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that the Pipeline forwards all packets matching the filter.

  If you have not specified any filters, Yes is the default.

- No specifies that the Pipeline does not forward packets matching the filter.

  If you have specified one or more filters, No is the default.

Example: If Forward=No in several filters, you must specify Forward=Yes in the last filter to allow data to pass. Consider this example:

```
In filter 01...Valid=Yes
In filter 01...Type=Generic
In filter 01...Generic...Forward=No
...
In filter 02...Valid=Yes
In filter 02...Type=Generic
In filter 02...Generic...Forward=No
...
In filter 03...Valid=Yes
In filter 03...Type=Generic
In filter 03...Generic...Forward=Yes
```

Location: Ethernet > Filters > Call or Data filter > *input or output filter* > *any numbered filter* > Generic

See Also: Call Filter, Data Filter.

Forward Disconnect

Description: Specifies if an off-hook click should be initiated when the far end hangs up, which helps tear down a call when the Pipeline is behind a PBX.

Usage: The available values are Yes or No. Select the parameter, and press enter to cycle through the available choices. No is the default.

Example: Forward Disconnect = No

Location: Configure menu

FR address

Description: The IP address which enables NAT for frame relay connections. Connections using Frame Relay encapsulation can translate local addresses into

the single, official address set by this parameter for networking over the wide area network and accessing the Internet.

Usage: Press Enter to open a text field and then type the official IP address.

The address consists of four numbers between 0 and 255, separated by periods. You must enter a valid IP address for the feature to work.

Dependencies: Keep this additional information in mind:

- In your connection profile, you must set Encaps=FR.
- The Routing parameter in the NAT menu must be set to Yes.

Location: Ethernet > NAT > NAT

See Also: Encaps, Routing, Profile, and Def Server.

FR Prof

Description: Specifies the name of the Frame Relay profile whose parameters the Pipeline should use in building the connection.

Usage: Press Enter to open a text field. Then, type the profile name. You can enter up to 15 alphanumeric characters. The default is null. Make sure that you enter the name exactly as it appears in the Name parameter of the Frame Relay profile. Press Enter again to close the text field.

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

See Also: Name

FR Type

Description: The type of interface between the Pipeline and a frame relay switch on the frame relay network.

Note: For DTE connections, the Pipeline 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 Pipeline dials the Connection profile specified in the Backup parameter in the Session Options submenu.

Usage: Specify one of the following values:

- DCE (data communications equipment)

  In a DCE connection, the Pipeline 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.

- DTE (data terminal equipment)

  In a DTE connection, the Pipeline is configured as a 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=DTE

Location: Ethernet > Frame Relay > *profile*

See Also: Link Mgmt, LinkUp, DCE N392, DCE N393, DTE N392, DTE N393

Framing Mode

Description: Specifies the framing mode that the physical layer uses. Your carrier can tell you which framing mode to choose.

Usage: Press Enter to cycle through the choices.

- D4 specifies the D4 format, also known as the Superframe format.

  This format consists of 12 consecutive frames, separated by framing bits. Do not use this setting with ISDN D-channel signaling; false framing and Yellow Alarm emulation can result.

- ESF specifies the Extended Superframe Format.

  This format consists of 24 consecutive frames, separated by framing bits. The ISDN specification advises that you use ESF with ISDN D-channel signaling.

Location: Nailed T1 > Mod Config

See Also: Encoding

FT1 Caller

Description: Specifies whether the Pipeline initiates a dial-up to add channels to an existing nailed-up or serial WAN connection. Whenever you have a mixture of nailed-up and switched channels in a connection, you need the FT1 Caller parameter. On purely switched calls, when the Pipeline needs to send packets across the WAN to a destination which is not online, it dials to bring up the connection to that destination. If additional channels are needed, the original caller dials, never the original answering side.

However, if the connection is already online over nailed-up channels, which end should dial to add switched channels? The only way to determine who calls (and therefore who is billed for the call) is by using this parameter.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that the Pipeline initiates the call.

  If you choose this setting, the Pipeline dials to bring online any switched circuits that are part of the call.

- No specifies that the Pipeline waits for the remote end to initiate the call.

  No is the default.

Dependencies: Keep this additional information in mind:

- If the remote end has FT1 Caller=No, set FT1 Caller=Yes on the local Pipeline; by the same token, if the remote end has FT1 Caller=Yes, set FT1 Caller=No on the local Pipeline.
- The FT1 Caller parameter applies only when Call Type=Nailed/MPP.

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

See Also: Call Type

Gateway

Description: Specifies the IP address of the router that a packet must go through to reach the destination station of the route.

Usage: Press Enter to open a text field. Then, type the IP address of the router.

An IP address consists of four numbers between 0 and 255, separated by periods. The default value is 0.0.0.0.

You must configure the network address of the destination station with the LAN Adrs parameter in the Connection profile; otherwise, the Pipeline assumes that the router is on the same Ethernet interface.

Press Enter to close the text field.

Example: `200.207.23.1`

Dependencies: Keep this additional information in mind:

- If you do not know the right IP address to enter, you must obtain it from the network administrator.

  Do not attempt to configure an IP address by guesswork!
- The Gateway parameter does not apply (Gateway=N/A) if the Pipeline does not support IP (Route IP=No).

Location: Ethernet > Static Rtes > *any profile*

See Also: Encaps, LAN Adrs, Route IP

Group 1 Count

Description: If the Pipeline is configured to be a DHCP server, this parameter determines the number of contiguous IP addresses in the first address pool.

Usage: Press Enter to open a text field and enter number between 0 and 20.

Enter 0 if the IP Group 1 parameter is `0.0.0.0/0` (which disables address assignment from the pool) or if the IP Group 1 parameter specifies a DHCP spoof address. Press Enter to close the text field.

The default is 1.

Dependencies: If the DHCP Spoofing and Always Spoof parameters are not both Yes, this parameter is N/A. The IP Group 1 parameter specifies the first address in the pool. All the addresses in the pool must be on the same subnet, and the subnet must be on the local network. If you are specifying a pool, the value cannot be 0.

Location: Ethernet > Mod Config > DHCP Spoofing

See Also: DHCP Spoofing, Always Spoof, IP Group 1

Group 2 Count

Description: If the Pipeline is configured to be a DHCP server, this parameter determines the number of contiguous IP addresses in the second address pool.

Usage: Press Enter to open a text field and then type a number between 0 and 20.

- If the value is 0, the pool is unavailable.
- The default is 0.

Press Enter to close the text field.

Dependencies: If the DHCP Spoofing and Always Spoof parameters are not both Yes, this parameter is N/A. The IP Group 2 parameter specifies the first address in the pool. All the addresses in the pool must be on the same subnet, and the subnet must be on the local network.

Location: Ethernet > Mod Config > DHCP Spoofing

See Also: DHCP Spoofing, Always Spoof, IP Group 1

Group (Connection)

Description: Points to the nailed-up channels used by the WAN link.

When the Group parameter of a Connection profile and the Nailed Group parameter of a Nailed T1 profile have the same value, the Connection profile uses the T1 line.

Usage: Press Enter to open a text field. Enter a number between 1 and 3.

Example: If Call Type=Nailed/MPP in a Connection profile, the setting Group=3 assigns one nailed-up group to the profile.

Dependencies: Keep this additional information in mind:

- The Group parameter does not apply (Group=N/A) if the link consists entirely of switched channels (Call Type=Switched).
- If you add channels to the Group parameter and save your changes, the Pipeline adds the additional channels to any online connection that uses the group.
- Do not assign more than one active Connection profile to a group.
- Do not assign a Connection profile to a group that a Frame Relay profile uses.
- If you are using an ISDN BRI line the Pipeline assigns the B channels to the following groups:

  1 represents the B1 channel

  2 represents the B2 channel
- If you are using a T1 line, the Nailed T1 Group parameter is set to Group 3. Currently, this is the only value supported.

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

See Also: Call Type, Nailed Grp

Group (Serial WAN)

Description: Assigns a group number to the serial WAN nailed channels. When the Group parameter of a Connection profile or the Nailed Grp parameter of a Frame Relay profile have the same value as the Group parameter in the Serial WAN profile, the Connection or Frame Relay profile uses the serial WAN port.

Usage: Press Enter to open a text field. Enter a number between 1 and 60. The default is 3.

Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- If you add channels to the Group parameter and save your changes, the Pipeline adds the additional channels to any online connection that uses the group.
- Do not assign more than one active Connection profile to a group.

- Do not assign a Connection profile to a group that a Frame Relay profile uses.

Location: V.35 > Serial WAN > Mod Config

See Also: Group (Connection), Nailed Grp

Handle IPX

Description: Enables you to configure a connection that bridges IPX.

Usage: Press Enter to cycle through the choices.

- None specifies that special IPX behavior does not take place.

  Choose this setting when the LAN on each side of the bridge has one or more IPX servers.

  None is the default.

- Client specifies that the Pipeline discards RIP (Routing Information Protocol) and SAP (Service Advertising Protocol) periodic broadcasts at its WAN interface, but forwards RIP and SAP queries.

  The WAN interface is the port on the Pipeline that is connected to a WAN line. RIP and SAP queries enable a client workstation to locate a NetWare server across the network. Choose this setting when both these conditions are true:

  – The local LAN has IPX clients but no servers.

  – The Pipeline is acting as a bridge to another LAN containing only IPX servers or a combination of IPX servers and clients.

- Server specifies that the Pipeline discards all RIP (Routing Information Protocol) and SAP (Service Advertising Protocol) periodic broadcasts and queries at its WAN interface.

  Server mode allows the Pipeline to bring down calls during idle periods without breaking client-server or peer-to-peer connections.

  Ordinarily, when a NetWare server does not receive a reply to the watchdog session *keepalive* packets it sends to a client, it closes the connection. When you select Server mode, however, the Pipeline replies to NCP watchdog requests on behalf of clients on the other side of the bridge; in other words, the Pipeline tricks the server watchdog process into believing that the link is still active. This process is called watchdog spoofing.

Choose this setting when both these conditions are true:

– The Pipeline is acting as a bridge to a remote LAN with IPX clients, but no servers.

– The local LAN contains only IPX servers, or a combination of IPX clients and servers.

Dependencies: Keep this additional information in mind:

- If you select the Server setting, you must also specify a value for the NetWare t/o parameter, indicating the maximum length of idle time during which the Pipeline performs watchdog spoofing for NetWare connections.
- If the connection does not bridge (Bridge=No), the Handle IPX parameter does not apply (Handle IPX= N/A).
- If the encapsulation for the connection is Frame Relay (Encaps=FR), the Handle IPX parameter does not apply (Handle IPX= N/A).
- If you have not specified an IPX frame type (IPX Frame=None), the Handle IPX parameter does not apply (Handle IPX=N/A).
- We highly recommend that you set Dial Brdcast=Yes when Handle IPX=Client, and Dial Brdcast=No when Handle IPX=Server.

  When a client on the local Ethernet interface sends out broadcast packets to locate a server, and the Pipeline must bridge these packets to another network, the Pipeline starts up a session for each Connection profile in which Dial Brdcast=Yes. The server need not broadcast and then dial, so set Dial Brdcast=No to keep broadcast packets from causing the Pipeline to dial automatically.
- If the Pipeline on one LAN sets Handle IPX=Server and the LAN on the other side of the connection has only NetWare clients, the Pipeline on the client-only LAN should set Handle IPX=Client.

  If both LANs contain servers, both sides of the connection should set Handle IPX=None.
- Although Handle IPX=N/A if Bridge=No or IPX Frame=None, the Pipeline automatically performs watchdog spoofing just as though you had set Handle IPX=Server; however, the Pipeline does not filter as though you had set Handle IPX=Server.

Location: Ethernet > Connections > *any profile* > IPX Options

See Also: Dial Brdcast, NetWare t/o

Handle IPX Type20

Description: Enables or prevents IPX Type 20 packet propagation.

Usage: Cycle through the choices:

- Select Yes to allow IPX Type 20 packet propagation.
- Select No to prevent IPX Type 20 packet propagation.

Dependencies: You must have IPX routing and IPX SAP Filter enabled.

Location: Configure > Ethernet > Mod Config > Ether Options > IPX SAP Filter

Hop Count

Description: Specifies the distance to the destination IPX network in hops. From the Pipeline, 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: Press Enter to open a text field. Then, type a valid hop count from 1 to 15. A hop count of 16 is considered unreachable and is not valid for static routes. Press Enter again to close the text field.

Dependencies: For the Hop Count parameter to apply, you must enable IPX routing in the Connection profile by setting Route IPX=Yes.

Location: Ethernet > IPX Route > *any profile*

See Also: Route IPX

Host n IP

Description: If the Pipeline is configured to be a DHCP server, this parameter reserves an IP address for the host whose MAC (Ethernet) address is specified by the respective Host *n* Enet parameter. When the host sends a DHCP message requesting an IP address, the Pipeline always assigns this address.

Usage: Press Enter to open a text field and then type the IP address and subnet mask for the host.

The address consists of four numbers between 0 and 255, separated by periods. Separate the subnet mask from the address with a slash. To assign an address, the IP address must be a valid IP address on the local Ethernet network. To disable address assignment, enter `0.0.0.0/0`.

The default value is `0.0.0.0/0`.

Press Enter to close the text field.

Example: `10.2.1.41/24`

Dependencies: If the DHCP Spoofing and Always Spoof parameters are not both Yes, this parameter is N/A. If you enter a value other than `0.0.0.0/0` for this parameter, you must enter a valid MAC address for the respective Host n Enet parameter. If you disable address assignment by entering `0.0.0.0/0` for this parameter, you must set the respective Host *n* Enet parameter to `000000000000`.

Location: Ethernet > Mod Config > DHCP Spoofing

See Also: DHCP Spoofing, Always Spoof

Host n Enet

Description: If the Pipeline is configured to be a DHCP server, this parameter specifies a host on the local network for which an IP address is reserved. The reserved address is specified by the respective Host *n* IP parameter. When the host sends a DHCP message requesting an IP address, it always receives this address.

Usage: Press Enter to open a text field.

To specify a host to be assigned an IP address, type the MAC address of the host's Ethernet interface. To disable address assignment, enter `000000000000`.

The default value is `000000000000`.

Press Enter to close the text field.

Example: `00d07b5e16e3`

Dependencies: If the DHCP Spoofing and Always Spoof parameters are not both Yes, this parameter is N/A. If you enter a value other than `000000000000` for this parameter, you must enter a valid IP address for the respective Host *n* IP parameter. If you disable address assignment by entering `000000000000` for this parameter, you must set the respective Host *n* IP parameter to `0.0.0.0/0`.

Location: Ethernet > Mod Config > DHCP Spoofing

See Also: DHCP Spoofing, Always Spoof

ICMP Redirects

Description: Specifies whether the Pipeline accepts or ignores Internet ICMP Redirect messages.

Usage: Press Enter to cycle through the choices.

- Accept specifies that the Pipeline processes incoming ICMP Redirect messages.

  Accept is the default.
- Ignore specifies that the Pipeline drops all incoming ICMP Redirect messages.

Dependencies: Set ICMP Redirects=Ignore whenever the Pipeline maintains a routing table, because counterfeit ICMP Redirects pose a potential security threat. You should accept ICMP Redirects only when the Pipeline has a single default route to another device.

Location: Ethernet > Mod Config

Id Auth

Description: Specifies whether the Pipeline uses the calling party's phone number to authenticate incoming calls. ID is the calling party's Caller ID (CLID).

Usage: Press Enter to cycle through the choices.

- Ignore indicates that calling party information is not required for authentication.

- Prefer specifies that whenever CLID is available, the calling party's phone number must match the Calling # parameter before the Pipeline answers the call.

  If CLID is not available or if the Pipeline cannot find a match to a calling number, the Pipeline applies authentication using the Recv Auth or Password Reqd parameters.

- Required indicates that the calling party's phone number must match the value of the Calling # parameter before the Pipeline can answer the call.

  If CLID is not available, the Pipeline does not answer the call

Dependencies: Keep this additional information in mind:

- In some installations, the WAN provider might not be able deliver CLIDs, or individual callers might choose to keep their CLIDs private; in addition, CLID is not available without end-to-end ISDN service on the call and ANI (Automatic Number Identification) from your WAN provider.

  Ask your WAN provider whether the calling party number is conveyed by the network to the receiving party. In some cases, the network does not deliver the calling party number, such as when the Pipeline is behind some PBXs.

- You cannot use a Connection profile in which AnsOrig=Call Only to authenticate incoming calls.

- If a call is CLID Authenticated (using the Id Auth parameter), name-password authentication might also be required, but the parameters of the call are established only by the CLID authentication.

Location: Ethernet > Answer > *any profile*

See Also: AnsOrig, Calling #, Id Auth

ID Fail Busy

Description: Indicates the Disconnect cause when Called ID authentication fails due to a timeout.

- No sets the Disconnect cause code to 'Normal call clearing' and is the default.

- Yes sets the Disconnect cause code to 'User Busy'.

Usage: Select the parameter and press Enter to cycle through the available settings. Press Esc to exit the parameter.

Dependencies: CLID authentication must be enabled in order to set this parameter. Set it in Ethernet > Answer > Id Auth.

Location: Ethernet > Mod Config > Auth.

See Also: Id Auth

Idle

Description: Specifies the number of seconds the Pipeline waits before clearing a call when a session is inactive.

Usage: Press Enter to open a text field; then, type a number between 0 and 65535. If you specify 0 (zero), Pipeline does not enforce a limit; an idle connection stays open indefinitely.

The default setting is 120 seconds.

Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- In an Answer profile or Connection profile, Idle does not apply to nailed-up links; that is, Idle=N/A when Call Type=Nailed.
- If MP+ encapsulation is in use and the bandwidth utilization *on both sides of the connection* drops below the value entered in the Idle Pct field, the Pipeline clears the call, regardless of the value you enter for the Idle parameter.
- Idle in the Answer profile applies to incoming calls for which no Connection profile exists; if a Connection profile exists, the setting of its Idle parameter takes precedence.
- If Profile Reqd=Yes in the Answer profile, Idle does not apply (Idle=N/A) in the Answer profile.
- Because the Idle Pct is parameter is dependent on traffic levels on both sides of the connection, we recommend that you use the Idle parameter in preference to it.

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

See Also: Call Type, Profile Reqd

Idle Logout

Description: Specifies the number of minutes the Control Monitor or Telnet session can remain inactive before the Pipeline logs out and hangs up.

Usage: Press Enter to open a text field. Then, type a number between 0 and 60. The default setting is 0; this setting disables automatic logout. Press Enter again to close the text field.

Location: System > Sys Config

Idle Pct

Description: Specifies a percentage of bandwidth utilization below which the Pipeline clears a single-channel MP+ call. Bandwidth utilization must fall below this percentage on *both sides* of the connection before the Pipeline clears the call.

Usage: Press Enter to open a text field. Then, type a number between 0 and 99. The default value is 0; this setting causes the Pipeline to ignore bandwidth utilization when determining whether to clear a call. Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- MP+ must be the selected encapsulation method (Encaps=MPP) in a Connection profile.
- If the device at the remote end of the link enters an Idle Pct setting lower than the value you specify, the Pipeline does not clear the call until bandwidth utilization falls below the lower percentage.
- If either end of a connection sets the Idle Pct parameter to 0 (zero), the Pipeline ignores bandwidth utilization when determining when to clear a call.
- If the time set by the Idle parameter expires, the call disconnects whether or not bandwidth utilization falls below the Idle Pct setting.

- When bandwidth utilization falls below the Idle Pct setting, the call disconnects regardless of whether the time specified by the Idle parameter has expired.
- Because the Idle Pct parameter is dependent on traffic levels on both sides of the connection, we recommend that you use the Idle parameter in preference to it.
- Idle Pct in the Answer profile applies to incoming calls for which no Connection profile exists; if a Connection profile exists, the setting of its Idle Pct parameter takes precedence.
- If Profile Reqd=Yes in the Answer profile, Idle Pct does not apply (Idle=N/A) in the Answer profile.

Location: Ethernet > Answer > *any profile* > PPP Options; Ethernet > Connections > *any profile* > Encaps Options

See Also: Call Filter, Encaps, Idle

IF Adrs

Description: Specifies the IP address of the interface at the near end of a link.

Usage: Press Enter to open a text field. Then, type the IP address of the numbered interface.

An IP address consists of four numbers between 0 and 255, separated by periods. If a netmask is in use on the network, you must specify it. Separate the netmask from the IP address with a slash. The default is 0.0.0.0/0.

Press Enter again to close the text field.

Example: 200.207.23.7/24

Dependencies: The IF Adrs parameter does not apply if the Pipeline does not support IP (Route IP=No).

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

See Also: WAN Alias, Route IP

Ignore Def Rt

Description: Specifies whether the Pipeline ignores RIP (Routing Information Protocol) updates to the default route (0.0.0.0/0) in its IP routing table.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that the Pipeline ignores updates to the default route.
- No specifies the Pipeline allows updates to the default route.
  No is the default.

Location: Ethernet > Mod Config > Ether Options

IP Adrs

Description: Specifies the IP address of the Pipeline on the local Ethernet network, and its subnet.

Usage: Press Enter to open a text field. Then, type the IP address of the Pipeline on the local Ethernet network.

The address consists of four numbers between 0 and 255, separated by periods. Separate the optional netmask from the address with a slash. The IP address must be a valid IP address on the local Ethernet network.

The default value is 0.0.0.0/0.

Press Enter to close the text field.

Example: `10.2.1.1/24`

In this example, 10.2.1.1 is the Pipeline's IP address. The number 24 represents the number of bits in the Pipeline's netmask. Masking 24 bits in the Pipeline's address provides a subnet of 10.2.1.0.

Dependencies: Keep this additional information in mind:

- The value of the IP Adrs parameter on the local Pipeline must match the LAN Adrs parameter of the unit at the remote end of the link.
- The IP Adrs parameter does not apply (IP Adrs=N/A) if the Pipeline does not support IP (Route IP=No).

- If you do not know the right IP address to enter, you must obtain it from the network administrator.

  Do not attempt to configure an IP address by guesswork!

- The IP Adrs parameter is the same as the My Addr parameter in the Configure menu.

Location: Ethernet > Mod Config > Ether Options

See Also: Encaps, Route IP

IP Group 1

Description: The meaning of this parameter depends on whether the Pipeline is configured to be a DHCP server (when both DHCP Spoofing and Always Spoof are Yes) or is configured to perform DHCP spoofing (when DHCP Spoofing is Yes and Always Spoof is No):

- If the Pipeline is configured to be a DHCP server, this is the address and subnet mask for the first IP address in a pool of addresses used for dynamic address assignment.
- If the Pipeline performs DHCP spoofing, this parameter specifies a spoof address: a temporary address that is provided to the host while the actual IP address is obtained from a DHCP server on the remote network.

Usage: Press Enter to open a text field and enter the IP address and subnet mask.

The address consists of four numbers between 0 and 255, separated by periods. Separate the subnet mask from the address with a slash. To specify the first address in the pool, the IP address must be a valid IP address on the local Ethernet network. To disable address assignment from this pool, enter `0.0.0.0/0`.

The default value is `192.0.2.1/24`.

Press Enter to close the text field.

Example: `10.2.1.1/24`

In this example, `10.2.1.1` is the IP address. The number 24 represents the number of bits in the subnet mask. Masking 24 bits provides a subnet of `10.2.1.0`.

Dependencies: If DHCP Spoofing is No, this parameter is N/A. The Group 1 Count parameter specifies the number of addresses in the pool. All the addresses in the pool must be on the same subnet, and the subnet must be on the local network. If this parameter is `0.0.0.0/0`, which disables address assignment from this pool, the Group 1 Count parameter must be 0.

Location: Ethernet > Mod Config > DHCP Spoofing

See Also: DHCP Spoofing, Always Spoof, Group 1 Count, IP Group 2

IP Group 2

Description: If the Pipeline is configured to be a DHCP server, this is the address and subnet mask for the first IP address in the second pool of addresses used for dynamic address assignment. A second pool is optional; you need it only if you need to assign more than 20 IP addresses or if you need up to 20 but not enough contiguous addresses are available. Addresses in the second pool are used only if there are no addresses available in the first pool.

Usage: Press Enter to open a text field and then type the IP address and subnet mask.

The address consists of four numbers between 0 and 255, separated by periods. Separate the subnet mask from the address with a slash. To specify the first address in the pool, the IP address must be a valid IP address on the local Ethernet network. To disable address assignment from this pool, enter `0.0.0.0/0`.

The default value is `0.0.0.0/0`.

Press Enter to close the text field.

Example: `10.2.1.21/24`

In this example, `10.2.1.21` is the IP address. The number 24 represents the number of bits in the subnet mask. Masking 24 bits provides a subnet of `10.2.1.0`.

Dependencies: If DHCP Spoofing is No, this parameter is N/A. The Group 2 Count parameter specifies the number of addresses in the pool. All the addresses in the pool must be on the same subnet, and the subnet must be on the local network. If this parameter is `0.0.0.0/0`, which disables address assignment from this pool, the Group 2 Count parameter must be 0.

Location: Ethernet > Mod Config > DHCP Spoofing

See Also: DHCP Spoofing, Always Spoof, IP Group 1, Group 2 Count

Location:

IPX Alias

Description: Specifies the network number assigned to a point-to-point link.

Generally, you need to enter a value in this parameter only if the Pipeline operates with a non-Ascend router that uses a numbered interface. It does not apply if you are routing from one Pipeline to another, or to a router that does not use a numbered interface.

Usage: Press Enter to open a text field. Then, enter an appropriate network number. The default value is 00000000. FFFFFFFF is invalid. Press Enter again to close the text field.

Dependencies: For the IPX Alias parameter to apply, you must enable IPX routing in the Connection profile by setting Route IPX=Yes.

Location: Ethernet > Connections > *any profile*

See Also: Route IPX

IPX Enet#

Description: Specifies a unique IPX network number for the Ethernet interface.

The Pipeline assigns an address to a workstation when it connects to the Pipeline; it derives the address from the network number.

Usage: Press Enter to open a text field. Then, type an IPX network number using an 8-digit (4-byte) hexadecimal value. The default is 00000000. The

number you specify must be unique within your wide-area IPX network, and must match the configuration of other routers on the local Ethernet network.

When you accept the default setting of 00000000, the Pipeline learns its IPX network number from other routers on the Ethernet network. If you enter a value other than zero, the Pipeline becomes the “seeding” router and sets its IPX network number for the other routers on the Ethernet network

Example: `DE040600`

Dependencies: The IPX Enet# parameter does not apply (IPX Enet#=N/A) if the Pipeline is not set up for IPX routing (Route IPX=No).

Location: Ethernet > Mod Config > Ether Options

IPX Frame

Description: Specifies the Ethernet frame type to use for IPX on the Ethernet interface. If you do not specify an Ethernet frame type, the Pipeline cannot route IPX or perform watchdog spoofing for its IPX clients.

IPX packets can appear in more than one Ethernet frame type on an Ethernet segment. If your Pipeline routes IPX, it can recognize only a single IPX frame type. The Pipeline does not route other IPX frame types, and may attempt to bridge them. In addition, the Pipeline can only route and perform watchdog spoofing for the IPX frame type specified by IPX Frame.

Usage: Press Enter to cycle through the choices.

- 802.3 specifies the 802.3 frame type.

  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.

  For NetWare 3.11 or earlier, select 802.3.

- 802.2 specifies the 802.2 frame type.

  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.

For NetWare 3.12 or later, select 802.2.

802.2 is the default.

- SNAP specifies the SNAP frame type.

  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 specifies the Ethernet II frame type.

  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 routing and other IPX-specific features.

  If you choose this setting, the Pipeline can bridge IPX, but without watchdog spoofing or the automatic RIP (Routing Information Protocol) and SAP (Service Advertising Protocol) data filters described in Handle IPX.

Dependencies: To determine the IPX frame type in use, enter the Config command on a NetWare server, or look at the NET.CFG file on an IPX client. Choose a setting based on this information:

- Select 802.3 if Frame=Ethernet_802.3.
- Select 802.2 if Frame=Ethernet_802.2.
- Select SNAP if Frame=Ethernet_SNAP.
- Select Enet II if Frame=Ethernet_II.

Location: Ethernet > Mod Config > Ether Options

IPX Net#

Description: Lets you create a static route to another Ethernet network through the Connection profile.

The value of IPX Net# specifies the network number of the router at the remote end of the connection.

Usage: Press Enter to open a text field. Then, type an Ethernet network number using an 8-digit (4-byte) hexadecimal value. The default is 00000000.

Specify the network number of the router at the remote end of the connection only if the router requires that the Pipeline know its network number before connecting. You almost never need to set this parameter in a Connection profile.

If you accept the default of 00000000, the Connection profile is still valid, but the Pipeline does not advertise the route until it makes a connection to the Ethernet network.

Example: `DE040600`

Dependencies: The IPX Net# parameter does not apply (IPX Net#=N/A) if the Pipeline is not set up for IPX routing (Route IPX=No).

Location: Ethernet > Connections > *any profile*

See Also: Route IPX

IPX Pool#

Description: Specifies a unique IPX network number for all NetWare clients that are running PPP encapsulation and dialing in directly. The Pipeline assigns network addresses to dial-in NetWare clients when they connect to the Pipeline; these addresses are derived from this network number.

When you enter a value for IPX Pool#, the Pipeline advertises a route to this network.

Usage: Press Enter to open a text field. Then, type an Ethernet network number using an 8-digit (4-byte) hexadecimal value. The default is 00000000.

The number you specify must be unique within your wide area IPX network, and must match the configuration of other routers on the local Ethernet network.

Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- The dial-in Netware client must accept the network number set by IPX Pool#, although it can provide its own node number or accept a node number provided by the Pipeline.
- If IPX Frame=None or IPX Routing=No, IPX Pool#=N/A.

Example: `FF0000037`

Location: Ethernet > Mod Config > Ether Options

IPX RIP

Description: Controls how IPX RIP will be handled on this WAN link. When a Pipeline is used to connect NetWare clients to a very large IPX network, the IPX routing table created by the Pipeline may become very large and unmanageable, and can cause the Pipeline to run out of memory. As an alternative to maintaining these large routing tables locally, the Pipeline may have a static IPX route to the corporate network and disable IPX RIP. Either end of the WAN link may disable or fine-tune IPX RIP behavior.

Usage: Press Enter to cycle through the choices.

- Both indicates that the device will both send and receive RIP updates on this WAN link.

  Both is the default.
- Send means the device will send RIP updates but will not receive them.
- Recv means the device will receive RIP updates but will not send them.
- Off means the device will neither send nor receive IPX RIP updates on this WAN link.

Dependencies: This parameter is N/A if Peer=Dialin. If it is Off, a static IPX route is required to the remote network. A static route is defined in an IPX Routes profile.

Location: Ethernet > Connections > *any profile* > IPX Options

See Also: IPX SAP, Peer

IPX Routing

Description: Specifies whether the Pipeline can perform these functions:

- Establish IPX routing
- Forward IPX packets
- Generate RIP and SAP packets

- Interpret incoming RIP and SAP packets

Usage: Press Enter to toggle between Yes and No.

- Yes enables the Pipeline to perform IPX routing functions.
  Yes is the default.
- No disables the Pipeline from performing IPX routing functions.
  You may want to choose No if your network uses a protocol other than IPX, or if your IPX network maintains such large RIP and SAP tables that the Pipeline is spending too much time maintaining them.

Dependencies: Keep this additional information in mind:

- The setting of the IPX Routing parameter does not affect watchdog spoofing in IPX bridging.
- If you set IPX Routing=No while a WAN connection routing IPX exists, the Pipeline does not tear down the connection, but no further IPX traffic can take place on the connection.
- If IPX Routing=No, these parameters do not apply and are set to N/A:
  - Route IPX
  - Dial Query
  - IPX Enet#
  - IPX Alias

  You can still configure IPX routes using the Active, Connection #, Hop Count, Network, Node, Server Name, Server Type, Socket, and Tick Count parameters. However, the routes have no effect until IPX Routing=Yes.
- The show netware command on the terminal server still operates when IPX Routing=No.

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: Controls how IPX SAP will be handled on this WAN link. When a Pipeline is used to connect NetWare clients to a very large IPX network, the IPX service table created by the Pipeline may become very large and unmanageable, and can cause the Pipeline to run out of memory. As an alternative to maintaining these large service tables locally, the Pipeline may create static service table entries and turn off IPX SAP. Either end of the WAN link may disable or fine-tune IPX SAP behavior.

Usage: Press Enter to cycle through the choices.

- Both indicates that the device will both send and receive SAP updates on this WAN link.

  Both is the default.
- Send means the device will send SAP updates but will not receive them.
- Recv means the device will receive SAP updates but will not send them.
- Off means the device will neither send nor receive IPX SAP updates on this WAN link.

Dependencies: This parameter is N/A if Peer=Dialin. If this parameter is set to Off, a static IPX service table entry is required to the remote network. A static service entry is configured in an IPX Routes profile.

Location: Ethernet > Connections > *any profile* > IPX Options

See Also: IPX RIP, Peer

IPX SAP Filter

Description: Specifies the number of an IPX SAP Filter profile to be applied to a WAN session or to the Ethernet interface. Depending on how the IPX SAP Filter profile has been defined, this parameter has one or both of the following effects:

- IPX SAP Input filters apply to all SAP packets that the Ascend unit receives.

  Input filters screen advertised services and exclude them from its service table as specified in the filters.
- IPX SAP Output filters apply to SAP response packets that the Ascend unit transmits.

If the Ascend unit receives a SAP request packet, it applies Output filters before transmitting the SAP response, and excludes services from the response packet as specified in the filters.

Usage: Press Enter to open a text field.

- Type a number between 1 and 8. The number corresponds to an IPX SAP Filter profile in the IPX SAP Filters menu.
- Setting IPX SAP Filter to 0 (zero) includes all SAP data in the service table. Zero is the default.
- Press Enter to close the text field.

Dependencies: For the Pipeline to run in proxy mode, you must supply the remote IPX network number and configure a static IPX route to that network.

Location: Ethernet > Mod Config > Ether Options; Ethernet > Answer > *any profile* > Session Options; Ethernet > Connections > *any profile* > Session Options

See Also: IPX SAP Proxy Net#n, IPX Enet#, IPX Frame, IPX Routing, Server Name, Server Type, Type, Valid (Filter)

IPX SAP Proxy

Description: Enables or disables IPX SAP proxy mode in the Pipeline. When a Pipeline is used to connect NetWare clients to a very large IPX network, the SAP table created by the Pipeline can become very large and unmanageable. As an alternative, the Pipeline operating in proxy mode discards all SAP broadcasts seen on the network and resolves SAP queries from NetWare clients as it receives them, by forwarding the queries over the WAN link.

SAP proxy mode is recommended when only NetWare clients (not servers) are on the Ethernet side of Pipeline.

Note: If the Pipeline running in SAP proxy mode has NetWare servers on its Ethernet, it stores the relevant SAP entries for those servers and advertises them across the WAN interface as a normal SAP broadcast.

Usage: Press Enter to toggle between Yes and No.

- Yes enables proxy mode.

- No disables proxy mode.
  No is the default.

Dependencies: For the Pipeline to run in proxy mode, you must supply the remote IPX network number and configure a static IPX route to that network.

Location: Ethernet > Mod Config > Ether Options

See Also: IPX SAP Proxy Net#n

IPX SAP Proxy Net#*n*

Description: Specifies a default IPX SAP proxy server (from 1 to 3).

Usage: For each parameter, specify the IPX network number of the server providing the SAP proxy. The default value is 0 (zero).

The Pipeline first attempts to use the server specified by IPX SAP Proxy Net#1. If that server is unavailable, the Pipeline then attempts to use the server specified by IPX SAP Proxy Net#2. If that server is also unavailable, the Pipeline attempts to use the server specified by IPX SAP Proxy Net#3.

Dependencies: If IPX SAP Proxy=No, the IPX SAP Proxy Net#*n* parameter does not apply.

Location: Ethernet > Mod Config > Ether Options.

Lan

Description: Selects whether the Pipeline is running single-address or multiple-address NAT.

Note: The LAN parameter in the System profile has a different function from the Lan parameter in the NAT profile.

A Pipeline can perform single-address NAT in these ways:

- For more than one host on the local network without borrowing IP addresses from a DHCP server on the remote network.
- When the remote network initiates the connection to the Pipeline.

- By routing packets it receives from the remote network for up to 10 different TCP or UDP ports to specific hosts and ports on the local network.

Usage: Select either of the following:

- Single IP addr

  With single-address NAT, the only host on the local network that is visible to the remote network is the Pipeline.

  For outgoing calls, the Pipeline performs NAT on the local network after getting a single IP address from the remote network during PPP negotiation. The Pipeline does not limit the number of hosts on the local network that can make simultaneous connections to hosts on the remote network. The translations between the local network and the Internet or remote network are dynamic and not preconfigured.

  For incoming calls, the Pipeline can perform NAT for multiple hosts on the local network using its own IP address. The Pipeline routes incoming packets for up to 10 different TCP or UDP ports to specific servers on the local network. See the Static mappings...

- Multiple IP addr

  Multiple-address NAT translates addresses for more than one host on the local network. To do this, the Pipeline borrows an official IP address for each host from a Dynamic Host Configuration Protocol (DHCP) server on the remote network or accessible from the remote network.

  When multiple-address NAT is enabled, the Pipeline attempts to perform IP address translation on all packets received. (It cannot distinguish between official and private addresses.)

  The Pipeline acts as a DHCP client on behalf of all hosts on the LAN and relies on a DHCP server to provide addresses suitable for the remote network from its IP address pool. On the local network, the Pipeline and the hosts all have “local” addresses on the same network that are only used for local communication between the hosts and the Pipeline over the Ethernet.

  When the first host on the LAN requests access to the remote network, the Pipeline gets this address through PPP negotiation. When subsequent hosts request access to the remote network, the Pipeline asks for an IP address from the DHCP server using a DHCP request packet. The server then sends an address to the Pipeline from its IP address pool. The Pipeline uses the dynamic addresses it receives from the server to translate IP addresses on

behalf of local hosts. While waiting for an IP address to be offered by the server, corresponding source packets are dropped.

Similarly, for packets received from the WAN, the Pipeline checks the destination address against its table of translated addresses. If the destination address exists and is active, the Pipeline forwards the packet. If the destination address does not exit, or is not active, the packet is dropped.

In some installations, the DHCP server could be handling both NAT DHCP requests and ordinary DHCP requests. In this situation, if the ordinary DHCP clients are connecting to the server over a non-bridged connection, you must have a separate DHCP server to handle the ordinary DHCP requests; the NAT DHCP server will only handle NAT DHCP requests.

Dependencies: The Routing parameter must be set to Yes.

Location: Ethernet > NAT

See Also: Routing

LAN Adrs

Description: Specifies the IP address of a station or router at the remote end of the link specified by the Connection profile.

Usage: Press Enter to open a text field. Then, type the IP address of a remote station or router; you can also specify a netmask.

An IP address consists of four numbers between 0 and 255, separated by periods. If a netmask is in use on the network, you must specify it. Separate a netmask from the IP address with a slash.

The default setting is 0.0.0.0/0; an answering Connection profile with this setting matches all incoming IP addresses.

If you do not enter a netmask, the Pipeline assumes the default for your network class:

- Class A: 1.0.0.0 to 127.255.255.255 /8
- Class B: 128.0.0.0 to 191.255.255.255 /16
- Class C: 192.0.0.0 to 223.255.255.255 /24

The netmask should not mask any network bits. For example, 130.15.3.44/12 is not valid because it is a Class B address whose netmask cannot be smaller than 16.

If you enter a 32-bit mask, you are specifying a connection to a specific host, rather than to a group of hosts on a subnet.

After you make your specifications, press Enter to close the text field.

Example: `200.207.23.101/24`

Dependencies: Keep this additional information in mind:

- The LAN Adrs parameter in the first Connection profile is the same as the Rem Addr parameter in the Configure menu.
- The value of the LAN Adrs parameter on the local Pipeline must match the IP Adrs parameter of the Ascend unit at the remote end of the link.
- No two calling Connection Profiles should have the same LAN Adrs.
- Setting LAN Adrs to 0.0.0.0/0 and clearing the Station parameter resets all parameters in the Connection profile to their defaults.
- The LAN Adrs parameter does not apply (LAN Adrs=N/A) if the Pipeline does not support IP (Route IP=No).
- If you do not know the right IP address to enter, you must obtain it from the network administrator.

  Do not attempt to configure an IP address by guesswork!

Location: Ethernet > Connections > *any profile*

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

Length (Filter)

Description: Indicates the number of bytes in a packet that the Pipeline compares to the setting of the Value parameter.

The Offset parameter specifies the starting position; the Pipeline ignores the portion of the packet that exceeds the Length specification. In other words, the Offset parameter hides the left-most bytes of data, while the Length parameter hides the right-most bytes of data.

The Pipeline applies the value of the Mask parameter before comparing the bytes to the setting of the Value parameter. The Mask value consists of the same number of bytes as the Length parameter. A mask hides the part of a number that appears behind the binary zeroes in the mask; for example, if Mask=ffff0000 in hexadecimal format, the Pipeline uses only the first 16 binary digits in the comparison, since f=1111 in binary format.

Usage: Press Enter to open a text field. Then, type the number of bytes to use for comparison. You can enter a number between 0 and 8.

The default value is 0. When you accept the default, Pipeline uses no bytes for comparison; all packets match the filter.

Press Enter again to close the text field.

Example: Suppose you have a filter that drops packets and has these specifications:

```
Forward=No
Offset=4
Length=3
Mask=ffffff
Value=123
More=No
```

When the 10-byte packet xycd123456 passes through the filter, the Pipeline removes the leading four bytes, because Offset=4. The data 123456 remains. Next, the Pipeline removes the trailing three bytes, because Length=3; only the value 123 remains. The Mask is ffffff, which contains all ones (1s) when converted to binary numbers; therefore, the Mask value does not hide any binary digits and passes 123 through. When the Pipeline compares 123 to the setting of the Value parameter, a match occurs and the Pipeline does not forward the packet.

Dependencies: In a Filter profile, Length does not apply (Length=N/A) for an IP filter (Type=IP).

Location: Ethernet > Filters > *any type of filter* > *any input or output filter* > *any numbered filter* > Generic

See Also: Offset, Mask, Value

Length (Firewall)

Description: Specifies the length of the firewall uploaded to the Pipeline from Secure Access Manager (SAM).

Usage: This parameter cannot be edited.

Location: Ethernet > Firewalls > *any firewall*

Link Comp

Description: Turns data compression on or off for a PPP link.

Usage: Press Enter to cycle through the choices.

- Stac or Stac-9 turns on data compression.

  The Pipeline applies the Stacker LZS compression/decompression algorithm. Stac is the default.

- MS-Stac turns on Microsoft LZS Coherency Compression for Windows95, a proprietary compression scheme for Windows 95 only (not for Windows NT).

  Both sides of the link must set Link Comp to a value other than None, and the value must be the same on both sides of the connection.

- None turns off data compression.

Dependencies: Keep this additional information in mind:

- Stacker LZS Compression (as defined in the Internet Draft of November 1995) and Microsoft LZS Coherency Compression for Windows 95 both use the same PPP option to indicate that their compression scheme is in use.

  Therefore, a router can have difficulty determining exactly which compression method a caller is requesting. Ascend units handle this ambiguity in the call by always using the compression scheme specified in the Connection profile; if there is no Connection profile, the Ascend unit uses the compression scheme specified in the Answer profile.

  If the caller requests MS-Stac and the profile does not specify MS-Stac compression, the connection seems to come up correctly, but no data is routed. If the profile is configured with MS-Stac and the caller does not acknowledge that compression scheme, the Pipeline attempts to use standard

Stac compression. If it cannot use standard Stac compression, it uses no compression at all.

- The Link Comp parameter applies only if the link uses PPP encapsulation (Encaps=PPP or Encaps=MPP).

  When you choose Encaps=MPP, both the dialing side and the answering side of the link must support MP+. If only one side supports MP+, the connection uses MP or standard single-channel PPP. When you choose Encaps=PPP, the connection uses only PPP.

- Link Comp in the Answer profile applies to incoming calls for which no Connection profile exists; if a Connection profile exists, the setting of its Link Comp parameter takes precedence.

- If Profile Reqd=Yes in the Answer profile, Link Comp does not apply (Link Comp=N/A) in the Answer profile.

Location: Ethernet > Answer > *any profile* > PPP Options; Ethernet > Connections > *any profile* > Encaps Options

See Also: VJ Comp

Link Mgmt

Description: Specifies the link management protocol used between the Pipeline and the frame relay switch.

From the viewpoint of the Pipeline, a frame relay switch is an endpoint for all DLCIs (Data Link Connection Indicators) connecting to it. A DLCI identifies a Connection profile as a logical link; because more than one Connection profile can connect to a frame relay switch, a physical circuit can carry more than one logical link. The DLCI parameter enables the frame relay switch to identify each Connection profile.

The frame relay switch connects the endpoints of the DLCIs to each other to make a virtual permanent circuit to which users can connect. The circuit acts like a wire between two endpoints with a fixed maximum bandwidth.

Usage: Press Enter to cycle through the choices.

- None specifies no link management.

The Pipeline assumes that the physical link is up and that all logical links (as defined by the DLCI parameter) are active on the physical link.

None is the default.

- T1.617D specifies the link management protocol defined in ANSI T1.617 Annex D.

  Ask your service provider whether you should specify T1.617D.

- Q.933A the link management protocol defined Q.933 Annex A.

Location: Ethernet > Frame Relay > *any profile*

See Also: DLCI

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.

- Specify Yes or No. No is the default.
- Yes causes the Pipeline 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 > *any profile*

See Also: FR Prof, DLCI

List Attempt

Description: Enables or disables the DNS (Domain Name System) List Attempt feature.

DNS can return multiple addresses for a hostname in response to a DNS query. Unfortunately, DNS has no information about the availability of those hosts. Users typically attempt to access the first address in the list. If that host is unavailable, the connection fails and the user must initiate a new DNS query or Telnet attempt. If the login attempt occurs automatically as part of Immediate Telnet, the Pipeline tears down the physical connection when the initial connection attempt fails.

The DNS List Attempt feature helps the Pipeline avoid tearing down physical links by enabling the user to try one entry in the DNS list of hosts when logging in through Telnet from the terminal server; if that connection fails, the user can try each succeeding entry.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that the Pipeline enables a user to try the next host in the DNS list if the first Telnet login attempt fails.
- No turns off the List Attempt feature.
  No is the default.

Dependencies: The List Attempt parameter does not apply (List Attempt=N/A) if Telnet and Immediate Telnet are both disabled.

Location: Ethernet > Mod Config > DNS

List Size

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

Usage: Press Enter to open a text field, and then specify a number between 0 and 35. The default value is 6.

Dependencies: This parameter is N/A if the List Attempt feature is disabled.

Location: Ethernet > Mod Config > DNS

See Also: List Attempt

Loc Adrs

Description: When the Pipeline is configured to perform single-address network address translation (NAT) and to provide services for users outside the private local LAN, this parameter specifies the IP address of one of the servers on the local LAN. The Pipeline routes packets whose destination port match a setting for Dst Port # to the corresponding Loc Adrs and Loc Port # parameters in the Static Mappings menu.

Usage: Enter the IP address of the local server in dotted decimal format. The default value is 0.0.0.0.

The address consists of four numbers between 0 and 255, separated by periods. Enter 0.0.0.0 to disable routing of packets.

The default value is 0.0.0.0.

Press Enter again to close the text field, press Esc to exit the menu, and then confirm the change when prompted.

Note: After you enter a value for this parameter, it does not take effect until the next time the link specified by the Profile parameter is brought up. To make the change immediately, bring the link down and back up.

Dependencies: Keep this additional information in mind:

- For routing of incoming packets for a particular port to occur, the Routing parameter in the NAT menu must be set to Yes, the Lan parameter in the NAT menu must be set to Single IP Addr, the Valid parameter in the same Static Mapping nn menu must be set to Yes, and other parameters in the same Static Mapping nn menu must be set to non-null values:
  - Dst Port# and Loc Port# parameters must be set to values other than 0.
  - If you enter 0 as the value of this parameter, you receive the message Invalid Input: Zero input is not Valid.
- If the Routing parameter in the NAT menu is set to No or the Lan parameter in the NAT menu is set to Multi IP Addr, this parameter is N/A.

Location: Ethernet > NAT > Static Mapping > Static Mapping *nn* (where *nn* is a number between 01 and 10)

See Also: Def Server, Dst Port # (Filters), Loc Port#, Lan, Routing, Protocol (Filter), Valid (Static Mapping)

Loc.DNS Tab Auto Update

Description: Enables or disables automatic updating of the local DNS table. When automatic updating is enabled, the list of IP addresses for each entry is replaced with a list from the remote DNS server when the remote DNS successfully resolves a connection to a host named on the table.

Usage: Set Loc.DNS Tab Auto Update to Yes to enable automatic updating of the IP addresses in the local DNS table. No disables automatic updating.

Dependencies: The Enable Local DNS Table parameter must be set to Yes. To display the list of IP addresses for a DNS table entry, the List Attempt parameter must also be set to Yes, and a value of 1-35 specified for the List Size parameter. If you set List Attempt=No, the Dnstab Entry command displays only the first IP address on the list.

Location: Ethernet > Mod Config > DNS

See Also: Enable Local DNS Table

Loc Port#

Description: When the Pipeline is configured to perform single-address network address translation (NAT) and to provide services for users outside the private local LAN, this parameter specifies the TCP or UDP port of one of the services on the local LAN. The Pipeline routes packets whose destination port match a setting for Dst Port # to the corresponding Loc Adrs and Loc Port # parameters in the Static Mappings menu.

Usage: Press Enter to open a text field and then type the port number.

Enter a port number between 1 and 65535, or enter 0 to disable routing of packets. 0 is the default.

Press Enter again to close the text field, press Esc to exit the menu, and then confirm the change when prompted.

Note: After you enter a value for this parameter, it does not take effect until the next time the link specified by the Profile parameter is brought up. To make the change immediately, bring the link down and back up.

Dependencies: Keep this additional information in mind:

- For routing of incoming packets for a particular port to occur, the Routing parameter in the NAT menu must be set to Yes, the Lan parameter in the NAT menu must be set to Single IP Addr, the Valid parameter in the same Static Mapping nn menu must be set to Yes, and other parameters in the same Static Mapping nn menu must be set to non-null values:
  - The Dst Port# parameter must be set to a value other than 0.
  - The Loc Adrs parameter must be set to an address other than 0.0.0.0.

  If you enter 0.0.0.0 as the value of this parameter, you receive the message Invalid Input: Zero input is not Valid.
- The Protocol parameter in the same Static Mapping nn menu determines whether the port you specify is a TCP or UDP port.
- If the Routing parameter in the NAT menu is set to No or the Lan parameter in the NAT menu is set to Multi IP Addr, this parameter is N/A.
- You cannot specify the same server and port in more than one Static Mapping nn menu.

Location: Ethernet > NAT > Static Mapping > Static Mapping *nn* (where *nn* is a number between 01 and 10)

See Also: Def Server, Dst Port # (Static Mapping), Loc Adrs, Lan, Routing, Protocol (Static Mapping), Valid (Static Mapping)

Location

Description: Specifies the location of the Pipeline.

Usage: Press Enter to open a text field. Then, type a description of the Pipeline's location. You can enter up to 80 characters. An SNMP management application can read this field, but the value you enter does not affect the operation of the Pipeline.

Press Enter again to close the text field.

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 Pipeline sends system logs.

Usage: Press Enter to cycle through the choices. You can select one of these settings:

- Local0
  Local0 is the default.
- Local1
- Local2
- Local3
- Local4
- Local5
- Local6
- Local7

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.

Dependencies: The Log Facility parameter applies only when you have enabled the Syslog host by setting Syslog=Yes.

Location: Ethernet > Mod Config > Log

See Also: Log Host, Syslog

Log Host

Description: Specifies the IP address of the Syslog host—the station to which the Pipeline sends system logs.

Usage: Press Enter to open a text field. Then, type the IP address of Syslog host.

An IP address consists of four numbers between 0 and 255, separated by periods. The default value is 0.0.0.0.

Press Enter to close the text field.

Example: `200.207.23.1`

Dependencies: Keep this additional information in mind:

- The Syslog host must be running UNIX.
- The Log Host parameter applies only if you enable the Syslog host by setting Syslog=Yes.

Location: Ethernet > Mod Config > Log

See Also: Log Facility, Syslog

Log Port

Description: Specifies the destination port on a syslog host where the unit's syslog messages will be received. Syslog messages include warning, notice, and Call Data Reporting (CDR) records from the unit's local system logs. Each Ascend unit can specify a different port, enabling the host to manage a number of units.

Usage: Select the Log Port parameter and enter a port number. The Log Port is the port on the Syslog host where the messages are received. The default is 514.

Dependencies: The Syslog parameter must be set to Yes. The Log Host parameter must contain the IP address of the station that will receive the syslog messages.

Location: Ethernet > Mod Config > Log

See Also: Syslog, Log Host

Loop Back

Description: Allows you to perform a loopback test of the Pipeline nailed T1 line. When the Pipeline T1 line is in loopback mode, it sends all the signals received from the switch back to the switch. Loopbacks can help diagnose whether the connection over the digital access line and the WAN is sound.

Usage: Press Enter to cycle through the choices.

- Normal. Specifies no loopback.
- Relay Loopback loops back to the network side whatever is sent to it. This is a metallic loopback of the NI generated signal through relays bypassing all of the unit's T1 circuitry.
- Line Loopback loops back to the network side whatever is sent to it. This is a loopback through all the unit's T1 circuitry. The looped back signal uses the programmed line buildout signal strength.
- Data Loopback expects the network side to loopback to it whatever is transmitted, regardless of the transmission method (such as relays, line loopbacks, crossed cables, and so on). The unit then compares what it sent with what it receives, makes a packet count and a packet data comparison.

Dependencies: The T1 line cannot be used for communication when it is in loopback mode.

Location: Nailed T1 > Mod Config

LQM

Description: Specifies whether the Pipeline requests Link Quality Monitoring (LQM) when answering a PPP call.

LQM is a feature that enables the Pipeline to monitor the quality of a link. 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.

LQM causes the generation of periodic link quality reports. Both ends of the link exchange these reports.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that the Pipeline requests LQM.
- No specifies that the Pipeline does not request LQM.

  No is the default.

Dependencies: Keep this additional information in mind:

- Both sides of the link negotiate the interval between periodic link quality reports; however, the interval must fall between the minimum interval (as set by LQM Min) and the maximum interval (as set by LQM Max).
- If LQM is turned off (LQM=No), the LQM Max and LQM Min parameters do not apply (LQM Max=N/A and LQM Min=N/A).
- LQM applies only if Encaps=PPP.
- LQM in the Answer profile applies to incoming calls for which no Connection profile exists; if a Connection profile exists, the setting of its LQM parameter takes precedence.
- If Profile Reqd=Yes in the Answer profile, LQM does not apply (LQM=N/A) in the Answer profile.

Location: Ethernet > Answer > *any profile* > PPP Options; Ethernet > Connections > *any profile* > Encaps Options

See Also: Encaps, LQM Max, LQM Min

LQM Max

Description: Specifies the maximum duration between link quality reports, measured in tenths of a second.

Usage: Press Enter to open a text field. Then, type a number between 0 and 600. The default is 600. Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- If LQM=No, the LQM Max parameter does not apply (LQM Max=N/A).
- LQM Max in the Answer profile applies to incoming calls for which no Connection profile exists; if a Connection profile exists, the setting of its LQM Max parameter takes precedence.
- If Profile Reqd=Yes in the Answer profile, LQM Max does not apply (LQM Max=N/A) in the Answer profile.

Location: Ethernet > Answer > *any profile* > PPP Options; Ethernet > Connections > *any profile* > Encaps Options

See Also: LQM, LQM Min

LQM Min

Description: Specifies the minimum duration between link quality reports, measured in tenths of a second.

Usage: Press Enter to open a text field. Then, type a number between 0 and 600. The default is 600. Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- If LQM=No, the LQM Min parameter does not apply (LQM Min=N/A).
- LQM Min in the Answer profile applies to incoming calls for which no Connection profile exists; if a Connection profile exists, the setting of its LQM Min parameter takes precedence.
- If Profile Reqd=Yes in the Answer profile, LQM Min does not apply (LQM Min=N/A) in the Answer profile.

Location: Ethernet > Answer > *any profile* > PPP Options; Ethernet > Connections > *any profile* > Encaps Options

See Also: LQM, LQM Max

Mask

Description: In a filter of type Generic, specifies a 16-bit hexadecimal bitmask that the Pipeline applies to the data contained in the specified bytes in a packet. A mask hides the part of a number that appears behind the binary zeroes in the mask; for example, if Mask=ffff0000, the Pipeline uses only the first 16 binary digits in the comparison, since f=1111 in binary format.

The Pipeline applies the Mask parameter starting at the position specified by the Offset parameter. The setting you specify for Mask must contain the same number of bytes as the Length parameter. The Pipeline then compares the unmasked portion of the packet with the value specified by the Value parameter.

Usage: Press Enter to open a text field. Then, type a hexadecimal number. You can enter a number between 00 and ffffffffffffffff.

The default is 00. When you accept the default, the Pipeline uses the data in the packet as is for comparison purposes.

Press Enter to close the text field.

Example: This example specifies that the Pipeline masks all but the first 24 bits of the data:

```
Mask=ffffff0000000000
```

Dependencies: Mask does not apply (Mask=N/A) for an IP filter (Type=IP).

Location: Ethernet > Filters > *any type of filter* > *any input or output filter* > *any numbered filter* > Generic

See Also: Length (Filter), Offset, Type, Value

Max Ch Count

Description: Specifies the maximum number of channels allowed on an MP+ call.

Usage: Press Enter to open a text field. Then, type a number between 1 and the maximum number of channels your system supports. For ISDN service on the Pipeline, this number cannot exceed 2. The default setting is 1.

Dependencies: Keep this additional information in mind:

- The Max Ch Count parameter applies only to dynamic MP+ calls (Encaps=MPP).
- If Profile Reqd=Yes in the Answer profile, Max Ch Count does not apply (Max Ch Count=N/A) in the Answer profile.
- For optimum MP+ performance, both sides of a connection must set these parameters to the same values:
  - Base Ch Count (in the Connection profile)
  - Min Ch Count (in the Answer profile)
  - Max Ch Count (in the Answer profile and the Connection profile)

- Max Ch Count in the Answer profile applies to incoming calls for which no Connection profile exists; if a Connection profile exists, the setting of its Max Ch Count parameter takes precedence.

Location: Ethernet > Answer > *any profile* > PPP Options; Ethernet > Connections > *any profile* > Encaps Options

See Also: Add Pers, Base Ch Count, Encaps

Maximum No Reply Wait

Description: When a Pipeline handles a DHCP message that requests an IP address and the value of the Validate IP parameter is Yes, it sends an ICMP echo (ping) message to check if the address is already in use. This parameter specifies a maximum duration, in seconds, for two actions related to this check:

- It specifies the length of time during which the Pipeline waits for a response to the ICMP echo message. If the Pipeline does not receive a response during this interval, it assumes that the address is not being used and reserves the address for the host requesting it.

  Note: During the time the Pipeline is validating the address, it ignores the original DHCP request and any subsequent requests from the same host. The host continues to send DHCP requests, however, as specified in the DHCP protocol.

- Once the Pipeline has determined that the address is available, it assigns the host the address if it receives another DHCP request from the host within the number of seconds specified by this parameter. If the Pipeline does not receive the DHCP request during this interval, the Pipeline stops reserving the address.

Usage: Press Enter to open a text field and enter a number between 5 and 300.

10 is the default.

Press Enter to close the text field.

Dependencies: If the DHCP Spoofing and Always Spoof parameters are not both Yes, this parameter is N/A. If Validate IP is No, the Pipeline does not validate the addresses it assigns, regardless of the value of this parameter.

Location: Ethernet > Mod Config > DHCP Spoofing

See Also: DHCP Spoofing, Always Spoof, Validate IP

Metric

Description: Appears in a Connection profile and a Static Rtes profile. Its functionality differs depending on the profile:

- In a Connection profile, determines the virtual hop count of the link.
- In a Static Rtes profile, determines the virtual hop count of the route.

If there are two routes available to a single destination network, you can ensure that the Pipeline uses any available nailed-up channel before using a switched channel by setting the Metric parameter to a value higher than the metric of any nailed-up route. The higher the value entered, the less likely that the Pipeline will bring the link or route online. The Pipeline uses the lowest metric.

Usage: Press Enter to open a text field, Then, type a number between 1 and 15. This value is the virtual hop count. The default setting is 7. Press Enter again to close the text field.

Example: If a route to a station takes three hops over nailed-up lines, and Metric=4 in a Connection profile that reaches the same station, the Pipeline does not bring the Connection profile's link online.

Dependencies: Keep this additional information in mind:

- The Metric parameter in a Connection profile does not apply to bridged connections.
- If you enable RIP (Routing Information Protocol) across the WAN in a Connection profile or an Answer profile (RIP=Recv or RIP=Both), the hop count for the route can differ from the value of the Metric parameter in the Route profile because the Pipeline always uses the lower hop count.
- The hop count includes the metric of each switched link in the route.
- The Metric only applies to IP connections.

Location: Ethernet > Connections > *any profile* > IP Options; Ethernet > Static Rtes > *any profile*

See Also: Private, RIP

Min Ch Count

Description: Specifies the minimum number of channels an MP+ call maintains.

Usage: Press Enter to open a text field. Then, type a number between 1 and 2 for ISDN, and 1 and 32 for T1. The default setting is 1. Press Enter again to close the text field. You cannot save a value greater than the capacity of your service's total bandwidth.

Dependencies: The Min Ch Count parameter applies only to MP+ calls (Encaps=MPP). For optimum MP+ performance, both sides of a connection must set these parameters to the same values:

- Base Ch Count (in the Connection profile)
- Min Ch Count (in the Answer profile)
- Max Ch Count (in the Answer profile and the Connection profile)

Location: Ethernet > Connections > *any profile* > Encaps Options; Ethernet > Answer > *any profile* > PPP Options

See Also: Max Ch Count

See Also:

Module Enabled

Description: Enables the Pipeline V.35 Serial WAN port.

Usage: Press Enter to cycle through the choices:

- Yes enables the Serial WAN port.
  Yes is the default.
- No disables the Serial WAN port.

Location: V.35 > Serial WAN > Mod Config

More

Description: In a filter of type Generic, specifies whether the Pipeline passes the packet to the next filter specification in the profile.

Use this parameter when you need a generic filter wider than the 8-byte limit of the Length parameter. For example, suppose a packet is 16 bytes long (128 bits). You can compare only 8 bytes in a filter because the maximum value of the Length parameter is 8. To compare all 16 bytes, you specify two 8-byte filters linked by the More parameter.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that the Pipeline applies the next filter in the profile before deciding whether to forward the packet.

  If you set More=Yes, the filter can examine multiple noncontiguous bytes within a packet by "marrying" the current filter to the one that immediately follows it.

- No specifies that the Pipeline does not apply the next filter in the profile before deciding whether to forward the packet.

  No is the default.

Example: Input filter 01 and input filter 02 examine different bytes of the same packet and apply a logical AND to the results in order to determine whether the packet matches the specification:

```
In filter 01...Valid=Yes
In filter 01...Type=Generic
In filter 01...Generic...Forward=No
In filter 01...Generic...Offset=04
In filter 01...Generic...Length=8
In filter 01...Generic...Value=abc
In filter 01...Generic...More=Yes

In filter 02...Valid=Yes
In filter 02...Type=Generic
In filter 02...Generic...Forward=No
In filter 02...Generic...Offset=2
In filter 02...Generic...Length=8
In filter 02...Generic...Value=123
In filter 02...Generic...More=No
```

In this example, the Pipeline compares 16 bytes of each data packet. The match occurs only if *all the* noncontiguous bytes contain the specified values.

Dependencies: Keep this additional information in mind:

- The More parameter does not apply (More=N/A) if you are using an IP filter (Type=IP).
- The next filter must be a Generic filter (Type=Generic) and must be activated (Valid=Yes); otherwise, the Pipeline ignores the filter.

Location: Ethernet > Filters > *any type of filter* > *any input or output filter* > *any numbered filter* > Generic

See Also: Forward, Length (Filter), Offset, Type, Value, Valid (Filter)

MRU

Description: Specifies the maximum number of bytes the Pipeline can receive in a single packet on a PPP link. MRU stands for Maximum Receive Unit.

Usage: The default setting is 1524; you should accept this default unless the device at the remote end of the link cannot support it.

If the administrator of the remote network specifies that you must change this value, press Enter to open a text field. For an Answer profile or a Connection profile, type a number between 1 and 1524. For a Frame Relay profile, type a value between 128 and 1600.

Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- The MRU parameter applies to any link using PPP encapsulation (Encaps=MPP or Encaps=PPP).

  When you choose Encaps=MPP, both the dialing side and the answering side of the link must support MP+. If only one side supports MP+, the connection uses MP or standard single-channel PPP. When you choose Encaps=PPP, the connection uses only PPP.
- MRU in the Answer profile applies to incoming calls for which no Connection profile exists; if a Connection profile exists, the setting of its MRU parameter takes precedence.

- If Profile Reqd=Yes in the Answer profile, MRU does not apply (MRU=N/A) in the Answer profile.

Location: Ethernet > Answer > *any profile* > PPP Options; Ethernet > Connections > *any profile* > Encaps Options; Ethernet > Frame Relay > *any profile*

See Also: Encaps

Multicast Forwarding

Description: Enables multicast forwarding on the Pipeline. By default, it is set to No.

Usage: Press Enter to toggle between Yes and No.

- Yes enables multicast forwarding.

  When set to Yes, the Pipeline appears to a Multicast router as a multicast client, which receives Internet Group Membership Protocol (IGMP) queries from the router and responds to them using IGMP. To dial-in clients, it appears as a multicast router, which sends IGMP queries and forwards multicast traffic.
- No, the default, turns off multicast forwarding.

Location: Ethernet > Mod Config > Ether Options

See Also: Multicast profile

Multicast profile

Description: Specifies the name of a Connection profile for a WAN link to a multicast router. If no profile name is specified and Multicast Forwarding is turned on, the Pipeline assumes that its Ethernet is the Multicast interface.

The specified Connection profile must be resident.

Usage: Press Enter to open a text field. Then, type the name of the Connection profile to the multicast interface. If no name is specified, the Pipeline assumes the presence of a multicast router on its Ethernet interface. Press Enter again to close the text field.

Location: Ethernet > Mod Config

Dependencies: Available only in the IP-only release for the Pipeline. It is not available if Multicast Forwarding is set to No.

See Also: Multicast Forwarding

My Addr

See “IP Adrs” on page 3-79.

My Name

See “Name” on page 3-117.

My Num A

Description: Specifies the phone number assigned to the line. If two phone numbers are assigned to the line, specify one here and one in My Num B.

When the Pipeline receives a multichannel MP+ call, it reports the primary phone number (My Num A) and the secondary phone number (My Num B) to the calling party. The calling Pipeline can then add more channels. If you do not specify a phone number and the calling Pipeline needs to add more channels, it redials the phone number it used to make the first connection.

Usage: Press Enter to open a text field and then type a telephone number. The character set is limited to the following characters:

1234567890()[]!z-*#”

You can include a hyphen in the phone number but no spaces.

Example: 5105551972

Location: Configure

Dependencies: You must get this number from the telephone company providing your service.

See Also: My Num B

My Num B

Description: Specifies the phone number assigned to the line. If two phone numbers are assigned to the line, specify one here and one in My Num A.

When the Pipeline receives a multichannel MP+ call, it reports the primary phone number (My Num A) and the secondary phone number (My Num B) to the calling party. The calling Pipeline can then add more channels. If you do not specify a phone number and the calling Pipeline needs to add more channels, it redials the phone number it used to make the first connection.

Usage: Press Enter to open a text field and then type a telephone number. The character set is limited to the following characters:

1234567890()[]!z-*#”

You can include a hyphen in the phone number but no spaces.

Example: 5105551972

Location: Configure

Dependencies: You must get this number from the telephone company providing your service.

See Also: My Num A

N391

Description: Specifies how many polling cycles the Pipeline waits before requesting a full status report.

Usage: Press Enter to open a text field. Then, type the number of polling cycles that you want the Pipeline to wait. You can specify a number from 1 to 255. If you specify 1, the Pipeline requests a full status report every polling cycle. The default is 6. Press Enter again to close the text field.

Dependencies: The N391 parameter applies only if Link Mgmt=T1.617D.

Location: Ethernet > Frame Relay > *any profile*

See Also: Link Mgmt

Nailed Grp

Description: Associates a nailed-up Frame Relay group with the profile.

Usage: Press Enter to open a text field. Type a number from 1 to the maximum number of nailed-up channels that your Pipeline allows. The default is 1. Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- The Nailed Grp parameter does not apply (Nailed Grp=N/A) if the link consists entirely of switched channels (Call Type=Switched).
- Do not associate a group with more than one active Frame Relay profile.
- To assign the nailed T1 line to a frame relay switch, set Nailed T1 Group parameter in the Nailed T1 profile equal to Nailed Grp in the Frame Relay profile.

Location: Ethernet > Frame Relay > *any profile*

See Also: Activation, Call Type, Nailed T1 Group, Group (Connection)

Nailed T1 Group

Description: Associates nailed-up T1 line group with the profile.

The T1 line on the Pipeline 130 is always a nailed-up line. A link to a bridge/router or to a frame relay switch can use this line.

When you assign a Nailed T1 Group to a Connection profile, the Pipeline bridges or routes packets over that link, rather than over an ISDN BRI or switched 56 link. When you assign a Nailed T1 Group to a Frame Relay profile, the DLCI number determines which frames are sent over the link.

Usage: Press Enter to open a text field. Type a number from 1 to the maximum number of nailed-up channels that your Pipeline allows. The default is 3. Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- To assign the nailed T1 line to a Connection profile's link to a bridge/router, set Nailed T1 Group in the Nailed T1 profile equal to Group in the Connection profile.

Location: Nailed T1 > Mod Config

See Also: Nailed Grp, Group (Connection)

Name

Description: Appears in each of these profiles:

- Filter profile
- IPX SAP Filters profile
- Security profile
- SNMP Traps profile
- Static Rtes profile
- System profile
- Firewalls

The functionality of the Name parameter differs depending on the profile:

- In a Filter profile, System profile, or IPX SAP Filters profile, specifies the name of the profile.

  The Pipeline sends the System profile name to the remote device whenever it establishes a PPP link. The System profile name appears in the top line of the Edit display of the Control Monitor. Always enter a system name to identify the Pipeline.

  When the Pipeline receives a PPP or MP+ call from an Ascend unit, it tries to match the caller's Name to the value of the Station parameter in some Connection profile. If the Pipeline finds a match and authentication is turned on, the Pipeline then tries to match the caller's Send PW value to the Recv PW value in that same Connection profile.

  The Control Monitor is the menu-based user interface for configuring, managing, and monitoring the Pipeline. It consists of nine windows—eight status windows and a single edit window.

  Note: The Name parameter in the System profile is the same as the My Name parameter in the Configure menu.

- In a Static Rtes profile, specifies the name of the route’s destination.

  Note: You cannot change the name of the first route; its value is always Default.

- In an SNMP Traps profile, specifies the SNMP manager to which the Pipeline sends traps-PDUs (Protocol Data Units).

  SNMP (Simple Network Management Protocol) provides a way for computers to share networking information. In SNMP, two types of communicating devices exist: agents and managers. An agent provides networking information to a manager application running on another computer. The agents and managers share a database of information, called the Management Information Base (MIB).

  A trap is a mechanism in SNMP for reporting system change in real time. To report system change, the Pipeline sends a traps-PDU across the Ethernet interface to the SNMP manager. A complete list specifying the events that cause the Pipeline to send a traps-PDU appears in the Ascend Enterprise Traps MIB.

- In a Firewall profile, specifies the name of the firewall. This name is originally created using the Secure Access Manager (SAM) graphical user interface.

Usage: Press Enter to open a text field. Then, type a name. You can enter up to 15 characters for the Name parameter in all profiles except the Static Rtes profile and the SNMP Traps profile. In these profiles, you can enter up to 31 characters for the Name parameter.

Because the Pipeline uses the Name parameter in the System profile for authentication, you must type it exactly as the remote network expects it. In this case, Name is case sensitive.

Press Enter again to close the text field.

Location: The Name parameter appears in these locations:
Ethernet > Filters > *any type* > *any input or output filter* > *any numbered filter*;
Ethernet > Firewalls > *any profile*
Ethernet > Mod Config > Ether Options > IPX SAP Filter > *any profile*;
Ethernet > SNMP Traps > *any profile*;
Ethernet > Static Rtes > *any profile*;
System > Security > *any profile*;
System > Sys Config

NAT Lan

Description: The NAT Lan parameter has the same functionality as the Lan parameter in the NAT profile. This parameter exists for backward compatibility.

Usage: Select either of the following:

- Single IP addr
- Multiple IP addr

Dependencies: The NAT Routing parameter must be set to Yes.

Location: Ethernet > NAT

See Also: Lan

NAT Profile

Description: The NAT Profile parameter has the same functionality as the Profile parameter in the NAT profile. This parameter exists for backward compatibility.

Usage: Enter a string matching the Name parameter of the one Connection profile that runs NAT.

Dependencies: The NAT Routing parameter in the NAT profile must be set to Yes. Route IP in the Connection profile must be set to Yes.

Location: Ethernet > Mod Config

See Also: Profile

NAT Routing

Description: The NAT Routing parameter has the same functionality as the Routing parameter in the NAT profile. This parameter exists for backward compatibility. Do not enable NAT using both NAT Routing and Routing. Only one should be enabled.

Note: NAT has fewer features when enabled from the Mod Config menu. Static mappings and a default server cannot be specified.

Usage: Select either of the following:

- Yes - Enables NAT
- No - Disables NAT

Dependencies: Route IP must be set to Yes. NAT automatically turns RIP off, so the address of the Pipeline is not propagated to the Internet or remote networks.

Dependencies: The Route IP in the Ethernet (Mod Config) profile must be set to Yes.

Location: Ethernet > Mod Config

See Also: Routing

Net Adrs

Description: In a Bridging profile, specifies the IP address of a device at the remote end of the link.

The Pipeline uses the Bridging profile to build a bridge table of matching MAC and IP addresses. The Net Adrs parameter corresponds to the IP address of each remote device; the Enet Adrs parameter corresponds to the MAC address of each remote device.

These parameters enable the Pipeline to perform proxy ARP (Address Resolution Protocol). Whenever the Pipeline receives an ARP request from a specified IP address, it checks to see whether the IP address matches one in its bridge table. If it does, the Pipeline returns its own MAC address.

Usage: Press Enter to open a text field. Then, type the IP address of the device on the remote network.

An IP address consists of four numbers between 0 and 255, separated by periods. If a netmask is in use on the network, you must specify it. Separate a netmask from the IP address with a slash.

The default value is 0.0.0.0/0.

Press Enter to close the text field.

Example: `200.207.23.101/24`

Location: Ethernet > Bridge Adrs > *any profile*

See Also: Enet Adrs

NetWare t/o

Description: Specifies the length of time, in minutes, that the Pipeline performs watchdog spoofing for NetWare connections. Here is an explanation of watchdog spoofing:

Ordinarily, when a NetWare server does not receive a reply to the watchdog session keepalive packets it sends to a client, it closes the connection. When you select Server mode for the Handle IPX parameter, however, the Pipeline replies to NCP watchdog requests on behalf of clients on the other side of the bridge; in other words, the Pipeline tricks the server watchdog process into believing that the link is still active.

The time period for watchdog spoofing specified by the NetWare t/o parameter begins when the WAN session goes offline. If the WAN session reconnects, the Pipeline cancels the timeout.

NetWare t/o applies when the Pipeline is on a LAN containing a NetWare server.

Usage: Press Enter to open a text field. Then, type the timeout value in minutes. You can enter any value from 0 to 65535. The default value is 0 (zero); when you accept the default, the Pipeline responds to server watchdog requests indefinitely. Press Enter again to close the text field.

Dependencies: The NetWare t/o parameter does not apply (NetWare t/o=N/A) if Handle IPX=None.

Location: Ethernet > Connections > *any profile* > IPX Options

See Also: Handle IPX

Network

Description: Specifies the unique internal network number assigned to the NetWare server.

Usage: Press Enter to open a text field. Then, type the unique 4-byte hexadecimal number provided by your network administrator. The values 00000000 and ffffffff are not valid. Press Enter again to close the text field.

Example: `A00100001`

Dependencies: For the Network parameter to apply, you must enable IPX routing in the Connection profile by setting Route IPX=Yes.

Location: Ethernet > IPX Route > *any profile*

See Also: Route IPX

Node

Description: Specifies the node number of the NetWare server.

Usage: Press Enter to open a text field. Then, type the node number of the server. Typically, a server running NetWare 3.11 or later has a node number of 0000000000001. Press Enter again to close the text field.

Dependencies: For the Node parameter to apply, you must enable IPX routing in the Connection profile by setting Route IPX=Yes.

Location: Ethernet > IPX Route > *any profile*

See Also: Route IPX

Offset

Description: In a filter of type Generic, specifies the number of bytes masked from the start of the packet. The byte position specified by the Offset parameter is called the byte-offset.

Starting at the position specified by the Offset parameter, the Pipeline applies the value of the Mask parameter. A mask hides the part of a number that appears behind the binary zeroes in the mask; for example, if Mask=ffff0000 in hexadecimal format, the Pipeline uses only the first 16 binary digits in the comparison, since f=1111 in binary format. The Pipeline then compares the unmasked portion of the packet specified by the Length parameter with the value specified by the Value parameter.

Usage: Press Enter to open a text field. Then, type the number of starting bytes in a packet that the Pipeline ignores for comparison and masking purposes.

The default is 0. When you accept the default, the Pipeline starts comparing and masking data at byte 1.

Press Enter again to close the text field.

Example: Suppose you have a filter that drops packets and has these specifications:

```
Forward=No
Offset=4
Length=3
Mask=ffffff
Value=123
More=No
```

When the 10-byte packet xycd123456 passes through the filter, the Pipeline removes the leading four bytes, because Offset=4. The data 123456 remains. Next, the Pipeline removes the trailing three bytes, because Length=3; only the value 123 remains. The Mask is ffffff, which contains all ones (1s) when converted to binary numbers; therefore, the Mask value does not hide any binary digits and passes 123 through. When the Pipeline compares 123 to the setting of the Value parameter, a match occurs and the it does not forward the packet.

Dependencies: Keep this additional information in mind:

- The Offset parameter does not apply (Offset=N/A) for an IP filter (Type=IP).
- If a previous filter set More=Yes, Offset starts at the endpoint of the previous segment.

Location: Ethernet > Filters > any type > input or output > any numbered filter

See Also: Length (Firewall), Mask, More

Operations

Description: Enables or disables read-only security.

Usage: Press Enter to toggle between Yes and No.

- Yes enables users to view Pipeline profiles and change the value of any parameter.

  Yes is the default.
- No permits users to view Pipeline profiles, but not to change the value of any parameter.

  If you specify No, users cannot access most DO commands. Only DO Esc, DO Close Telnet, and DO password are available.

Location: System > Security > *any profile*

Passwd

Description: Specifies the password that activates a Security profile. The first Security profile, Default, has no password.

Usage: Press Enter to open a text field. Then, type up to 20 characters. Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- Passwd is case sensitive.

  The user must enter the password exactly as you specify it here.
- If the value of the Passwd parameter in the Security profile is *SECURE*, you cannot edit Security Profiles.

  If you want to edit Security Profiles, you must log into a Security profile whose Edit Security parameter is set to Yes.

Location: System > Security > *any profile*

See Also: Edit Security

Peer

Description: Lets you select between two classes of peers to connect via the Pipeline—IPX routers and stand alone workstations. It is best to allow two classes of peers to connect through an Ascend unit; other IPX routers, and stand alone workstations. Typically, stand alone workstations are mobile stations that connect via modem. By specifying a peer class for each Connection profile, you can improve network security.

Usage: Press Enter to cycle through the choices.

- Router specifies that the caller is an IPX router.

  Router is the default.
- Dialin specifies that the caller is a dial-in NetWare client that incorporates PPP software and dial-out hardware, but does not have an Ethernet interface.

  This setting causes the Pipeline to assign the caller an IPX address derived from the value of IPX Pool#.

Dependencies: If IPX Routing=No or Route IPX=No, the Peer parameter does not apply (Peer=N/A).

Location: Ethernet > Answer > IPX Options; Ethernet > Connections > *any profile* > IPX Options

See Also: IPX Pool#, IPX Routing, Route IPX

Preempt

Description: Specifies the number of idle seconds the Pipeline waits before using one of the channels of an idle link for a new call.

Usage: Press Enter to open a text field. Then, type a number between 0 and 65535. The Pipeline sets no time limit if you enter 0 (zero). The default setting is 60. Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- If all channels of a link are nailed up (Call Type=Nailed), the Preempt parameter does not apply (Preempt=N/A) in either the Answer or Connection profile.
- Preempt in the Answer profile applies to incoming calls for which no Connection profile exists; if a Connection profile exists, the setting of its Preempt parameter takes precedence.
- If Profile Reqd=Yes in the Answer profile, Preempt does not apply (Preempt=N/A) in the Answer profile.

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

See Also: Call Type

Preference

Description: Specifies the preference value for a specific statically configured IP route, which may be defined in an IP Route profile or Connection profile. When selecting which routes to put in the routing table, the router first compares the Preference value, selecting the lower number. If the Preference values are equal, then the router compares the Metric field, selecting the route with the lower Metric.

Usage: Press Enter to open a text field. Type 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,” which is meaningful only for Connection profiles.

These are the default values for other types of routes:

- Routes learned from ICMP Redirects=30
- Routes learned from RIP=100
- Static routes (configured in an IP Route profile or Connection profile)=100

This set of preference values gives static routes and RIP routes an equal value, with ICMP Redirects taking precedence over both.

Location: Connections > *any profile* > IP Options; Ethernet > Static Rtes > *any profile*

Pri DNS

Description: Specifies the IP address of the primary domain name server.

Domain Name System (DNS) is a TCP/IP service that enables you to specify a symbolic name instead of an IP address. A symbolic name consists of a username and a domain name in the format *username@domain name*. The *username* corresponds to the host number in the IP address. The *domain name* corresponds to the network number in the IP address. A symbolic name might be steve@abc.com or joanne@xyz.edu.

DNS maintains a database of network numbers and corresponding domain names on a domain name server. When you use a symbolic name, DNS translates the domain name into an IP address, and sends it over the network. When the Internet

service provider receives the message, it uses its own database to look up the username corresponding to the host number.

Usage: Press Enter to open a text field. Then, type the IP address of the primary domain name server.

The address consists of four numbers between 0 and 255, separated by periods. The default value is 0.0.0.0. Accept this default if you do not have a domain name server.

Press Enter again to close the text field.

Example: `200.207.23.1`

Location: Ethernet > Mod Config > DNS

See Also: Domain Name, Sec DNS

Private

Description: Appears in a Connection profile and a Static Rtes profile. Its functionality differs depending on the profile:

- In a Connection profile, specifies whether the Pipeline discloses the IP address indicated by LAN Adrs when queried by RIP (Routing Information Protocol) or another routing protocol.
- In a Static Rtes profile, specifies whether the Pipeline discloses the existence of the IP address indicated in the route when queried by RIP or another routing protocol.

Usage: Press Enter to toggle between Yes and No.

- Yes disables advertising.

  The Pipeline does not advertise the IP address in RIP updates that it sends.
- No enables advertising.

  The Pipeline advertises the IP address in RIP updates that it sends.

  No is the default.

Dependencies: Keep this additional information in mind:

- The Private parameter does not apply (Private=N/A) if the Pipeline does not support IP (Route IP=No).

Location: Ethernet > Connections > *any profile* > IP Options; Ethernet > Static Rtes > *any profile*

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

Profile

Description: Specifies the name of a Connection profile used to connect a remote network to the Pipeline. If the Pipeline is configured to perform network address translation (NAT), the Pipeline automatically performs NAT whenever a connection is made with this profile. The profile can be configured for incoming connections, outgoing connections, or both. If the profile is used for an outgoing connection, the remote server must be configured provide valid IP addresses for NAT, either through PPP negotiation for a single address or DHCP for the multiple addresses needed for NAT for LAN.

Usage: Press Enter to open a text field and then enter the name of a Connection profile.

Press Enter again to close the text field, press Esc to exit the menu, and then confirm the change when prompted.

Note: The change does not take effect until the next time the link is brought up. To make the change immediately, bring the link down and back up.

Dependencies: The Routing parameter in the NAT profile must be set to Yes. Route IP in the Connection profile must be set to Yes.

Location: Ethernet > NAT > NAT

See Also: Routing

Profile Reqd

Description: Specifies whether the Pipeline rejects incoming calls for which it could find no Connection profile and no entry on a remote authentication server.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that the Pipeline rejects incoming calls for which it can find no Connection profile and no entry on a remote authentication server.
- No specifies that the Pipeline does not require a Connection profile or a remote authentication entry.

  No is the default.

You can satisfy the Profile Reqd parameter in one of these ways:

- The source IP address of the caller matches the LAN Adrs parameter in a local Connection profile.

  In this case, Encaps=MPP or Encaps=PPP.
- The source name of the caller matches the Station parameter in a local Connection profile.

  In this case, Encaps=PPP or Encaps=MPP, and Recv Auth=PAP or Recv Auth=CHAP.
- The source MAC address of the caller matches the Station parameter in a local Connection profile.

Dependencies: If you get incoming PPP bridging calls (Route IP=No) and Profile Reqd=Yes, you must also specify that the Pipeline authenticate incoming calls using PAP or CHAP (Recv Auth=PAP or Recv Auth=CHAP). A Connection profile cannot match a PPP bridging call except through the name of the caller that PAP or CHAP authentication provides.

Location: Ethernet > Answer > *any profile*

See Also: Encaps, Recv Auth, Route IP

Protocol (Filter)

Description: In a filter of type IP, Protocol specifies the protocol number to which the Pipeline compares a packet's protocol number.

Usage: Press Enter to open a text field. Then, type 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 Pipeline disregards the Protocol parameter when applying the filter.

Protocols and their associated numbers appear in Table 3-2.

Table 3-2. Protocols

Number	Name
1	ICMP (Internet Control Message Protocol)
2	IGMP (Internet Group Management Protocol)
3	GGP (Gateway-to-Gateway Protocol)
4	IP (Internet Protocol)
5	ST (Stream)
6	TCP (Transmission Control Protocol)
7	UCL
8	EGP (Exterior Gateway Protocol)
9	Any private interior gateway protocol
10	BBN-RCC-MON (BBN RCC Monitoring)
11	NVP-II (Network Voice Protocol II)
12	PUP
13	ARGUS
14	EMCOM
15	XNET (Cross-Net Debugger)
16	CHAOS
17	UDP (User Datagram Protocol)
18	MUX (Multiplexing)

Table 3-2. Protocols (continued)

Number	Name
19	DCN-MEAS (DCN Measurement Subsystems)
20	HMP (Host Monitoring Protocol)
21	PRM (Packet Radio Measurement)
22	XNS IDP (Xerox Networking System Internetwork Datagram Protocol)
23	TRUNK-1
24	TRUNK-2
25	LEAF-1
26	LEAF-2
27	RDP (Reliable Data Protocol)
28	IRTP (Internet Reliable Transport Protocol)
29	ISO-TP4 (International Standards Organization Transport Protocol Class 4)
30	NETBLT (Bulk Data Transfer Protocol)
31	MFE-NSP (MFE Network Services Protocol)
32	MERIT-INP (MERIT Internodal Protocol)
33	SEP (Sequential Exchange Protocol)
34	3PC (Third Party Connect Protocol)
35	IDPR (Inter-Domain Policy Routing Protocol)
36	XTP

Table 3-2. Protocols (continued)

Number	Name
37	DDP (Datagram Delivery Protocol)
38	IDPR-CMTP (IDPR Control Message Transport Protocol)
39	TP++ (TP++ Transport Protocol)
40	IL (IL Transport Protocol)
41	SIP (Simple Internet Protocol)
42	SDRP (Source Demand Routing Protocol)
43	SIP-SR (SIP Source Route)
44	SIP-FRAG (SIP Fragment)
45	IDRP (Inter-Domain Routing Protocol)
46	RSVP (Reservation Protocol)
47	GRE (General Routing Encapsulation)
48	MHRP (Mobile Host Routing Protocol)
49	BNA
50	SIPP-ESP (SIPP Encap Security Payload)
51	SIPP-AH (SIPP Authentication Header)
52	I-NLSP (Integrated Net Layer Security Protocol)
53	SWIPE (IP with Encryption)
54	NHRP (Next Hop Resolution Protocol)
55-60	Unassigned

Table 3-2. Protocols (continued)

Number	Name
61	Any Host Internet Protocol
62	CFTP
63	Any local network
64	SAT-EXPAK (SATNET and Backroom EXPAK)
65	KRYPTOLAN
66	RVD (MIT Remote Virtual Disk Protocol)
67	IPPC (Internet Pluribus Packet Core)
68	Any distributed file system
69	SAT-MON (SATNET Monitoring)
70	VISA (VISA Protocol)
71	IPCU (Internet Packet Core Utility)
72	CPNX (Computer Protocol Network Executive)
73	CPHB (Computer Protocol Heart Beat)
74	WSN (Wang Span Network)
75	PVP (Packet Video Protocol)
76	BR-SAT-MON (Backroom SATNET Monitoring)
77	SUN-ND PROTOCOL-Temporary
78	WB-MON (WIDEBAND Monitoring)
79	WB-EXPAK (WIDEBAND EXPAK)

Table 3-2. Protocols (continued)

Number	Name
80	ISO-IP (International Standards Organization Internet Protocol)
81	VMTP
82	SECURE-VMTP
83	VINES
84	TTP
85	NSFNET-IGP (National Science Foundation Network Interior Gateway Protocol)
86	DGP (Dissimilar Gateway Protocol)
87	TCF
88	IGRP
89	OSPF (Open Shortest Path First)
90	Sprite-RPC
91	LARP (Locus Address Resolution Protocol)
92	MTP (Multicast Transport Protocol)
93	AX.25 (AX.25 Frames)
94	IPIP (IP-within-IP Encapsulation Protocol)
95	MICP (Mobile Internetworking Control Protocol)
96	SCC-IP (Semaphore Communications Security Protocol)
97	ETHERIP (Ethernet-within-IP Encapsulation)

Table 3-2. Protocols (continued)

Number	Name
98	ENCAP (Encapsulation Header)
99	Any private encryption scheme
100	GMTP
101-254	Unassigned
255	Reserved

Dependencies: The Protocol parameter applies only if the filter is of type IP (Type=IP) and is activated (Valid=Yes).

Location: Ethernet > Filters > *any type* > *any input or output filter* > *any numbered filter* > Ip

See Also: Type, Valid (Filter)

Protocol (Static Mapping)

Description: When the Pipeline is configured to perform single-address network address translation (NAT) and to provide services for users outside the private local LAN, this parameter specifies whether the Dst Port# and Loc Port# parameters in the same Static Mapping nn menu (where nn is a number between 01 and 10) specify TCP or UDP ports.

Usage: Enter TCP or UDP.

- TCP specifies that the Dst Port# and Loc Port# parameters in the same Static Mapping nn menu are TCP port numbers. TCP is the default.
- UDP specifies that the Dst Port# and Loc Port# parameters in the same Static Mapping nn menu are UDP port numbers.

Note: After you enter a value for this parameter, it does not take effect until the next time the link specified by the Profile parameter is brought up. To make the change immediately, bring the link down and back up.

Dependencies: The Routing parameter in the NAT profile must be set to Yes. The Lan parameter in the NAT profile must be set to Single IP addr. Valid in Static Mappings must be set to Yes.

Location: Ethernet > NAT > Static Mappings....> Static Mapping nn (where nn is a number between 01 and 10)

See Also: Routing, Lan, Dst Port # (Static Mapping), Loc Adrs, Loc Port#, Valid (Static Mapping)

Proxy Mode

Description: Specifies under what conditions the Pipeline performs a proxy ARP (Address Resolution Protocol). The Pipeline performs a proxy ARP when it recognizes the IP address of a remote device in an ARP request, and then responds to the ARP request by sending its own MAC address.

Usage: Press Enter to cycle through the choices.

- Always specifies that the Pipeline responds to an ARP request regardless of whether a connection to the remote site is up.
- Inactive specifies that the Pipeline 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 Pipeline 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.
- Off disables proxy mode.

  Off is the default.

Dependencies: Keep this additional information in mind:

- The Proxy Mode parameter does not apply (Proxy Mode=N/A) if the v does not support IP (Route IP=No).
- Enabling Proxy Mode may prevent the Pipeline from placing calls simply for address lookups.

Location: Ethernet > Mod Config > Ether Options

See Also: Net Adrs, Route IP

Queue Depth

Description: The maximum number of SNMP requests stored for processing. If SNMP requests arrive at a rate that is faster than they can be processed, they are sent to the queue. This parameter sets the maximum depth of the queue. After the queue fills up, packets destined for it are discarded.

Usage: Enter a value from 0 to 1024. A setting of 0 stores SNMP requests until the Pipeline runs out of memory. Zero is the default.

Note: Setting Queue Depth to zero is not recommended. An unlimited queue depth can result in an out-of-memory condition if a flood of packets are received on the SNMP port.

Location: Ethernet > Mod Config > SNMP Options

See Also: Rip Queue Depth

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.

SNMP security is implemented with the community name sent with each request. Ascend supports two community names: one with read-only access to the MIB (the Read Comm parameter), and the other with read/write access to the MIB (the R/W Comm parameter).

Usage: Press Enter to open a text field. Then, type the community name that the Pipeline will use for authenticating the SNMP management station. You can enter letters and numbers, up to a limit of 32 characters. The default is Write.

The community name can contain a secret key, that is specified in the R/W string after a vertical bar (|). When the secret key is present in the community string, the Pipeline requires SNMP SET REQUEST packets to be authenticated using the password as well as the shared (but not transmitted) secret.

Example: `R/W Comm=password|secret`

Location: Ethernet > Mod Config > SNMP Options

See Also: Read Comm

R/W Comm Enable

Description: Enables and disables the use of SNMP set commands.

Usage: Press Enter to select Yes or No.

- Yes enables the use of SNMP set commands. To use a set command, you must know the SNMP read-write community string specified in the R/W Comm parameter.
- No disables the use of set commands.
  No is the default.

Location: Ethernet > SNMP Options > Mod Config

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.

SNMP (Simple Network Management Protocol) provides a way for computers to share networking information. In SNMP, two types of communicating devices exist: agents and managers. An agent provides networking information to a manager application running on another computer. The agents and managers share a database of information, called the Management Information Base (MIB).

SNMP security is implemented with the community name sent with each request. Ascend supports two community names: one with read-only access to the MIB (the Read Comm parameter), and the other with read/write access to the MIB (the R/W Comm parameter).

Usage: Press Enter to open a text field. Then, type the community name that the Pipeline uses for authenticating the SNMP management station. 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 that the Pipeline uses when receiving and verifying a password for an incoming PPP call.

Usage: Press Enter to cycle through the choices.

- None specifies that the Pipeline does not use an authentication protocol to validate incoming calls.

  None is the default.

- PAP (Password Authentication Protocol) is a PPP 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.

  If you choose PAP, the Pipeline uses this protocol for authentication. The remote device must support PAP.

- CHAP (Challenge Handshake Authentication Protocol) is a PPP authentication protocol.

  CHAP is more secure than PAP. CHAP 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 Pipeline can repeat the authentication process any time after the connection is made.

  If you choose CHAP, the Pipeline uses this protocol for authentication. The remote device must support CHAP.

- MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) is a PPP protocol.

  Similar to CHAP, MS-CHAP allows authentication only if the remote peer uses MS-CHAP for authentication. It is supported in Windows NT environments only.

- Either specifies that the Pipeline can use any authentication if the remote peer can authenticate the designated scheme.

Dependencies: Keep this additional information in mind:

- The link must use PPP or MPP encapsulation (Encaps=PPP or Encaps=MPP).
- If you choose PAP or CHAP, you must also specify a password using Recv PW in a Connection profile.

- When you set Recv Auth=PAP, CHAP, or Either, the Pipeline can determine the IP address of a caller, even if the caller does not specify an address; the Pipeline derives the IP address from the Connection profile.

Location: Ethernet > Answer > *any profile* > PPP Options

See Also: Recv PW, Send Auth, Send PW

Recv PW

Description: Specifies the password that the remote end of the link must send; if the password specified by Recv PW does not match the remote end's value for Send PW, the Pipeline disconnects the link.

Usage: Press Enter to open a text field. Then, type a password. You can enter up to 20 characters; the password is case sensitive. The default is null. Press Enter again to close the text field.

Dependencies: Keep this additional information in mind concerning the Recv PW parameter in the Connection profile:

- If Recv Auth=None, the Recv PW parameter does not apply (Recv PW=N/A).
- You must specify a value for Recv PW when the link uses PPP encapsulation (Encaps=PPP or Encaps=MPP) and the Pipeline uses either PAP or CHAP authentication (Recv Auth=PAP or Recv Auth=CHAP).

  When you choose Encaps=MPP, both the dialing side and the answering side of the link must support MP+. If only one side supports MP+, the connection uses MP or standard single-channel PPP. When you choose Encaps=PPP, the connection uses only PPP.

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

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

Rem Addr

See "LAN Adrs" on page 3-92.

Rem Name

See “Station” on page 3-169.

Remote Mgmt

Description: Specifies whether the device at the remote end of a call can operate the Pipeline remotely.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that the remote device can remotely operate the Pipeline.
  Yes is the default.
- No specifies that the remote device cannot remotely operate the Pipeline.
  If the remote device tries to do so, the error message Remote Management Denied appears.

Dependencies: The Call Type parameter must be set to MPP or Nailed/MPP.

Location: System > Sys Config

See Also: Call Type

Renewal Time

Description: Specifies the lease time for a dynamically assigned IP address. This is the time in which the host is assigned the IP address, as defined by the DHCP protocol. If the host renews the address before its lease period expires, the DHCP service reassigns the same address.

Usage: Enter a length of time in seconds. The default is 10.

Location: Ethernet > Mod Config > DHCP Spoofing

Restore Cfg

Description: Restores profiles saved using the Save Cfg parameter, or transfers the profiles to another Pipeline. Because the Save Cfg command does not save passwords, the Restore Cfg command does not restore them.

Usage: Follow these instructions to restore your configuration from backup:

1. Enable the Upload parameter in the Security profile (Upload=Yes).
2. Verify that your terminal emulation program has a disk capture feature; this feature enables your emulator to capture to disk the ASCII characters it receives at its serial host port.
3. Verify that your terminal emulation program has an autotype feature; this feature enables your emulator to transmit over its serial host port the contents of a file it has built through disk capture.
4. Connect the backup device to the Pipeline Control port.
5. Set the data rate of your terminal emulation program to 9600 baud or lower.
6. Set the Term Rate parameter in the System profile to 9600.
7. Make certain that you have the Edit Security privilege; if you restore without having the Edit Security privilege, you can be locked out of some or all operations.
8. Select Restore Cfg from the Sys Diag menu.
9. When the `Waiting for upload data` prompt appears, turn on the autotype function on your emulator and supply the filename of the saved Pipeline data.
10. Verify that the configuration data is going to your terminal emulation screen and is being restored to the target Pipeline.

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

Location: System > Sys Diag

See Also: Save Cfg

Reuse addr timeout

Description: Specifies the time the Pipeline uses a dynamically assigned IP address when running in single-address NAT mode. See Reuse last addr parameter for details.

Usage: Enter a numeric value from 0 to 1440. The value 0 means the Pipeline reuses the IP address without a time limit. The maximum setting is 1440 seconds.

Dependencies: The Routing parameter in the NAT profile must be set to Yes. The Lan parameter in the NAT profile must be set to Single IP addr. Reuse last addr parameter must be set to Yes.

Location: Ethernet > NAT

See Also: Routing, Lan, Reuse last addr

Reuse last addr

Description: Specifies that the last IP address given by the remote unit during PPP negotiations should be reused in subsequent PPP negotiations (for the duration specified in the Reuse addr timeout parameter). Reuse last addr applies only to single-address NAT.

Usage: The possible values are Yes or No. The default is No.

- Yes - After an IP address is obtained by PPP negotiations, the MAX uses that IP address in all other PPP negotiations as long as the limit set by the Reuse addr timeout parameter has not been exceeded.

  Set this parameter to Yes when you need to use the same IP address for TCP applications that might need to reestablish a connection during the session, such as Telnet. For example, suppose a Telnet session is idle for a long period of time and as a result, disconnects, but the Telnet session remains alive. If Reuse last addr = No, when the connection reestablishes, a new IP address is assigned by the PPP negotiations, which creates a problem for Telnet which expected to be using the original IP address.

  If the Pipeline attempts to reuse the IP address and the remote unit rejects the address, it will accept an IP address offered by the remote unit in PPP negotiations.

- No - Each PPP session renegotiates the IP address.

Dependencies: The Routing parameter in the NAT profile must be set to Yes. The Lan parameter in the NAT profile must be set to Single IP addr.

Location: Ethernet > NAT

See Also: Routing, Lan, Reuse addr timeout

RIP

Description: Specifies whether the Pipeline send and/or receives RIP-v1 (version 1) or RIP-v2 (version 2) packets on the selected interface.

The RIP parameter appears in the Answer profile, Connection Profiles, and the Ethernet profile. Its functionality differs depending on the profile:

- In the Answer profile or a Connection profile, the RIP parameter controls RIP updates between the Pipeline and a remote router.
- In the Ethernet profile, the RIP parameter controls RIP updates between the Pipeline and other IP routers on the local Ethernet network.

The most significant difference between RIP (Routing Information Protocol) versions 1 and 2 is that RIP-v2 allows neighboring hosts to communicate netmasks to each other. RIP-v1 forces routers to guess the netmask.

If the Pipeline is communicating with other RIP-v2 routers and hosts, all routing tables contain the same addresses and routes. However, if the Pipeline is communicating with a RIP-v1 router, that router ignores the netmask field in the RIP-v2 packet, making use only of the IP address without the netmask. For this reason, we do not recommend that you run RIP-v1 and RIP-v2 on the same network in such a way that both RIP-v1 and RIP-v2 hosts hear each other's advertisements.

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: Press Enter to cycle through the choices.

- Off specifies that the Pipeline does not transmit or receive RIP updates.

  Off is the default.
- Recv-v1

  This setting specifies that the Pipeline receives RIP-v1 updates, but does not transmit RIP updates on this interface (WAN or Ethernet).
- Send-v1

  This setting specifies that the Pipeline transmits RIP-v1 updates, but does not receive RIP updates on this interface (WAN or Ethernet).
- Both-v1

This setting means that the Pipeline transmits and receives RIP-v1 updates on this interface (WAN or Ethernet).

- Send-v2

  This setting specifies that the Pipeline transmits RIP-v2 updates, but does not receive RIP updates on this interface (WAN or Ethernet).

- Recv-v2

  This setting specifies that the Pipeline receives RIP-v2 updates, but does not transmit RIP updates on this interface (WAN or Ethernet).

- Both-v2

  This setting means that the Pipeline transmits and receives RIP-v2 updates on this interface (WAN or Ethernet).

Dependencies: Keep this additional information in mind:

- The RIP parameter does not apply if the Pipeline does not support IP (Route IP=No).
- RIP in the Answer profile applies to incoming calls for which no Connection profile exists; if a Connection profile exists, the setting of its RIP parameter takes precedence.
- If Profile Reqd=Yes in the Answer profile, RIP does not apply (RIP=N/A) in the Answer profile.

Location: Ethernet > Answer > *any profile* > Session Options; Ethernet > Connections > *any profile* > IP Options; Ethernet > Mod Config > Ether Options

See Also: Route IP

RIP Policy

Description: Determines whether the Pipeline uses split horizon or poison reverse to handle RIP broadcasts over an interface that includes routes received from that interface. In either case, the Pipeline keeps track of where it received RIP updates

Note: RIP Policy only applies to RIP version 1.

Usage: Press Enter to cycle through the choices.

- Split Hrzn specifies the split horizon policy.

The Pipeline does not propagate routes back to the subnet from which they were received.

- Poison Rvrs selects the poison reverse policy.

  The Pipeline propagates routes back to the subnet from which they were received, but with a metric of 16.

  Poison Rvrs is the default.

Location: Ethernet > Mod Config

Rip Preference

Description: Specifies the preference value for routes learned from the RIP protocol. When selecting which routes to put in the routing table, the router first compares the Preference value, selecting the lower number. If the Preference values are equal, then the router compares the Metric field, selecting the route with the lower Metric.

Usage: Press Enter to open a text field. Then, type 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.”

These are the default values for other types of routes:

- Routes learned from ICMP Redirects=30
- Static routes from IP address pools and the Terminal Server IPROUTE ADD command=100
- Static routes in an IP Route profile or Connection profile=100

Location: Ethernet > Mod Config > Route Pref

Rip Queue Depth

Description: The maximum number of RIP requests stored for processing. If RIP requests arrive at a rate that is faster than they can be processed, they are sent to the queue. This parameter sets the maximum depth of the queue. After the queue fills up, packets destined for it are discarded. The value of this parameter applies to every RIP socket.

Usage: Enter a value from 0 to 1024. A setting of 0 stores RIP requests until the Pipeline runs out of memory. 50 is the default.

Note: Setting Queue Depth to 0 is not recommended. An unlimited queue depth can result in an out-of-memory condition if a flood of packets are received on a RIP port.

Dependencies: This parameter does not apply if the Pipeline does not listen to RIP updates.

Location: Ethernet > Mod Config > Route Pref

See Also: Queue Depth, RIP

RIP Summary

Description: Specifies whether the Pipeline summarizes subnet information when advertising routes.

Note: RIP Summary only applies to RIP version 1.

Summarizing means that when the Pipeline has a route to a subnet, it advertises a route to all the subnets in a network of the same class. For example, if the Pipeline has a routing table entry to 200.5.8.13/28, it advertises a route to 200.5.8.0, because 200.5.8.13/28 is part of a class C network. When the Pipeline does not summarize information, it advertises each route in its routing table "as-is;" in our example, the Pipeline advertises a route only to 200.5.8.13.

RIP (Routing Information Protocol) is defined without consideration for subnetting; entries in a RIP packet do not include a subnet mask. Therefore, the recipient of such updates must know or assume information about subnet masks. To work around this standard RIP behavior, the Pipeline includes the RIP Summary parameter. You can set this parameter to specify that the Pipeline modify RIP to advertise implied subnet information.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that the Pipeline summarizes subnet information when advertising routes outside its own network, but does not summarize subnet information when advertising routes inside its own network.

  For example, suppose the Pipeline has an IP address of 200.8.143.5/28 and advertises across the WAN to a router that has the address 200.8.143.31/28.

Even though the Pipeline and the recipient are on different subnets, they are on the same network; therefore, no summarization takes place. The routes are sent “as-is.”

Yes is the default.

- No specifies that the Pipeline never summarizes subnet information.

  When you select No, the recipient must know the subnet mask to apply to each route.

Dependencies: Keep this additional information in mind:

- The RIP Summary parameter applies only to RIP version 1 and has no affect on RIP version 2 advertisements.
- RIP Summary does not affect host routes.

  Suppose the Pipeline has a routing table entry to 200.8.143.5/32. Regardless of whether routes are summarized, this route is advertised as 200.8.143.5.

Location: Ethernet > Mod Config

RIP2 Use Multicast

Description: Specifies that Multicast IP is to be used for RIP 2 packets.

Usage: The possible values are Yes or No.

- No sends out RIP 2 packets using the settings of the Ethernet > Mod Config > Ether Options > RIP parameter.

  No is the default.
- Yes sends RIP 2 packets with the IP Multicast address of 224.0.0.9 and the Multicast MAC address, and receives packets with a Multicast MAC address.

Dependencies: The RIP2 Use Multicast parameter does not apply if the Pipeline does not support IP (Route IP=No).

Location: Ethernet > Mod Config > Ether Options

See Also: RIP

Route

Description: Specifies what type of routing (if any) applies to the first Connection profile as well as to the Answer profile.

Usage: Press Enter to cycle through the choices.

- None sets your Pipeline as a bridge (default).
- IP sets your Pipeline as an IP router.
- IPX sets your Pipeline as an IPX router.
- IP + IPX sets your Pipeline as a router for both IP and IPX.

Dependencies: Keep this additional information in mind:

- The Route setting in the Configure menu determines the value of the Route IP and Route IPX parameters in the first Connection profile and in the Answer profile.
- If IP routing is enabled, you must set appropriate options in the IP Options submenu. Both sides of the connection must have IP routing enabled, so each side can be managed as a separate IP network or subnetwork.
- If IPX routing is enabled, you must set the IPX Frame type its associated parameters in the IPX Options submenu. Both sides of the connection must have IPX routing enabled, so each side can be managed as a separate IPX network.
- If routing is disabled, bridging must be enabled.

Location: Configure

See Also: Route IP, Route IPX

Route IP

Description: Enables or disables the routing of IP data packets over the link specified in the profile.

Usage: Press Enter to toggle between Yes and No.

- Yes enables IP routing
  Yes is the default.
- No disables IP routing.

Dependencies: The effect of the Route IP parameter depends upon how you set the Bridge parameter:

- If Bridge=Yes and Route IP=Yes, the Pipeline routes IP packets, and bridges all other packets.
- If Bridge=Yes and Route IP=No, the Pipeline bridges all packets.
- If Bridge=No and Route IP=Yes, the Pipeline routes only IP packets.
- If Bridge=No and Route IP=No, an error occurs and you cannot save the profile.

  You must enable bridging or routing, or both.

These additional dependencies apply:

- The Route parameter in the Configure menu affects the Route IP value in the first Connection profile. For example, if you set Route=IPX in the Configure menu (that is, route *only* IPX), Route IP=No in the first Connection profile.
- IP routing must be enabled on both the dialing and answering sides of the link.

  The Connection profile on the dialing side and the Answer profile on the answering side must both set the Route IP parameter to Yes. Otherwise, the Pipeline does not route IP packets.
- Route IP in the Answer profile applies to incoming calls for which no Connection profile exists; if a Connection profile exists, the setting of its Route IP parameter takes precedence.
- If Profile Reqd=Yes in the Answer profile, Route IP does not apply (Route IP=N/A) in the Answer profile.

Location: Ethernet > Answer > *any profile* > PPP Options; Ethernet > Connections > *any profile*

See Also: Bridge, Encaps, Profile Reqd, Route, Route IPX

Route IPX

Description: Specifies whether or not the Pipeline requests IPX routing for the connection.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that the Pipeline requests IPX routing.

- No specifies that the Pipeline does not route IPX.

  No is the default.

Dependencies: If the link supports PPP or MP+ (Encaps=PPP or Encaps=MPP), both sides of the connection must set Route IPX=Yes for IPX routing to take place.

In addition, the effect of the Route IPX parameter depends upon how you set the Bridge parameter:

- If Bridge=Yes and Route IPX=Yes, the Pipeline routes IPX packets, and bridges all other packets.
- If Bridge=Yes and Route IPX=No, the Pipeline bridges all packets.
- If Bridge=No and Route IPX=Yes, the Pipeline routes only IPX packets.
- If Bridge=No and Route IPX=No, an error occurs and you cannot save the profile.

  You must enable bridging or routing, or both.

This additional dependency applies:

- The Route parameter in the Configure menu affects the Route IPX value in the first Connection profile. For example, if you set Route=IP in the Configure menu (that is, route *only* IP), Route IPX=No in the first Connection profile.

Location: Ethernet > Answer > *any profile* > PPP Options; Ethernet > Connections > *any profile*

See Also: Bridge, Route, Route IP

Routing

Description: Enables or disables network address translation (NAT).

NAT is a service provided to one or more hosts on the local network that do not have official IP addresses for a remote network. It works as follows:

- When the local host sends packets to the remote network, the Pipeline automatically translates the host's private address on the local network to an official address on the remote network.

- When the local host receives packets from the remote network, the Pipeline automatically translates the official address on the remote network to the host's private address on the local network.

NAT can be implemented to use a single address or multiple addresses. Using multiple IP addresses requires that the Pipeline can access a DHCP server through the remote network.

Note: The Pipeline itself does not have an address on the remote network. This means that the Pipeline can only be accessed from the local network, not from the WAN. For example, you can Telnet to the MAX from the local network, but not from a remote network.

Usage: Press Enter to toggle between Yes and No, press Esc to exit the menu, and then confirm the change when prompted.

- Yes enables NAT.
- No disables NAT.

  No is the default.

  Note: The change does not take effect until the next time the link is brought up. To make the change immediately, bring the link down and back up.

Dependencies: Keep this additional information in mind:

- To use NAT, IP routing must be enabled on the Pipeline.
- The IP addresses of hosts on the local network that use NAT and the Pipeline must be on the same subnet. These addresses are only used for local communication between the host and the Pipeline over the Ethernet.
- You should restrict IP addresses used on the local LAN so that hosts on the network connecting to the Pipeline have each octet of their IP addresses greater than 99 (this only applies to FTP sessions). For example, 192.168.121.101 is a recommended address, but 192.168.121.99 is not.
- When the Pipeline connects to a remote network, the remote device must be configured to assign dynamic IP addresses through PPP negotiations (when the Pipeline uses a single IP address for NAT) or through DHCP (when the Pipeline requires multiple IP addresses when performing NAT for a LAN).
- Once a connection is terminated, there is no guarantee that the same IP address will be used for subsequent connections. You can set the Idle timer (in the Sessions Options submenu of the Connection profile) to 0 to prevent

the Pipeline from terminating an idle connection. But note that the device on the remote network may have the Idle timer configured to a lower value, which overrides any settings you have set.

- Once NAT has been configured and the Pipeline is translating addresses from clients on the local LAN, the Pipeline can only be accessed from the local LAN or through the serial port; it cannot be directly accessed from the WAN side.
- Note that the Pipeline itself can be a NAT client. That is, the Pipeline can translate an address for itself as long as it is not translating addresses for other clients on the local LAN.
- Make sure to set Ignore Def Rt=Yes. When NAT is active, it routes using its own default route. Configuring the Pipeline to ignore default routes avoids the possibility that a default route from the ISP will overwrite the NAT route.

Location: Ethernet > NAT > NAT

See Also: Def Server, Dst Port # (Static Mapping), Loc Adrs, Loc Port#, Lan, Routing, Protocol (Static Mapping)

Save Cfg

Description: Enables you to save all Pipeline profiles (except Security Profiles) to disk.

The process does not save passwords; that is, the Save Cfg command does not save the Send PW and Recv PW parameters in a Connection profile, or the Passwd parameter in a Security profile or an Ethernet profile.

Usage: Follow these instructions to save your configuration:

1 Enable the Download parameter in the Security profile (Download=Yes).

2 Verify that your terminal emulation program has a disk capture feature; this feature enables your emulator to capture to disk the ASCII characters it receives at its serial host port.

3 Verify that your terminal emulation program has an autotype feature; this feature enables your emulator to transmit over its serial host port the contents of a file it has built through disk capture.

4 Connect the backup device to the Pipeline Control port.

5 Set the data rate of your terminal emulation program to 9600 baud or lower.

6 Set the Term Rate parameter in the System profile to 9600.

7 Select Save Cfg from the Sys Diag menu.

8 Turn on the autotype function on your emulator, and start the save process by typing any key on the emulator.

9 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.

10 Turn off the autotype feature.

Location: System > Sys Diag

See Also: Restore Cfg

Sec DNS

Description: Specifies the IP address of the secondary domain name server.

Domain Name System (DNS) is a TCP/IP service that enables you to specify a symbolic name instead of an IP address. A symbolic name consists of a username and a domain name in the format *username@domain name*. The *username* corresponds to the host number in the IP address. The *domain name* corresponds to the network number in the IP address. A symbolic name might be steve@abc.com or joanne@xyz.edu.

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

Usage: Press Enter to open a text field. Then, type the IP address of the secondary domain name server.

The address consists of four numbers between 0 and 255, separated by periods. The default value is 0.0.0.0. Accept this default if you do not have a secondary domain name server.

Press Enter again to close the text field.

Example: `200.207.23.1`

Dependencies: The Sec DNS parameter applies only to Telnet connections running under the Pipeline terminal server interface.

Location: Ethernet > Mod Config > DNS

See Also: Domain Name, Pri DNS

Sec Domain Name

Description: Specifies a secondary domain name that the Pipeline can search using DNS. The Pipeline 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

Sec History

Description: Specifies the number of seconds the Pipeline uses as a sample for calculating average line utilization (ALU) of transmitted data; the Pipeline arrives at this average using the algorithm specified by the Dyn Alg parameter.

When ALU exceeds the Target Util threshold for a period of time greater than the value of the Add Pers parameter, the Pipeline attempts to add a channel.When ALU falls below the Target Util threshold for a period of time greater than the value of the Sub Pers parameter, the Pipeline attempts to remove a channel.

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 Pipeline 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.

Usage: Press Enter to open a text field. Then, type 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. Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- The Sec History parameter applies only to dynamic MP+ calls (Encaps=MPP).
- 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.

Location: Ethernet > Answer > *any profile* > PPP Options; Ethernet > Connections > *any profile* > Encaps Options

See Also: Add Pers, Dyn Alg, Encaps, Sub Pers, Target Util

Secondary

Description: Specifies a secondary Connection profile to be dialed in the event that a session using the primary Connection profile cannot be established.

Usage: Press Enter to open a text field. Then, type the name of the secondary Connection profile. The name you specify must match the value of the Name parameter in a local Connection profile.

Dependencies: Keep this additional information in mind:

- Secondary Profiles cannot be chained. That is, secondary Connection Profiles cannot also have Secondary Connection profiles.
- Do not confuse the Secondary parameter with the Backup parameter. A BackUp Connection profile is used to re-establish an existing connection that has terminated; a Secondary Connection profile is used to establish a new connection if the primary Connection profile cannot.

- Parameters that you define in the primary Connection profile do not automatically apply to the secondary Connection profile.

  For example, if you set the primary Connection profile to filter Telnet packets, you must set the secondary profile to filter Telnet packets as well.
- Outgoing Frame Relay packets are the only packets that follow the primary Connection profile definitions. All other packets follow the backup Connection profile definitions.

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

See Also: Backup

Security

Description: Specifies whether the Pipeline enables trapping of particular system events.

Usage: The Security parameter in this profile enables you to specify whether the Pipeline traps these events:

- authenticationFailure

  This event occurs when authentication has failed. See RFC-1215 for a full explanation of this event.
- consoleStateChange

  This event occurs when a VT100 or Telnet port changes its state.

Press Enter to toggle between Yes and No.

- Yes specifies that the Pipeline traps the events.
- No specifies that the Pipeline does not trap the events.

  No is the default.

Location: Ethernet > SNMP Traps > *any profile*

See Also: Comm, Dest

Send Auth

Description: Specifies the authentication protocol that the Pipeline requests when initiating a connection using PPP or MP+ encapsulation. The answering

side of the connection determines which authentication protocol, if any, the connection uses.

Usage: Press Enter to cycle through the choices.

- None specifies that the Pipeline does not request an authentication protocol for outgoing calls.

  None is the default.

- PAP (Password Authentication Protocol) is a PPP authentication protocol.

  PAP provides a simple method for the Pipeline to establish its identity in a two-way handshake. Authentication takes place only upon initial link establishment, and does not use encryption.

  If you choose PAP, the Pipeline requests this protocol for authentication. The remote device must support PAP.

  Note that if you choose this setting, the Pipeline requests PAP authentication but will use CHAP authentication if the called unit requires CHAP. Choose this setting for non-token card authentication if you would allow sending your password unencrypted.

- CHAP (Challenge Handshake Authentication Protocol) is a PPP authentication protocol. If you choose CHAP, the Pipeline requests this protocol for authentication. The remote device must support CHAP.

  CHAP is more secure than PAP. CHAP provides a way for the remote device to periodically verify the identity of the Pipeline using a three-way handshake and encryption. Authentication takes place upon initial link establishment; a device can repeat the authentication process any time after the connection is made.

  Note that if you choose this setting, the Pipeline will not bring up the connection using PAP. Choose this setting for non-token card authentication if you do not wish to send your password unencrypted; that is, if you do not wish to be authenticated through PAP.

- PAP-TOKEN is an extension of PAP authentication. This requires the following:

  – the Network Access Server (NAS) must be running the Ascend RADIUS daemon

  – there is a RADIUS profile that matches the caller's name

  – the RADIUS profile accesses an ACE or SAFEWORD authentication server

In PAP-TOKEN, the user making outgoing calls from the Pipeline authenticates his or her identity by entering a password derived from a hardware device, such as a hand-held security card. The Pipeline prompts the user for this password, possibly along with a challenge key. The NAS obtains the challenge key from a security server that it accesses through RADIUS.

RADIUS (Remote Authentication Dial In User Service) is a protocol by which users can have access to secure networks through a centrally managed server. You can store virtually all Connection profile information on the RADIUS server in a flat ASCII database.

- PAP-TOKEN-CHAP is nearly identical to PAP-TOKEN. This requires the following:
  - the NAS be running the Ascend RADIUS daemon
  - there is a RADIUS profile that matches the caller's name
  - the RADIUS profile accesses an ACE or SAFEWORD authentication server
  - the user profile must specify an auxiliary password (Ascend-Receive-Secret) that matches the Aux Send PW parameter in the Connection profile.

    Note that if Aux Send PW and Ascend-Receive-Secret do not match, it does not prevent the initial connection from succeeding, but the Pipeline cannot extend an MP+ call beyond a single channel.

  In all authentication protocols, including PAP-TOKEN and PAP-TOKEN-CHAP, the Pipeline individually authenticates all channels of an MP+ call. If 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 Pipeline 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 at the remote site. This requires the following:
  - the NAS must be running the Ascend RADIUS daemon

– there is a RADIUS user profile that matches the caller's name

– the RADIUS user profile accesses an ACE or SAFEWORD authentication server

– the RADIUS user profile must specify an auxiliary password (Ascend-Receive-Secret) which matches the Send PW parameter in the Connection profile and defines Ascend-Token-Expiry in its first line.

Note that if Send PW and Ascend-Receive-Secret do not match, it does not prevent the initial connection from succeeding, but subsequent connections (specifically, disconnecting/reconnecting or adding channels) fail until the cached token expires.

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.

Dependencies: Keep this additional information in mind:

- The link must use PPP or MP+ encapsulation (Encaps=PPP or Encaps=MPP).
- If you request PAP or CHAP, you must also specify a password using Send PW in a Connection profile.
- On a nailed-up link (Call Type=Nailed), you must set Recv Auth and Send Auth to the same value at both ends of the connection; that is, Recv Auth at the local and remote ends, and Send Auth at the local and remote ends, must all contain the same value.
- For information on prompting the user for his or her password at the Pipeline terminal server, see the description of the `set password` command in the *User's Guide*.
- For information on prompting for a password at a host, see the APP Server, APP Host, and APP Port parameters.
- Dial Brdcast must be enabled when a PC on the same Ethernet as the Pipeline runs APPSRVR1 or APPSRVR2 to open a connection protected by security-card authentication.

Location: Configure; Ethernet > Connections > *any profile* > 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 Pipeline sends to the remote end of a connection on outgoing calls. If the password specified by Send PW does not match the remote end's value for Recv PW, the remote end disconnects the link.

Usage: Press Enter to open a text field. Then, type the password that the remote end requires the Pipeline to send.

You can enter up to 20 characters; the password is case sensitive. Leave the field blank if the remote end does not require a password.

Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- You must specify a value for Send PW when the link uses PPP encapsulation (Encaps=PPP or Encaps=MPP) and the Pipeline uses PAP, CHAP, or CACHE-TOKEN authentication (Send Auth=PAP, Send Auth=CHAP, or Send Auth=CACHE-TOKEN).

  When you choose Encaps=MPP, both the dialing side and the answering side of the link must support MP+. If only one side supports MP+, the connection uses MP or standard single-channel PPP. When you choose Encaps=PPP, the connection uses only PPP.

Location: Configure; Ethernet > Connections > *any profile* > Encaps Options

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

Server

Description: Specifies a Bootstrap Protocol (BOOTP) server for handling BOOTP requests. If a server is on the same local-area network as the Pipeline, 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 Pipeline are relayed to the remote server.

Note: This parameter appears twice. Each copy can be used to specify a different BOOTP server.

Usage: Press Enter to open a text field and then type the IP address of the BOOTP server. When you're done, press Enter to close the text field.

Dependencies: If you specify two BOOTP servers, the Pipeline 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.

Location: Ethernet > Mod Config > BOOTP Relay

See Also: BOOTP Relay Enable

Server Name

Description: Appears in an IPX Routes profile and an IPX SAP Filter profile. Its functionality differs depending on the profile.

- In an IPX Routes profile, specifies the name of an IPX server.
- In an IPX SAP Filters profile, specifies the name of a NetWare server to be excluded from or included in the Ascend unit's service table.

Usage: You usage differs depending on the profile.

IPX Routes profile

Press Enter to open a text field. Then, type the name of an IPX server. You can enter up to 48 characters, and you must limit your specification to uppercase letters, numbers, and the underscore symbol. Press Enter again to close the text field.

Note: You can specify a route to a destination IPX network without defining an IPX server name. To do so, enter the network number (for example, Network=00123456) without specifying the Server Name and Server Type.

IPX SAP Filter profile

Press Enter to open a text field. Then, type the server's name. You can specify letters, digits, and the underscore, up to a maximum of 20 characters. The wildcard characters "*" and "?" may be used for partial name matches. Press Enter again to close the text field.

Dependencies: For the Server Name parameter to apply in an IPX Route profile, you must enable IPX routing in the Connection profile by setting Route IPX=Yes.

Location: Ethernet > IPX Routes > *any profile*; Ethernet > IPX SAP Filter > *any profile*

See Also: Route IPX, Server Type

Server Type

Description: Appears in an IPX Route profile and an IPX SAP Filter profile. Its functionality differs depending on the profile:

- In an IPX Route profile, specifies the SAP (Service Advertising Protocol) service type for the server.
- In an IPX SAP Filters profile, specifies the SAP Service Type that will be excluded from or included in the service table.

Usage: Your usage differs depending on the profile.

IPX Route profile

Press Enter to open a text field. Then, type a valid SAP service type for the server. The SAP service type for a NetWare server is type 4. Press Enter again to close the text field.

For information on SAP service types, refer to your Novell NetWare documentation.

IPX SAP Filter profile

Press Enter to open a text field. Then type a hexadecimal number. You can enter a number from 1 to FFFE. The default value is 0. Press Enter again to close the text field.

Location: Ethernet > IPX Routes > *any profile*; Ethernet > IPX SAP Filter > *any profile*

See Also: Server Name, Type, Valid (Filter)

See Also:

Shared Prof

Description: Enables multiple incoming calls to share a local Connection profile.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that multiple incoming calls can share a local Connection profile.

  The Pipeline must first authenticate the caller by using the Name and Recv PW parameters in the profile. If an incoming call has an IP address that conflicts with an existing caller IP address the Pipeline rejects the call.
- No specifies that multiple incoming calls cannot share a local Connection profile.

  No is the default.

Location: Ethernet > Mod Config

See Also: Encaps, Name, Recv PW

Socket

Description: Specifies the socket number of the NetWare server.

Usage: Press Enter to open a text field. Then, type the socket number for the server. You should advertise only those NetWare servers that have well-known socket numbers. Press Enter again to close the text field.

Example: `DE040600`

Dependencies: For the Socket parameter to apply, you must enable IPX routing in the Connection profile by setting Route IPX=Yes.

Location: Ethernet > IPX Routes > *any profile*

See Also: Route IPX

See Also:

Split Code.User

Description: Enables the name of the Pipeline to change to the name of the user who is attempting to authenticate with an Ascend RADIUS server using CACHE-TOKEN using CHAP to a token-based security system. Used when multiple users on a LAN need to authenticate.

Usage: When using Split Code.User, the user enters his or her passcode and name at the authentication prompt two times (at two prompts). The first time the name of the Pipeline changes to the user's name. The second time, the user's passcode and name are interpreted by the authentication server.

Dependencies: Only use this parameter with CACHE-TOKEN and CHAP authentication in conjunction with an Ascend RADIUS server and a token card system.

Location: Ethernet > Connections > *profile* > Encaps.

Src Adrs

Description: In a filter of type IP, specifies the source address to which the Pipeline compares a packet's source address.

Usage: Press Enter to open a text field. Then, type the source address the Pipeline should use for comparison when filtering a packet. The address consists of four numbers between 0 and 255, separated by periods.

The null address 0.0.0.0 is the default; this setting matches all packets.

Press Enter to close the text field.

Example: `200.62.201.56`

Dependencies: Src Adrs does not apply (Src Adrs=N/A) if you are using a generic filter (Type=Generic) or if you have not activated the IP filter (Valid=No).

Location: Ethernet > Filters > *any type of filter* > *input or output filter* > *any numbered filter* > Ip

See Also: Src Mask

Src Mask

Description: In a filter of type IP, specifies the bits that the Pipeline should mask when comparing a packet's source address to the value of the Src Adrs parameter. The masked part of an address is hidden; the Pipeline does not use it for comparisons with Src Adrs. A mask hides the part of a number that appears behind each binary 0 (zero) in the mask; the Pipeline uses only the part of a number that appears behind each binary 1 for comparison.

The Pipeline applies the mask to the address using a logical AND after the mask and address are both translated into binary format.

Usage: Press Enter to open a text field. Then, type the IP mask in dotted decimal format. The value 0 (zero) hides all bits, because the decimal value 0 is the binary value 00000000; the value 255 does not mask any bits, because the decimal value 255 is the binary value 11111111.

The null address 0.0.0.0 is the default; this setting indicates that the Pipeline 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 Pipeline uses for comparison.

Press Enter to close the text field.

Example: Suppose a packet has the source address 10.2.1.1. If Src Adrs=10.2.1.3 and Dst Mask=255.255.255.0, the Pipeline masks the last digit and uses only 10.2.1, which matches the packet.

Dependencies: Src Mask does not apply (Src Mask=N/A) if you are using a generic filter (Type=Generic) or if you have not activated the IP filter (Valid=No).

Location: Ethernet > Filters > *any type of filter* > *input or output filter* > *any numbered filter* > Ip

See Also: Src Adrs

Src Port

Description: In a filter of type IP, specifies the source port number to which the Pipeline compares the packet's source port number.

The Src Port Cmp criterion determines how the Pipeline carries out the comparison.

Usage: Press Enter to open a text field. Then, type the number of the source port the Pipeline should use for comparison when filtering packets. You can enter a number between 0 and 65535.

The default setting is 0 (zero); this setting means that the Pipeline forwards all packets.

Press Enter to close the text field.

Example: `25`

Port 25 is reserved for SMTP, so 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 sessions.

Location: Ethernet > Filters > *any type of filter* > *input or output filter* > *any numbered filter* > Ip

See Also: Dst Port # (Filters), Src Port Cmp

Src Port Cmp

Description: In a filter of type IP, specifies the type of comparison the Pipeline makes when filtering for source port numbers using the Src Port # parameter.

Usage: Press Enter to cycle through the choices.

- None specifies that the Pipeline does not compare the packet's source port number to the value specified by Src Port #.

  None is the default.
- Less specifies that port numbers with a value less than the value specified by Src Port # match the filter.
- Eql specifies that port numbers equal to the value specified by Src Port # match the filter.
- Gtr specifies that port numbers with a value greater than the value specified by Src Port # match the filter.
- Neq specifies that port numbers not equal to the value specified by Src Port # match the filter.

Dependencies: Keep this additional information in mind:

- This parameter works only for TCP and UDP packets.

  You must set Src Port Cmp=None if the Protocol parameter is not set to 6 (TCP) or 17 (UDP).
- Src Port Cmp does not apply (Src Port Cmp=N/A) if you are using a generic filter (Type=Generic) or if you have not activated the IP filter (Valid=No).

Location: Ethernet > Filters > *any type of filter* > *input or output filter* > *any numbered filter* > Ip

See Also: Src Port #

Static Preference

Description: Specifies the preference value for statically configured routes created from IP address pools and the Terminal Server IPROUTE ADD command. When selecting which routes to put in the routing table, the router first compares the Preference value, selecting the lower number. If the Preference values are equal, then the router compares the Metric field, selecting the route with the lower Metric.

Usage: Press Enter to open a text field. Then, type 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."

These are the default values for other types of routes:

- 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 remote device to which the Pipeline makes a connection.

Usage: Press Enter to open a text field. Then, type the name or MAC address of the remote device.

You can enter up to 31 characters.

The value you specify is case sensitive, and must exactly match the name of the remote device. If you are not sure about the exact name, contact the administrator of the remote network.

Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- The Station parameter for the first Connection profile is the same as Rem Name parameter in the Configure menu.
- The Station parameter setting appears in the list of Connection Profiles in the Connection menu; however, if you leave the parameter blank, the LAN Adrs setting appears instead.
- The remote device that the Station parameter specifies is the device actually placing or answering the call; it is not necessarily the same as the source or destination of packets using the link.
- The Pipeline does not currently use the Domain Name System (DNS) to determine the IP address of the device specified by the Station parameter.
- When the Pipeline receives a PPP or MP+ call from an Ascend unit, it tries to match the caller's Name to the value of the Station parameter in some Connection profile.

  If the Pipeline finds a match and authentication is turned on, the Pipeline then tries to match the caller's Send PW value to the Recv PW value in that same Connection profile.

Location: Ethernet > Connections > *any profile*

Sub-Adr

Description: Determines how the Pipeline treats incoming calls based on whether they convey an ISDN subaddress.

Usage: Press Enter to cycle through the options.

- Termsel specifies that the Pipeline must use an ISDN subaddress to determine whether a call is answered.

  The called-party number must have a subaddress. Otherwise, the Pipeline ignores the call. If the Pipeline accepts the call, the subaddress becomes part of the incoming phone number.

- None specifies that the Pipeline does not use subaddressing.

Dependencies: Keep this additional information in mind:

- Sub-Adr applies only to ISDN lines.
- Sub-Adr=TermSel is intended for a scenario in which equipment is connected to a multidrop ISDN BRI line.

Location: System > Sys Config

See Also: Dial #

Sub Pers

Description: Specifies the number of seconds average line utilization (ALU) of transmitted data must fall below the threshold indicated by the Target Util parameter before the Pipeline begins removing bandwidth from a session. The Pipeline determines the ALU for a session using the algorithm specified by the Dyn Alg parameter.

When utilization falls below the threshold for a period of time greater than the value of the Sub Pers parameter, the Pipeline attempts to remove a channel. Using 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.

Usage: Press Enter to open a text field. Type a number between 1 and 300. Press Enter again to close the text field.

When the Pipeline is using MP+ (Encaps=MPP), the default value is 10.

Dependencies: Keep this additional information in mind:

- One channel must be up at all times.
- Removing bandwidth cannot (a) cause the ALU to exceed the threshold specified by the Target Util parameter or (b) cause the number of channels to fall below the amount specified by the Min Ch Count parameter.
- Sub Pers in the Answer profile applies to incoming calls for which no Connection profile exists; if a Connection profile exists, the setting of its Sub Pers parameter takes precedence.
- If Profile Reqd=Yes in the Answer profile, Sub Pers does not apply (Sub Pers=N/A) in the Answer profile.
- 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.

Location: Ethernet > Answer > *any profile* > PPP Options; Ethernet > Connections > *any profile* > Encaps option

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

Switch Type

Description: Specifies the network switch type that provides ISDN BRI service to the Pipeline.

A network switch is the central office switch or PBX that terminates the ISDN BRI line at the Pipeline and connects the Pipeline 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:.

Table 3-3. Configure menu switch types

Switch type	Explanation
AT&T/Multi-P	AT&T Multipoint.
AT&T/P-T-P	AT&T Point-to-Point is the default.
AUSTRALIA	Australia and New Zealand
AUTO SPID	Automatically detects the switch and the SPIDs associated with the ISDN numbers. The line 1 and line 2 numbers must be entered. Then the unit connects to the switch, resets the switch parameter to the appropriate value, and then finds the SPIDs. (Only available in North America.)
BELGIUM	Belgium: Pre-Euro ISDN Belgacom Aline
DUTCH	Netherlands 1TR6 version: PTT Netherlands BRI
FRANCE	France: FT Numeris
GERMAN	Germany 1TR6 version: DBP Telecom
IDSL	Identical to AT&T Point-to-Point, but has support for Q.931 en-bloc dialing.
JAPAN	Japan: NTT INS-64
MP GERMAN	Germany: 1TR6 multipoint
NET 3	In the UK, use this switch with integrated voice service. (Please refer to www.ascend.com for the latest information about configuring your unit when using British Telecom ISDN-2 service. Search for “British Telecom” or “ISDN-2”.)

Table 3-3. Configure menu switch types (continued)

Switch type	Explanation
NI-1	National ISDN 1.
NI-2	National ISDN-2
NTI	Northern Telecommunications, Inc. Use this setting if your switch is DMS-100 Custom.
SWISS	Switzerland: Swiss Net 2
U.K.	United Kingdom: ISDN-2 (also see NET 3) Hong Kong: HKT Switchline BRI Singapore: ST BRI Euro ISDN countries: Austria, Belgium, Denmark, Germany, Finland, Italy, Netherlands, Portugal, Spain, and Sweden. Identical to NET 3.

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: Configure

Switch Usage

Description: Enables or disables the serial WAN feature in the Pipeline. If serial WAN is disabled or if the sliding switch on the back panel of the unit is in the Off

position, the Control port of the Pipeline is used only for configuration purposes. If the switch is in the On position (away from the terminal port if the switch is horizontal or down if the switch is vertical) and serial WAN is enabled, all Connection Profiles are sampled once every 10 seconds. If a Connection profile is configured for leased line operation and the Nailed Group parameter in that profile is set to 3, then the Control port is programmed for synchronous HDLC mode and an attempt is made to bring up the connection on that port.

Usage: Press Enter to cycle through the choices.

- Unused (default) means that the sliding switch on the back panel of the unit has no effect.
- Serial WAN means that the terminal port of the Pipeline will be used as the serial WAN port when the sliding switch on the back panel is in the On position

Dependencies: Keep this additional information in mind:

- The sliding switch on the back panel of the unit must be set to the On position for this parameter to take effect.

Location: System > Sys Config

See Also: Activation, Group (Serial WAN)

Sys Reset

Description: Restarts the Pipeline and clears all calls without disconnecting the device from its power source. The Pipeline logs off all users, and returns user security to its default state. In addition, the Pipeline performs power-on self tests (POSTs) when it restarts. These POSTs are diagnostic tests.

A system reset of a Pipeline 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 Ascend unit to the switch will be incorrect.

Usage: To perform a system reset, follow these steps:

1 Select Sys Reset and press Enter.

The Pipeline prompts you to confirm that you want to perform the reset.

2 Confirm the reset.

The Pipeline displays the message `System reset in progress`. In addition to clearing calls, the Pipeline performs a series of POSTs. The POST display appears.

If you do not see the POST display, press Ctrl-L.

While the yellow CON LED on the front panel remains solidly lit, the Pipeline checks system memory, configuration, and line connections. If the Pipeline fails any of these tests, the CON LED remains lit or blinks.

When the tests are complete, this message appears:

```
Power-On Self Test PASSED
```

3 Press any key to display the Main Edit menu.

Location: System > Sys Diag

Syslog

Description: Specifies whether the Pipeline sends warning, notice, and CDR (Call Detail Reporting) records from the system logs to the Syslog host.

CDR is a feature that provides a database of information about each call, including date, time, duration, called number, calling number, call direction, service type, and associated inverse multiplexing session and port. Because the network carrier bills for bandwidth on an as-used basis, and bills each connection in an inverse multiplexed call independently, you can use CDR to understand and manage bandwidth usage and the cost of each inverse multiplexed session.

The Syslog host is the station to which the Pipeline sends system logs.

Usage: Press Enter to toggle between Yes and No.

- Yes enables the Pipeline to send warning, notice, and CDR records to the Syslog host.
- No disables the Syslog host, or specifies that a Syslog host is not available.

  No is the default.

Dependencies: If Syslog=Yes, you must enter the IP address of the Syslog host in the Log Host field.

Location: Ethernet > Mod Config

See Also: Log Facility, Log Host

T391

Description: Specifies the number of seconds between Status Enquiry messages.

Usage: Press Enter to open a text field. Then, type a number between 5 and 30. The default is 10. Press Enter again to close the text field.

Dependencies: The T391 parameter applies only if Link Mgmt=T1.617D and T392 is set to a nonzero value.

Location: Ethernet > Frame Relay > *any profile*

See Also: Link Mgmt

T392

Description: Specifies the number of seconds that the Pipeline waits for a Status Enquiry message before recording an error.

Usage: Press Enter to open a text field. Then, type 0 (zero), or a number between 5 and 30. The default is 15.

If you specify 0 (zero), the Pipeline does not process WAN-side Status Enquiry messages. If you specify a nonzero value, the Pipeline uses T1.617D (a link management protocol defined in ANSI T1.617 Annex D) to monitor another Ascend unit over a nailed-up connection.

Press Enter again to close the text field.

Dependencies: The T392 parameter applies only if Link Mgmt=T1.617D.

Location: Ethernet > Frame Relay > *any profile*

See Also: Link Mgmt

Target Util

Description: Specifies the percent of bandwidth utilization at which the Pipeline adds or subtracts bandwidth dynamically, or specifies the target percentage of bandwidth utilization for an MP+ call (Encaps=MPP).

The Pipeline uses the historical time period specified by the Sec History parameter as the basis for calculating average line utilization (ALU) of transmitted data. It then compares ALU to the amount specified in the Target Util parameter.

When ALU exceeds the threshold defined by Target Util for a period of time greater than the value of the Add Pers parameter, the Pipeline attempts to add a channel. When ALU falls below the threshold defined by Target Util for a period of time greater than the value of the Sub Pers parameter, the Pipeline attempts to remove a channel.

Usage: Press Enter to open a text field. Then, type a number between 0 and 100. Press Enter again to close the text field.

The default is 70. 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.

Dependencies: When selecting a target utilization value, keep these guidelines in mind:

- Monitor how the application behaves when using different bandwidths.

  For example, an application might be able to use 88% of a 64-kbps link, but only 70% of a 256-kbps link.
- Monitor the application at different loads.

Location: Ethernet > Answer > *any profile* > PPP Options; Ethernet > Connections > *any profile* > Encaps Options

See Also: Add Pers, Call Type, Dyn Alg, Sec History, Sub Pers

TCP Estab

Description: In a filter of type IP, specifies whether the filter should match only established TCP connections.

An established TCP connection is one in which the TCP session has already sent its first packet. A not established TCP connection is one in which the TCP sessions has not sent its first packet. Specifically, the first packet is the "connection request" packet which has SYN bit set to 1, while both the ACK and RST bits are set to 0.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that you want the filter to match only those TCP connections that are established.

  Yes causes the filter to accept TCP connection request packets, then begin filtering on the rest of the incoming packets.

- No specifies that you want the filter to match both initial and established TCP connections.

  No is the default.

Dependencies: The TCP Estab parameter does not apply (TCP Estab=N/A) if the Protocol field is set to any value other than 6 (TCP).

Location: Ethernet > Filters > *any type* > *any input or output filter* > *any numbered filter* > Ip

Telnet PW

Description: Specifies the password that you must enter before you can access the Pipeline user interface through Telnet.

Telnet is a protocol used to link two computers in order to provide a terminal with a connection to the remote machine. The remote machine is known as the Telnet host. When you start a Telnet session, you connect to the Telnet host and log in. The connection enables you to work with the remote machine as though you were at a terminal connected to it.

Usage: Press Enter to open a text field. Then, type a password containing up to 20 alphanumeric characters. The default is [].

If you leave Telnet PW blank, the Pipeline does not prompt you for a password. If you specify a password for Telnet PW, you have three tries of 60 seconds each to enter the correct password.

Location: Ethernet > Mod Config > Ether Options

TCP Timeout

Description: Specifies the maximum time a Pipeline will wait to connect to an address in a list provided by a DNS server.

Applies to all TCP connections initiated from the Pipeline, including Telnet, Rlogin, TCP-Clear, and the TCP portion of DNS queries.

Usage: To set the timeout value, select TCP Timeout and enter the number of seconds the Pipeline should wait to connect to an IP address on the DNS list.

- The range of values for TCP timeout is 0 to 200 seconds. This specifies the number of seconds after which the Pipeline will stop attempting to connect to an IP address and will proceed to the next address on the list. Since the first host on the list may not be available, the timeout should be short enough to allow the Pipeline to go on to the next address on the list before the client software times out.

  The default for TCP Timeout is 0.

  Note: There is a built-in maximum number of connect messages the Pipeline will send to attempt to connect to a remote host. When the Pipeline has sent the maximum number of messages to an address on the DNS list it will stop attempting to make a connection to that address, even if the maximum time set in TCP Timeout has not yet elapsed.

- If TCP timeout=0, the Pipeline will retry the connection to the address at increasingly larger intervals until it sends the maximum number of start-connection messages. This takes approximately 170 seconds, but can take longer if the Pipeline is running a large number of other tasks. If the client software times out before the Pipeline makes a connection or proceeds to the next address on the DNS list, the physical connection is dropped.

Dependencies: The List Attempt parameter must be enabled (set it in Ethernet > Mod Config > DNS). List Attempt permits the Pipeline to attempt a series of IP addresses. Note that the List Attempt parameter does not apply if Telnet and Immediate Telnet are both disabled.

Location: Ethernet > Mod Config

Temporary

Description: Specifies whether the Pipeline stops advertising the route to the address in this Connection profile when the session terminates, and whether the Pipeline removes this route and all routes dynamically learned on this connection from the routing table.

Usage: You can specify one of these settings:

- Yes removes a route from the routing table to a connection when the link is off-line, including all routes dynamically learned on this connection, and discontinues advertising the route.

  The routes are advertised and appear in the routing table only when you re-establish the connection.

- No continues to advertise the route to the connection found in the LAN Adrs and WAN Alias parameters, even when the connection is off-line.

  The route appears in the Pipeline's routing table, along with all other routes dynamically learned on this connection. All routes age normally. The default value is No.

Example: Pipeline1 has a nailed connection with an address of 128.50.69.69. Pipeline1 advertises this route when the connection is up. Pipeline1 also learns through RIP that the remote side is advertising 198.5.248.72. If the connection goes down and Temporary=Yes, the Pipeline removes 128.50.69.69 and 198.5.248.72 from its routing table and no longer advertises them. If the connection goes down and Temporary=No, the Pipeline maintains 128.50.69.69 in the routing table (pointing to the idle interface—wanidle), and allows 198.5.248.72 to age normally.

Dependencies: A frame relay link is a nailed-up connection defined in a Connection profile. A frame relay link can also have a designated backup Connection profile; if the link goes down, the Pipeline uses the backup profile for the connection. To specify the backup profile, you use the Backup parameter. For frame relay links, the effect of the Temporary parameter varies depending upon whether the link has an associated backup profile:

- If a frame relay connection goes down and the frame relay link has a backup Connection profile, the Pipeline ignores a setting of Temporary=Yes.

  The Pipeline does not remove routes from the routing table when the frame relay connection goes down.

- If a frame relay connection goes down and the Frame Relay profile does not have a backup Connection profile, the Pipeline follows a setting of Temporary=Yes.

  The Pipeline removes routes from the routing table when the frame relay connection goes down.

Location: Ethernet > Connections > *any profile* > IP Options > Temporary

Term Rate

Description: Specifies the data rate for the Control Monitor port in bits per second.

Usage: Press Enter to cycle through the choices.

- 57600
- 38400
- 19200
- 9600

  9600 is the default.
- 4800
- 2400
- 1200
- 300

Dependencies: Whenever you modify the Term Rate parameter, you must set the data rate of your terminal accordingly.

- When you operate the Pipeline from a local terminal, the most common data rate is 9600 bps.
- If you are managing an Ascend unit remotely, you may want to increase the baud rate on the local terminal to a higher speed for improved performance.

Location: System > Sys Config

Term Serv

Description: Starts a local terminal server session.

The Pipeline supports local terminal server sessions only. A local terminal server session takes place when a terminal (or a computer emulating a terminal) is connected to the Pipeline Terminal port, or when you open a Telnet connection to the Pipeline from a local IP host.

Select the Term Serv command from the Sys Diag menu and press Ctrl-D and select E-Terminal Server from the DO menu.

The Pipeline supports all the common capabilities of standard terminal servers, including Telnet, Domain Name Services (DNS), login and password control, call detail reporting, and authentication services.

Usage: Highlight Term Serv and press Enter to begin the local terminal server session.

Do not use the Term Serv parameter to return to the terminal server command-line interface from a local Telnet session; use Ctrl-D-C instead.

Location: System > Sys Diag

See Also: Telnet PW, Chapter 1, "DO Command Reference"

Tick Count

Description: Identifies 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: In most cases, the default value (12) is appropriate. If you need to change this value, press Enter to open a text field. Then, type an appropriate value. Press Enter again to close the text field.

Dependencies: For the Tick Count parameter to apply, you must enable IPX routing in the Connection profile by setting Route IPX=Yes.

Location: Ethernet > IPX Routes > *any profile*

See Also: Route IPX

Type

Description: Appears in a Filter profile or an IPX SAP Filter profile. Its functionality differs depending on the profile:

- In a Filter profile, specifies how the Pipeline applies a filter to a packet.
- In an IPX SAP profile, specifies whether the filter excludes the service from the service table.

Usage: Your usage differs depending on the profile.

Filter profile

Press Enter to cycle through the choices.

- Generic specifies that the filter examines byte and offset values within a packet, regardless of which protocol is in use.
- Ip specifies that the filter examines the protocol ID number, address, and port specifications in an IP packet.

IPX SAP Filter profile

Press Enter to cycle through the choices.

- Exclude specifies that the filter excludes the service from the service table. Exclude is the default.
- Include specifies that the filter includes the service in the service table.

Dependencies: Keep this additional information in mind:

- In a Filter profile for a filter of type Generic, the Pipeline uses these parameters to specify how the filter operates:
  - Length
  - Mask
  - More
  - Offset
  - Value

- In a Filter profile for a filter of type IP, the Pipeline uses these parameters to specify how the filter operates:
  - Dst Adrs
  - Dst Mask
  - Dst Port #
  - Dst Port Cmp
  - Protocol
  - Src Adrs
  - Src Mask
  - Src Port #
  - Src Port Cmp
  - TCP Estab

Location: Ethernet > Filters > *any type of filter* > *input or output filter* > *any numbered filter*; Ethernet > IPX SAP Filters > *any profile*

See Also: Server Name, Server Type, Station, Validate IP

UDP Cksum

Description: Specifies that the Pipeline generates a UDP checksum whenever it sends out a UDP packet.

Currently the Pipeline uses UDP when generating queries and responses for the following protocols:

- ATMP
- SYSLOG
- DNS
- ECHOSERV
- RIP
- SNTP
- TFTP

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that the Ascend unit generates a UDP checksum when transmitting a UDP packet.

  Specify this setting 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.

- No specifies that the Ascend unit does not generate a UDP checksum when transmitting a UDP packet.

  No is the default. Accept this setting if you plan to use the data integrity guarantee of the Ethernet or PPP checksum only.

Location: Ethernet > Mod Config

Valid (Filter)

Description: Activates or deactivates a filter. Its functionality differs depending on the profile:

- In a Filter profile, the Valid parameter activates or deactivates a call filter or a data filter.
- In an IPX SAP Filter profile, the Valid parameter activates or deactivates the Input filter or the Output filter.

Usage: Press Enter to toggle between Yes and No.

- Yes activates the filter.
- No deactivates the filter.

  No is the default.

Dependencies: Keep this additional information in mind:

- When Valid=No, N/A appears in all fields of the filter specification; therefore, you cannot define a filter specification unless Valid=Yes.
- If you are using more than one filter, set Valid=Yes and Forward=Yes in at least one filter; otherwise, the Pipeline drops all packets.
- To forward all packets, set all filters to Valid=No.

Location: Ethernet > Filters > *any type of filter* > *input or output filter* > *any numbered filter*; Ethernet > IPX SAP Filters > *any profile*

See Also: Server Name, Server Type, Type

Valid (Static Mapping)

Description: This parameter enables or disables the routing of incoming packets for a particular TCP or UDP port to a specific server and port on the local network. This routing, which occurs only in conjunction with network address translation (NAT), is controlled by the parameters in the same Static Mapping nn menu (where nn is a number between 01 and 10).

Note: If you change the value of this parameter or of any of the other parameters in a Static Mapping nn menu, the change does not take effect until the next time a connection is made to the remote network specified in the NAT profile. To make the change immediately, you must terminate the connection to the remote network and then reopen it.

Usage: Press Enter to toggle between Yes and No, press Esc to exit the menu, and then confirm the change when prompted.

- Yes enables the routing of incoming packets specified by the other parameters in the same Static Mapping nn menu.
- No disables the routing of incoming packets specified by the other parameters in the same Static Mapping nn menu.

  No is the default.

  Note: The change does not take effect until the next time the link is brought up. To make the change immediately, bring the link down and back up.

Dependencies: For routing of incoming packets for a particular port to occur, the Routing parameter in the NAT menu must be set to Yes, the Lan parameter in the NAT menu must be set to Single IP Addr, and other parameters in the same Static Mapping nn menu must be set to non-null values:

- The Dst Port# and Loc Port# parameters must be set to values other than 0.
- The Loc Adrs parameter must be set to an address other than 0.0.0.0.

Location: Ethernet > NAT > Static Mapping > Static Mapping *nn* (where *nn* is a number between 01 and 10)

See Also: Def Server, Dst Port # (Static Mapping), Loc Adrs, Loc Port#, Lan, Routing, Protocol (Static Mapping)

Validate IP

Description: When a Pipeline receives a DHCP message requesting an IP address, this parameter determines whether the Pipeline checks to see if the address is already in use. If it is, the Pipeline assigns another address.

Usage: Press Enter to cycle through the choices:

- Yes enables validation of IP addresses.
- No disables validation of IP addresses.

  No is the default.

Dependencies: If DHCP Spoofing and Always Spoof are not both Yes, this parameter is N/A.

Location: Ethernet > Mod Config > DHCP Spoofing

See Also: DHCP Spoofing, Always Spoof

Value

Description: In a filter of type Generic, specifies a 16-bit hexadecimal value to compare against the data contained within the specified bytes in a packet. You specify the bytes using the Length, Offset, and Mask parameters.

Usage: Press Enter to open a text field. Then, type a hexadecimal number. You can enter a number from 00 to ffffffffffffffff.

The default is 00. When you accept the default, the bytes must contain nothing to match the filter.

Press Enter again to close the text field.

Example: `e0e0030000000000`

Dependencies: Keep this additional information in mind:

- The Pipeline 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.

Location: Ethernet > Filters > *any type of filter* > *input or output filter* > *any numbered filter* > Generic

See Also: Length (Filter), Mask, Offset

Version

Description: 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 router. Secure Access Manager (SAM) checks the version number before uploading a firewall. In the event that a router with a stored firewall profile receives a code update that make the existing firewall incompatible, a default firewall is enabled, permitting only Telnet access to the Pipeline.

Usage: This parameter cannot be edited.

Location: Ethernet > Firewalls > *any firewall*

VJ Comp

Description: Turns TCP/IP header compression on or off. VJ Comp stands for Van Jacobson Compression.

Usage: Press Enter to toggle between Yes and No.

- Yes turns on TCP/IP header compression for both ends of the link.

  Yes is the default. The Ascend unit must include the optional compression module.
- No turns off TCP/IP header compression.

Dependencies: Keep this additional information in mind:

- VJ Comp applies only to packets in TCP applications, such as Telnet.

  Telnet is a protocol used to link two computers in order to provide a terminal with a connection to the remote machine. The remote machine is known as

the Telnet host. When you start a Telnet session, you connect to the Telnet host and log in. The connection enables you to work with the remote machine as though you were at a terminal connected to it.

- Turning on header compression is most effective in reducing overhead when the data portion of the packet is small.

Location: Ethernet > Answer > *any profile* > PPP Options; Ethernet > Connections > *any profile* > Encaps Options

WAN Alias

Description: Specifies the IP address of the link's remote interface to the WAN.

The WAN Alias parameter applies only if the remote end of a link uses an implementation of PPP that requires that both ends of a WAN connection be on the same subnet.

If a router requires an IP number for each interface over which it sends or receives packets, that router is said to use numbered interfaces. The WAN Alias parameter assigns a single IP number to all WAN lines connected to the Pipeline. Furthermore, the Pipeline assumes that all devices using numbered interfaces have agreed on the network number of the WAN; that is, if 10.0.2.1 is the Pipeline interface to the WAN, then the WAN has a network number 10.0.2.0 and all other devices using numbered interfaces agree to have a 10.0.2.*x* address.

Usage: Press Enter to open a text field. Then, type the IP address of the remote device.

An IP address consists of four numbers between 0 and 255, separated by periods. If a netmask is in use on the network, you must specify it. Separate the netmask from the IP address with a slash.

The default is 0.0.0.0/0.

Press Enter again to close the text field.

Example: `200.207.23.7/24`

Dependencies: The WAN Alias parameter does not apply if the Pipeline does not support IP (Route IP=No).

Location: Ethernet > Connections > *any profile*

See Also: Route IP, Route

Status Window Reference

4

This chapter lists the Pipeline status windows. Each listing provides information in this format:

Window Name

Description: The Description text explains the menu.

Usage: The Usage text explains how to interpret the menu display.

Dependencies: The Dependencies text tells you what other information you need to interpret status menu information.

See Also: The See Also text points you to related information.

Status window listing

Dyn Stat

Description: The Dyn Stat menu shows the name, quality, bandwidth, and bandwidth utilization of each online connection.

Usage: This screen shows an example Dyn Stat display:

```
20-500 Dyn Stat
Qual Good 00:02:03
56K     1 channels
CLU  12%  ALU  23%
```

You can press the Down Arrow key to see other connections; more than one connection can be online at once.

Each line of the menu is described in the following paragraphs.

Line 1

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

Line 2

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 Pipeline reports the duration in number of days. The link quality can have one of the values listed in Table 4-1.

Table 4-1. Link quality values

Value	Description
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.

Line 3

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

Line 4

The last line displays these values:

- CLU

  CLU specifies the current line utilization—the percentage of bandwidth currently being used by the call, divided by the total amount of bandwidth available.

- ALU

  ALU specifies the average line utilization—the average amount of available bandwidth used by the call during the current history period as specified by the Sec History and Dyn Alg parameters.

Dependencies: The Dyn Stat menu applies only to links whose Encaps parameter in the Connection Profile has the value MPP.

See Also: Dyn Alg, Encaps, and Sec History in Chapter 3, "Parameter Reference."

Ether Stat

Description: The Ether Stat menu displays the number of Ethernet frames received and transmitted and the number of collisions at the Ethernet interface.

Usage: This screen shows an example Ether Stat display:

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

The screen contains the following fields:

- Rx Pkt

  Displays the number of Ethernet frames received from the Ethernet interface.

- Col

  Indicates the number of collisions detected at the Ethernet interface.

- Tx Pkt

Specifies the number of Ethernet frames transmitted over the Ethernet interface.

Dependencies: Keep this additional information in mind:

- The counts return to zero when the Pipeline is switched off or reset; otherwise, the counts continuously increase up to the maximum allowed by the display.

HW Config

Description: The HW Config menu displays the hardware installed on the Pipeline.

Usage: This screen shows an example HW Config display:

```
00-400 HW Config
>BRI Interface
 Adrs: 00c07b547960
 Enet I/F: AUI
```

This screen contains the following fields:

- BRI interface

  The type of interface used.

- Adr

  MAC address of the Pipeline

- Enet I/F

  The Ethernet interface you are using on the Pipeline (UTP or AUI).

Line Status

Description: The Line Status menu shows the dynamic status of each WAN line, the condition of its electrical link to the carrier, and the status of each line's individual channels. The Link Status menu appears only if an ISDN line is installed.

For a Serial WAN connection, the 10-100 Line Status window contains a field next to the Link field that indicates the presence of the V.35 port and its status. The Pipeline monitors CTS and DTR signals to determine the link integrity.

If the V.35 port is present but inactive, a Line Status window similar to the following is displayed

```
10-100 1
Link   D   V.35
B1     *.....
B2     *.....
```

If the V.35 port is present and active, a Line Status window similar to the following is displayed

```
10-100 1
Link   D   V.35
B1     *....*
B2     *.....
```

If the Loop Back parameter in the Nailed T1 Mod Config profile is set to Normal, a Line Status window similar to the following is displayed

```
10-100 1   T1/CSU
Link   X   CARRIER
B1     *.....
B2     *.....
:
```

If Loop Back parameter in the Nailed T1 Mod Config profile is set to Loopback, a Line Status window similar to the following is displayed

```
10-100 1   T1/CSU
Link   X   LOOPBACK
B1     *.....
B2     *.....
:
```

```
10-100 1
Link   P
B1     ***.....
B2     ***.....
```

Each line of the menu is described in the following paragraphs.

Line 1

The first line of the Line Status menu contains the menu number of lines connected and whether the nailed T1 line contains a DSU or CSU.

Line 2

The second line of the Line Status menu uses one-character abbreviations to characterize the overall state of the line. Table 4-2 lists the abbreviations.

Table 4-2. Line status abbreviations

Abbreviation	Description
A	Line status is up.
P	The line is in a point-to-point active state and is physically connected.
D	The line is in a multipoint active state, initialized in dual-terminal mode, and is physically connected.
L	Line status looped back.
M	The line is in a multipoint active state, initialized in single-terminal mode, and is physically connected.
.	The line is not active at this time, but it is physically connected.
X	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.

Table 4-2. Line status abbreviations (continued)

Abbreviation	Description
-	The line is disabled. The Chan Usage parameter in the Configure Profile is set to disable one of the B channels.
CARRIER	For T1 lines, this indicates the line is active and physically connected.
RED	For T1 lines, this indicates the line is in a Red Alarm/Loss of Sync state. The line is not connected, improperly configured, experiencing a very high error rate, or is not supplying adequate synchronization.
YELLOW	For T1 lines, this indicates the line is a Yellow Alarm state. The Pipeline is receiving a Yellow Alarm pattern. The Yellow Alarm pattern is sent to the Pipeline to indicate that the other end of the line cannot recognize the signals the Pipeline is transmitting.
BLUE	This signal is coming into the Pipeline from the WAN and indicates a problem has been detected. Further, your data has been converted to all ones, which means there are no packets. All the data is unframed and all ones. This is also known as Alarm Indication Signal (AIS) and All Ones. You should contact your Telco service provider because this means there is a problem with the line, rather than the Pipeline.
Loopback	Manual loopback active if the terminal command is executed. Or line loopback is active if an inband signal is received from the network (CO).
DL-GOOD	T1 line is receiving what it is transmitting.
DL-FAIL	T1 line is not receiving what it is transmitting

Line 3 and Line 4

The third and fourth lines describe the state of the B1 and B2 channels, respectively. The state is represented by a single character. Table 4-3 lists each line status character.

Table 4-3. Line status characters

Character	Description
.	The channel is not available because the line is disabled, has no physical link, or does not exist, or because the Chan Usage parameter in the Configure Profile is set to disable one of the B channels.
*	The channel is connected in a current call
-	The channel is currently idle (but in service).
d	The Pipeline is dialing from this channel for an outgoing call.
r	The channel is ringing for an incoming call.
n	The channel is marked Leased in the Configure Profile.

See Also: Chan Usage in Chapter 3, “Parameter Reference.”

Sessions

Description: The Sessions status menu indicates the number of active bridging/routing links. An online link, as configured in the Connection Profile, constitutes a single active session. A session can be PPP encapsulated. The Pipeline treats each multichannel MP+ or MP link as a single session.

Usage: This screen shows the Sessions display when the Ethernet module is installed in expansion slot #5:

```
20-100 Sessions
>5 Active
 O Headquarters
```

Each line of the menu is described in the following paragraphs.

Line 1

The first line specifies the menu number and name of the menu.

Line 2

The second line indicates the number of active sessions.

Line 3 and succeeding lines

The third and all remaining lines indicate the state of each active session, and the name, address, or CLID of the remote end. Each line uses the format *y zzzzz*, where *y* is a session status character and *zzzzz* indicates the name, address, or CLID of the remote device.

Table 4-4 lists the session status characters that can appear.

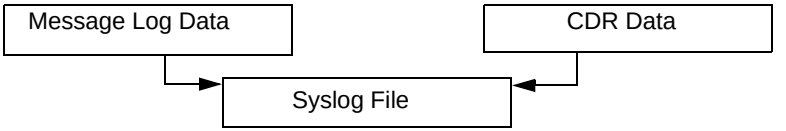
Table 4-4. Session status characters

Character	Description
Blank	No calls exist and no other Pipeline operations are being performed
R	R indicates Ringing; an incoming call is ringing on the line, ready to be answered.
A	A indicates Answering; the Pipeline is answering an incoming call.
C	C indicates Calling; the Pipeline is dialing an outgoing call.
O	O indicates Online; a call is up on the line.
H	H indicates Hanging up; the Pipeline is clearing the call.

Syslog

Description: Syslog is not a Pipeline 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 data and the CDR data.



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

System Events

Description: The System Events Status window provides a log of up to 32 of the most recent system events the Pipeline has recorded.

This example shows a System Event record generated by an incoming call not yet assigned to a channel:

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

The message logs update dynamically. Press the Up Arrow key to display the previous entry. Press the Down Arrow key to display the next entry. To clear all messages from the Message Log while using the Palmtop Controller, enter the SHFT-> command (delete). When you are using the Control Monitor, the Delete key clears all the messages in the log.

The Message Log displays the information described in the following paragraphs.

Line 1

The first line of the menu shows the status menu number and the time the event occurred.

Line 2

The second line identifies the log entry number (M00-M31) and, if applicable, the line and channel on which the event occurred.

Lines are numbered starting with the base system ISDN lines—lines 1 and 2. A T1 or DDS 56 line is line 3.

Line 3

The third line contains the text of the message. The message can contain either basic information or a warning. Table Table 4-5 on page 4-11 lists the possible system event messages.

Table 4-5. System Events

Event Message	Meaning
Busy	Number at other end is busy.
Call Disconnected	The call ended unexpectedly.
Call Refused	An incoming call could not be connected to the specified serial host port because it was busy or otherwise unavailable.
Call Terminated	An active call was disconnected normally, although not necessarily by operator command.
Ethernet Up	Appears after the ethernet interface has been initialized and is running.
Far End Hung Up	The far end terminated the call normally.
Incoming Call	The Pipeline has answered an incoming call at the T1 PRI network interface, but has not yet assigned the call to the IP router.

Table 4-5. System Events (continued)

Event Message	Meaning
Incoming Glare	The Pipeline 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 Configure or Nailed T1 Profile parameters.
Internal Error	Call setup failed because of a lack of system resources, such as insufficient memory. If this type of error occurs, notify the Ascend Technical Assistance Center.
LAN Security Error	An MPP, PPP, or terminal server session is terminated because of a security violation; for example, you entered an incorrect password.
LAN Session Down	Appears before call terminated if a PPP or an MPP session is terminated.
LAN Session Up	Appears after incoming call if a PPP or an MPP session is established.
Missing Wink-start	The switch did not reply with the wink-start signal, either because the line was out of service or because the switch was busy. In either case, the Pipeline could not even start to dial a call over that line.
Network Problem	Call could not be completed because of a network problem.
No Chan Other End	No channel was available on the far end to establish the call.
No Channel Avail	No channel was available for the call.
No Connection	The far end did not answer when the call was dialed.
No Phone Number	There is no phone number entered in the Connection profile from which you tried to place a call.

Table 4-5. System Events (continued)

Event Message	Meaning
No Trunk Available	All lines are out of service.
Not Enough Chans	A request to dial multiple channels or to increase bandwidth could not be completed because there were not enough channels available at that time.
Outgoing Call	The Pipeline has dialed a call.
Remote Mgmt Denied	A request to run the remote Pipeline by remote management was rejected.
Removed Bandwidth	Bandwidth has been subtracted from an active call.
Request Ignored	The request to manually change bandwidth during a call was denied.
Trunk Down	One or more lines are out of service.
Trunk Up	One or more lines were out of service, but have now returned to service.
Wrong Sys Version	The software at the far end is incompatible with the Pipeline system software.

Sys Option

Description: The Sys Option menu provides a read-only list that identifies your Pipeline and names each of the features with which it has been equipped.

Usage: This screen shows the Sys Options menu:

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

The Sys Options menu can contain the information listed in Table 4-6.

Table 4-6. Sys Options information

Option	Description
Security Prof: #	Indicates the Security Profile in use.
Software	Indicates the version of the on-board software.
S/N	Displays the serial number of the unit.
Up	Indicates length of time since the unit was reset.
Access Router	Indicates the name of the product family.
Load	Indicates the name of the binary installed on the unit.
Switched (Installed or Not Installed)	Indicates if calls can be placed over switched circuits.
POTS (Installed or Not Installed)	Indicates if the phone ports are enabled.
FR Rel (Installed or Not Installed)	Indicates if the Frame Relay option is installed
Dyn Bnd (Installed or Not Installed)	Indicates if DBA is available.
Sec Acc (Installed or Note Installed)	Indicates if the Secure Access product is installed.
ISDN Sig (Installed or Not Installed)	Indicates if ISDN signaling is available.
Net Mgmt (Installed or Not Installed)	Indicates if network management is available.
AdvAgent (Installed or Not Installed)	Indicates if Navis Access support is available.

WAN Stat

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

Usage: This screen shows WAN statistics:

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

Each line of the menu is described in the following paragraphs.

Line 1

The first line displays the menu number and name of the menu. 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.

Line 2

The second line specifies the number of received frames.

Line 3

The third line displays the number of transmitted frames.

Line 4

The fourth line indicates the number of corrupt frames. CRC checking is performed on PPP and MP+ links. A corrupt CRC frame contains at least one data error.

ISDN Cause Codes

5

This appendix includes the following topics:

Checking the status windows

ISDN cause codes help you diagnose problems with calls. They appear in the System Events status window:

Refer to the *User's Guide* for administrative information about displaying ISDN line status in the Terminal server.

List of cause codes

The cause codes listed on this table are not valid for German 1TR6 networks. Refer to “1TR6 ISDN cause codes” on page 5-7 for German 1TR6 cause codes.

Note: Cause code implementations can be different depending on how your switch is configured. Consult your ISDN service provider if you have any questions about the cause codes supported for your switch type.

Table 5-1. ISDN cause codes

Code	Cause
0	Valid cause code not yet received
1	Unallocated (unassigned) number.
2	No route to specified transit network (WAN).
3	No route to destination
4	send special information tone
5	misdialed trunk prefix
6	Channel unacceptable.
7	Call awarded and being delivered in an established channel
8	Prefix 0 dialed but not allowed
9	Prefix 1 dialed but not allowed
10	Prefix 1 dialed but not required
11	More digits received than allowed, call is proceeding
16	Normal clearing.
17	User busy.

Table 5-1. ISDN cause codes (continued)

Code	Cause
18	No user responding.
19	No answer from user (user alerted)
21	Call rejected.
22	Number changed.
23	Reverse charging rejected
24	Call suspended
25	Call resumed
26	Non-selected user clearing
27	Destination out of order
28	Invalid number format (incomplete number).
29	Facility rejected.
30	Response to STATUS ENQUIRY.
31	Normal, unspecified.
33	Circuit out of order
34	No circuit/channel available.
35	Destination unattainable
37	Degraded service
38	Network (WAN) out of order.
39	Transit delay range cannot be achieved

Table 5-1. ISDN cause codes (continued)

Code	Cause
40	Throughput range cannot be achieved
41	Temporary failure.
42	Switching equipment congested.
43	Access information discarded.
44	Requested circuit channel not available.
45	Pre-emptied.
46	Precedence call blocked
47	Resource unavailable, unspecified
49	Quality of service unavailable
50	Requested facility not subscribed.
51	Reverse charging not allowed
52	Outgoing calls barred.
53	Outgoing calls barred within CUG
54	Incoming calls barred.
55	Incoming calls barred within CUG
56	Call waiting not subscribed
57	Bearer capability not authorized
58	Bearer capability not presently available.
63	Service or option not available, unspecified.

Table 5-1. ISDN cause codes (continued)

Code	Cause
65	Bearer service not implemented.
66	Channel type not implemented.
67	Transit network selection not implemented
68	Message not implemented
69	Requested facility not implemented.
70	Only restricted digital information bearer capability is available
79	Service or option not implemented, unspecified
81	Invalid call reference value.
82	Identified channel does not exist.
83	A suspended call exists, but this call identity does not
84	Call identity in use
85	No call suspended
86	Call having the requested call identity has been cleared
87	Called user not member of CUG
88	Incompatible destination.
89	Non-existent abbreviated address entry
90	Destination address missing, and direct call not subscribed
91	Invalid transit network selection (national use)
92	Invalid facility parameter

Table 5-1. ISDN cause codes (continued)

Code	Cause
93	Mandatory information element is missing
95	Invalid message, unspecified
96	Mandatory information element is missing.
97	Message type non-existent or not implemented.
98	Message not compatible with call state or message type non-existent or not implemented.
99	information element nonexistent or not implemented
100	Invalid information element contents.
101	Message not compatible with call state
102	Recovery on timer expired.
103	Parameter non-existent or not implemented, passed on
111	Protocol error, unspecified
127	Internetworking, unspecified.

1TR6 ISDN cause codes

All products that support BRI can optionally support 1TR6 switch types. The ISDN cause codes for 1TR6 are different from AT&T, NI-1, NTI switch types and other switch types. Table 5-2 lists the ISDN cause codes for 1TR6 switch types.

Table 5-2. 1TR6 ISDN cause codes

Code	Cause	Explanation
1	Invalid call reference value	Invalid CR value
3	Bearer service not implemented	Service not available in the A-exchange or at another position in the network, or no application has been made for the specified service.
7	Call identity does not exist	Unknown call identity
8	Call identity in use	Call identity has already been assigned to a suspended link.
10	No channel available	No useful channel available on the subscriber access line (only local significance).
16	Requested facility not implemented	The specified FAC code is unknown in the A-exchange or at another point in the network.
17	Request facility no subscribed	Request facility rejected because the initiating or remote user does not have appropriate authorization.
32	Outgoing calls barred	Outgoing call not possible due to access restriction which has been installed.
33	User access busy	If the total made up of the number of free B-channels and the number of calling procedures without any defined B-channel is equal to four, then any new incoming calls will be cleared down from within the network. The calling party receives a DISC with cause “user access busy” (= 1st busy instance) and engaged tone.
34	Negative CUG comparison	Link not possible due to negative CUG comparison.
35	Non existent CUG	This CUG does not exist.

Table 5-2. 1TR6 ISDN cause codes (continued)

Code	Cause	Explanation
37	Communication as semi-permanent link not permitted	Link not possible, e.g. because RFNR check is negative.
48 - 50	Not used	
53	Destination not obtainable	Link cannot be established in the network due to incorrect destination address, services or facilities
56	Number changed	Number of B-subscriber has changed.
57	Out of order	Remote TE not ready
58	No user responding	No TE has responded to the incoming SETUP or call has been interrupted, absence assumed (expiry of call timeout T3AA).
59	User busy	B-subscriber busy
61	Incoming calls barred	B-subscriber has installed restricted access against incoming link or the service which has been requested is not supported by the B-subscriber
62	Call rejected	To A-subscriber: Link request actively rejected by B-subscriber (by sending a DISC in response to an incoming SETUP.) To a TE during the phase in which an incoming call is being established: The call has already been accepted by another TE on the bus.
89	Network congestion	Bottleneck situation in the network; e.g. all-trunks-busy, no conference set free
90	Remote user initiated	Rejected or cleared down by remote user or exchange.

Table 5-2. 1TR6 ISDN cause codes (continued)

Code	Cause	Explanation
112	Local procedure error	In REL: Call cleared due to local errors (invalid messages or parameters, expiry of timeout, etc.) In SUS REJ: The link must not be suspended because another facility is already active. In RES REJ: No suspended call available. In FAC REJ: No further facility can be requested because one facility is already being processed, or the specified facility may not be requested in the present call status.
113	Remote procedure error	Call cleared down due to error at remote end.
114	Remote user suspended	The call has been placed on hold or suspended at the remote end.
115	Remote user resumed	Call at remote end is no longer on hold, suspended or in the conference status.
127	User Info discarded locally	The USER INFO message is rejected locally. This cause is specified in the CON message.

Pipeline Specifications

A

Hardware specifications

Table A-1. Hardware specifications

Dimensions	8.63 in x 6.19 in x 1.25 in 22 cm x 15.7 cm x 3.2 cm
Weight	2.25 lbs 1.13 kg
LAN Interface	10 mbps Ethernet (AUI, 10Base-T) See “Ethernet interface” on page A-5 for a discussion of related equipment required.
WAN Interfaces	BRI U Interface (model: P50-1UBRI) BRI S/T Interface (model: P50-1SBRI)
Software Upgrade	Via built-in flash RAM
Power Requirements	90-130VAC 0.4A 22-24VAC 0.2A 47-63Hz The Pipeline configuration profiles are stored in battery-protected memory. When the Pipeline is turned off, the profiles are not lost. **Note:** Use a protected AC power source, or add surge protection between the power source and the Pipeline.

Table A-1. Hardware specifications (continued)

Environment requirements	For best results, you should house the Pipeline in a room with constant temperature and humidity. In general, cooler environments are better. Operating temperature: 32-104°F or 0-40°C Storage temperatures of -40° to 176° Fahrenheit (-71.4° to 80° Celsius) are acceptable. Altitude: 0-14,800 feet or 0-4,500 meters Relative Humidity: 5-90% (noncondensing) Humidity should be high enough to prevent accumulation of static electricity, but low enough to prevent condensation. An operating relative humidity of up to 90% (non condensing) is acceptable.
Safety Certifications	FCC Class B, CSA, UL
EMI/RF	FCC Part 68, FCC Part 15

Software Specifications

Table A-2. Software specifications

Protocols Supported	TCP/IP, IPX routing, BCP standard bridging of all protocols
WAN Protocols Supported	PPP, Multilink PPP (MP), Multilink Protocol Plus (MP+)
Bandwidth Management	Multilink PPP (MP), Multilink Protocol Plus (MP+), TCP header compression, STAC data compression
Security	PAP, CHAP, MS-CHAP, Callback, Telnet, password, token-based security, CLID, packet filtering, optional Secure Access
Firewall	Firewall Integrated dynamic firewall (optional)
Management	SNMP, Telnet, SYSLOG, Ascend's remote management protocol, direct serial cable connection (DB-9)

Terminal port and cabling pinouts

The Terminal port uses a standard DE-9 female connector that conforms to the EIA RS-232 standard for serial interfaces.

All Pipeline models use the RS-232 pinouts listed in Table A-3.

Table A-3. Terminal port and cabling pinouts

DE-9 pin number	RS-232 signal name	Function	I/O
1	DCD	Data Carrier Detect	O
2	RD	Serial Receive Data	O
3	SD	Serial Transmit Data	I
4	DTR	Data Terminal Ready	I

Table A-3. Terminal port and cabling pinouts (continued)

DE-9 pin number	RS-232 signal name	Function	I/O
5	GND	Signal Ground	
6	DSR	Data Set Ready	O
7	RTS	Request to Send	I
8	CTS	Clear to Send	O
*9	*RI	*Ring Indicator	*O

*Pin 9 is not active (Ring Indication signal not supplied).

Basic Rate interface pinouts

The Pipeline BRI interface is a Western Electric-type RJ-45 port. Connection between this port and the WAN is via a (non-integral) interconnecting cable/ connector set.

Table A-4. ISDN S interface pinouts

BRI Logical Interface	RJ-45 TE (Terminal Equipment)
Transmit (output) + Transmit (output) -	Pin 3 Pin 6
Receive (input) + Receive (input) -	Pin 4 Pin 5
The S interface cable can be up to 1000m in length.	

The pin-outs for the Pipeline U interface BRI port are shown in Table A-5.

Table A-5.ISDN U interface pinouts

BRI Logical Interface	RJ-45 TE (Terminal Equipment)
Transmit (output) + Transmit (output) -	Pin 3 Pin 6
Transmit/Receive (output) + Transmit/Receive (output) -	Pin 4 Pin 5
The U interface cables can be up to 18000 ft (5486m) in length.	

Ethernet interface

A Pipeline supports the physical specifications of IEEE l802.3 with Ethernet 2 (Ethernet/DIX) framing. It provides a single Ethernet interface and can support any one of the following Ethernet types:

- Coax (Coaxial): Thin Ethernet and IEEE 802.3 (10Base-2) with a BNC connector. (Note that the Pipeline is not equipped with a Coax Ethernet interface.)
- 10Base-T (Unshielded Twisted Pair): Twisted pair Ethernet and IEEE 802.3 (10Base-T) with an RJ-45 connector.
- AUI (Attachment Unit Interface): Standard Ethernet and IEEE (10Base-5) with a 15-pin AUI connector.

Required equipment

To install the Ethernet interface, you must have the equipment described in the sections below.

Coax

You need a BNC T-connector. If your connection is at the end of a cable segment, you need a 50 Ohm terminator as well. To install, attach a LAN BNC T-connector to the BNC port on the back of the Pipeline. Use a standard 10Base-250 Ohm cable, such as RG-58 A/U or RG58 C/U.

Caution: Breaking the LAN's continuity by inserting a cable segment or removing either of the 50 Ohm terminations disrupts and disables the Ethernet.

10Base-T

You need an Ethernet adapter installed in your PC. Use the supplied 10Base-T crossover cable to connect the adapter to the Pipeline.

AUI

You need an transceiver unit installed in your PC and a transceiver cable.

Switched-56 interface specifications

This section provides the specifications for the Pipeline Switched-56 interface and covers cabling requirements.

Switched-56 cable specifications

Use only cables specifically constructed for transmission of 4-wire Switched-56 signals. The cables should meet standard attenuation and transmission requirements. The following specifications are recommended:

- 135 Ω
- Two twisted pairs
- 26AWG (or greater diameter) stranded
- 13100 ft (4.0 km) or less

Information required from the Switched-56 provider

Request the following information from your WAN provider. The information you receive characterizes your Switched-56 interface and is required when configuring your Pipeline:

- the phone numbers assigned to your Switched-56 interface, line-by-line
- Nailed-up lines (if any)

T1 interface specifications

This section provides the specifications for the Pipeline T1 interface and covers cabling requirements.

T1 CSU requirements

The Pipeline is equipped with an internal Channel Service Unit (CSU). This means you can connect the port directly to the metallic interface of the WAN.

To avoid harming the WAN, you must contact your carrier for approval before installation. Once you install the Pipeline, you must notify the carrier before disconnecting the Pipeline from the WAN. If you disconnect or turn off the Pipeline without prior notification, the carrier might temporarily discontinue your T1 service.

The Pipeline internal CSUs are compatible with dry-loop T1 lines, and with span-powered or wet-loop powered T1 lines.

Table A-6 lists CSU specifications.

Table A-6. CSU specifications

Information	Value
CSU Registration	TBD
Critical Circuitry Power Source	Dry Loop from local AC power source
Line Capture Frequency	1.544 Mb/s +/- 200 b/s
Line Code	AMI or B8ZS
Line Framing	D4 or ESF
Line Input/Output Impedance	100 Ohms +/- 5%
Received Signal Level Range	DSX-1 level to -27.5 db
Transmitted Signal Level	DSX-1 level into 100 Ohms

Table A-6. CSU specifications (continued)

Information	Value
Line Buildout	0.0, 0.6, 1.2, 1.8, 2.4, 3.0, 7.5, 15.0, or 22.5 db
Pulse Density and Consecutive Zeros Enforcement	In accordance with requirements of AT&T Pub 62411
Line Loopback (LLB) Set Inband Code	(10000) repeating binary pattern
Line Loopback (LLB) Reset Inband Code	(100) repeating binary pattern

Note: During loss of power or whenever the Pipeline restarts, a relay closure returns the T1 signal to the WAN; that is, the T1 line is looped back.

T1 cable specifications

The maximum cable distance between the T1 WAN interface equipment and the Pipeline should not exceed 655 feet (200 m) for a Pipeline without CSUs. Measure the line length and record it when you install the Pipeline.

Use only cables specifically constructed for transmission of T1 signals. The cables should meet standard T1 attenuation and transmission requirements. The following specifications are recommended:

- 100 Ω
- Two twisted pairs, Category 3 or better

The WAN interface cables and plugs described in the following sections are available for the Pipeline's WAN interfaces.

T1 crossover cable: RJ48C/RJ48C

Install this cable when the WAN transmits on pins 5 and 4 and receives on pins 2 and 1.

Table A-7. RJ48C/RJ48C crossover cable specifications

Model number RJ48C-X **Part number 2510-0059-001**			
Pair #	**Signal**	**Male RJ48C**	**Male RJ48C**
1	Receive	2 1	5 4
2	Transmit	5 4	2 1

T1 straight-through cable: RJ48C/RJ48C

Before installing this cable, verify that the WAN transmits on pins 2 and 1 and receives on pins 5 and 4.

Table A-8. RJ48C/RJ48C straight-through cable specifications

Model number RJ48C-S **Part number 2510-0064-001**			
Pair #	**Signal**	**Male RJ48C**	**Male RJ48C**
1	Receive	1 2	1 2
2	Transmit	5 4	5 4

T1 crossover cable: RJ48C/DA-15

Before installing this cable, verify that the WAN transmits on pins 3 and 11 and receives on pins 1 and 9.

Table A-9.RJ48C/DA-15 crossover cable specifications

Model number DB15-X **Part number 2510-0082-001**			
Pair #	**Signal**	**Male RJ48C**	**Male DA-15P**
1	Receive	1 2	3 11
2	Transmit	5 4	1 9

T1 straight-through cable: RJ48C/DA

Before installing this cable, verify that the WAN transmits on pins 1 and 9 and receives on pins 3 and 11.

Table A-10.RJ48C/DA straight-through cable specifications

Model number DB15-S **Part number 2510-0065-001**			
Pair #	**Signal**	**Male RJ48C**	**Male DA-15P**
1	Receive	1 2	1 9
2	Transmit	5 4	3 11

T1 straight-through cable: RJ48C/Bantam

The WAN side of the cable connects to dual bantam jacks.

Table A-11.RJ48C/Bantam straight-through cable specifications

Model number DBNT-RJ45 **Part number 2510-0066-001**			
Pair #	**Signal**	**Male RJ48**	**Male Dual - 310P**
1	Receive	1 2	Tip 1 Ring 1
2	Transmit	5 4	Tip 2 Ring 2

T1 RJ48C-Loopback plug

This plug loops the transmit signal back to the Pipeline.

Table A-12.RJ48C-Loopback plug specifications

Pair #	**Signal**	**Male RJ48C**
1	Receive	1 (connects to 5) 2 (connects to 4)
2	Transmit	5 (connects to 1) 4 (connects to 2)

T1 WAN connectors

Table A-13 lists the pins on the T1 WAN port used for Transmit and Receive. The remaining pins are not connected.

Table A-13.Transmit and Receive pins

T1 interface	RJ48C DTE
Receive (input) pair, Tip (T1) Receive (input) pair, Ring (R1)	Position 2 Position 1
Transmit (output) pair, Tip (T) Transmit (output) pair, Ring (R)	Position 5 Position 4

Pipeline 130 V.35 physical specifications

The Pipeline weighs 1.25 pounds (563 g) and has these dimensions: 1.25" x 8.69" x 6.25" (3.28 cm x 22.1 cm x 15.9 cm). The Pipeline has the following physical interfaces:

Table A-14.Pipeline 130 V.35 physical interfaces

Ports	Function or Operation
Power connector.	For 18 VDC power input.
Terminal (Control) port, type DE-9.	For system management and setup. 9600 bit/s (default), 8 bits per character, no parity bits, no flow control, and 1 stop bit.
One BRI port, type RJ-45, labeled WAN 1.	Far-right port: for BRI access to WAN. Factory options: U interface or S interface.
One V.35 port, type DB-44, labeled WAN 2.	Port adjacent to far-right: for V.35 access to WAN. See the Pipeline user documentation for channel usage restrictions.
Two Ethernet ports, type DA-15 (labeled AUI) and type RJ-45 (labeled UTP (10 BaseT)).	Single Ethernet interface, automatically selected by software when connected.

The table below shows the pinouts for the Pipeline unit's V.35 interface:

Table A-15.Pipeline 130 V.35 pinouts

V.35 Signal	Female DB-44
FGND RI	1 8
SD+ SD-	39 40
RD+ RD-	30 29
ST+ ST-	41 42
RT+ RT-	32 31
TT+ TT-	38 37
DTR DSR	6 11
DCD SGND	9 25
CTS RTS	7 36

Index

Symbols

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

Y