Pipeline 220 VT100 Interface Reference Guide

Ascend Communications, Inc.

Part Number: 7820-0561-001

For software version 5.1Ap5

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
- 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

This guide describes the parameters and commands for the Pipeline 220 VT100 interface.

How to use this guide

This guide contains the following chapters:

- Chapter 1, “DO Command Reference,” describes the DO commands, which allow you to manually connect or disconnect sessions and access the Pipeline configuration interfaces.
- Chapter 2, “Pipeline Alphabetic Parameter Reference,” describes each of the parameters in the VT100 interface.
- Chapter 3, “VT100 Interface System Administration,” explains how to use the VT100 interface to monitor the Pipeline.
- Chapter 4, “Pipeline Diag Command Reference,” describes the Pipeline diagnostic commands.
- Appendix A, “Pipeline Profile Reference, ” contains a complete listing of all the parameters in he VT100 interface grouped by profile.

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.
`Boldface monospace text`	Represents characters that you enter exactly as shown (unless the characters are also in ***`italics`***—see *Italics*, below). If you could enter the characters, but are not specifically instructed to, they do not appear in boldface.

Convention	**Meaning**
Italics	Represent variable information. Do not enter the words themselves in the command. Enter the information they represent. In ordinary text, italics are used for titles of publications, for some terms that would otherwise be in quotation marks, and to show emphasis.
[ ]	Square brackets indicate an optional argument you might add to a command. To include such an argument, type only the information inside the brackets. Do not type the brackets unless they appear in bold type.
|	Separates command choices that are mutually exclusive.
>	Points to the name of an item you select from a menu. This symbol appears between the name of a menu and the name of the item you should select from the menu. (The *menu* does not necessarily appear at the top of the screen. For example, you might open it by clicking a button.)
Key1-Key2	Represents a combination keystroke. To enter a combination keystroke, press the first key and hold it down while you press one or more other keys. Release all the keys at the same time. (For example, Ctrl-H means hold down the Control key and press the H key.)
Press Enter	Means press the Enter, or Return, key or its equivalent on your computer.
Note:	Introduces important additional information.
⚠ **Caution:**	Warns that a failure to follow the recommended procedure could result in loss of data or damage to equipment.
⚡ **Warning:**	Warns that a failure to take appropriate safety precautions could result in physical injury.

Manual set

The Pipeline 220 Documentation Set consists of the following manuals:

- Pipeline 220 User’s Guide

  Explains how to install the hardware and configure the Pipeline using the Java Configurator.
- Pipeline 220 VT100 Interface Guide

  Explains how to use the VT100 user interface to configure the Pipeline 220.
- Pipeline 220 VT100 Interface Reference Guide.

  Describes each command in the VT100 user interface.

Related RFCs

RFCs are available on the Web at http://ds.internic.net.

Information about PPP connections

For information about PPP connections and authentication, you might want to download one or more of the following:

- RFC 2153: *PPP Vendor Extensions*
- RFC 1994: *PPP Challenge Handshake Authentication Protocol (CHAP)*
- RFC 1990: *The PPP Multilink Protocol (MP)*
- RFC 1989: *PPP Link Quality Monitoring*
- RFC 1974: *PPP Stac LZS Compression Protocol*
- RFC 1962: *The PPP Compression Control Protocol (CCP)*
- RFC 1877: *PPP Internet Protocol Control Protocol Extensions for Name Server Addresses*
- RFC 1662: *PPP in HDLC-like Framing*
- RFC 1661: *The Point-to-Point Protocol (PPP)*
- RFC 1638: *PPP Bridging Control Protocol (BCP)*
- RFC 1332: *The PPP Internet Protocol Control Protocol (IPCP)*

Information about IP routers

RFCs that describe the operation of IP routers include:

- RFC 2030: *Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI*
- RFC 2002: *IP Mobility Support*
- RFC 1812: *Requirements for IP Version 4 Routers*
- RFC 1787: *Routing in a Multi-provider Internet*
- RFC 1519: *Classless Inter-Domain Routing (CIDR): An Address Assignment and Aggregation Strategy*
- RFC 1433: *Directed ARP*
- RFC 1393: *Traceroute Using an IP Option*
- RFC 1256: *ICMP Router Discovery Messages*

Information about OSPF routing

For information about OSPF routing, see:

- RFC 1850: *OSPF Version 2 Management Information Base*
- RFC 1587: *The OSPF NSSA Option*
- RFC 1586: *Guidelines for Running OSPF Over Frame Relay Networks*
- RFC 1583: *OSPF Version 2*
- RFC 1246: *Experience with the OSPF protocol*

- RFC 1245: *OSPF protocol analysis*

Information about multicast

For information about multicast, see:

- RFC 1949: *Scalable Multicast Key Distribution*
- RFC 1584: *Multicast Extensions to OSPF*
- RFC 1458: *Requirements for Multicast Protocols*

Information about packet filtering

RFCs that describe firewalls and packet filters include:

- RFC 1858: *Security Considerations for IP Fragment Filtering*
- RFC 1579: *Firewall-Friendly FTP*

Information about general network security

RFCs pertinent to network security include:

- RFC 1704: *On Internet Authentication*
- RFC 1636: *Report of IAB Workshop on Security in the Internet Architecture*
- RFC 1281: *Guidelines for the Secure Operation of the Internet*
- RFC 1244: *Site Security Handbook*

ITU-T recommendations

ITU-T recommendations (formerly CCITT) are available commercially. You can order them at http://www.itu.ch/publications/.

Related publications

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

Here are some related publications that you might find useful:

- William Flanagan. *The guide to T1 Networking*.
- Uyless Black. *Data Link Protocols*
- W. Richard Stevens. *TCP/IP Illustrated*
- William R. Cheswick and Steven M. Bellovin. *Firewalls and Internet Security*

DO Command Reference

1

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

Using DO commands

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

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

To type a DO command, press and release the Ctrl-D combination, and then press and release the next key in the sequence; for example, press 1 to invoke the DO 1 (Dial) command. The PF1 function key on a VT100 monitor is equivalent to the DO key or Ctrl-D.

List of supported commands

Table 1-1 lists the DO commands. Different commands are available in the DO menu depending on your location in the VT100 menus and your permission level.

Table 1-1. DO commands

Command	Description
Close Telnet (DO C)	Close the current Telnet session.
ESC (DO 0)	Abort and exit the DO menu.
Dial (DO 1)	Establish a connection.
Hang Up (DO 2)	Disconnect a session in progress.
Diagnostics (DO D)	Access the diagnostic interface.

Table 1-1. DO commands (continued)

Command	Description
Termserv (DO E)	Access the terminal server interface.
Load (DO L)	Load parameter values into the current profile.
Menu Save (DO M) 8	Save the VT100 interface menu layout.
Save (DO S)	Save parameter values into the specified profile.
Password (DO P) 9	Log into or out of the Pipeline.

Example use of DO commands to establish and tear down a connection

To manually establish a connection, the Connection profile for that connection must be open or selected in the list of profiles. To tear down a connection, you can either open the Connection profile for the active connection, or tab over to the status window in which that connection is listed. (See Chapter 3, “VT100 Interface System Administration.”)

To manually bring up a connection, proceed as in the following example:

1 Open the Connection profile for the destination you want to establish a session with.

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 a message that the network session is up.

To manually bring down a connection, proceed as in the following example:

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)

The DO Close Telnet command closes the current Telnet session to the Pipeline.

Diagnostics (DO D)

The DO Diagnostics command invokes diagnostics mode. The user must have sufficient privileges in the active Security profile. In diagnostics mode, the VT100 interface displays a command-line prompt:

```
>
```

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

```
> help ascend
```

To exit diagnostics mode and return to the VT100 interface, type quit.

```
> quit
```

Dial (DO 1)

The DO Dial command 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 2, “Pipeline Alphabetic Parameter Reference.”

Esc (DO 0)

The DO ESC command exits the DO menu.

Hang Up (DO 2)

The DO Hang up command ends an online session. Either end of the connection can terminate at any time.

Keep this additional information in mind:

- You must be in an active Connection profile to use this command.
- The DO Hangup command does not appear if you are not logged in with operational privileges.

For related information, see the Operations parameter in Chapter 2, “Pipeline Alphabetic Parameter Reference.”

Load (DO L)

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

```
20-100 Connections
  20-101 Factory
  20-102 Tucson
 >20-103 Memphis
```

When you execute DO Load, this screen appears:

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

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

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

The Connections menu shows the results of the load operation:

```
20-100 Directory
  20-1** Memphis
  20-101 Tucson
 >20-102 Memphis
```

The DO Load command does not appear if you are not logged in with operational privileges. For more information, see the Operations parameter in Chapter 2, “Pipeline Alphabetic Parameter Reference.”

Menu Save (DO M)

The DO Menu Save command saves the entire current VT100 interface layout. The current layout replaces the default layout.

Keep this additional information in mind:

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

  To change the default Edit display, you must configure the Edit parameter in the System profile after using the DO Menu Save command.

For related information, see the Edit parameter in Chapter 2, "Pipeline Alphabetic Parameter Reference."

Password (DO P)

The DO password command 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.
- Auto Logout=Yes in the System profile and you are connected to the VT100 control port.

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

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

For related information, see the Auto Logout and Idle Logout parameters in Chapter 2, “Pipeline Alphabetic Parameter Reference.”

Save (DO S)

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

Keep this additional information in mind:

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

For more information, see the Operations parameter in Chapter 2, “Pipeline Alphabetic Parameter Reference.”

Termserv (DO E)

The DO Termserv command invokes the terminal-server command-line interface. The user must have sufficient privileges in the active Security profile. In terminal server mode, the VT100 interface displays a command-line prompt, by default the prompt is:

```
ascend%
```

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

```
ascend% help
```

For examples that use terminal-server commands, see the *Pipeline 220 Interface Configuration Guide*. To exit terminal server mode and return to the VT100 interface, use the Quit command:

```
ascend% quit
```

Pipeline Alphabetic Parameter Reference 2

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

Numeric

2nd Adrs

Description: Assigns a second IP address to the Ethernet interface. It gives the Pipeline a logical interface on two networks or subnets on the same backbone, a feature called “dual IP.”

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

Example: 2nd Adrs=10.65.212.56/24

Location: Ethernet>Mod Config>Ether Options

See Also: IP Adrs

3rd Prompt

Description: Specifies an optional third prompt for a terminal server login. If this value is null, no third prompt is displayed.

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

Example: 3rd Prompt=Password2>>

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

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

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

Location: Ethernet>Mod Config>TServ Options

See Also: TS Enabled

3rd Prompt Seq

Description: This parameter is not supported on the Pipeline.

A

Activation

Description: In the Serial WAN > Mod Config submenu, selects the signals at the serial WAN port that indicate that the DCE (Data Circuit-Terminating Equipment) is ready to connect. Flow control is always handled by the CTS (Clear To Send) signal. In the Serial Port E1-Nailed > Mod Config, enables or disables the E1 line.

Usage: Specify one of the following values for the Serial WAN port:

- Static specifies that the Pipeline does not use flow control signals because the DCE is always connected.

- DSR Active specifies that the DCE raises the DSR signal when it is ready.
- DSR+DCD specifies that the DCE raises the DSR and DCD signals when it is ready.

Usage: Specify one of the following values for the Nailed-E1 line:

- Enabled activates the E1 line. This is the default.
- Disabled deactivates the E1 line.

Example: Activation=Static

Location: Serial Port E1-Nailed > Mod Config, Serial WAN>Mod Config

Active

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

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

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

Example: Active=Yes

Location: Ethernet>Connections, Ethernet>Frame Relay, Ethernet>Static Rtes

Adv Dialout Routes

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

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

Usage: Specify one of the following values:

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

Example: Adv Dialout Routes=Always

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

Location: Ethernet>Mod Config

Alarm

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

- coldStart (RFC-1215 trap-type 0)

  A coldStart trap signifies that the Pipeline sending the trap is reinitializing itself so that the configuration of the SNMP manager or the unit might be altered.
- warmStart (RFC-1215 trap-type 1)

  A warmStart trap signifies that the Pipeline sending the trap is reinitializing itself so that neither the configuration of SNMP manager or the unit is altered.
- linkDown (RFC-1215 trap-type 2)

  A linkDown trap signifies that the Pipeline sending the trap recognizes a failure in one of the communication links represented in the SNMP manager’s configuration.
- linkUp (RFC-1215 trap-type 3)

  A linkUp trap signifies that the Pipeline sending the trap recognizes that one of the communication links represented in the SNMP manager's configuration has come up.
- frDLCIStatusChange (RFC-1315 trap-type 1)

  A DLCIStatusChange trap signifies that the Pipeline sending the trap recognizes that one of the virtual circuits (to which a DLCI number has been assigned) has changed state; that is, the link has either been created, invalidated, or it has toggled between the active and inactive states.
- eventTableOverwrite (ascend trap-type 16)

  A new event has overwritten an unread event. This trap is sent only for systems that support Ascend's accounting MIB. Once sent, additional overwrites will not cause another trap to be sent until at least one table’s worth of new events have occurred.

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

- Yes causes the Pipeline to generate alarm-event traps and send the trap-PDF to the SNMP host.
- No means alarm-events traps are not generated.

Example: Alarm=Yes

Location: Ethernet>SNMP Traps

Alarm Threshold

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

```
Trap type: TRAP_ENTERPRISE
Code: TRAP_MULTICAST_TREE_BROKEN (19)
Arguments:
1) Multicast group address being monitored (4 bytes),
2) Source address of last heartbeat packet received (4 bytes)
3) Slot time interval configured in seconds (4 bytes),
4) Number of slots configured (4 bytes).
```

```
5) Total number of heartbeat packets received before the Pipeline
started sending SNMP Alarms (4bytes).
```

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

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

Usage: Specify a number.

Example: Alarm Threshold=3

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

Location: Ethernet>Mod Config>Multicast

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

All Port Diag

Description: This parameter is not supported on the Pipeline.

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 prevent clients from using the local DNS servers.

Example: Allow as Client DNS=No

Location: Ethernet>Mod Config>DNS

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

APP Host

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

Usage: Specify the IP address of the authentication server. Separate the optional netmask from the address using a slash. The default value is 0.0.0.0/0. The default setting specifies that no APP server is available.

Example: APP Host=200.65.207.63/29

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

Location: Ethernet>Mod Config>Auth

See Also: APP Server, Send Auth

APP Port

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

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

Example: APP Port=35

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

Location: Ethernet>Mod Config>Auth

See Also: APP Server, Send Auth

APP Server

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

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

- Yes enables the Pipeline to respond to password challenges via the APP Server utility running on a local host.
- No disables the use of the APP Server utility

Example: APP Server=Yes

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

Location: Ethernet>Mod Config>Auth

See Also: Send Auth

AppleTalk

Description: Specifies whether AppleTalk routing is globally enabled.

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

- Yes globally enables AppleTalk routing for the Pipeline.
- No globally disables AppleTalk routing for the Pipeline.

Location: Ethernet > Mod Config

See Also: Route AppleTalk

AppleTalk Router

Description: Specifies whether the Pipeline is an AppleTalk seed or non-seed router. A routed AppleTalk network must have at least one seed router. Appletalk routers can get configuration information such as network range and zone names from seed routers. The Pipeline can act as a seed router for up to 32 Appletalk zones. A non-seed router learns network number and zone information from other routers.

Usage: Specify one of the following values:

- Off (the default). The Appletalk router is disabled.
- Seed. If you configure the Pipeline as a seed router, you must also specify the network range and zone names for the network.
- Non-Seed

Location: Ethernet > Mod Config > Appletalk

See Also: Net End, Net Start, Route Appletalk, Zone Name #*n*

Area

Description: Specifies the OSPF area that this interface belongs to.

Usage: Specify an area ID in dotted-decimal format. The default 0.0.0.0 represents the backbone network.

Example: Area=0.0.0.1

Dependencies: At this release, we recommend that you configure the local and WAN interfaces in the same area.

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

AreaType

Description: Specifies the type of OSPF area this interface belongs to. If a network is large, the size of the database, time required for route computation, and related network traffic become excessive. An administrator can partition an AS into areas to provide hierarchical routing connected by a backbone.

The backbone area is special and always has the area number 0.0.0.0. Other areas are assigned area numbers that are unique within the autonomous system.

Note: You must set the area-type parameter consistently on all OSPF routers within the area.

Usage: Specify one of the following values:

- Normal (the default).
  In a normal OSPF area, the router maintains information about external routes.
- Stub
  For areas that are connected only to the backbone by one ABR (that is, the area has one exit point), there is no need to maintain information about external routes. To reduce the cost of routing, OSPF supports sub areas, in which all external routes are summarized by a default route. Stub areas are similar to regular areas except that the routers do not enter external routes in the area's databases.
- NSSA
  Specifies whether the area is a Not So Stubby Area (NSSA). NSSAs are similar to stub areas, except that they allow limited importing of Autonomous System (AS) external routes. NSSAs use type-7 LSAs to import external route information into an NSSA. NSSAs are described in RFC 1587.

Example: AreaType=Normal

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

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

ASE-tag

Description: Specifies the OSPF ASE tag of this link. The tag is a 32-bit hexadecimal number attached to each external route. This field is not used by the OSPF protocol itself. It may be used by border routers to filter this record.

Usage: Specify a 32-bit hexadecimal number. The factory default is c0:00:00:00.

Example: ASE-tag=c8:ff:00:00

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

ASE-type

Description: Specifies the OSPF ASE type of this link-state advertisement. A type-1 external metric is expressed in the same units as the link-state metric (the same units as interface cost). Type-1 is the default.

A Type-2 external metric is considered larger than any link state path. Use of type-2 external metrics assumes that routing between autonomous systems is the major cost of routing a packet, and eliminates the need for conversion of external costs to internal link-state metrics.

Usage: Specify Type-1 or Type-2.

Example: ASE-type=Type-1

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

See Also: Ospf-Cost

ATMP Gateway

Description: Instructs the Pipeline to send data it receives back from the home network on this connection to the mobile node.

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

- Yes enables the Pipeline to send data it receives back from the home network on this connection to the mobile node.
- No disables this function.

Example: ATMP Gateway=Yes

Dependencies: This parameter is not applicable unless the Pipeline is configured as an ATMP home agent in gateway mode.

Location: Ethernet>Connections>Session Options

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

ATMP Mode

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

Usage: Specify one of the following values:

- Disabled (the default) specifies that ATMP is not enabled.
- Home specifies that this unit is a home agent.
- Foreign is not supported on the Pipeline.
- Both is not supported on the Pipeline.

Example: ATMP Mode=Home

Dependencies: If you set ATMP Mode=Disabled, all other fields in the ATMP Options menu are not applicable.

Location: Ethernet>Mod Config>ATMP Options

See Also: ATMP Gateway, Password, Type, UDP Port

Auth

Description: This parameter is not supported on the Pipeline.

Auth Host #N (N=1–3)

Description: This parameter is not supported on the Pipeline.

Auth Key

Description: This parameter is not supported on the Pipeline.

Auth Pool

Description: This parameter is not supported on the Pipeline.

Auth Port

Description: This parameter is not supported on the Pipeline.

Auth Reset Timeout

Description: This parameter is not supported on the Pipeline.

Auth Send Attr 6,7

Description: This parameter is not supported on the Pipeline.

Auth Src Port

Description: Specifies the source port used to send a remote authentication requests. You can define a source port for all the external authentication services the Pipeline supports. You can specify the same source port for authentication and accounting requests.

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

Example: Auth Src Port=0

Dependencies: This parameter does not apply if external authentication is not in use.

Location: Ethernet>Mod Config>Auth

See Also: Acct Src Port

Auth Timeout

Description: Specifies the number of seconds between retries to the external authentication server.

If the Pipeline is acting as a Defender or SecurID client (which support only one server address), the Pipeline waits the specified number of seconds before assuming that the server has become nonfunctional. For more information about SecurID timeouts, see SecurID Host Retries.

Note: Because remote authentication is tried first if the Local Profiles First parameter set to No, the Pipeline waits for the remote authentication to time out before attempting to authenticate locally. This timeout may take longer than the timeout specified for the connection and could cause all connection attempts to fail. To prevent this, set the authentication timeout value low enough to not cause the line to be dropped, but still high enough to permit the unit to respond if it is able to. The recommended time is 3 seconds.

Usage: Specify a number from 1 to 10. The default is 1.

Example: Auth Timeout=20

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

Location: Ethernet>Mod Config>Auth

See Also: SecurID Host Retires.

Auth TS Secure

Description: This parameter is not supported on the Pipeline.

AuthKey

Description: Specifies an authentication key (a password). for OSPF routing. The value of this parameter is a 64-bit clear password inserted into the OSPF packet header. It is used by OSPF routers to allow or exclude packets from an area. The default value for OSPF is “ascend0”.

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

Example: AuthKey=Ascend

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

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

See Also: AuthType

AuthType

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

Usage: Specify one of the following values:

- None

  Routing exchanges are not authenticated. The 64-bit authentication field in the OSPF header may contain data, but it is not examined on packet reception. When you use this setting, the Pipeline performs a checksum on the entire contents of each OSPF packet (other than the 64-bit authentication field) to ensure against data corruption.

- Simple

  This setting requires that you specify a 64-bit field in the auth-key parameter. Each packet sent on a particular network must have the configured value in its OSPF header 64-bit authentication field. Simple is the default.

Example: AuthType=Simple

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

See Also: AuthKey

Auto Logout

Description: Specifies whether to log out the current User profile and go back to default privileges on loss of DTR from the Control port.

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

- Yes causes the Pipeline to log out the current User profile and go back to default privileges on loss of DTR from the Control port.
- No disables auto-logout.

Example: Auto Logout=Yes

Location: System>Sys Config

B

Backup

Description: This parameter is not supported on the Pipeline.

Banner

Description: Specifies the text to be used as the terminal server login banner.

Usage: Specify the banner text. You can enter up to 84 alphanumeric characters. The default is ** Ascend Pipeline Terminal Server **.

Example: Banner=”Welcome to ABC Corporation”

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

Location: Ethernet>Mod Config

See Also: Remote Conf, TS Enabled

Block Calls After

Description: This parameter is not supported on the Pipeline.

Blocked Duration

Description: This parameter is not supported on the Pipeline.

BOOTP Relay Enable

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

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

- Yes enables the Pipeline to relay BOOTP requests to a server on another network.
- No disables BOOTP relay.

Example: BOOTP Relay Enable=Yes

Dependencies: For the BOOTP relay feature to work, DHCP Spoofing must be disabled.

Location: Ethernet>Mod Config>BOOTP Relay

See Also: Server

Bridge

Description: Enables or disables link-level packet bridging for this connection. If you disable bridging, you must enable routing. Enabling bridging in the Answer profile enables the Pipeline to answer a call that contains packets other than the routed protocols (IP or IPX).

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

- Yes enables the Pipeline to bridge packets across this connection based on the packet's destination MAC address (if specified in a Connection profile) or to answer incoming bridged connections (if specified in the Answer profile).
- No disables link-level bridging.

Example: Bridge=Yes

Dependencies: This parameter does not apply unless Bridging is enabled in the Ethernet profile.

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

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

Bridging

Description: Enables or disables packet-bridging system-wide. It causes the Pipeline unit's Ethernet controller to run in promiscuous mode. In promiscuous mode, the Ethernet driver accepts all packets regardless of address or packet type and passes them up the protocol stack for a higher-layer decision on whether to route, bridge, or reject the packets.

Note: Running in promiscuous mode incurs greater processor and memory overhead than the standard mode of operation for the Ethernet controller. On heavily loaded networks, this increased overhead can result in slower performance, even if no packets are actually bridged.

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

- Yes enables the Pipeline to bridge packets based on MAC addresses by running its Ethernet controller in promiscuous mode, which causes it to accept all packets regardless of packet type or address.
- No disables packet bridging and turns off promiscuous mode in the Ethernet controller.

Example: Bridging=Yes

Location: Ethernet>Mod Config

See Also: Bridge

Buildout

Description: Specifies the line buildout value for T1 lines with an internal Channel Service Unit (CSU). The buildout value is the amount of attenuation 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 build-out value, 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: Check with your carrier to determine the correct value for this parameter. Specify one of the following values (db stands for decibels):

- 0 db (the default)
- 0.6 db
- 1.2 db
- 1.8 db
- 2.4 db
- 3.0 db
- 7.5 db
- 15 db
- 22.5 db

Example: Buildout=0

Dependencies: This parameter is not applicable if the T1 line does not have an internal CSU to connect to the local digital telephone system.

Location: Serial Port T1-CSU > Mod Config

C

Circuit

Description: Circuit specifies an alphanumeric name for a DLCI endpoint. When combined as a circuit, the two DLCI endpoints act as a tunnel—data received on one DLCI bypasses the Ascend router and is sent out on the other DLCI.

A circuit is a permanent virtual circuit (PVC) segment that consists of two DLCI end points and possibly two Frame Relay profiles. It requires two and only two DLCI numbers: data is dropped if the circuit has only one DLCI and if more than two are defined, only two are used. Circuits are defined in two Connection profiles. Data coming in on the DLCI configured in the first Connection profile is switched to the DLCI configured in the second one.

Usage: Specify a name for the circuit, up to 16 characters. The other end-point of the PVC must specify the same name in its Circuit configuration.

Example: Circuit=circuit-1

Dependencies: This parameter applies only to FR_CIR-encapsulated calls.

Location: Ethernet>Connections>Encaps options

See Also: Encaps

Clear Call

Description: Specifies whether the session is cleared when an interactive Telnet or TCP session terminates. If set to No, the user is returned to the terminal server menu when the Telnet or TCP session terminates.

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

- Yes means the Pipeline clears the session when a Telnet or TCP session terminates.
- No means the Pipeline returns the user to the terminal server menu when a Telnet or TCP session terminates.

Example: Clear Call=Yes

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

Location: Ethernet>Mod Config>TServ Options

CLID Fail Busy

Description: Specifies whether to return Busy when Caller ID authentication fails.

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

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

Location: Ethernet>Mod Config>Auth

See Also: Auth

Client

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

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

- Yes means the Pipeline begins handling IGMP client requests and responses on the interface. It does not begin forwarding multicast traffic until the rate limit is set. The Rate Limit parameter specifies the rate at which the Pipeline accepts multicast packets from its clients. It does not affect the MBONE interface.
- No means the Pipeline does not handle IGMP client requests and responses on the interface.

Example: Client=Yes

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

Location: Ethernet>Mod Config>Multicast

See Also: Multicast Forwarding, Mbone profile

Client Assign DNS

Description: Specifies whether client DNS server addresses will be presented while this connection is being negotiated.

Usage: Specify Yes (to use client DNS servers) or No. No is the default.

Example: Client Assign DNS = No

Location: Ethernet>Connections>IP Options

See Also: Client Pri DNS, Client Sec DNS

Client Gateway

Description: Specifies a connection-specific default route to be used for forwarding packets received on this connection. The Pipeline uses this default route instead of the system-wide Default route in its routing table. This route is connection-specific, so it is not added to the routing table.

Note: The Pipeline must have a direct route to the address you specify.

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

Example: Client Gateway=10.1.2.3

Location: Ethernet>Connections>IP Options

Client Pri DNS

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

Clock Source

Description: Specifies whether the T1 or E1 line may be used as the clock source for timing synchronous transmissions. If it is enabled, the line provides timing as long as it is active and not in Red Alarm mode, and the Pipeline runs in recovered loop timing mode. If the Pipeline connects to more than one line, selecting Yes for each one gives the Pipeline the option of using any of the lines as a source of synchronous timing.

Usage: Specify Yes or No. Yes is the default, and is the proper setting for normal operations.

- Yes means the line may be used as the clock source for timing synchronous transmissions.
- No means the line may not be used as the clock source. When this setting is disabled, the Pipeline uses another line for timing or uses its internal clock. This is recommended only when two Pipeline units connect to each other by a crossover cable (with optional T1 repeaters) between their network ports

Example: Clock Source=Yes

Location: Serial Port T1-CSU > Mod Config, Serial Port E1-Nailed > Mod Config

Clr Scrn

Description: Specifies whether the screen is cleared when a terminal server session begins.

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

- Yes means the Pipeline clears the screen when a terminal server session begins.
- No means the Pipeline does not clear the screen.

Example: Clr Scrn=Yes

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

Location: Ethernet>Mod Config>TServ Options

See Also: TS Enabled

Comm

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

Usage: Specify the community name, up to 31 characters. The default is “public.”

Example: Comm=Ascend

Dependencies: If this parameter and the Dest parameter are null, the Pipeline does not generate SNMP traps.

Location: Ethernet>SNMP Traps

See Also: Dest

Compare

Description: Specifies the type of comparison to make between the specified value in a filter and the specified location in the contents of a packet.

Usage: Specify one of the following values:

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

Dependencies: This parameter does not apply if the filter is not Valid or if the filter type is IP.

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

See Also: Length, Mask, Offset, Value, Valid

Connection

Description: Specifies the number of a Connection profile needed to bring up a bridged or routed connection. The Pipeline uses this number to locate the profile and bring up the connection needed to forward packets whose destination address is not on the local network.

If it receives a packet whose destination MAC address is not on the local Ethernet, it looks in the bridging table for a matching MAC address and uses the specified Connection profile to bring up a bridged connection.

If it receives an IPX packet whose destination address is not on the NetWare LAN, it checks its IPX routing table and uses the specified Connection profile to bring up an IPX connection.

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

Usage: Specify a Connection profile number.

Location: Ethernet>Bridge Adrs, Ethernet>IPX Routes

See Also: Route IPX

Console

Description: Specifies the interface established at the VT100 port labeled Control on the back panel of the Pipeline.

Usage: Specify one of the following values:

- Standard means the standard set of edit menus comes up in the VT100 window at system startup. This is the default.
- MIF means MIF (Machine Interface Format) is accessible at system startup. From the MIF interface you can display the edit menus by pressing Ctrl-C, and return to MIF again by using the Use MIF command.
- Limited is not supported on the Pipeline.

Location: System>Sys Config

Contact

Description: Specifies the person or department to contact to report error conditions. This field is SNMP readable and settable.

Usage: Specify the name of the contact person or department. You can enter up to 80 characters.

Example: Contact=rchu

Location: System>Sys Config

See Also: Location

Cost

Description: Specifies the cost of an OSPF link. The cost is a configurable metric that must take into account the speed of the link and other issues. The lower the cost, the more likely the interface will be used to forward data traffic.

With the exception of links to stub networks, the output cost must always be non-zero. A link with a cost of 0xFFFFFF (16777215) is considered non-operational.

In a static route, the interpretation of this cost depends on the type of external metrics set in the ASE-Type parameter. If the Pipeline is advertising type 1 metrics, OSPF can use the specified number as the cost of the route. Type 2 external metrics are an order of magnitude larger. Any type 2 metric is considered greater than the cost of any path internal to the AS (autonomous system).

Usage: Specify a number greater than 0 and less than 16777215. The default is 1 on the Ethernet interface and 10 on the WAN links.

Example: Cost=50

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

D

Data Filter

Description: Specifies the number of a filter used to determine if packets should be forwarded or dropped.

Usage: Specify a number between 0 and 199. The number you enter depends on the whether you are applying a filter you created using the VT100 interface, or a firewall you created using Secure Access Manager (SAM).

If you are applying a filter created using the VT100 interface, enter the last 2 digits of the filter number as it appears in the Filters menu.

If you are applying a firewall created with SAM, add 100 to the last 2 digits of the firewall number as it appears in the Firewalls menu. For example, if the number of your firewall is 90-601, specify 101. The numbering scheme for filters and firewalls is:

- 0 indicates that no filtering is being used (this is the default). with this setting, the Pipeline forwards all data packets.
- 1-99 indicates that a filter created using the VT100 interface is being used.
- 100-199 indicates that a filter created using SAM is being used.

Refer to your SAM documentation for information on downloading firewalls to the Pipeline.

Example: Data Filter=7

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

See Also: Filter

Data Svc

Description: A data service is provided over a WAN line and is characterized by the unit measure of its bandwidth. A data service can transmit either data or digitized voice. The Data Svc parameter specifies the how much bandwidth the Pipeline routes to the host for each channel in the connection.

Note: Either party can request a data service that is unavailable. In this case, the Pipeline cannot establish the session.

Usage: Specify one of the following values:

- 56KR

  The connection contains restricted data, guaranteeing that the data the Pipeline transmits meets the density restrictions of D4-framed TI lines, and connects to the Switched-56 data service. The only service available to lines using inband signaling (T1 or E1 lines containing one or more switched channels) are 56K and 56KR.
- 64K

  The call contains any type of data and connects to the Switched-64 data service.

Location: Ethernet>Connections>Telco Options, Ethernet>Frame Relay

Date

Description: Specifies the month, day, and year. You should set this parameter when installing the Pipeline.

Usage: Specify the current date in the format *month*/*day*/*year*. The default is 00/00/00.

Location: System>Sys Config

DCE N392

Description: DCE N392 specifies the number of errors during DCE N393 monitored events which causes the network side to declare the user side procedures inactive.

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

Example: DCE N392=5

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

Location: Ethernet>Frame Relay

DCE N393

Description: DCE N393 specifies the DCE monitored event count (between 1 and 10).

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

Example: DCE N393=7

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

Location: Ethernet>Frame Relay

DeadInterval

Description: Specifies the number of seconds the Pipeline will wait before declaring its neighboring routers down after it stops receiving the router's Hello packets.

Usage: Specify a number. In a Connection profile, the default is 120 seconds. In the Ethernet profile, the default is 40 seconds.

Example: DeadInterval=240

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

See Also: HelloInterval

Def Server

Description: When the Pipeline is configured to perform network address translation (NAT), it can route packets from a remote network for up to 10 different TCP or UDP ports to specific servers and ports on the local network. This parameter specifies a local server to which the Pipeline routes any incoming packets that are not routed to a specific server and port.

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: Specify the IP address. The default value of 0.0.0.0 to disables routing of packets to a default server.

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 can't 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

See Also: Dst Port#, Loc Adrs, Loc Port#, Lan, Routing, Protocol, Valid

Def Telnet

Description: Specifies whether the Pipeline will interpret a command that does not include a keyword as a hostname for a Telnet command. To display the terminal server command keywords, enter help or a question mark (?) from the terminal server command-line interface.

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

- Yes specifies that the Pipeline interprets any terminal server command that does not begin with a keyword as though it began with the keyword Telnet. (That is, it interprets the string typed at the prompt as a Telnet hostname.)
- No specifies that all terminal server commands must begin with a keyword.

Example: Def Telnet=Yes

Location: Ethernet> Mod Config>TServ Options

Default Zone

Description: Specifies the AppleTalk zone used by a node until another zone name is explicitly selected by the node.

Usage: Specify an Appletalk zone name of up to 33 alphanumeric characters. This name will appear in the AppleTalk Zones window of the Chooser. The default is null.

Dependencies: In the Ascend AppleTalk router, zone names are not case-sensitive. However, since some routers regard zone names as case-sensitive you should be consistent in spelling zone names when you configure multiple connections or routers.

Location: Ethernet > Mod Config > Appletalk

See Also: Zone Name #*n*

Dest

Description: In a Static Rtes profile, Dest specifies the route’s target IP address. This is the destination address that will cause the Pipeline to use this route. In a Static Rtes profile, the default null address indicates the default route, used for all destinations that have no explicit route in the routing table.

In an SNMP Traps profile, Dest is the IP address to which the Pipeline sends traps (the IP address of the station running an SNMP management utility). The default null address means that no traps are sent. If the Comm parameter is also null, traps are turned off altogether.

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

Example: Dest=10.207.23.1

Location: Ethernet>Static Rtes, Ethernet>SNMP Traps

See Also: Gateway

Detect End of Packet

Description: Specifies whether data is buffered internally while the Pipeline attempts to detect a logical packet. In some systems, wholly encapsulating logical packets within TCP can reduce load and latency in downstream applications.

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

- Yes enables logical packet detection, and is controlled by the pattern given in the End Of Packet Pattern parameter.
- No. disables logical packet detection.

Dependencies: Detect End of Packet does not apply unless Encaps is set to TCP-CLEAR in the Connection profile.

Location: Ethernet > Connections > Any Connection profile > Encaps Options submenu.

See Also: Encaps, End of Packet Pattern, Max Packet Length, Packet Flush Time

Disc on Auth Timeout

Description: Enables you to specify whether the Pipeline gracefully shuts down the PPP connection on a timeout from an external authentication server.

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

- Yes causes the Pipeline to hang up a PPP connection on an authentication server timeout.
- No causes it to shut down cleanly when an authentication server times out.

Dependencies: This parameter applies only to PPP connections.

Location: Ethernet>Answer>PPP Options

See Also: PPP

DLCI

Description: Specifies a Frame Relay DLCI number for a gateway or circuit connection. A DLCI is a number between 16 and 991, which is assigned by the Frame Relay administrator. A DLCI is not an address, but a local label that identifies a logical link between a device and a Frame Relay switch. The switch uses the DLCI to route frames through the network, and the DLCI may change as frames are passed through multiple switches.

The Pipeline receives an incoming PPP packet, examines the destination address, and uses the appropriate Connection profile to that destination to route the packet, as usual. If the Connection profile specifies Frame Relay encapsulation, the Frame Relay profile, and a DLCI, the Pipeline encapsulates the packets in Frame Relay (RFC 1490) and forwards the data stream out to the Frame Relay switch using the specified DLCI. The Frame Relay switch uses the DLCI to route the frames. This is known as gateway mode.

Usage: Specify a number between 16 and 991. The default is 16. Ask your Frame Relay network administrator for the value you should enter.

Example: DLCI=17

Dependencies: This parameter applies only to FR and FR_CIR encapsulated calls.

Location: Ethernet>Connections>Encaps Options

See Also: Encaps, FR Direct, FR DLCI

Domain Name

Description: Specifies the local DNS domain name. The domain name is used for DNS lookups. When the Pipeline is given a hostname to look up, it tries various combinations including appending the configured domain name. The secondary domain name (Sec Domain Name) can specify another domain name that the Pipeline can search using DNS.

Usage: Specify the domain name of the Pipeline. You can enter up to 63 characters.

Location: Ethernet>Mod Config>DNS

See Also: Pri DNS, Sec DNS, Sec Domain Name

Download

Description: Enables or disables permission to download the configuration of the Pipeline using the Save Cfg parameter.

Note: Passwords are not saved when the configuration is downloaded. If you upload a saved configuration, all passwords are wiped out.

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

- Yes means the operator can download the Pipeline configuration (without the password values) by using the Save Cfg command in the Sys Diag menu.
- No disables this permission.

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

Location: System>Security

See Also: Chapter 4, “MAX Diag Command Reference.”

Dst Adrs

Description: Specifies a destination IP address. After this value has been modified by applying the specified Dst Mask, it is compared to a packet’s destination address.

Usage: Specify a destination IP address the Pipeline should use for comparison when filtering a packet. The zero 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.

Example: Dst Adrs=10.62.201.56

Dependencies: This parameter applies only to filters of type IP.

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

See Also: Dst Mask

Dst Mask

Description: Specifies a mask to apply to the Dst Adrs before comparing it to the destination address in a packet. You can use it to mask out the host portion of an address, for example, or the host and subnet portion.

The Pipeline applies the mask to the address using a logical AND after the mask and address are both translated into binary format. The mask hides the portion of the address that appears behind each binary 0 (zero) in the mask. A mask of all zeros (the default) masks all bits, so all destination addresses are matched. A mask of all ones (255.255.255.255) masks no bits, so the full destination address to a single host is matched.

Usage: Specify the mask in dotted decimal format. The zero address 0.0.0.0 is the default; this setting indicates that the 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.

Example: Dst Mask=255.255.255.0

Dependencies: This parameter applies only to filters of type IP.

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

See Also: Dst Adrs

Dst Network Adrs

Description: The destination IPX network address. Either the source or destination address (or both) must be specified.

Usage: Enter the hexadecimal value for the destination network.

Example: Dst Network Adrs=cf088888

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

See Also: Src Network Adrs

Dst Node Adrs

Description: Specifies a destination node address to filter.

Usage: Specify a destination node address. You must specify a value if the Dest Network Adrs is not null. The node address ffffffffffff means all nodes in the specified destination network.

Example: Dst Node Adrs=aaabbbccc

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

See Also: Src Node Adrs

Dst Port # (Filters)

Description: Specifies a value to compare with the destination port number in a packet. The default setting (zero) indicates that the Pipeline disregards the destination port in this filter. Port 25 is reserved for SMTP; that socket is dedicated to receiving mail messages. Port 20 is reserved for FTP data messages, port 21 for FTP control sessions, and port 23 for telnet.

Note: The Dst Port Cmp parameter specifies the type of comparison to be made.

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

Example: Dst Port #=25

Dependencies: This parameter applies only to filters of type IP.

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

See Also: Dst Port Cmp, Src Port Cmp, Src Port #

Dst Port# (NAT)

Description: Specifies a TCP or UDP port on the Pipeline to which the remote network sends packets. The Pipeline can route packets for this 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: Enter a port number between 1 and 65535.

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, Valid

Dst Port Cmp

Description: Specifies the type of comparison the Pipeline makes when using the Dst Port # parameter.

Usage: Specify one of the following values:

- 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: This parameter works only for TCP and UDP packets. You must set it to None if the Protocol parameter is not set to 6 (TCP) or 17 (UDP).

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

See Also: Dst Port #

Dst Socket

Description: Some NetWare services communicate across specific sockets; for example, file servers typically use socket 0451. In conjunction with Dst Socket Cmp, Dst Socket # enables you to filter based on socket number.

Usage: Specify the source socket number. Refer to your Novell documentation for NetWare socket numbers.

Example: Dst Socket #=0451

Dependencies: Dst Socket # does not apply if Dst Socket Cmp is set to None.

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

See Also: Dst Socket Cmp

Dst Socket Cmp

Description: Specifies the type of comparison the Pipeline makes when filtering for destination socket numbers using the Dst Socket # parameter. Some NetWare services communicate across specific sockets; for example, file servers typically use socket 0451. If you specify the destination socket number, you can also specify the type of comparison to be made between the destination socket for an IPX packet and the value specified in this filter.

Usage: Specify one of the following values:

- None (the default) means the Pipeline does not compare source port numbers.
- Less means the comparison succeeds if the number is less than the value of Dst Socket #.
- Eql means the comparison succeeds if the number equals the value of Dst Socket #.
- Gtr means the comparison succeeds if the number is greater than the value of Dst Socket #.
- Neq means the comparison succeeds if the number is not equal to the value of Dst Socket #.

Dependencies: Dst Socket Cmp does not apply if Dst Socket # is null.

Example: Dst Socket Comp=Gtr

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

See Also: Dst Socket Cmp

DTE N392

Description: DTE N392 specifies the number of errors during DTE N393 monitored events which cause the user side to declare the network side procedures inactive.

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

Example: DTE N392=3

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

Location: Ethernet>Frame Relay

DTE N393

Description: DTE N393 specifies the DTE monitored event count (between 1 and 10). It is N/A when FR Type is DCE.

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

Example: DTE N393=5

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

Location: Ethernet>Frame Relay

E

Edit

Description: Enables you to customize which status windows are displayed in the VT100 interface at system startup.

Usage: Specify a slot and port address using the format XY-NNN.

- X is the slot number
  The system itself is assigned slot number 0 (00-000).
  The built-in WAN interfaces are lines are slot 1 (10-000).
  The Ethernet is slot 3 (30-000).
- *Y* is the port number.
  Zero means any port on the slot.
- The three digits after the dash are the root number.
  A root number of 000 identifies a top-level branch of the menu tree. If *N* is not zero, the root number identifies a submenu.

Example: Edit=00-000

Location: System>Sys Config

Edit All Calls

Description: Enables or disables permission to edit all the parameters in all Connection profiles. The operator may access the profiles via Telnet or by local management.

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

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

- Yes means the operator can edit all parameters in Connection profiles.
- No means the operator cannot edit parameters in Connection profiles.

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

Location: System>Security

Edit All Ports

Description: This parameter is not supported on the Pipeline.

Edit Com Call

Description: This parameter is not supported on the Pipeline.

Edit Cur Call

Description: This parameter is not supported on the Pipeline.

Edit Line

Description: This parameter is not supported on the Pipeline.

Edit Own Call

Description: This parameter is not supported on the Pipeline.

Edit Own Port

Description: This parameter is not supported on the Pipeline.

Edit Security

Description: Enables or disables permission to edit Security profiles.

Note: Do not set the Edit Security parameter to No in all Security profiles; if you do, you will be unable to edit any of them. This is the most powerful security permission, because it gives the operator the ability to modify his or her own permissions.

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

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

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

Location: System>Security

Edit System

Description: Enables or disables permission to edit the System profile and the Read Comm and R/W Comm parameters in the Ethernet > Mod Config profile.

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

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

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

Location: System>Security

Enable ASBR

Description: Enable ASBR can be used to stop the Pipeline from performing autonomous system border router (ASBR) calculations. ASBRs perform calculations related to external routes. The Pipeline imports external routes from RIP—for example, when it establishes a WAN link with a caller that does not support OSPF—and the ASBR calculations are always performed. If you must prevent the Pipeline from performing ASBR calculations, you can disable the calculations by setting this parameter.

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

- Yes means the Pipeline performs normal operations related to external routes.
- No means the Pipeline does not perform the standard ASBR calculations.

Example: Enable ASBR=Yes

Dependencies: This parameter does not apply unless OSPF is in use.

Location: Ethernet>Mod Config>OSPF global options

Enable Local DNS Table

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

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

- Yes enables the local DNS table.
- No disables the local DNS table.

Location: Ethernet > Mod Config > DNS

See Also: Loc. DNS Tab Auto Update

Enable Channel 16

Description: Specifies whether the E1 line should use channel 16 for data, or should ignore it. Various types of E1 signaling (such as ISDN or R2) use channel 16 for signaling. Although the Pipeline does not support these types of signaling, in some environments you may need to disable channel 16 on the E1 line.

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

- Yes allows channel 16 to carry data.
- No disables channel 16.

Dependencies: Enable Channel 16 is not applicable if Ending DS0 channels is less than 16.

Location: Serial Port E1-Nailed > Mod Config

See Also: Ending DS0 Channel

Encaps

Description: Specifies the encapsulation method to use when exchanging data with a remote network. Both sides of the link must use the same encapsulation for the connection to be established.

Note: When you specify an encapsulation method, the Encaps Options submenu displays a group of parameters relevant to your selection; you must set the appropriate Encaps Options parameters.

Usage: Specify one of the following values:

- PPP (Point-to-Point Protocol) for standard PPP
- FR (Frame Relay)
- FR_CIR (Frame relay circuit)
- TCP-CLEAR (raw TCP using a proprietary encapsulation)

Example: Encaps=PPP

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

Location: Ethernet>Connections

See Also: PPP, FR, TCP-CLEAR

Encoding

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

Usage: Specify one of the following values:

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

Example: Encoding=AMI

Dependencies: This parameter applies only to T1 lines.

Location: Serial Port T1-CSU > Mod Config

End Of Packet Pattern

Description: Specifies the string containing a pattern the Pipeline compares to an incoming WAN packet to determine whether a valid TCP packet is buffered. When the pattern is matched, the Pipeline writes all data up to and including this pattern out to the TCP socket, usually in an Ethernet packet.

Enter a maximum of 64 characters as the pattern the Pipeline compares with incoming WAN packets to determine the end of the packet. You can enter ASCII characters and other binary data using the backslash (\) as an escape mechanism. To insert a literal backslash in the pattern, you must escape it using two backslash characters (\\). You can mix ASCII and other binary data in the pattern.

Usage: Enter an octal value followed by two backslash characters. If your pattern includes literal ASCII characters 0 through 7, you can avoid confusion by padding your escaped octal value with leading zeros to force it to be 3 octal digits long. For example, \015 represents a carriage return. You can set a hexadecimal value by entering \x followed by a 1 to 2 digit hexadecimal number. For example, \x0D represents a carriage return. Other special escape sequences are:

Table 4-1. Escape sequences for TCP end of packet pattern

Escape Sequence	**Description**	**Value**
`\a`	Alarm	7
`\b`	Backspace	8
`\f`	Form feed	12
`\n`	New line	10
`\r`	Carriage return	13
`\t`	Tab	9
`\v`	Vertical tab	11
`\\`	Backslash	92
`\′`	Apostrophe	44
`\″`	Double Quote	34
`\?`	Wildcard Matches any single character	

Dependencies: Keep this additional information in mind:

- Depending upon the values set for Max Packet Length and Packet Flush Time, the Pipeline may write data from the buffer to the TCP socket before a pattern match has been made, since the Pipeline clears this buffer and flushes the data to TCP if any of the following occur:
  - a packet is matched with pattern specified in the End of Packet Pattern parameter.
  - the time specified the Packet Flush Time parameter elapses
  - the data stored in the buffer has reached the value set in Max Packet Length
- End Of Packet Pattern is not applicable when Detect End of Packet is set to No.

Location: Ethernet > Connections > Any Connection profile > Encaps Options submenu.

See Also: Encaps, Detect End of Packet, Max Packet Length, Packet Flush Time

Ending DS0 Channel

Description: Specifies the last channel in the E1 line. All channels after the Ending DS0 channel are disabled.

Usage: Enter a number between 1 and 31. The default is 31. Get this information form your E1 service provider.

Location: Serial Port E1-Nailed > Mod Config

See Also: Enable Channel 16

Enet Adrs

Description: Specifies the physical Ethernet address (MAC address) of a device at the remote end of the link. The Bridge profile correlates a remote MAC address with a Connection profile number, enabling the Pipeline to bring up that Connection when it receives packets destined for the remote device.

Usage: Specify the physical address of the device on the remote network. An Ethernet address is a 12-digit hexadecimal number. The default setting is 000000000000.

Example: Enet Adrs=0180C2000000

Location: Ethernet>Bridge Adrs

See Also: Net Adrs

Excl Routing

Description: This parameter is not supported on the Pipeline.

F

FDL

Description: Specifies the Facilities Data Link (FDL) 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: Serial Port T1-CSU

See Also: Framing Mode

Field Service

Description: Enables or disables permission to perform Ascend-provided field service operations, such as uploading new system software. Field service operations are special diagnostic routines not available through Pipeline menus.

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

- Yes means the operator can upgrade the system software and perform other field service operations.
- No disables this permission.

Example: Field Service=No

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

Location: System>Security

Filter

Description: Specifies the number of a data filter that plugs into the Ethernet profile. The data filter manages data flow on the Ethernet interface. The filter examines each incoming or outgoing packet, and uses the Forward parameter to determine whether to forward or discard it.

Usage: Specify a number between 0 and 199. The number you enter depends on the whether you are applying a filter you created using the VT100 interface, or a firewall you created using Secure Access Manager (SAM).

If you are applying a filter created using the VT100 interface, enter the last 2 digits of the filter number as it appears in the Filters menu.

If you are applying a firewall created with SAM, add 100 to the last 2 digits of the firewall number as it appears in the Firewalls menu. For example, if the number of your firewall is 90-601, specify 101. The numbering scheme for filters and firewalls is:

- 0 indicates that no filtering is being used (this is the default). With this setting the Pipeline forwards all data packets.
- 1-99 indicates that a filter created using the VT100 interface is being used.
- 100-199 indicates that a filter created using SAM is being used.

Refer to your SAM documentation for information on downloading firewalls to the Pipeline.

Example: Filter=7

Location: Ethernet>Mod Config>Ether Options

See Also: Data Filter

First DSO

Description: Specifies the first DS0 for the nailed T1 line. Get this information from your WAN service provider.

Usage: Specify the first DS0. You can specify a number between 1 and 24.

Dependencies: First DS0 must be set to a value less than the Last DS0.

Location: Serial Port T1-CSU > Mod Config

See Also: Last DS0

Forward

Description: Defines whether the Pipeline discards or forwards packets that match the filter specification. When no filters are in use, the Pipeline forwards all packets by default. When a filter is in use, the default is to discard matching packets (Forward=No).

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

- Yes means the Pipeline forwards packets that match the filter.
- No means the Pipeline discards packets that match the filter.

Example: Forward=No

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

See Also: Data Filter, Filter, More

Forwarding

Description: Enables or disables multicast forwarding in the Pipeline.

Note: When you change the Forwarding parameter from No to Yes, the multicast subsystem reads the values in the Ethernet profile and initiates the forwarding function. If you modify a multicast value in the Ethernet profile, you must set this parameter to No and then set it to Yes again to force a read of the new value.

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

- Yes turns on multicast forwarding in the Pipeline.
- No disables multicast forwarding.

Example: Forwarding=Yes

Location: Ethernet>Mod Config>Multicast

See Also: Mbone profile, Multicast Client

Framing Mode

Description: Specifies the framing mode the T1 or E1 physical layer uses. Your carrier can tell you which framing mode to choose.

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

- D4 specifies the D4 format, also known as the Superframe format.
  This format consists of 12 consecutive frames, separated by framing bits.
- ESF specifies the Extended Superframe Format.
  This format consists of 24 consecutive frames, separated by framing bits.

For an E1 line, specify one of the following values:

- G.703 (the default) specifies the standard framing mode used by most E1 ISDN providers and by DASS 2.
- 2DS specifies a variant of G.703 required by most E1 DPNSS providers in the U.K.

Location: Serial Port T1-CSU > Mod Config, Serial Port E1-Nailed > Mod Config

FR

Description: Specifies whether the Pipeline accepts incoming Frame Relay-encapsulated connections.

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

- Yes means the Pipeline accepts calls that use Frame Relay encapsulation, provided that they meet all other connection criteria.
- No means the Pipeline will not accept inbound calls using Frame Relay encapsulation.

Location: Ethernet>Answer>Encaps

See Also: Encaps, FR Prof, DLCI

FR address

Description: The single IP address used when translating local addresses into a single, official IP address for networking over the wide area network and accessing the Internet.

Usage: Enter the official IP address.

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 to FR. For connection that do not use Frame Relay, the Routing parameter in the NAT menu must be set to Yes.

Location: Parameter Ethernet > NAT

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

FR Direct

Description: Specifies whether the Pipeline redirects incoming packets to the Frame Relay switch without processing. A redirect connection is an IP routing connection (typically using PPP), for which the Pipeline simply forwards the packets automatically to the Frame Relay switch without examining destination addresses or its routing table. In effect, the Pipeline passes on the responsibility of routing those packets to a later hop on the Frame Relay network. This is known as redirect mode, and is not commonly used.

Note: A Frame Relay redirect connection is not a full-duplex tunnel between the PPP connection and the switch. The IP packets coming back from the Frame Relay switch are handled by the Pipeline router software, so they must contain the destination IP address to be routed correctly back across the WAN.

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

- Yes means this connection is a Frame Relay redirect connection.
- No means this is not a redirect connection.

Example: FR Direct=No

Dependencies: This parameter is not applicable for FR or FR_CIR encapsulated calls.

Location: Ethernet>Connections>Session Options

See Also: FR DLCI, FR Prof

FR DLCI

Description: Specifies a Frame Relay DLCI number to be used for redirect connections. A redirect connection is an IP routing connection (typically using PPP), for which the Pipeline simply forwards the packets automatically to the frame-relay switch without examining destination addresses or its routing table. In effect, the Pipeline passes on the responsibility of routing those packets to a later hop on the Frame Relay network. This is known as redirect mode, and is not commonly used.

Note: More than one redirected PPP connection can share a Frame Relay DLCI.

Usage: Specify the DLCI obtained from the Frame Relay administrator for redirect links.

Example: FR DLCI=72

Dependencies: This parameter is not applicable if Frame Relay encapsulation is in use.

Location: Ethernet>Connections>Session Options

See Also: FR Direct

FR Prof

Description: Specifies the name of the Frame Relay profile to use for forwarding this link on the Frame Relay network.

Usage: Specify the name of a configured Frame Relay profile. This is the string assigned in the Name parameter of the Frame Relay profile, specified exactly including case changes.

Example: FR Prof=pacbell

Location: Ethernet>Connections>Encaps Options, Ethernet>Connections>Session Options

See Also: FR Type, DLCI

FR Type

Description: Specifies the type of interface between the Pipeline and a Frame Relay switch or CPE (customer premises equipment) on the Frame Relay network.

Note: For NNI or 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:

- NNI (Network to network interface)

  An NNI interface connection allows the Pipeline to appear as a Frame Relay network interface based on the NNI specifications. It performs both DTE and DCE link management, and allows two separate Frame Relay networks to connect via a common protocol.
- 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=NNI

Location: Ethernet>Frame Relay

See Also: LinkUp, FR Prof, DLCI, Circuit

Frame Length

Description: Sets the maximum number of bytes allowed in the information field by the X.75 terminal adapters that might connect to this unit.

Usage: Specify a number between 128 and 2048. The default value is 2048.

Example: Frame Length-2048

Dependencies: This parameter applies only to X.75 terminal adapter connections.

Location: Ethernet>Answer>X.75 Options

See Also: K Window Size, N2 Retransmission Count, T1 Retransmission Timer, X.75

FT1 Caller

Description: This parameter is not supported on the Pipeline.

G

Gateway

Description: Specifies the IP address of the next-hop router that a packet must go through to reach the route's destination address. A next-hop router is either directly connected (on Ethernet) or is one hop away on a WAN link.

Usage: Specify the IP address of the next-hop router.

Example: Gateway=200.207.23.1

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

Location: Ethernet>Static Rtes

See Also: Dest

Group

Description: Assigns a group of nailed channels to a connection.

Note: Nailed channels are used for permanent connections, which are typically leased. It is important to keep those channels dedicated to the connection. Do not assign the same group number to more than one profile of any type.

Usage: Specify the group number assigned to nailed channels in the WAN interface profile.

Example: Group=1

Location: Ethernet>Connections>Telco Options

H

Handle IPX

Description: Specifies IPX server or IPX client bridging.

Note: If NetWare servers are supported on both sides of the WAN connection, we strongly recommend that you use an IPX routing configuration instead of bridging IPX.

Usage: Specify one of the following values:

- None (the default) disables IPX server or IPX client bridging.
- Client (for IPX client bridging). IPX client bridging is used when the local Ethernet supports NetWare clients but no servers. In an IPX client bridging configuration, you want the local clients to be able to reach the Pipeline by querying (broadcasting) for a NetWare server on a remote network.
- Server (for IPX server bridging). IPX server bridging is used when the local Ethernet supports NetWare servers (or a combination of clients and servers) and the remote network supports NetWare clients only.

Example: Handle IPX=Client

Dependencies: This parameter does not apply if IPX routing is enabled for this connection.

Location: Ethernet>Connections>IPX Options

Handle IPX Type 20

Description: Specifies whether the Pipeline will propagate IPX type 20 packets over all its interfaces. Some applications (like NETBIOS) use IPX Type 20 packets to broadcast names over a network. By default, these broadcasts are not propagated over routed links (as Novell recommends) and are not forwarded over links that have less than 1 Mbps throughput. However, if you are using an application such as NetBIOS over IPX, which requires these packets in order to operate, you can enable the router to propagate IPX type 20 packets over a LAN interface by using this parameter.

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

- Yes enables the Pipeline to propagate IPX type-20 packets.
- No means these broadcasts are not propagated.

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

Location: Ethernet>Mod Config>Ether options

HeartBeat Addr

Description: Specifies a multicast address. The Pipeline listens for packets to and from this group to perform the heartbeat-monitoring feature. When it is running as a multicast forwarder, the Pipeline is continually receiving multicast traffic. The heartbeat-monitoring feature enables the administrator to monitor possible connectivity problems by continuously polling for this traffic and generating an SNMP alarm trap if there is a traffic breakdown.

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

Usage: Specify a multicast address to use for heartbeat monitoring.

Example: HeartBeat Addr=224.1.1.1

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

Location: Ethernet>Mod Config>Multicast

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

HeartBeat Udp Port

Description: Specifies a UDP port number. The Pipeline listens only to packets received on that port to perform the heartbeat-monitoring feature. When it is running as a multicast forwarder, the Pipeline is continually receiving multicast traffic. The heartbeat-monitoring feature enables the administrator to monitor possible connectivity problems by continuously polling for this traffic and generating an SNMP alarm trap if there is a traffic breakdown.

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

Usage: Specify a UDP port to use for heartbeat monitoring.

Example: HeartBeat Udp Port=16387

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

Location: Ethernet>Mod Config>Multicast

See Also: HeartBeat Addr, Source Addr, Source Mask, HeartBeat Slot Time, HeartBeat Slot Count, Alarm Threshold

HeartBeat Slot Count

Description: Specifies how many times to poll for multicast traffic before comparing the number of heartbeat packets received to the Alarm Threshold. The Pipeline polls for multicast traffic the specified number of times, waits for the interval specified in the HeartBeat Slot Time parameter, and then polls again.

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

Usage: Specify a number of seconds.

Example: HeartBeat Slot Count=10

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

Location: Ethernet>Mod Config>Multicast

See Also: HeartBeat Addr, Heartbeat Udp Port, Source Addr, Source Mask, HeartBeat Slot Time, Alarm Threshold

HeartBeat Slot Time

Description: Specifies how often (in seconds) the Pipeline should poll for multicast traffic. The Pipeline polls for multicast traffic, waits for this interval, and then polls again.

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

Usage: Specify a number of seconds.

Example: HeartBeat Slot Time=10

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

Location: Ethernet>Mod Config>Multicast

See Also: HeartBeat Addr, Heartbeat Udp Port, Source Addr, Source Mask, HeartBeat Slot Count, Alarm Threshold

HelloInterval

Description: Specifies the number of seconds between sending OSPF Hello packets on the interface. OSPF routers use Hello packets to recognize when a router is down.

Usage: Specify a number. In a Connection profile, the default is 40 seconds. In the Ethernet profile, the default is 10 seconds.

Example: HelloInterval=60

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

See Also: DeadInterval

High BER

Description: Specifies the maximum bit-error rate for any PRI line. The bit-error rate consists of the number of bit errors that occur per second. The number that comes after the double asterisks specifies the power of 10 for the current ratio of error bits to total bits.

Usage: Specify one of the following values:

- 10**-3 (the default)
- 10**-4
- 10**-5

Location: System>Sys Config

See Also: High BER Alarm

High BER Alarm

Description: Specifies whether the back panel alarm relay closes when the bit-error rate exceeds the value specified by the High BER parameter.

The Pipeline has an alarm relay whose contacts remain open on the back panel's alarm relay terminal block during normal operation. If you enable them, the alarm relay contacts close during loss of power, hardware failure, or a system reset. The High BER Alarm parameter specifies whether the contacts also close when the bit-error rate exceeds the High BER parameter value.

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

- Yes causes the Pipeline to close the back panel alarm relay when the bit-error rate exceeds the High BER value.
- No causes the Pipeline to log the event but not close the alarm relay.

Location: System>Sys Config

See Also: High BER

Hop Count

Description: Specifies the number of hops to the destination IPX network. From the 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: Specify a valid hop count from 1 to 15. A hop count of 16 is considered unreachable and is not valid for static routes.

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

Location: Ethernet>IPX Routes

See Also: Route IPX

Host #N Addr (N=1–4)

Description: Specifies the IP address of the first, second, third, and fourth hosts listed in the terminal server menu-mode interface.

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

Example: Host # Addr=10.207.23.6/24

Dependencies: This parameter is ignored if Remote Conf=Yes. It is not applicable if terminal services are disabled.

Location: Ethernet>Mod Config>TServ Options

See Also: Remote Conf

Host #N Text (N=1–4)

Description: Specifies a text description of the first, second, third, and fourth hosts listed in the terminal server menu-mode interface.

Usage: Specify a text description of the host.

Example: Host # Text=Database Server

Dependencies: This parameter is ignored if Remote Conf=Yes. It is not applicable if terminal services are disabled.

Location: Ethernet>Mod Config>TServ Options

See Also: Remote Conf

I

ICMP Redirects

Description: Specifies whether the Pipeline accepts or ignores Internet ICMP Redirect packets. ICMP was designed to dynamically find the most efficient IP route to a destination. ICMP redirect packets are one of the oldest route discovery methods on the Internet and one of the least secure, because it is possible to counterfeit ICMP redirects and change the way a device routes packets.

Usage: Specify one of the following values:

- Accept (to process ICMP redirects). This is the default.
- Ignore (to drop ICMP redirects)

Location: Ethernet>Mod Config

Idle Logout

Description: Specifies the number of minutes an administrative login can remain inactive before the Pipeline logs it out.

Usage: Specify a number between 0 and 60. The default setting is 0; this setting disables automatic logout.

Location: System>Sys Config

IF Adrs

Description: Specifies the IP address of the interface at the near end of a link.

Usage: Specify the IP address of the numbered interface.

Example: IF Adr=10.207.23.7/24

Dependencies: This parameter does not apply if the Pipeline does not route IP.

Parameter Location: Ethernet>Connections>IP options

See Also: WAN Alias, Route IP

Ignore Def Rt

Description: Specifies whether the Pipeline ignores the default route when updating its routing table via RIP updates. The default route specifies a static route to another IP router, which is often a local router such as a Cisco router or another kind of LAN router. When the Pipeline is configured to ignore the default route, RIP updates will not modify the default route in the Pipeline routing table.

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

- Yes means the Pipeline ignore advertised default routes. This is recommended.
- No means the Pipeline may modify its default route based on RIP updates.

Example: Ignore Def Rt=Yes

Dependencies: This parameter is not applicable if IP routing is not enabled on the Pipeline.

Location: Ethernet>Mod Config>Ether Options

Initial Scrn

Description: Specifies the type of user interface displayed at the start of a terminal server connection.

Usage: Specify one of the following values:

- Cmd (the default) to display the command-line interface (“terminal mode”).
- Menu to display the menu interface (“menu mode”).

Location: Ethernet>Mod Config>TServ Options

IP Adrs

Description: Specifies the LAN interface IP address.

Usage: Specify the IP address of the Pipeline on the local IP network or subnet.

Example: IP Adrs=10.2.1.1/24

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

Location: Ethernet>Mod Config>Ether Options

See Also: Encaps, Route IP

IPX Alias

Description: Specifies the IPX network number assigned to a point-to-point link. This parameter is used only when 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: Specify an IPX network number. The default value is 00000000. FFFFFFFF is invalid.

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

Location: Ethernet>Connections>IPX Options

See Also: Route IPX

IPX Enet#

Description: Specifies the IPX network number for the Ethernet interface of the Pipeline. The easiest way to ensure that the number is correct is to leave the default null address. This causes the Pipeline to listen for its network number and acquire it from another router on that interface. If you enter a number other than zero, the Pipeline becomes a “seeding” router and other routers can learn their IPX network number from the Pipeline. For details about seeding routers, see the Novell documentation.

Usage: Specify the IPX network number in use on the Ethernet segment to which the Pipeline is connected. The default 00000000 causes the Pipeline to learn its network number from other routers on that interface.

Example: IPX Enet #=DE040600

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

Location: Ethernet>Mod Config>Ether Options

IPX Frame

Description: Specifies the packet frame used by the majority of NetWare servers on Ethernet. The Pipeline routes and spoofs only one IPX frame type (IEEE 802.2 by default), which is specified in the IPX Frame parameter. If some NetWare software transmits IPX in a frame type other than the type specified here, the Pipeline drops those packets, or if bridging is enabled, it bridges them. If you are not familiar with the concept of packet frames, see the Novell documentation.

Usage: Specify one of the following values:

- 802.2 (NetWare 3.12 or later)

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

- 802.3 (for NetWare 3.11 or earlier)

  This setting indicates that IPX clients and servers on the local Ethernet cable follow the IEEE 802.3 protocol for the MAC header, also called Raw 802.3. The frame does not contain the LLC (Logical Link Control) header in addition to the MAC (Media Access Control) header.

- SNAP

  This setting indicates that the IPX clients and servers on the local Ethernet network follow the SNAP (SubNetwork Access Protocol) for the MAC header. This specification includes the IEEE 802.3 protocol format plus additional information in the MAC header.

- Enet II

  This setting indicates that IPX clients and servers on the local Ethernet network follow the Ethernet II protocol for the MAC header.

- None disables IPX-specific features.

  If you choose this setting, the Pipeline can bridge or route IPX, but without the automatic RIP and SAP handling.

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

Location: Ethernet>Mod Config>Ether Options

IPX Net

Description: Specifies the network number of the remote-end router. If specified, it creates a static route to that device. It is needed only when the remote-end router requires that the Pipeline know its network number before connecting.

Usage: Specify the remote device's IPX network number. The default 00000000 is appropriate for most installations. The default causes the Pipeline not to advertise the route until it makes a connection to the remote network.

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

Location: Ethernet>Connections>IPX Options

See Also: Route IPX

IPX RIP

Description: IPX RIP in a Connection profile defines how RIP packets are handled across this WAN connection. IPX RIP is set to Both by default, indicating that RIP broadcasts will be exchanged in both directions. You can disable the exchange of RIP broadcasts across a WAN connection, or specify that the Pipeline will only send or only receive RIP broadcasts on that connection.

Usage: Specify one of the following values:

- Both (send and receive RIP updates). This is the default.
- Send (send RIP updates but do not receive them).
- Recv (receive RIP updates but do not send them).
- Off (do not send or receive RIP updates).

Example: IPX RIP=Both

Dependencies: This parameter does not apply if the Pipeline does not route IPX.

Location: Ethernet>Connection> IPX options...

See Also: IPX SAP

IPX Routing

Description: This enables IPX routing mode. When you turn on IPX routing in the Pipeline and close the Ethernet profile, the Pipeline comes up in IPX routing mode, uses the default frame type 802.2 (which is the suggested frame type for NetWare 3.12 or later), and listens on the Ethernet to acquire its IPX network number from other IPX routers on that segment.

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

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

Example: IPX Routing=Yes

Dependencies: If IPX routing is disabled, the Pipeline can still bridge IPX packets, provided that Bridging is enabled.

Location: Ethernet>Mod Config

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

IPX SAP

Description: IPX SAP in a Connection profile defines how SAP packets are handled across this WAN connection. IPX SAP is also set to Both by default, indicating that SAP broadcasts will be exchanged in both directions. If SAP is enabled to both send and receive broadcasts on the WAN interface, the Pipeline broadcasts its entire SAP table to the remote network and listens for SAP table updates from that network. Eventually, both networks have a full table of all services on the WAN. To control which services are advertised and where, you can disable the exchange of SAP broadcasts across a WAN connection, or specify that the Pipeline will only send or only receive SAP broadcasts on that connection.

Usage: Specify one of the following values:

- Both (send and receive SAP updates). This is the default.
- Send (send SAP updates but do not receive them).
- Recv (receive SAP updates but do not send them).
- Off (do not send or receive SAP updates).

Example: IPX SAP=Both

Dependencies: This parameter does not apply if the Pipeline does not route IPX.

Location: Ethernet>Connections>IPX Options

See Also: IPX RIP, Peer

IPX SAP Filter

Description: This applies a SAP filter to the LAN or WAN interface. You can apply an IPX SAP filter to exclude or explicitly include certain remote services from the Pipeline SAP table. If you apply a SAP filter in a Connection profile, you can exclude or explicitly include services in both directions.

Usage: Specify the unique portion of the number preceding an IPX SAP Filter profile name in the IPX SAP Filters menu. The default zero means no filter is applied.

Example: IPX SAP Filter=4

Dependencies: This parameter does not apply if the Pipeline does not route IPX.

Location: Ethernet>Answer>Session Options, Ethernet>Connections>Session Options, Ethernet>Mod Config>Ether Options

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

K

K Window Size

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

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

Location: Ethernet>Answer>X.75 Options

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

L

LAN Adrs

Description: Specifies the IP address of remote-end host or router.

Usage: Specify the IP address of the remote device.

Example: LAN Adrs=200.207.23.101/24

Dependencies: This parameter does not apply if the Pipeline does not support IP routing. No two calling Connection profiles should have the same LAN Adrs.

Location: Ethernet>Connections>IP Options

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

Last DSO

Description: Specifies the last DS0 for the nailed T1 line. Get this information from your WAN service provider.

Usage: Specify the last DS0. You can specify a number between 1 and 24.

Dependencies: Last DS0 must be set to a value greater than the First DS0.

Location: Serial Port T1-CSU > Mod Config

See Also: First DS0

Length

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

In a filter of type Generic, this parameter specifies the number of bytes to test in a frame, starting at the specified Offset. The Pipeline compares the contents of those bytes to the value specified in the filter’s Value parameter. For example, with this specification:

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

and the following packet contents:

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

The filter applies the mask only to the eight bytes following the two-byte offset.

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

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

See Also: Offset, Mask, Value

Link Comp

Description: Specifies the link compression method for a PPP session. Both sides of the connection must set the same type of link compression or it will not be used.

Usage: Specify one of the following values:

- None (the default in the Answer profile)
- Stac (Use an Ascend modified version of draft 0 of the CCP protocol)
- Stac-9 (Use draft 9 of the Stac LZS Compression protocol)
- MS-Stac

  Use Microsoft/Stac compression (the same method as Windows95). If the caller does not acknowledge Microsoft/Stac compression, the Pipeline attempts to use standard Stac compression; if that doesn’t work, it uses no compression.

Example: Link Comp=Stac

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

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

Link Mgmt

Description: Specifies the link management protocol to use between the Pipeline and the Frame Relay switch. The Frame Relay administrator or service provider can tell you which value to use.

Usage: Specify one of the following values:

- None specifies no link management.

  The Pipeline assumes that the physical link is up and that all logical links (as defined by the DLCI and FR DLCI parameters) are active on the physical link.

  None is the default.
- T1.617D specifies the link management protocol defined in ANSI T1.617 Annex D.
- Q.933A the link management protocol defined Q.933 Annex A.

Location: Ethernet>Frame Relay

See Also: DLCI, FR DLCI

LinkUp

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

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

- Yes causes the 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

See Also: FR Prof, DLCI, Circuit

List Attempt

Description: Enables or disables the DNS List Attempt feature. DNS can return multiple addresses for a hostname in response to a DNS query, but it does not include information about availability of those hosts. Users typically attempt to access the first address in the list. If that host is unavailable, the user must try the next host, and so forth. However, if the access attempt occurs automatically as part of immediate services, the connection is brought down when the initial connection fails. To avoid tearing down physical links when a host is unavailable, you can use the List Attempt parameter to enable the user to try one entry in the DNS list of hosts, and if that connection fails, to try the next entry, and so on, without losing the WAN session. The List Size parameter specifies the maximum number of hosts listed.

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

- Yes enables a user to try the next host in the DNS list if the first Telnet login attempt fails, which may prevent the physical connection from being torn down.
- No means the connection fails if the first Telnet attempt is refused.

Example: List Attempt=Yes

Location: Ethernet>Mod Config>DNS

See Also: List Size

List Size

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

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

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

Location: Ethernet>Mod Config>DNS

See Also: List Attempt

Loc Adrs

Description: When the Pipeline is configured to perform network address translation (NAT) and to route packets for a particular TCP or UDP port it receives from a remote network to a specific server and port on the local network, this parameter specifies the server to which to route the packets.

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: Enter the IP address. Enter 0.0.0.0 to disable routing of packets.

The default value is 0.0.0.0.

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.

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

See Also: Def Server, Dst Port#, Loc Port#, Lan, Routing, Protocol, Valid

Loc. DNS Tab Auto Update

Description: Enables or disables automatic updating. When automatic updating is enabled, the list of IP addresses for each entry is replaced with a list from the remote DNS when the remote DNS successfully resolves a connection to a host named in the table.

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

- Yes enables automatic updating of the IP addresses in the local DNS table.
- No disables automatic updating.

Dependencies: Loc. DNS Tab Auto Update is not applicable if Enable Local DNS Table parameter is set to No.

Location: Ethernet > Mod Config > DNS

See Also: Enable Local DNS Table

Loc Port#

Description: When the Pipeline is configured to perform network address translation (NAT) and to route packets for a particular TCP or UDP port it receives from a remote network to a specific server and port on the local network, this parameter specifies the port on the local server to which to route the packets. This port does not have to be the same as the port on the Pipeline to which the packets were originally sent.

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: Enter a port number between 1 and 65535. The default of 0 (zero) disables routing of packets.

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#, Loc Adrs, Lan, Routing, Protocol, Valid

Local Profiles First

Description: Specifies whether the Pipeline should attempt local authentication before remote (external) authentication. By default, the Pipeline first attempts to authenticate the connection using local profiles. If that fails, the Pipeline tries to authenticate the connection using an external authentication server.

If this parameter set to No, the Pipeline first tries to authenticate the connection using a remote authentication server. If that fails, the Pipeline attempts to authenticate the connection using local profiles. In this case, some dynamic password challenges behave differently than when authentication is local. (PAP and CHAP work the same either way.)

- PAP-TOKEN

  Authentication will not produce a challenge if there is a local profile. This defeats the security of using PAP-TOKEN.
- PAP-TOKEN-CHAP

  Brings up one channel, but all other channels fail.
- CACHE-TOKEN

  If the far end of the connection has ever authenticated using a challenge, CACHE-TOKEN will not work with local profiles. If the far end has not ever authenticated, there will be no problem with the local profiles.

Note: Because the remote authentication is tried first if this parameter set to No, the Pipeline waits for the remote authentication to time out before attempting to authenticate locally. This timeout may take longer than the timeout specified for the connection and could cause all connection attempts to fail. To prevent this, set the authentication timeout value low enough to not cause the line to be dropped, but still high enough to permit the unit to respond if it is able to. The recommended time is 3 seconds.

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

- Yes retains the default authentication order.
- No reverses the default and attempts remote authentication first.

Example: Local Profiles First=Yes

Dependencies: This parameter is not applicable if Auth is set to None. See the Note above for related dependencies.

Location: Ethernet>Mod Config>Auth

See Also: Auth Timeout

Location

Description: This is an SNMP-readable parameter that specifies the physical location of the Pipeline. It does not affect the unit’s operations.

Usage: Specify a description of the Pipeline unit’s location. You can enter up to 80 characters.

Location: System>Sys Config

See Also: Contact

LogCallInfo

Description: This parameter is not supported on the Pipeline.

Log Facility

Description: Specifies how the Syslog host sorts system logs. The Syslog host is the station to which the Pipeline sends system logs.

All system logs using the same setting are grouped together in the host's file system. That is, all system logs using the Local0 facility are grouped together, all system logs using the Local1 facility are grouped together, and so on.

Usage: Specify one of the following values:

- Local0 (the default)
- Local1
- Local2
- Local3
- Local4
- Local5
- Local6
- Local7

Dependencies: This parameter applies only when Syslog=Yes.

Location: Ethernet>Mod Config>Log

See Also: Log Host, Syslog

Log Host

Description: Specifies the IP address of the Syslog host, a UNIX station to which the Pipeline sends system logs.

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

Example: Log Host=10.207.23.1

Dependencies: This parameter applies only when Syslog=Yes.

Location: Ethernet>Mod Config>Yes

See Also: Log Facility, Syslog

Login Host

Description: Specifies the IP address or DNS hostname of the host to which raw TCP connections will be directed.

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

Location: Ethernet>Connections>Encaps Options

See Also: Login Port

Login Port

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

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

Location: Ethernet>Connections>Encaps Options

See Also: Login Host

Login Prompt

Description: Specifies the string used to prompt for a user name when authentication is in use and an interactive user initiates a connection. If the Prompt Format parameter is set to Yes, you can include multiple lines in the login prompt by including carriage-return/line-feed (\n) and tab (\t) characters. To include an actual backslash character, you must "escape" it with another backslash. For example, you could enter this string:

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

to display the following text as a login prompt:

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

Usage: Specify up to 31 characters. The default value is "Login:".

Example: Login Prompt="Enter your name:"

Dependencies: This parameter does not apply if terminal services are disabled. If the Prompt Format parameter is set to No, this parameter is limited to 15 characters and cannot include newlines or tabs.

Location: Ethernet>Mod Config>TServ Options

Login Timeout

Description: Specifies the number of seconds a terminal-server user can use for logging in. After the specified number of seconds, the login attempt times out.

Usage: Specify between 0 and 300 seconds. The default is 300. A zero value disables the timer.

Example: Login Timeout=300

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

Location: Ethernet>Mod Config>TServ Options

LQM

Description: Specifies whether the Pipeline requests Link Quality Monitoring (LQM) when establishing a PPP connection. LQM counts the number of packets sent across the link and periodically asks the remote end how many packets it has received. Discrepancies are evidence of packet loss and indicate link quality problems.

Both sides of the link negotiate the interval between periodic link quality reports; however, the interval must fall between the minimum interval (LQM Min) and the maximum interval (LQM Max).

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

- Yes enables link quality monitoring for PPP connections.
- No turns off LQM.

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

Dependencies: This parameter applies only to PPP sessions.

See Also: Encaps, LQM Max, LQM Min

LQM Max

Description: Specifies the maximum duration between link quality reports for PPP connections, measured in 10ths of a second.

Usage: Specify a number between 0 and 600. The default is 600.

Dependencies: This parameter applies only to PPP sessions. It is not applicable if LQM is set to No.

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

See Also: LQM, LQM Min

LQM Min

Description: Specifies the minimum duration between link quality reports for PPP connections, measured in 10ths of a second.

Usage: Specify a number between 0 and 600. The default is 600.

Dependencies: This parameter applies only to PPP sessions. It is not applicable if LQM is set to No.

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

See Also: LQM, LQM Max

LSA-Type

Description: Specifies the OSPF ASE type of this link-state advertisement.

Usage: Specify one of the following values:

- ExternalType-1 (the default)

  A type-1 external metric is expressed in the same units as the link-state metric (the same units as interface cost). Type-1 is the default.
- ExternalType-2

  A Type-2 external metric is considered larger than any link state path. Use of type-2 external metrics assumes that routing between autonomous systems is the major cost of routing a packet, and eliminates the need for conversion of external costs to internal link-state metrics.
- Internal

  This indicates that this static route should be advertised in an internal LSA.

Dependencies: Keep this additional information in mind.

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

Location: Ethernet> Static Rtes

See Also: Ospf-Cost

M

Mask

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

The Pipeline applies the mask to the specified value using a logical AND after the mask and value are both translated into binary format. The mask hides the bits that appear behind each binary 0 (zero) in the mask. A mask of all ones (FF FF FF FF FF FF FF FF) masks no bits, so the full Compare To value must match the packet contents. For example, with this filter specification:

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

and the following packet contents:

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

The mask is applied as shown below, resulting in a value that matches the Value.

```
                 2-byte Byte Offset         8-byte Comparison

                   2A 31 97 FE 45 70 12 22 33 99 B4 80 75
Mask ------------------  0F FF FF FF 00 00 00 F0
Result of mask --------  07 FE 45 70 00 00 00 90

Value to test ---------  07 FE 45 70 00 00 00 90
```

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

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

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

Example: Mask=0FFFFFFF000000F0

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

See Also: Length, Offset, Type, Value

Max ATMP Tunnels

Description: Defines the maximum number of active ATMP sessions for units configured as an ATMP Home agent.

Usage: Enter the number of simultaneous ATMP sessions you want to allow through this ATMP Gateway. The default, 0 (zero) disables the parameter.

Note: Changes take effect after the Connection Profile is saved, the connection is cleared, then reestablished.

Dependencies: Applies only to units configured as ATMP Home agents.

Location: Ethernet > Connections > any profile > Session Options menu.

See Also: See Also: ATMP Mode, ATMP Gateway

Max Packet Length

Description: Specifies the maximum length of the packet that can be buffered.

Usage: Enter a value between 1 and 8192. If End Of Packet Detection is set to Yes and a packet has not been matched, the buffered data is flushed to TCP once the number of bytes specified in Max Packet Length is cleared.

Dependencies: Keep this additional information in mind:

- Max Packet Length does not apply unless Encaps is set to TCP-CLEAR in the Connection profile or Detect End of Packet is set to Yes.
- Buffering a large packet size will impact the overall performance of the system, and may run the risk of running out of memory.

Location: Ethernet > Connections > Any Connection profile > Encaps Options submenu.

See Also: Encaps, Detect End of Packet, End of Packet Pattern, Detect End of Packet, Packet Flush Time

Mbone profile

Description: Specifies the name of a resident Connection profile to a multicast router on the WAN. If the Mbone profile name is null and Multicast Forwarding is turned on, the Pipeline assumes that its Ethernet is the MBONE interface.

Usage: Specify the name of the Connection profile to a remote multicast router. If no name is specified, the Pipeline assumes the presence of a multicast router on its Ethernet interface.

Example: Mbone profile=newyork

Location: Ethernet>Mod Config>Multicast

Dependencies: This parameter does not apply if Multicast Forwarding is set to No.

See Also: Multicast Forwarding, Multicast Client

Metric

Description: In a Connection or Route profile, this parameter specifies a Routing Information Protocol (RIP) metric (a virtual hop count) associated with the IP route. (In the Answer profile, the Metric parameter is not supported.)

The specified metric is a virtual hop count. The actual hop count includes the metric of each switched link in the route.

If two routes have the same preference value, the Pipeline chooses the route with the lowest metric. If you enable RIP across the WAN in a Connection profile, 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.

Usage: Press Specify a number between 1 and 15. The default setting is 7. The higher the number you specify, the less likely that the Pipeline will bring the link or route online.

Example: Metric=4

Dependencies: This parameter does not apply if the Pipeline does not route IP.

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

See Also: Private, RIP

Module Name

Description: Specifies an optional name to the Ethernet interface.

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

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

More

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

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

- Yes links the current filter rule to the next one, so the next filter is applied before the forwarding decision is made.
- No does not link the current filter rule. The forwarding decision is made based solely on this rule.

Example: More=Yes

Dependencies: The next filter must be enabled.

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

See Also: Forward, Length, Offset, Type, Value, Valid

MRU

Description: Specifies the maximum number of bytes the Pipeline can receive in a single packet. Usually the default is the right setting, unless the far end requires a lower number.

Usage: Specify a number lower than the default MRU if the far end requires it.

- In the Answer or a Connection profile, specify a number between 1 and 1524.

- In a Frame Relay profile, specify a number between 128 and 1600.

Example: MRU=1524

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

See Also: Encaps

Multicast Client

Description: Enables the Pipeline to respond to multicast clients on the WAN link. Clients cannot be supported on the MBONE interface, so this means another WAN link or the local Ethernet supports a multicast router.

When this parameter is set to Yes, the Pipeline begins handling IGMP requests and responses on the interface. It does not begin forwarding multicast traffic until the rate limit is set.

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

- Yes enables the Pipeline to respond to IGMP client requests and responses on the interface.
- No means the Pipeline does not respond to multicast clients on the interface.

Example: Multicast Client=Yes

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

Location: Ethernet>Connections>IP options

See Also: Multicast Rate Limit

Multicast Rate Limit

Description: Specifies the rate at which the Pipeline accepts multicast packets from clients on this interface. It does not affect the MBONE interface.

Note: By default, the Rate Limit parameter is set to 100. *This disables multicast forwarding on the interface.* The forwarder handles IGMP packets, but does not accept packets from clients or forward multicast packets from the MBONE router.

To begin forwarding multicast traffic on the interface, you must set the rate limit to a number less than 100. For example if you set it to 5, the Pipeline accepts a packet from multicast clients on the interface every 5 seconds. Any subsequent packets received in that 5-second window are discarded.

Usage: Specify a number lower than the default 100 to begin forwarding multicast traffic on the interface.

Example: Multicast Rate Limit=5

Dependencies: This parameter has no effect when applied to the MBONE interface.

Location: Ethernet>Connections>IP Options

See Also: Multicast Client

N

N2 Retransmission Count

Description: Indicates the retry limit, the maximum number of times the Pipeline can resend a frame on an X.75 connection when the T1 Retransmission Timer expires.

Usage: Specify a number between 2 and 15. The default value is 10. A higher value increases the probability of a correct transfer of data. A lower value allows for quicker detection of a permanent error condition.

Location: Ethernet>Answer>X.75 Options

See Also: Frame Length, K Window Size, T1 Retransmission Timer, X.75

N391

Description: Specifies the interval at which the Pipeline requests a Full Status Report on a Frame Relay link.

Usage: Specify a number from 1 to 255 seconds. The default is 6.

Example: N391=15

Dependencies: This parameter does not apply if FR Type is DCE.

Location: Ethernet>Frame Relay

See Also: Link Mgmt

Nailed E1 Group

Description: Associates the nailed E1 line with a group number. When you assign this same group number to a Connection profile (using the Group parameter), the Connection profile uses the E1 line to connect to its destination. When you assign this same group number to a Frame Relay Profile (using the Nailed Grp parameter), the DLCI number determines which frames are sent over the link.

Usage: Nailed E1 Group cannot be changed from its default value of 1.

Location: Serial Port E1-Nailed > Mod Config

See Also: Nailed Grp, Group

Nailed Grp

Description: Specifies a number assigned to a group of nailed channels or a serial WAN port. In a Frame Relay profile, it assigns those channels to the link represented by the profile. Only one active link can be assigned to use a particular group number.

Usage: Nailed Grp cannot be changed from its default value of 1.

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

See Also: Activation, Group

Nailed T1-Group

Description: Associates the nailed T1 line with a group number. When you assign this same group number to a Connection profile (using the Group parameter), the Connection profile uses the T1 line to connect to its destination. When you assign this same group number to a Frame Relay Profile (using the Nailed Grp parameter), the DLCI number determines which frames are sent over the link.

Usage: Nailed T1 Group cannot be changed from its default value of 1.

Location: Serial Port T1-CSU > Mod Config

See Also: Nailed Grp, Group

Name

Description: Specifies the name of a profile, host, or user.

Note: When the Name parameter specifies an existing host, user, the Pipeline system itself, or a Firewall profile, the name is case-sensitive. The name you specify must be unique within the list of profiles of the same type. In addition, Ascend strongly recommends that you do not use the same name for a Connection profile.

Usage: Specify a name.

- In most profiles, the name can contain up to 16 characters.
- In the Route profile and SNMP Traps profile, the name can contain up to 31 characters.

Example: Name=PacBell

Location: Ethernet>Filters, Ethernet>Firewalls, Ethernet>Frame Relay, Ethernet>IPX SAP Filters, Ethernet>Static Rtes, System>Security, Ethernet>SNMP Traps, System>Sys Config

Net Adrs

Description: In a Bridge profile, this parameter specifies the IP address of a device at the remote end of the link. If you are bridging between two segments of the same IP network, you can use the Net Adrs parameter in a Bridge profile to enable the Pipeline to respond to ARP requests while establishing the bridged connection. If an ARP packet contains an IP address that matches the Net Adrs parameter of a Bridge profile, the Pipeline responds to the ARP request with the Ethernet (physical) address specified in the Bridge profile and establishes the specified connection. In effect, the Pipeline as a proxy for the node that actually has that address.

Usage: Specify the IP address of the device on the remote network.

Example: Net Adrs=10.207.23.101/24

Location: Ethernet>Bridge Adrs

See Also: Enet Adrs

Net End

Description: Specifies the last in the range of AppleTalk network numbers available for packets that are to be routed to this static route. Network numbers are assigned to network segments, and must be unique within the internetwork. Each of the numbers within a network range can represent up to 253 devices.

Usage: Specify a network starting number from 1 to 65199.

Location: Ethernet > Connections> *any Connection profile* > AppleTalk Options, Ethernet > Mod Config > Appletalk

Dependencies: Keep this additional information in mind:

- If AppleTalk routing is disabled, Net End does not apply.

See Also: Net Start, Zone Name #*n*

Net Start

Description: Specifies the first in the range of AppleTalk network numbers available for packets that are to be routed to this static route. Network numbers are assigned to network segments, and must be unique within the internetwork. Each of the numbers within a network range can represent up to 253 devices.

Usage: Specify a network starting number from 1 to 65199.

Dependencies: Keep this additional information in mind:

- If AppleTalk routing is disabled, Net Start does not apply.

Location: Ethernet > Connections> *any Connection profile* > AppleTalk Options, Ethernet > Mod Config > Appletalk

See Also: Net End, Zone Name #*n*

Network

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

Usage: Specify the NetWare server’s internal network number. The values 00000000 and fffffff are not valid.

Example: Network=A00100001

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

Location: Ethernet>IPX Routes

See Also: Route IPX

Node

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

Usage: Specify the server’s node address on its own internal network. Typically, a server running NetWare 3.11 or later has a node number of 000000000001.

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

Location: Ethernet>IPX Routes

See Also: Route IPX, Network

No Trunk Alarm

Description: Specifies whether the back panel alarm relay closes when the T1 line goes out of service. The Pipeline has an alarm relay whose contacts remain open on the back panel’s alarm relay terminal block during normal operation. If you enable them, the alarm relay contacts close during loss of power, hardware failure, or a system reset. The No Trunk Alarm parameter enables you to specify whether the contacts also close when the T1 line goes out of service.

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

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

Location: System>Sys Config

Number of DS0 Channels

Description: Specifies the number of DS0 channels on the Pipeline T1 line. Get this information from your WAN service provider.

Usage: Enter the number of DS0 channels on the T1 line. The default is 24.

Location: Serial Port T1-CSU profile > Mod Config

See Also: Nailed T1 Group

O

Offset

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

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

and the following packet contents:

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

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

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

Usage: Specify a number indicating a byte-offset.

Example: Offset=2

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

See Also: Length, Mask, More

Operations

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

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

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

- Yes means the operator can view and edit profiles.
- No disables this permission as well as all other permissions in the Security profile.

Example: Operations=No

Location: System>Security

OSPF ASE Preference

Description: Specifies the OSPF ASE preference the Pipeline uses when importing an ASE.

Usage: Specify a value from 0 to 255. A value of 255 means that the Pipeline never puts any ASEs into the routing table.

The default route preferences are:

- Connected routes 0
- OSPF internal routes10
- ICMP routes 30
- Static routes 60
- RIP routes 100
- Unconnected WAN routes 120
- OSPF ASE 150
- Do not use route 255

Dependencies: Keep this additional information in mind.

- When specifying a preference for a route, make sure that routes that are learned from more reliable sources have a lower preference (and are therefore more likely to be used).
- When specifying a preference for a route, you should set a lower preference for connected routes that for disconnected routes.

Location: Ethernet>Mod Config>Route Pref

OSPF Preference

Description: Specifies the preference value for routes learned from the OSPF protocol.

When choosing which routes to put in the routing table, the router first compares the OSPF Preference values, preferring the lower number. If the OSPF Preference values are equal, the router compares the Metric values, using the route with the lower Metric. These are the default values for other types of routes:

- Connected routes have a default preference of 0
- OSPF routes have a default preference of 10
- ICMP redirects have a default preference of 30
- RIP routes have a default preference of 100
- Static routes have a default preference of 100
- ATMP routes have a default preference of 100

Usage: Specify a number between 0 and 255. The default value is 10. Zero is the default for connected routes (such as the Ethernet). The value of 255 means “Don't use this route.”

Location: Ethernet>Mod Config>Route Pref

Ospf-Cost

Description: Specifies the cost of an OSPF route. The interpretation of this cost depends on the type of external metrics set in the ASE-type parameter. If the Pipeline is advertising Type 1 metrics, OSPF can use the specified number as the cost of the route. Type 2 external metrics are an order of magnitude larger. Any Type 2 metric is considered greater than the cost of any path internal to the AS (autonomous system).

Usage: Specify a number greater than zero. The default is 1.

Example: Ospf-Cost=1

Location: Ethernet>Static Rtes

See Also: ASE-type, ASE-tag

Own Port Diag

Description: This parameter is not supported on the Pipeline.

P

Packet Characters

Description: Specifies the minimum number of bytes of received data that should accumulate before the data is passed up the protocol stack for encapsulation.

Usage: Specify an integer between 0 and 500. The default value is 0 (zero).

Dependencies: If your application is so specialized that it demands you use this parameter, be sure to set the Packet Wait Time parameter to an appropriate value. This parameter does not apply if terminal services are disabled.

Location: Ethernet>Mod Config>TServ Options

See Also: Packet Wait Time

Packet Flush Time

Description: Specifies the amount of time in milliseconds that the Pipeline before flushing that data to TCP.

Usage: Enter a number between 1 and 1000 to specify the number of milliseconds between the time the Pipeline receives the first byte of data and flushes that data to TCP. After receiving the first byte of data, the Pipeline attempts to match the pattern specified in End Of Packet Pattern with the incoming WAN data stream. During this time, the Pipeline buffers the incoming data up to the limit specified in Max Packet Length. If there is no match, the Pipeline flushes the buffered data to TCP when the Packet Flush Time elapses.

Dependencies: Packet Flush Time does not apply unless Encaps is set to TCP-CLEAR in the Connection profile or Detect End of Packet is set to Yes.

Location: Ethernet > Connections > Any Connection profile > Encaps Options submenu.

See Also: Encaps, Detect End of Packet, End of Packet Pattern, Max Packet Length

Packet Wait time

Description: Specifies the maximum amount of time in milliseconds that any received data can wait before being passed up the protocol stack for encapsulation.

Usage: Specify an integer between 0 and 600 milliseconds. The default value is 0 (zero).

Dependencies: If your application is so specialized that it demands you use this parameter, be sure to take into account your modem speeds when calculating its value. This parameter does not apply if terminal services are disabled.

Location: Ethernet>Mod Config>TServ Options

See Also: Packet Characters

Passwd

Description: In the Ethernet > Mod Config profile, specifies the terminal-server password; in a Security profile it specifies the password required to authenticate a Security profile. The first Security profile, Default, has no password.

Note: Passwords are case-sensitive.

Usage: Specify up to 20 characters.

Dependencies: In the Ethernet profile, this parameter does not apply if terminal services are disabled.

Location: Ethernet>Mod Config>TServ Options, System>Security

See Also: Edit Security, TS Enabled

Passwd Prompt

Description: Specifies the prompt the terminal server displays when asking users for their password.

Usage: Specify up to 31 characters. The default value is “Password:”.

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

Location: Ethernet>Mod Config>TServ Options

Password

Description: Specifies the password the foreign agent must specify under the Ascend Tunnel Management Protocol (ATMP) in order to access this unit.

Note: Passwords are case-sensitive.

Usage: Specify up to 20 characters.

Dependencies: Password is not applicable unless ATMP is enabled and the ATMP Mode is Home.

Location: Ethernet>Mod Config>ATMP Options

See Also: ATMP Gateway, ATMP Mode, Type, UDP Port

Port

Description: This parameter is not supported on the Pipeline.

PPP

Description: Enables incoming Point-to-Point Protocol (PPP) connections. PPP sessions are single-channel connections to any remote device running PPP software.

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

- Yes in the Answer profile means the Pipeline accepts inbound PPP connections, provided that they meet all other connection criteria.
- No means it will not accept inbound PPP connections.

Location: Ethernet>Answer>Encap

Preference

Description: Specifies the preference value for a route. RIP is a distance-vector protocol, which uses a hop count to select the shortest route to a destination network. OSPF is a link-state protocol, which means that OSPF can take into account a variety of link conditions, such as the reliability or speed of the link, when determining the best path to a destination network. Because these two metrics are incompatible, the Pipeline supports route preferences.

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

- Connected routes have a default preference of 0
- OSPF routes have a default preference of 10
- ICMP redirects have a default preference of 30
- RIP routes have a default preference of 100
- Static routes have a default preference of 100
- ATMP routes have a default preference of 100

Usage: Specify a number between 0 and 255. Zero is the default for connected routes (such as the Ethernet). The value of 255 means “Don't use this route;” this value is meaningful only for Connection profiles.

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

Pri DNS

Description: Specifies the IP address of the primary domain name server. You can specify a primary and secondary name server of each type. The secondary server is accessed only if the primary one is inaccessible.

Usage: Specify the IP address of the primary domain name server. The default value is 0.0.0.0. Accept this default if you do not have a domain name server.

Example: Pri DNS=10.207.23.1

Location: Ethernet>Mod Config>DNS

See Also: Domain Name, Sec DNS

Priority

Description: Specifies the priority of this router with respect to the designated router and backup designated router elections under OSPF. When two routers attached to a network attempt to become the designated router, the one with the highest Priority value takes precedence. A router whose Priority is set to 0 (zero) is ineligible to become the designated router on the attached network.

Usage: Specify a number. The default value is 5.

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

Private

Description: Specifies whether the Pipeline will disclose the existence of this route when queried by RIP or another routing protocol. Private routes are used internally but are not advertised.

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

- Yes makes the route private. The Pipeline does not advertise the route.
- No means the route is advertised via routing protocols.

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

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

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

Pri WINS

Description: Specifies the IP address of the primary Windows Internet Name Service (WINS) server.

Usage: Specify an IP address in dotted decimal notation. The default is 0.0.0.0.

Dependencies: Pri WINS applies only to Telnet and raw TCP connections running under the Pipeline unit’s terminal server interface.

Location: Ethernet>Mod Config>DNS

See Also: Sec WINS

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: Enter the name of a Connection Profile.

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.

Dependencies: Keep this additional information in mind.

- If the Routing parameter in the NAT menu is set to No, this parameter is N/A.
- If you specify a Connection Profile that does not exist, the Pipeline does not perform NAT.

Location: Ethernet > NAT

See Also: Routing

Profile Reqd

Description: Specifies whether the Pipeline rejects incoming connections for which it could find no Connection profile and no entry on a remote authentication server. If you don’t require a configured profile for all connections, the Pipeline builds a temporary profile for unknown users based on the settings in the Answer profile. Many sites consider this a security breach.

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

- Yes means a configured profile is required for all callers.
- No means that if a configured profile is not found, the Pipeline builds a temporary profile for the unknown user based on the settings in the Answer profile.

Dependencies: This parameter does not apply to terminal server sessions.

Location: Ethernet>Answer

See Also: AppleTalk, Encaps, Recv Auth, Route IP

Prompt

Description: Specifies the prompt the Pipeline displays during a terminal server session.

Usage: Specify a string containing up to 15 characters. The default is “ascend%”.

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

Location: Ethernet>Mod Config>TServ Options

See Also: TS Enabled

Prompt Format

Description: Determines whether you are able to use the multi-line format for the terminal server login prompt.

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

- Yes causes the Pipeline to interpret carriage-return/line-feed and tab characters in the string specified as the Login Prompt.
- No means the Pipeline does not interpret the line feed/carriage return character or the tab character.

Example: Prompt Format=No

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

Location: Ethernet>Mod Config>TServ Options

See Also: TS Enabled, Login Prompt

Protocol (Filters)

Description: In a filter of type IP, this parameter specifies the protocol number to which the Pipeline compares a packet's protocol number. f you specify a protocol number, the Pipeline compares it to the protocol number field in packets to match them to this filter. The default protocol number of zero matches all protocols. Common protocols are listed below, but protocol numbers are not limited to this list. For a complete list, see the section on Well-Known Port Numbers in RFC 1700, *Assigned Numbers*, by Reynolds, J. and Postel, J., October 1994.

- 1: ICMP
- 5: STREAM
- 8: EGP
- 6: TCP
- 9: Any private interior gateway protocol (such as Cisco's IGRP)
- 11: Network Voice Protocol
- 17: UDP
- 20: Host Monitoring Protocol
- 22: XNS IDP
- 27: Reliable Data Protocol
- 28: Internet Reliable Transport Protocol
- 29: ISO Transport Protocol Class 4
- 30: Bulk Data Transfer Protocol

- 61: Any Host Internal Protocol
- 89: OSPF

Usage: Specify the number of the protocol. You can enter a number between 0 and 255. The default setting is 0 (zero). When you accept the default, the Pipeline disregards the Protocol parameter when applying the filter.

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

See Also: Type, Valid

Protocol (NAT)

Description: 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.

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: Specify one of the following values:

- 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.

Dependencies: 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 not applicable.

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

See Also: Dst Port#, Loc Port#

Proxy Mode

Description: Specifies under what conditions the Pipeline responds to ARP requests for remote devices that have been assigned an address dynamically. It responds to the ARP request with its own MAC address while bringing up the connection to the remote device. This feature is referred to as Proxy ARP.

Description: Specify one of the following values:

- Off (the default) disables proxy ARP.
- Always specifies that the 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.

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

Location: Ethernet>Mod Config>Ether 1 Options, Ethernet>Mod Config>Ether2 Options

See Also: Net Adrs, Route IP

R

R/W Comm

Description: Specifies a read/write SNMP community name. If an SNMP manager sends this community name, it can access the Get, Get-Next, and Set SNMP agents.

Usage: Specify the community name that the Pipeline will use for authenticating the SNMP management station for read-write access. You can enter letters and numbers, up to a limit of 16 characters. The default is Write.

Location: Ethernet>Mod Config>SNMP Options

See Also: Read Comm

R/W Comm Enable

Description: Enables and disables the use of SNMP set commands.

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

- Yes enables the use of SNMP set commands. To use a set command, you must know the SNMP read-write community string specified in the R/W Comm parameter.
- No disables the use of set commands.

Location: Ethernet > Mod Config > SNMP Options

See Also: R/W Comm, Read Comm

Rate Limit

Description: Specifies the rate at which the Pipeline accepts multicast packets from clients on this interface. It does not affect the MBONE interface.

Note: By default, the Rate Limit parameter is set to 100. *This disables multicast forwarding on the interface.* If multicast forwarding is enabled on the interface but the Rate Limit parameter is left at the default 100, he forwarder handles IGMP packets, but does not accept packets from clients or forward multicast packets from the MBONE router.

To begin forwarding multicast traffic on the interface, you must set the rate limit to a number less than 100. For example if you set it to 5, the Pipeline accepts a packet from multicast clients on the interface every 5 seconds. Any subsequent packets received in that 5-second window are discarded.

Usage: Specify a number lower than the default 100 to begin forwarding multicast traffic on the interface.

Example: Multicast Rate Limit=5

Dependencies: This parameter has no effect when applied to the MBONE interface.

Location: Ethernet>Mod Config>Multicast

See Also: Multicast Forwarding, Mbone Profile, Client, Multicast Rate Limit

RD MgrN (N=1–5)

Description: Specify up to five IP addresses of SNMP managers that have SNMP read permission. The Pipeline responds to SNMP get and get-next commands from these SNMP managers only.

Usage: Specify the IP address of a host running an SNMP manager. The default is 0.0.0.0.

Dependencies: The Security parameter must be set to Yes for the RD Mgr1-5 parameters to have any effect. If the Security parameter is set to Yes, only SNMP managers at the IP addresses you specify can execute the SNMP get and get-next commands.

Location: Ethernet>Mod Config>SNMP Options

See Also: Security, WR Mgr1-5

Read Comm

Description: Specifies a read-only SNMP community name. If an SNMP manager sends this community name, it can access the Get and Get-Next SNMP agents.

Usage: Specify the community name that the Pipeline uses for authenticating the SNMP management station for read-only access. You can enter up to 16 alphanumeric characters. The default is Public.

Location: Ethernet>Mod Config>SNMP Options

See Also: R/W Comm

Recv Auth

Description: Specifies the authentication protocol the Pipeline uses to receive and verify a password for an incoming PPP connection.

Usage: Specify one of the following values:

- None (the default) means the Pipeline does not use an authentication protocol to validate incoming PPP sessions.
- PAP indicates the Password Authentication Protocol.

  PAP provides a simple method for a host to establish its identity in a two-way handshake. Authentication takes place only upon initial link establishment, and does not use encryption. The remote device must support PAP.
- CHAP indicates the Challenge Handshake Authentication Protocol.

CHAP is more secure than PAP. It provides a way to periodically verify the identity of a host using a three-way handshake and encryption. Authentication takes place upon initial link establishment; the Pipeline can repeat the authentication process any time after the connection is made. The remote device must support CHAP.

- MS-CHAP means the connection must use Microsoft's extension of CHAP.

  MS-CHAP was designed mostly for Windows NT/Lan Manager platforms. For details, see ftp://ftp.microsoft.com/DEVELOPR/RFC/chapexts.txt.)
- Either specifies any of the supported authentication schemes.

  When you select Either, the Pipeline allows authentication if the remote peer can authenticate using any of the designated authentication schemes.

Dependencies: If you specify an authentication method, you must also specify a password in the Connection profile associated with the session. For a nailed connection, you must set Recv Auth and Send Auth to the same value at both ends of the connection.

Location: Ethernet>Answer>PPP Options

See Also: Auth Host, Recv PW, Send Auth, Send PW

Recv PW

Description: Specifies the password that the Pipeline expects to receive from the far-end while the connection is being authenticated. If this password is not sent by the far-end device, authentication fails. For PPP links, the password can contain up to 20 characters.

Usage: Specify a password. The password is case sensitive. The default is null.

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

Location: Ethernet>Connections>Encaps Options

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

Remote Conf

Description: This parameter is not supported on the Pipeline.

Remote Mgmt

Description: This parameter is not supported on the Pipeline.

Retransmit Interval

Description: Specifies the number of seconds between retransmissions of OSPF packets. OSPF uses this value for LSA transmissions and when retransmitting Database Description and Link State Request Packets.

Usage: Specify a number greater than zero. The default is 5.

Example: Retransmit Interval=15

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

Reuse Addr Timeout

Description: Specifies the number of minutes to lease the IP address obtained during DHCP negotiation when Reuse Last Addr is set to Yes. During the period of time set in this parameter, even if the WAN session is idle and times out, the same address will be associated with the WAN connection each time it is re-established.

Usage: Set the value to a number of minutes, from 0 to 1440.

- When set to 0, the timer is disabled. This is the default.
- The maximum setting is 1440, which is 24 hours.

Dependencies: Reuse Addr Timeout is not applicable if NAT routing is disabled, or if NAT is enabled, but Multiple-address NAT is being used.

Location: Parameter Ethernet > NAT

See Also: Reuse Last Addr

Reuse Last Addr

Description: Specifies that the last IP address given by the DHCP server should be reused in subsequent DHCP negotiations (for the duration specified in the Reuse Addr Timeout parameter). Set this parameter when you need to use the same IP address for TCP applications that do not time out, such as Telnet. When the WAN session is idle for a long enough period of time, it will timeout, and the next time the WAN session is established, a new IP address will be assigned by the DHCP server. This creates a problem for users of applications that don't time out, since they expect to be using the same IP address.

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

Dependencies: This setting is not applicable if NAT routing is disabled, or when using Multiple-address NAT. Additionally, it does not apply if the value of Reuse Addr Timeout has been reached.

- If the original IP address given during DHCP negotiation is lost, and cannot be reused, applica-tions requiring the same IP address will need to be reset.

Location: Parameter Ethernet > NAT

See Also: Reuse Addr Timeout

RIP

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

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

Usage: Specify one of the following values:

- Off specifies that the Pipeline does not transmit or receive RIP updates. Off is the default.
- Recv-v2 indicates that the Pipeline receives RIP-v2 updates on the interface but does not send RIP updates.

- Send-v2

  This setting indicates that the Pipeline transmits RIP-v2 updates on the interface but does not send RIP updates.
- Both-v2 means the Pipeline sends and receives RIP-v2 updates on the interface.
- Recv-v1 indicates that the Pipeline receives RIP-v1 updates on the interface but does not send RIP updates.
- Send-v1

  This setting indicates that the Pipeline transmits RIP-v1 updates on the interface but does not send RIP updates.
- Both-v1 means the Pipeline sends and receives RIP-v1 updates on the interface.

Dependencies: This parameter does not apply if the Pipeline does not route IP.

Location: Ethernet>Answer>Session Options, Ethernet>Connections>IP Options, Ethernet> Mod Config>Ether Options

See Also: Route IP

RipASEType

Description: Specifies how RIP routes are propagated into OSPF.

Usage: Specify one of the following values:

- Type1 is a metric expressed in the same units as the link-state metric (the same units as interface cost).
- Type2 is considered larger than any link-state path.

  Type 2 is the default. It assumes that routing between autonomous systems is the major cost of routing a packet, and eliminates the need for conversion of external costs to internal link-state metrics.

Dependencies: This parameter does not apply if the Pipeline does not route OSPF.

Location: Ethernet>Mod Config>Route Pref

RIP Policy

Description: Specifies a split horizon or poison reverse policy to handle update packets that include routes that were received on the same interface on which the update is sent. Split-horizon means that the Pipeline does not propagate routes back to the subnet from which they were received. Poison-reverse means that it propagates routes back to the subnet from which they were received with a metric of 16.

Usage: Specify Split Hrzn or Poison Rvrs. Poison Rvrs is the default.

Example: RIP Policy=Poison Rvrs

Dependencies: This parameter does not apply to RIP-v2. It applies only to RIP-v1 packets.

Location: Ethernet>Mod Config

Rip Preference

Description: Specifies the preference value for routes learned from the RIP protocol.

When choosing which routes to put in the routing table, the router first compares the Rip Preference values, preferring the lower number. If the Rip Preference values are equal, the router compares the Metric values, using the route with the lower Metric.

Usage: Specify a number between 0 and 255. The default value is 100. Zero is the default for connected routes (such as the Ethernet). The value of 255 means “Don't use this route.”

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

- Connected routes have a default preference of 0
- OSPF routes have a default preference of 10
- ICMP redirects have a default preference of 30
- RIP routes have a default preference of 100
- Static routes have a default preference of 100
- ATMP routes have a default preference of 100

Location: Ethernet>Mod Config>Route Pref

RIP Summary

Description: Specifies whether to summarize subnet information when advertising routes. If the Pipeline summarizes RIP routes, it advertises a route to all the subnets in a network of the same class; for example, the route to 200.5.8.13/28 (a class C address) would be advertised as a route to 200.5.8.0. When the 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.

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

- Yes causes the Pipeline to summarize RIP-v1 subnet information.
- No means the Pipeline advertises each route as-is.

Dependencies: This parameter does not apply to RIP-v2. It applies only to RIP-v1 packets. In addition, note that RIP Summary does not affect host routes.

Location: Ethernet>Mod Config

Rip Tag

Description: This parameter assigns a specific tag to all routes propagated from RIP into OSPF. A tag is a 32-bit hexadecimal number border routers can use to filter this record.

Usage: Specify a 32-bit hexadecimal number. The default is c0000000.

Dependencies: This parameter does not apply if the Pipeline does not route OSPF.

Location: Ethernet>Mod Config>Route Pref

Route Appletalk

Description: In a Connection profile, enables or disables Appletalk routing for this connection. In the Answer profile, enables or disables Appletalk routing for users connection without authentication, or those who are using Names/Password profiles.

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

- Yes enables Appletalk routing for this connection.
- No disables Appletalk routing for this connection.

Dependencies: Route Appletalk is not applicable if Appletalk is set to No in the Ethernet > Mod Config profile.

Location: Ethernet > Connections> *any Connection profile*, Ethernet > Answer profile > PPP Options

Route IP

Description: Enables or disables the routing of IP data packets on the interface. IP routing must be enabled on both sides of the connection, and the Pipeline unit must be configured with an IP address in the Ethernet profile. To establish an inbound connection, IP routing must also be enabled in the Answer profile.

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

- Yes enables IP routing.
- No means the Pipeline will not route IP for this connection (if set in the Connection profile) or accept inbound IP routing connections (if set in the Answer profile).

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

See Also: Encaps, Profile Reqd

Route IPX

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

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

- Yes enables IPX routing.
- No means the Pipeline will not route IPX for this connection (if set in the Connection profile) or accept inbound IPX routing calls (if set in the Answer profile).

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

See Also: Bridge, IPX Frame, IPX Net

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 configured to work in one of two ways:

- The Pipeline makes a connection to a remote network, gets an official IP address for the remote network through PPP negotiation, and uses the official address for all address translations.
- The Pipeline makes a connection to a remote network, borrows multiple official IP addresses from a DHCP server on the remote network, and uses each address for translating the packets to and from a specific host on the local network.

When NAT is disabled, the Pipeline releases any IP addresses it has borrowed from the remote network, translation stops, and packets flow between LAN and WAN as they normally would.

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

- Yes enables NAT.
- No disables NAT.

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 Pipeline or other 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.

  Note: But note that the Pipeline or other 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: 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 to 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

See Also: Def Server, Dst Port#, Loc Adrs, Loc Port#, Lan, Routing, Protocol

RunOSPF

Description: Enables or disables OSPF on the interface. When OSPF is active, the Pipeline sends update packets out on the interface. These packets set the correct link state for the interface and make sure that the local link-state database is an exact copy of the database maintained by other OSPF routers.

Usage: Specify Yes No. No is the default.

- Yes turns on OSPF routing on the interface. OSPF is meant to run on nailed connections.
- No turns off OSPF on the interface.

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

S

SAP HS Proxy

Description: Specifies whether the Pipeline performs SAP Home Server Proxy. SAP Home Server Proxy enables you to direct NetWare SAP broadcasts to specified networks. By default, when you initially load any IPX client software on your PC, a SAP Request packet is broadcast asking for any servers to reply. The first SAP reply received is taken to be the nearest server, and your PC is attached to that server.

If you load your client software from another PC, or use the same PC when travelling, the initial SAP Request could receive responses from different servers and attaching you to different servers. NetWare SAP Home Server Proxy adds the ability for you to direct SAP Requests to specific networks. The SAP Responses come from servers on these specified networks rather than coming from servers that are near the Pipeline.

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

- Yes enables NetWare SAP Home Server Proxy.
- No disables NetWare SAP Home Server Proxy.

Dependencies: The SAP HS Proxy parameter does not apply if IPX routing is disabled.

Location: Ethernet > Connections > Any Connection Profile > IPX Options

See Also: SAP HS Proxy Net #n

SAP HS Proxy Net#n (n=1-6)

Description: Specifies an IPX network to which SAP broadcasts should be directed.

Usage: Enter an IPX network number using an 8-digit (4-byte) hexadecimal value. The default is 00000000.

Dependencies: The SAP HS Proxy Net#n parameter does not apply if either IPX routing is disabled or if SAP Home Server Proxy is disabled.

Location: Location: Ethernet > Connections > Any Connection Profile > IPX Options

See Also: SAP HS Proxy

SAP Reply

Description: Enables or disables a home agent's ability to reply to the mobile node's IPX Nearest Server Query if the home agent knows about a server on the home network. It is used only when accessing this unit as a home agent.

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

- Yes enables the Pipeline configured as ATMP home agent to reply to a mobile node's Nearest Server Query with the address of a server on the home network.
- No means the Pipeline will not respond to these queries from a mobile node.

Location: Ethernet>Mod Config>ATMP Options

See Also: ATMP Gateway, ATMP Mode

Sec DNS

Description: Specifies the IP address of the secondary domain name server. It will be accessed only if the primary DNS server is unavailable.

Usage: Specify the IP address of the secondary domain name server. The default is 0.0.0.0. Accept this default if you do not have a secondary domain name server.

Example: Sec DNS=200.207.23.1

Location: Ethernet>Mod Config>DNS

See Also: Domain Name, Pri DNS

Sec Domain Name

Description: Specifies a secondary domain name that the 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

See Also: Domain Name

Security

Description: Enables or disables a kind of security, which differs depending on where the parameter appears.

Usage: Specify one of the following values:

For SNMP address security, the default is No.

- Yes means the Pipeline compares the source IP address of packets containing SNMP commands against a list of qualified IP addresses specified in the RD Mgr1-5 and WR Mgr1-5 parameters. (The Pipeline always checks the version and community strings before making source IP address comparisons. The Security parameter does not affect those checks.)
- No means the Pipeline does not compare IP addresses, so address-security is not used.

For SNMP traps, the default is No.

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

For terminal-server security, the default is None.

- Full means users are prompted for a name and password upon initial login and when they switch between terminal mode and menu mode.
- Partial means they are prompted for a name and password only when entering terminal mode, not for menu mode.
- None means they are not prompted for a login name and password to enter the terminal-server interface.

Location: Ethernet>Mod Config>TServ Options, Ethernet>Mod Config>SNMP Options, Ethernet>SNMP Traps

See Also: Initial Scrn, Max DS0 Mins, Passwd, RD Mgr1-5, Toggle Scrn, WR Mgr1-5

Sec WINS

Description: Specifies the IP address of the secondary NetBIOS server.

Usage: Specify an IP address. The default is 0.0.0.0.

Example: Sec WINS=10.2.3.4

Location: Ethernet>Mod Config>DNS

See Also: Pri WINS

Send Auth

Description: Specifies the authentication protocol that the Pipeline uses to send a password to the far-end of a PPP connection.

Usage: Specify one of the following values:

- None (the default) means the Pipeline does not use an authentication protocol to validate incoming sessions.
- PAP indicates the Password Authentication Protocol.

  PAP provides a simple method for a host to establish its identity in a two-way handshake. Authentication takes place only upon initial link establishment, and does not use encryption. The remote device must support PAP, and you must specify a password in the Send PW parameter.
- CHAP indicates the Challenge Handshake Authentication Protocol.

  CHAP is more secure than PAP. It provides a way to periodically verify the identity of a host using a three-way handshake and encryption. Authentication takes place upon initial link establishment; the Pipeline can repeat the authentication process any time after the connection is made. The remote device must support CHAP, and you must specify a password in the Send PW parameter.
- PAP-TOKEN is an extension of PAP authentication.

  In PAP-TOKEN, the user making outgoing calls from the 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 (Network Access Server) obtains the challenge key from a security server that it accesses through RADIUS.

  If you specify PAP-TOKEN-CHAP, you must enter a password in the Aux Send PW parameter; this password must match the password in the RADIUS entry for authenticating the call. If you do not enter identical passwords in the Aux Send PW parameter and the RADIUS entry, the Pipeline cannot extend the MP+ call beyond a single channel.
- CACHE-TOKEN begins authentication using a hand-held security card, and fills a token cache set up for you on the RADIUS server.

  CHAP authenticates your subsequent calls without using your hand-held security card. After a period of time configured in your entry in the RADIUS users file, the token cache expires and the next call you place must again be authenticated using your hand-held security card.

  If you request CACHE-TOKEN, the Send PW parameter must match the Ascend-Receive-Secret attribute in the RADIUS entry that authenticated the call. If you do not enter identical passwords in the Send PW parameter and Ascend-Receive-Secret attribute, CACHE-TOKEN calls are rejected after initial access through hand-held security card authentication.

Dependencies: For a nailed connection, you must set Recv Auth and Send Auth to the same value at both ends of the connection. PAP-TOKEN and PAP-TOKEN-CHAP require configuration of a SAFEWORD or ACE entry in the NAS’s RADIUS users file with the caller’s name. See the *MAX Security Supplement* for details.

Location: Ethernet>Connections>Encaps Options

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

Send PW

Description: Specifies the password that the Pipeline sends to the far-end while the connection is being authenticated. If this password is not received by the far-end device, authentication fails.

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

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

Location: Ethernet>Connections>Encaps Options

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

Server

Description: Specifies the IP address of a BOOTP server that handles 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. 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.

Usage: To enable the Pipeline to communicate with a BOOTP server, specify the server's IP address. The default is 0.0.0.0.

Location: Ethernet>Mod Config>BOOTP Relay

See Also: BOOTP Relay Enable

Server Name

Description: Specifies the name of a NetWare server. In an IPX Route profile, it is the server that will be reached via the specified route.

In an IPX SAP Filters profile, it is the name of a local or remote NetWare server. If the server is on the local network and this is an Output filter, this parameter specifies whether to include or exclude advertisements for this server in SAP response packets. If the server is on the remote IPX network and this is an Input filter, the Server Name parameter specifies whether to include or exclude this server in the Pipeline service table.

Usage: Specify a NetWare server name. In an IPX SAP filter, you can use the wildcard characters * and ? for partial name matches.

Dependencies: These parameters do not apply if IPX routing is not in use.

Location: Ethernet>IPX Routes, Ethernet>IPX SAP Filters>Input SAP Filters>In filter *N*, Ethernet>IPX SAP Filters>Output SAP Filters>Out filter *N*

See Also: Route IPX, Server Type

Server Type

Description: Specifies an SAP service type. SAP advertises services by a type number. For example, NetWare file servers are SAP Service type 0004. For complete information on SAP service types, refer to your Novell NetWare documentation.

In an IPX Route profile, this specifies the type of service advertised by the server that will be reached via the specified route.

In an IPX SAP Filters profile, the Server Type parameter specifies whether to include or exclude advertisements for the specified service type in SAP response packets. In an Input filter, it specifies whether to include or exclude remote services of this type in the Pipeline service table.

Usage: Specify a a hexadecimal number that represents a valid SAP service type.

Location: Ethernet>IPX RoutesEthernet>IPX SAP Filters>Input SAP Filters>In filter *N*, Ethernet>IPX SAP Filters>Output SAP Filters>Out filter *N*

See Also: Server Name, Type, Valid

Sess Timer

Description: This parameter is not supported on the Pipeline.

Session Key

Description: This parameter is not supported on the Pipeline.

Shared Prof

Description: Enables multiple connections to share a local Connection profile. Sharing a profile cannot result in two IP addresses sharing the same interface, so this parameter is typically used to share profiles that are bridged.

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

- Yes means the Pipeline will allow more than one caller to share the same profile, provided that no IP address conflicts will result.
- No means the Pipeline will not allow shared profiles.

Location: Ethernet>Mod Config

See Also: Encaps, Name, Recv PW

SNTP Enabled

Description: Enables or disables the Pipeline to use Simple Network Time Protocol (SNTP), as described in RFC 1305, to set and maintain its system time by communicating with an SNTP server. SNTP must be enabled for the Pipeline to communicate using that protocol.

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

- Yes enables the Pipeline to use an SNTP server to maintain its time.

- No disables SNTP.

Dependencies: If enable SNTP, you must specify at least one SNTP server address.

Location: Ethernet>Mod Config>SNTP Server

See Also: SNTP Host #N, Time Zone

SNTP Host #N (N=1–3)

Description: Specifies the IP address of up to three SNTP servers. If the server specified by SNTP Host #1 is not active, the Pipeline sends its requests to SNTP Host #2. If that server is not active, the Pipeline sends its requests to SNTP Host #3.

Usage: Specify an IP address. The default is 0.0.0.0.

Dependencies: This parameter does not apply if SNTP is not enabled.

Location: Ethernet>Mod Config>SNTP Server

See Also: SNTP Enabled, Time Zone

Socket

Description: This parameter should specify a well-known socket number.

Usage: Specify the socket number for the server.

Example: Socket=0000

Dependencies: This parameter does not apply if the Pipeline does not route IPX.

Location: Ethernet>IPX Routes

See Also: Route IPX

Source Addr

Description: Specifies an IP address. If specified, the Pipeline ignores packets from that source for monitoring purposes. If a Source Mask is also specified, the Pipeline uses the combined address and mask to ignore packets from the specified source.

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

Usage: Specify an IP address.

Example: Source Addr=10.2.3.4

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

Location: Ethernet>Mod Config>Multicast

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

Source Mask

Description: Specifies an IP netmask. If specified, the Pipeline uses the combined address and mask to ignore packets from the specified source for heartbeat monitoring purposes.

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

Usage: Specify a netmask.

Example: Source Mask=255.255.255.248

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

Location: Ethernet>Mod Config>Multicast

See Also: HeartBeat Addr, Heartbeat Udp Port, Source Addr, HeartBeat Slot Time, HeartBeat Slot Count, Alarm Threshold

Split Code.User

Description: This parameter is not supported on the Pipeline.

Src Adrs

Description: Specifies a source IP address. After this value has been modified by applying the specified Src Mask, it is compared to a packet's source address.

Usage: Specify a source IP address the Pipeline should use for comparison when filtering a packet. The zero address 0.0.0.0 is the default. If you accept the default, the Pipeline does not use the source address as a filtering criterion.

Example: Src Adrs=10.62.201.56

Dependencies: This parameter applies only to filters of type IP.

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

See Also: Src Mask

Src Mask

Description: Specifies a mask to apply to the Src Adrs before comparing it to the source address in a packet. You can use it to mask out the host portion of an address, for example, or the host and subnet portion.

The Pipeline applies the mask to the address using a logical AND after the mask and address are both translated into binary format. The mask hides the portion of the address that appears behind each binary 0 (zero) in the mask. A mask of all zeros (the default) masks all bits, so all source addresses are matched. A mask of all ones (255.255.255.255) masks no bits, so the full source address to a single host is matched.

Usage: Specify the mask in dotted decimal format. The zero mask 0.0.0.0 is the default; this setting indicates that the 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.

Example: Src Mask=255.255.255.0

Dependencies: This parameter applies only to filters of type IP.

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

See Also: Src Adrs

Src Network Adrs

Description: The source IPX network address. Either the source or destination address (or both) must be specified.

Usage: Enter the hexadecimal value for the source network.

Example: Src Network Adrs=cfff0000

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

See Also: Dst Network Adrs

Src Node Adrs

Description: Specifies a source node address to filter.

Usage: Specify a valid IPX node address. You must specify a value if the Src Network Adrs is not null. The node address ffffffffffff means all nodes in the specified source network.

Example: Src Node Adrs=111222333

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

See Also: Dest Node Adrs

Src Port # (Filters)

Description: Specifies a value to compare with the source port number in a packet. The default setting (zero) indicates that the Pipeline disregards the source port in this filter. Port 25 is reserved for SMTP; that socket is dedicated to receiving mail messages. Port 20 is reserved for FTP data messages, port 21 for FTP control sessions, and port 23 for telnet.

Note: The Src Port Cmp parameter specifies the type of comparison to be made.

Usage: Specify a number between 0 and 65535.

Example: Src Port #=25

Dependencies: This parameter applies only to filters of type IP.

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

See Also: Dst Port #, Dst Port Cmp, Src Port Cmp

Src Port Cmp

Description: Specifies the type of comparison the Pipeline makes when filtering for source port numbers using the Src Port # parameter.

Usage: Specify one of the following values:

- None (the default) means the Pipeline does not compare source port numbers.
- Less means the comparison succeeds if the number is less than the value of Src Port #.
- Eql means the comparison succeeds if the number equals the value of Src Port #.
- Gtr means the comparison succeeds if the number is greater than the value of Src Port #.
- Neq means the comparison succeeds if the number is not equal to the value of Src Port #.

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

See Also: Src Port #

Src Socket

Description: Some NetWare services communicate across specific sockets; for example, file servers typically use socket 0451. In conjunction with Src Socket Cmp, Src Socket # enables you to filter based on socket number.

Usage: Specify the source socket number. Refer to your Novell documentation for NetWare socket numbers.

Example: Src Socket #=0451

Dependencies: Src Socket # does not apply if Src Socket Cmp is set to None.

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

See Also: Src Socket Cmp

Src Socket Cmp

Description: Specifies the type of comparison the Pipeline makes when filtering for source socket numbers using the Src Socket # parameter. Some NetWare services communicate across specific sockets; for example, file servers typically use socket 0451. If you specify the source socket number, you can also specify the type of comparison to be made between the source socket for an IPX packet and the value specified in this filter.

Usage: Specify one of the following values:

- None (the default) means the Pipeline does not compare source port numbers.
- Less means the comparison succeeds if the number is less than the value of Src Socket #.
- Eql means the comparison succeeds if the number equals the value of Src Socket #.
- Gtr means the comparison succeeds if the number is greater than the value of Src Socket #.
- Neq means the comparison succeeds if the number is not equal to the value of Src Socket #.

Dependencies: Src Socket Cmp does not apply if Src Socket # is null.

Example: Src Socket Comp=Gtr

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

See Also: Src Socket Cmp

Static Preference

Description: Specifies the default preference value for statically configured routes.

Usage: Specify a number between 0 and 255. The default value is 100. Zero is the default for connected routes (such as the Ethernet). The value of 255 means “Don't use this route.”

Example: Static Preference=100

Dependencies: These are the default route preference values:

- Routes learned from OSPF=10
- Routes learned from ICMP Redirects=30
- Routes learned from RIP=100
- Static routes in an IP Route profile or Connection profile=100

Location: Ethernet>Mod Config>Route Pref

Station

Description: Specifies the name of the far-end device in this Connection profile.

Note: If this Connection profile specifies a nailed link to the home network for a Pipeline acting as an ATMP home agent in gateway mode, the Station name must match the Ascend-Home-Network-Name attribute in the foreign agent’s RADIUS configuration.

Usage: Specify the name of the far-end device. You can enter up to 31 characters. Make sure you specify the name exactly, including case changes.

Example: Station=NewYork

Location: Ethernet>Connections

See Also: ATMP Mode, Type

Status N (N=1–8)

Description: Enables you to customize the status windows in the VT100 interface so that particular screens appear at startup. The numbers 1 through 8 indicate the position of the status window, starting with the upper left. You can also use Ctrl-D-M to automatically configure the Status parameter.

Usage: Specify a window number in the format *XY-NNN*.

- *X* is the module number, and indicates a virtual or real module.

  A virtual module (0–2) reflects a function of the base system. Virtual module 0 manipulates overall system functions. Virtual module 1 is the WAN interface module, which manipulates the base system's WAN interface. Virtual module 2 is the Ethernet module.
- *Y* is the port number.

  Zero indicates information pertinent to any portion of the module. For system and T1 network windows, the port number is always 0.
- The three digits after the dash are the root number.

  A root number of 000 identifies a top-level branch of the tree. If *N* is not 0 (zero), the root number identifies a window lower in the tree.

Example: Status 1=20-100

Location: System>Sys Config

Sys Diag

Description: Enables or disables permission to perform all system diagnostics.

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

- Yes means the operator can use the commands in the Sys Diag menu.
- No specifies that an operator cannot use any of those commands.

Location: System>Security

See Also: Chapter 4, "MAX Diag Command Reference."

Syslog

Description: Specifies whether the Pipeline sends warning, notice, and CDR (Call Detail Reporting) records from the system logs to the Syslog host.

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

- Yes enables the Pipeline to communicate with the Syslog host.
- No disables this function.

Dependencies: If you enable Syslog, you must enter the IP address of the Syslog host in the Log Host parameter.

Location: Ethernet>Mod Config > Auth

See Also: Log Facility, Log Host

T

T1 Retransmission Timer

Description: Specifies the maximum amount of time in ticks the transmitter should wait for an acknowledgment before initiating a recovery procedure.

Usage: Specify a number between 500 and 2000. The default value is 1000 (1 second).

Location: Ethernet>Answer>X.75 Options

See Also: Frame Length, K Window Size, N2 Retransmission Count, X.75

T391

Description: Specifies the number of seconds between Status Enquiry messages.

Usage: Specify a number between 5 and 30. The default is 10.

Dependencies: This parameter applies only if Link Mgmt=T1.617D and T392 is set to a non-zero value.

Location: Ethernet>Frame Relay

See Also: Link Mgmt

T392

Description: Specifies the number of seconds the Pipeline waits for a Status Enquiry message before recording an error. If you specify 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 Pipeline over a nailed-up connection.

Usage: Specify 0 (zero), or a number between 5 and 30. The default is 15.

Dependencies: The T392 parameter applies only if Link Mgmt=T1.617D.

Location: Ethernet>Frame Relay

See Also: Link Mgmt

TCP-Clear

Description: Specifies whether the Pipeline can establish connections that use a proprietary encapsulation method and rely on raw TCP sessions to a local host for processing that encapsulation.

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

- Yes means the Pipeline will answer TCP-Clear connections, provided they meet all other connection criteria.
- No means the Pipeline will not accept raw TCP sessions.

Location: Ethernet>Answer>Encaps

See Also: Encaps

TCP Estab

Description: In a filter of type IP, this specifies whether the filter should match only established TCP connections. You can use it to restrict the filter to packets in an established TCP session. You can only use it if the Protocol number has been set to 6 (TCP); otherwise, it does not apply.

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

- Yes means the filter matches only packets that are part of established TCP connections.
- No removes this restriction.

Dependencies: This parameter does not apply if the Protocol field is set to a value other than 6 (TCP).

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

TCP Timeout

Description: Specifies the length of time during which a Pipeline will attempt to connect to an IP host in the list provided by the DNS server. Since the first host on the list may not be available, the timeout should be short enough to allow the Pipeline to go on to the next address on the list before the client software times out. 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.

After the TCP Timeout period expires, the Pipeline stops attempting to connect to an IP address and will proceed to the next address on the list.

Note, however, that after 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 DNS Timeout has not yet elapsed. The number of start-connection messages the Pipeline will send is fixed.

TCP Timeout applies to all TCP connections initiated from the Pipeline, including Telnet, TCP-Clear, and the TCP portion of DNS queries.

Usage: Enter a timeout period between 0 and 200 seconds. The default is 0. With the default value, the Pipeline will retry the connection to the address at increasingly large 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 large number of other tasks.

Dependencies: TCP Timeout does not apply if List Attempt is disabled.

Location: Ethernet > Mod Config

See Also: List Attempt

Telnet

Description: Enables or disables the Telnet command from the terminal server interface.

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

- Yes means operators can invoke Telnet sessions from the terminal-server interface.
- No disables the use of Telnet in the terminal server.

Example: Telnet=Yes

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

Location: Ethernet>Mod Config>TServ Options

See Also: TS Enabled

Telnet Host Auth

Description: Determines whether immediate Telnet sessions require local authentication in the terminal server or if authentication is the responsibility of the telnet host.

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

- Yes means rely on the Telnet host for authentication.
- No means the immediate Telnet session must be authenticated locally first.

Example: Telnet Host Auth=Yes

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

Location: Ethernet>Mod Config>TServ Options

See Also: Immed Service

Telnet Mode

Description: Specifies the default Telnet mode for terminal-server Telnet users.

Usage: Specify one of the following values:

- ASCII

  Standard 7-bit mode. In 7-bit mode, bit 8 is set to 0 (zero); 7-bit telnet is also known as NVT (Network Virtual Terminal) ASCII. This is the default if no other mode is specified.
- Binary

  The Pipeline attempts to negotiate the telnet 8-bit binary option with the server at the remote end. You can run X -Modem and other 8-bit file transfer protocols using this mode.

  In 8-bit binary mode, the telnet escape sequence does not operate. The telnet session can close only if one end of the connection quits the session. If you are a local user not connected through a digital modem, the remote-end user must quit.

A user can override the binary setting on the Telnet command line.

- Transparent

  You can send and receive binary files without having to be in Binary mode. You can run the same file transfer protocols available in Binary mode.

Example: Telnet mode=ASCII

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

Location: Ethernet>Mod Config>TServ Options

See Also: TS Enabled

Telnet PW

Description: Specifies the password users must enter to access the Pipeline unit via telnet. If you specify a password, users are allowed three tries of 60 seconds each to enter the correct password.

Usage: Specify a password containing up to 20 characters. The default is null. If you leave this parameter blank, the Pipeline does not prompt users for a password.

Example: Telnet PW=Ascend

Location: Ethernet>Mod Config

Term Rate

Description: Specifies the bit rate of the Pipeline Control port. When you modify the bit rate of the Control port, you may also need to change the data rate setting of the terminal accessing that port.

Usage: Specify one of the following values:

- 57600
- 38400
- 19200
- 9600 (the default)
- 4800
- 2400

Example: Term Rate=9600

Location: System>Sys Config

Term Type

Description: Specifies the default terminal type for Telnet sessions.

Usage: Specify the a terminal type. You can enter up to 15 characters. The default is VT100.

Example: Term Type=VT100

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

Location: Ethernet>Mod Config>TServ Options

See Also: TS Enabled

Third-Party

Description: This enables OSPF third-party routing for a static route. When enabled, the gateway address is used as the third-party router for this route. Third-party routing enables an OSPF router to advertise a route to a destination network through a remote router (Router-A advertises a route to Network-B via Router-C). This is accomplished by specifying the address of the remote router (Router-C) in the next-hop field of an LSA.

Note: In some cases, third-party routing results in more efficient routes, because other OSPF routers (such as Router-D and Router-E) might be able to trim one hop off of the packet's path and send it to the specified address (Router-C) directly. In practice, it requires that the third-party router is on an Ethernet that is running OSPF, and that its designated router is advertising that network into the OSPF cloud.

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

- Yes enables third-party routing for the OSPF router.
- No disables third-party routing.

Example: Third Party=Yes

Location: Ethernet>Static Rtes

See Also: Gateway

Tick Count

Description: Specifies the distance to the destination network in IBM PC clock ticks (18 Hz). This value is for round-trip timer calculation and for determining the nearest server of a given type.

Usage: Specify an appropriate value. In most cases, the default value (12) is appropriate.

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

Location: Ethernet>IPX Routes

See Also: Route IPX

Time

Description: Specifies the time of day.

Usage: Specify the time of day in the format *hour*:*minutes*:*seconds*. The default is 00:00:00.

Example: Time=13:24:24

Location: System>Sys Config

Time Zone

Description: Specifies your time zone as an offset from the UTC (Universal Time Configuration) to enable the Pipeline to update its system time from an SNTP server. UTC is in the same time zone as Greenwich Mean Time (GMT), and the offset is specified in hours using a 24-hour clock. Because some time zones, such as Newfoundland, cannot use an even hour boundary, the offset includes four digits and is stated in half-hour increments. For example, in Newfoundland the time is 1.5 hours ahead of UTC, which is represented as follows:

```
UTC+0130
```

For San Francisco, which is 8 hours ahead of UTC:

```
UTC+0800
```

For Frankfurt, which is 1 hour behind UTC:

```
UTC-0100
```

Usage: Specify the value that represent your time zone.

Example: Time zone=UTC -0700

Dependencies: This parameter is not applicable unless SNTP Enabled is Yes.

Location: Ethernet>Mod Config>SNTP Server

See Also: SNTP Enabled, SNTP Host #

Timeout Busy

Description: This parameter is not supported on the Pipeline.

Toggle Scrn

Description: Specifies whether an interactive user is allowed to switch between menu mode and the terminal server command line. Users switch to menu mode by using the terminal server Menu command, and switch from menu mode to the command line by pressing the zero key. If this parameter is set to No, the menu command and 0 command are disabled.

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

- Yes means terminal-server users can switch between terminal mode and menu mode.
- No means users have access only to the screen configured to come up initially.

Example: Toggle Scrn=No

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

Location: Ethernet>Mod Config>TServ Options

See Also: Initial Scrn

TransitDelay

Description: Specifies the estimated number of seconds it takes to transmit a Link State Update (LSU) Packet over this interface. Before transmission, link state advertisements (LSAs) contained in the LSU packet have their ages incremented by the amount you specify.

Usage: Specify a number greater than 0 (zero). This value should take into account transmission and propagation delays. The default is 1.

Example: TransitDelay=1

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

TS Enabled

Description: Enables or disables terminal services.

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

- Yes enable the terminal server.
- No disables the terminal server.

Example: TS Enabled=Yes

Location: Ethernet>Mod Config>TServ Options

Type

Description: Specifies the type of ATMP functionality supported in the Pipeline, or if it appears in a filter, the action performed by the filter.

Usage: Specify one of the following values:

In an Ethernet profile:

- Router specifies that the Pipeline is an ATMP home agent in routing mode (the default for ATMP home agents)
- Gateway specifies that the Pipeline is an ATMP home agent in gateway mode.

In a Filter profile:

- Generic means the filter examines byte and offset values within packets, regardless of which protocol is in use (the default in Filter profiles).
- IP means the filter examines the IP-specific fields within packets.

In an IPX SAP Filter profile:

- Exclude means the filter excludes the service defined in the filter (the default).
- Include specifies that the filter includes the service in the service table (if inbound) or in SAP response packets (if outbound).

Location: Ethernet>Mod Config>ATMP Options, Ethernet>Filters>Input filters>In filter N,Ethernet>Filters>Output filters>Out filter N, Ethernet>IPX SAP Filters>Input SAP Filters>In filter *N*, Ethernet>IPX SAP Filters>Output SAP Filters>Out filter *N*

See Also: ATMP Gateway, ATMP Mode, Password, Server Name, Server Type, Station, UDP Port, Valid

U

UDP Cksum

Description: Enables or disables the use of UDP checksums on this interface. If enabled, the Pipeline generates a checksum whenever it sends out a UDP packet. It sends out UDP packets for queries and responses related to the following protocols:

- ATMP
- SYSLOG
- DNS
- ECHOSERV
- RADIUS
- TACACS
- RIP
- SNTP
- TFTP

Note: You may want to enable this parameter if data integrity is of the highest concern for your environment, and having redundant checks is important; this setting is also appropriate if your UDP-based servers are located on the remote side of a WAN link that is prone to errors.

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

- Yes generates UDP checksums for queries and responses related to protocols that use UDP.
- No disables UDP checksums.

Example: UDP Cksum=Yes

Location: Ethernet>Mod Config

UDP Port

Description: Specifies the UDP port on which the Pipeline listens when using ATMP. Units that use UDP to communicate for a particular purpose must all agree on the assigned port number. For ATMP, both agents must specify the same UDP port number.

Usage: Specify a valid UDP port number (0–65535). The default port number is 5150.

Example: UDP Port=5150

Dependencies: This parameter must match the UDP port configured in other units that communicate with the Pipeline using ATMP.

Location: Ethernet>Mod Config>ATMP Options

See Also: ATMP Gateway, ATMP Mode, Password, Type

Upload

Description: Enables or disables permission to upload the Pipeline configuration from another device.

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

- Yes means the operator can upload the Pipeline configuration from another device. This has the potential of clearing all passwords in the Pipeline.
- No disables this permission.

Example: Upload=Yes

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

Location: System>Security

See Also: Restore Cfg

Use Answer as Default

Description: This parameter is not supported on the Pipeline.

V

Valid (NAT)

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

- 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.

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#, Loc Adrs, Loc Port#, Lan, Routing, Protocol

Valid (Filters)

Description: Enables or disables the current input or output filter. When it is set to No, that input or output filter is skipped when filtering the data stream. You must set this parameter to Yes to configure the filter specification.

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

- Yes activates the filter and enables its configuration.
- No disables the filter, causing the Pipeline to skip it when filtering the data stream.

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

See Also: Server Name, Server Type, Type

Value

Description: Specifies a hexadecimal number to be compared to specific bits contained in packets after the Offset, Length, and Mask calculations have been performed. The 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.

Usage: Specify a hexadecimal number up to 12 bytes.

Example: Value=e0e0030000000000

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

See Also: Length, Mask, Offset

Version

Description: Specifies the version number of a Secure Access Firewall. Each firewall contains a version number to ensure that any firewall that is uploaded to the router will be compatible with the firewall software on the Pipeline. Secure Access Manager (SAM) checks the version number before uploading a firewall. In the event that an Pipeline with a stored firewall profile receives a code update that makes the existing firewall incompatible, a default firewall is enabled, permitting only Telnet access to the Pipeline.

Usage: This parameter cannot be edited.

Location: Ethernet>Firewalls

VJ Comp

Description: Specifies whether Van Jacobson IP header prediction should be negotiated on incoming connections using encapsulation protocols that support this feature. VJ Comp applies only to packets in TCP applications, such as Telnet. Turning on header compression is most effective in reducing overhead when the data portion of the packet is small.

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

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

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

W

WAN Alias

Description: Specifies the IP address of the link's remote interface to the WAN. It is used to identify a numbered interface at the remote end of the link. If an address is specified for WAN alias, the following events occur:

- Host routes are created both to the Lan Adrs and the WAN Alias address. The WAN Alias will be listed in the routing table as a gateway (next hop) to the Lan Adrs.
- A route is created to the remote system's subnet, showing the WAN Alias as the next hop.
- Incoming PPP connections must report their IP addresses as the WAN Alias (rather than the Lan Adrs). That is, the other side of the connection must be using a numbered interface, and its interface address must agree with the WAN Alias on the receiving side.

If you want to create static routes to hosts at the remote end, you can use the WAN Alias address as the "next hop" (gateway) field. (The Lan Adrs address will also work, as would be used for system-based routing.)

Usage: Specify the IP address of the remote interface. The default is 0.0.0.0/0.

Example: WAN Alias=10.207.23.7/24

Dependencies: This parameter does not apply if the connection does not route IP.

Location: Ethernet>Connections>IP Options

See Also: Route IP, IF Adrs

WAN Interface

Description: Specifies the type of WAN interface the Pipeline uses.

Usage: Specify one of the following values:

- Nailed T1-CSU specifies that the WAN interface is the nailed T1 line. This is the default for T1 units.
- Nailed-E1 specifies that the WAN interface is the nailed E1 line. This is the defualt for E1 units.

- Serial WAN specifies that the WAN interface is the Serial WAN line.

Note: You must reset the Pipeline before any changes to this parameter take effect.

Location: System > Sys Config

WR MgrN (N=1–5)

Description: These parameters specify up to five IP addresses of SNMP managers that have SNMP write permission. The Pipeline responds to SNMP SET, GET, and GET-NEXT commands from these SNMP managers only, provided that the Security parameter is set to Yes.

Usage: Specify the IP address of a host running an SNMP manager. The default setting is 0.0.0.0; this setting indicates no host.

Example: WR Mgr1= 10.5.6.7/29

Dependencies: The Security parameter must be set to Yes for these parameters to restrict read-write access to the Pipeline.

Location: Ethernet>Mod Config>SNMP Options

See Also: Security, RD Mgr1-5

X

X.75

Description: Specifies whether the Pipeline accepts connections that use X.75 encapsulation.

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

- Yes indicates that the Pipeline accepts incoming X.75 connections.
- No indicates that the Pipeline does not accept incoming X.75 connections.

Location: Ethernet>Answer>Encaps

See Also: Frame Length, K Window Size, N2 Retransmission Count, T1 Retransmission Timer

Z

Zone Name

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

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

Dependencies: Keep this additional information in mind:

- If AppleTalk routing is disabled, Zone Name does not apply.
- In the Ascend AppleTalk router, zone names are not case-sensitive. However, since some routers regard zone names as case-sensitive you should be consistent in spelling zone names when you configure multiple connections or routers.

Location: Ethernet>Mod Config>AppleTalk

Zone Name *# n*

Description: An Appletalk zone is a multicast address containing an arbitrary subset of the AppleTalk nodes in an internet. Each node belongs to only one zone, but a particular extended network can contain nodes belonging to any number of zones. Zones provide departmental or other groupings of network entities that a user can easily understand.

Usage: Specify an Appletalk zone name of up to 33 alphanumeric characters. This name will appear in the AppleTalk Zones window of the Chooser. The default is null.

Dependencies: Keep this additional information in mind:

- If AppleTalk routing is disabled, Zone Name #*n* does not apply.
- In the Ascend AppleTalk router, zone names are not case-sensitive. However, since some routers regard zone names as case-sensitive you should be consistent in spelling zone names when you configure multiple connections or routers.

Location: Ethernet > Connections> *any Connection profile* > AppleTalk Options, Ethernet > Mod Config > Appletalk

See Also: Appletalk, Appletalk Router, Net End, Net Start

VT100 Interface System Administration

3

This chapter covers the following topics:

Introduction to Pipeline administration

The Pipeline's VT100 interface provides a wide variety of features for monitoring and administering the unit's activities.

The initial display of the VT100 interface shows the Main Edit menu and a group of status windows. The status windows display a variety of information about the operation of your Pipeline. You also have access to DO commands, which enable you to perform additional tasks. (To perform any of the administrative tasks, you must activate administrative permissions.)

An additional advantage of being able to use the VT100 interface is that it provides access to the terminal-server command-line interface, which features a large assortment of powerful commands. For example: You can view the Pipeline unit's routing tables and statistical information. You can access detailed information about the unit's IP routing table, OSPF routing table, and Frame Relay connections. You can also use the administrative commands Ping, Traceroute, Telnet, and IPXping to establish and test connectivity. You can manually add, delete or change routes in your IP routing table. Descriptions of the commands available through the terminal-server command-line interface form the major part of the this chapter.

Accessing the VT100 interface

You can access the VT100 user interface either through the Pipeline Control port or via a Telnet connection over Ethernet. This section describes both access methods.

Using the Pipeline control port

Before you can use the control port, some settings in your PC's communications software must match those on the Pipeline. Set the terminal emulation software as follows:

- 9600 bps
- 8 data bits
- No parity
- 1 stop bit
- No flow control
- Direct connect

To access the Pipeline's VT100 user interface via its control port:

1 Connect your PC's serial port to the Pipeline's control port using a serial cable.

2 On your PC, launch your communications software in terminal emulation mode.

3 Press Ctrl-L to refresh the screen display.

The VT100 interface appears on your computer screen. The VT100 interface consists of a Main Edit menu on the left side of the display, and eight status windows on the right side of the display.

Using Telnet

To be accessible through Telnet, the Pipeline must have a valid IP address and be reachable by your PC over Ethernet. If you are unsuccessful, but believe the PC and Pipeline are configured correctly, contact your network administrator for help. To connect to the Pipeline's VT100 interface through Telnet:

1 From your PC, launch your Telnet software.

2 Telnet to the Pipeline's IP address. If prompted, enter the Telnet password.

The VT100 interface appears on your computer screen. The VT100 interface consists of a Main Edit menu on the left side of the display, and eight status windows on the right side of the display.

Using the VT100 interface

This section explains how to explain how to navigate the VT100 interface.

Making a menu or status window active

You can interact with only one display at a time. The active display has a thick double line border on the left, right, and top sides.

If you press the Tab key, the thick double lines move to 00-200, the next screen to the right. If you continue pressing the Tab key, you activate each window from left to right and down, until you reach the last display in the lower right-hand corner. Back-Tab or Ctrl-O moves you in the opposite direction.

Opening menus and profiles

The Main Edit Menu contains a list of menus, each of which can contain profiles and submenus. In the menu that is currently open, the cursor character (>) points to one item in the menu. To move the cursor down, press Ctrl-N (next) or the down-arrow key. To move it up, press Ctrl-P (previous) or the up-arrow key. (Some VT100 emulators do not support the use of arrow keys.) For a complete list of key combinations used to navigate the interface, see Table 3-1 on page 3-6.

```
Main Edit Menu
     00-000 System
     >10-000 Serial Port T1-CSU
     20-000 Ethernet
```

To open a menu, move the cursor to the menu's name and press Enter. For example, press Ctrl-N until the cursor points to 30-000 Ethernet, and press Enter. The Ethernet menu opens.

```
  90-000 Ethernet
    90-100 Connections
    90-200 Bridge Adrs
    90-300 Static Rtes
    90-400 Filters
    90-500 Firewalls
    90-600 Frame Relay
    90-700 Answer
    90-800 SNMP Traps
    90-900 IPX Routes
    90-A00 IPX SAP Filters
    90-B00 NAT
    90-C00 Mod Config
```

The Ethernet menu contains submenus and profiles related to network functionality, such as bridging, routing, WAN connections, and so forth. The Mod Config Profile in this menu relates to the configuration of the Ethernet interface itself, as shown next.

```
   90-B00 Mod Config
     Module Name=
     Ether1 options...
     Ether2 options...
     WAN options...
     SNMP options...
     OSPF options...
     OSPF global options...
     Route Pref...
     TServ options...
     Bridging=No
     IX Routing=No
     Appletalk=No
     Shared Prof=No
     Telnet PW=****
     RIP Policy=Poison Rvrs
     RIP Summary=Yes
```

```
    ICMP Redirects=Accept
```

Note: With the exception of parameters designated N/A (not applicable), you can edit all parameters in any profile. A profile is a group of parameters listed under a particular menu entry. N/A that means a parameter does not apply within the context of how some other parameter(s) or profile has been set.

Opening edit fields

To open an edit field for a text-based parameter (such as a password, for example), move the cursor to that parameter and press Enter. An edit field opens, delimited by brackets, as shown for the Telnet PW parameter, next.

```
90-B00 Mod Config
  Module Name=
  Ether1 options...
  Ether2 options...
  WAN options...
  SNMP options...
  OSPF options...
  OSPF global options...
  Route Pref...
  TServ options...
  Bridging=No
  IX Routing=No
  Appletalk=No
  Shared Prof=No
  Telnet PW:
  [ ]

  ICMP Redirects=Accept
```

Note: See “About Pipeline passwords” on page 3-7 for related information.

A blinking text cursor appears in the brackets, indicating that you can start typing text. If the field already contains text, it is cleared when you type a character. To modify only a few characters of existing text, use the arrow keys to position the cursor and then delete or overwrite the characters.

To close the edit field and accept the new text, press Enter.

Setting enumerated parameters

An enumerated parameter is one for which there is a set of predefined values.You modify it by simply placing the cursor beside the parameter and typing the Enter, Return, or the Right-Arrow key until the proper value appears.

Saving your changes

When you exit a profile, you are prompted to confirm that you want to save changes.

```
EXIT?
>0=ESC (Don’t exit)
 1=Exit and discard
 2=Exit and accept
```

You can save the profile values by choosing the Exit and Save option and pressing Enter, or by pressing 2.

Special display characters and keys

The following characters have special meaning within the displays:

- The plus character (+) indicates that an input entry is too long to fit onto one line, and that the Pipeline is truncating it for display purposes.
- Ellipses (...) mean that a submenu displays the details of a menu option.

  The Pipeline displays the submenu when you select the menu option.

The following table lists the special-purpose keys and key combinations you can use in the Control Monitor displays.

Table 3-1. Special purpose keys for Control Monitor displays

Key combination	Operation
Right-Arrow, Return, Enter, Ctrl-Z, Ctrl-F	Enumerated parameter: Select the next value. String value: Move one character to the right or enter the current input. Menu: Open the current selection.
Left-Arrow, Ctrl-X, Ctrl-B	Enumerated parameter: Select the previous value. String value: Move left one character or exit the current input. Menu: Close the current selection.
Down-Arrow, Ctrl-N	Move down to the next selection.
Up-Arrow, Ctrl-U, Ctrl-P	Move up to the previous selection.
Ctrl-V	Move to the next page of the list.
Tab, Ctrl-I	Move to the next window.
Back-Tab, Ctrl-O	Move to the previous window.
N/A	Toggle to a status menu from the edit menu and vice versa.
Delete	Delete the character under the cursor.
Backspace	Delete the character to the left of the cursor.
none	Overwrite the character under the cursor with a space.
Ctrl-D	Open the DO menu.
Ctrl-T	Return from or go to the Simplified Menus.
Ctrl-L	Refresh the VT-100 screen.
Ctrl-C	Return from the MIF to the normal menus.
D	Dial the currently selected profile.

Note: You always use the Control and Shift keys in combination with other keys. This document represents key combinations as two characters separated by a hyphen, such as Shift-T, which types the capital letter T.

About Pipeline passwords

The Pipeline has up to nine security levels, each of which is defined in a Security Profile. When shipped from the factory, all nine levels are wide open, with no defined restrictions. To see the list of Security Profiles, open the System menu in the Main Edit Menu, and then select Security and press Enter.

```
00-300 Security
>00-301 Default
 00-302
 00-303
 00-304
 00-305
 00-306
 00-307
 00-308
 00-309 Full Access
```

Whenever the Pipeline is powered on, it activates the first Security Profile in this list, which is always named Default and always has no password. (See the *Pipeline Security Supplement* for full details on modifying Security Profiles and assigning passwords.)

Before you can use the administrative commands and profiles, you must log in as the superuser by activating a Security profile, such as the Full Access profile, that has sufficient permissions.

Note: For a session established via Telnet, you must first supply the Telnet password to establish a Telnet session. Then, the Default security level is set for that session. To configure the Pipeline via Telnet, the user must activate the appropriate Security Profile.

To log in as the superuser, proceed as follows:

1 Press Ctrl-D to open the DO menu, then press P (or select P=Password).

2 In the list of Security profiles that opens, select Full Access.

The Pipeline prompts you for the Full Access password. For example:

```
00-300 Security
Enter Password:
 []

 Press > to accept
```

3 Type the password assigned to the profile and press Enter.

When you enter the correct password, the Pipeline displays a message informing you that the password was accepted and that the Pipeline is using the new security level:

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

If the password you enter is incorrect, the Pipeline prompts you again for the password.

Note: The default password for the Full Access login is *Ascend*.

One of the first thing most administrators do is to reset the privileges in the Default profile to restrict what can be done by anyone accessing the Pipeline configuration menus. To do this:

1 Open the Default Security Profile and set the Operations privilege to No.

2. Assign a password to the Full Access Security Profile. (Do not restrict privileges in the Full Access Profile.)
3. Activate the Full Access Security Profile and proceed to configure the Pipeline.

Using the Pipeline status windows

In the Pipeline VT100 interface, the right side of the screen displays eight status windows. The status windows provide a great deal of read-only information about what is currently happening in the Pipeline.

```
|--------------------| |--------------------|
|10-100 1234567890   | |20-200 Routes       |
| L1/LA nnnnnnnnnn   | |>D: Default         |
|   12345678901234   | | G: 10.10.10.10     |
|   nnnnnnnnnnnnnn   | | LAN Active         |
|--------------------| l--------------------|
|20-100 Sessions     | |00-200 15:10:34     |
|> 2 Active          | |>M31  Line    Ch    |
| 0 dave1-gw         | | LAN session up     |
| 0 lnemo.Ascend.COM | | dave1-gw           |
|--------------------| |--------------------|
|20-300 WAN Stat     | |90-400 Ether Stat   |
|>Rx Pkt:     184318^| |>Rx Pkt:    3486092 |
| Tx Pkt:     159232 | | Tx Pkt:      10056 |
|    CRC:          0v| |    Col:       3530 |
|--------------------| |--------------------|
|00-100 Sys Option   | |20-700 Ether Opt    |
|>Security Prof: 1  ^| |>Enet I/F: UTP      |
| Software +5.1Ap2+  | | Adr0: 00c07b6fd5b8 |
| S/N: 5210003      v| | Adr1: 00c07b6eadc0 |
|--------------------| |--------------------|
```

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

Line status window

Slots 1 and 2 contain the built-in T1 (or E1) lines, with Slot 1 containing the two leftmost lines when you look at the unit's back panel. By default, the status of the lines in Slot 1 is shown in the top two status windows:

```
|--------------------|
|10-100 1234567890   |
| L1/LA nnnnnnnnnn   |
|   12345678901234   |
|   nnnnn.........   |
|--------------------|
```

Each window displays four lines of information, as follows:

- The first line shows the menu number and column numbers for channels 1–10.
- The second line identifies the line (the Pipeline will always indicate L1), and shows a a 2-character link status indicator for the line and a 1-character status indicator for each channel. For example:
  - LA indicates *Link Active* (the line is physically connected).
  - n indicates a channel is nailed.
  - . indicates a channel is not in use.
- The third line has column headers for channels 11–24.
- The fourth line shows a 1-character channel status indicator for channels 11–24.
  - n indicates a channel is nailed.
  - . indicates a channel is not in use.

System Events

The System Events status window provides a log of up to 32 of the most recent system events the Pipeline has recorded:

```
|--------------------|
|00-200 11:23:55     |
|>M31 Line  Ch       |
| LAN session up     |
| REMOTEGW           |
|--------------------|
```

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. 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 window shows the status-window 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.

Line 3

The third line includes the text of the message. The message can contain either basic information or a warning.

Line 4

The fourth line includes a message parameter.

Sessions

The Sessions status window 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:

```
|--------------------|
|20-100 Sessions     |
|>1 Active           |
| 0 REMOTEGW         |
|                    |
|--------------------|
```

The following paragraphs describe each line of the window.

Line 1

The first line specifies the window number and name of the window.

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 3-2 lists the session status characters that can appear.

Table 3-2. Session status characters

Character	Description
Blank	No connection exists and no other Pipeline operations are being performed.
R	Ringing—an incoming call is ringing on the line, ready to be answered.
A	Answering—the Pipeline is answering an incoming call.
C	Calling—the Pipeline is dialing an outgoing call.
O	Online—a call is up on the line.
H	Hanging up—the Pipeline is clearing the call.

Dyn Stat

The Dyn Stat window shows the name, quality, bandwidth, and bandwidth utilization of each online connection:

```
|--------------------|
| 20-500 Dyn Stat    |
| Qual Good 00:02:04 |
| OK      0 channels |
| CLU   0%  ALU  0%  |
|--------------------|
```

You can press the Down Arrow key to see other connections. More than one connection can be online at once.

The following paragraphs describe each line of the window.

Line 1

The first line of the Dyn Stat window shows its window number and the name of the current Connection Profile. If no connection is currently active, the window 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 3-3.

Table 3-3. 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 window shows the current data rate in Kbps, and how many channels the data rate represents.

Line 4

The fourth line displays the CLU and ALU values.

CLU is the Current Line Utilization: the percentage of bandwidth currently being used by the call, divided by the total amount of bandwidth available.

ALU is 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.

WAN Stat

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

```
|--------------------|
|20-300 WAN Stat     |
|>Rx Pkt:  387112    |
| Tx Pkt:   22092    |
|    CRC:  0         |
|--------------------|
```

The following paragraphs describe each line of the menu.

Line 1

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

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 errored frames. CRC checking is performed on PPP and MP+ links. An errored CRC frame includes at least one data error.

Ether Stat

The Ether Stat window shows the number of Ethernet frames received and transmitted and the number of collisions at the Ethernet interface:

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

The window includes the fields described in Table 3-4.

Table 3-4. Ether Stat fields

Field	**Contents**
Rx Pkt	Number of Ethernet frames received from the Ethernet interface.
Tx Pkt	Number of Ethernet frames transmitted over the Ethernet interface.
Col	Number of collisions detected at the Ethernet interface.

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.

Sys Options

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

```
|--------------------|
|00-100 Sys Options  |
|>Security Prof:1    |
| Software +5.1Ap2+  |
|S/N:42901           |
|--------------------|
```

The Sys Options window can contain the information listed in Table 3-5.

Table 3-5. Sys Options information

Option	**Description**
Security Prof: 1, Security Prof: 2...	Identifies which of the nine Security Profiles as currently in use.
Software	Shows the version and revision of the system ROM code.
S/N	Shows the serial number of the Pipeline. The serial number of your Pipeline can also be found on the model number/serial number label on the Pipeline’s bottom panel.
Up: 00:18:02:17	Shows how long since the Pipeline was reset. Time appears in dd:hh:mm:ss format.
Pipeline 220	Shows the Ascend unit is a Pipeline. If there are several types of Ascend units at your site, this helps differentiate between units.
Switched Installed or Switched Not Inst	Shows whether the Pipeline can place calls over switched circuits.

Table 3-5. Sys Options information (continued)

Option	Description
Frm Rel Installed or Frm Rel Not Inst	Shows whether or not the Frame Relay option is installed
Sec Acc Installed or Sec Acc Not Inst	Shows whether or not the Secure Access option is installed.
IPsec Installed or IPsec Not Inst	Shows whether or not the IPsec option is installed.
Dyn Bnd Installed or Dyn Bnd Not Inst	Shows whether Dynamic Bandwidth Allocation functionality is available.
ISDN Sig Installed or ISDN Sig Not Inst	Shows whether ISDN signalling is available.

Ether Opt

The Ether Opt window shows the hardware installed on the Pipeline:

```
|--------------------|
|20-700 Ether Opt    |
|>Enet I/F: UTP      |
| Adr0: 00c07b6e06f7 |
| Adr1: 00c07b6037b8 |
|--------------------|
```

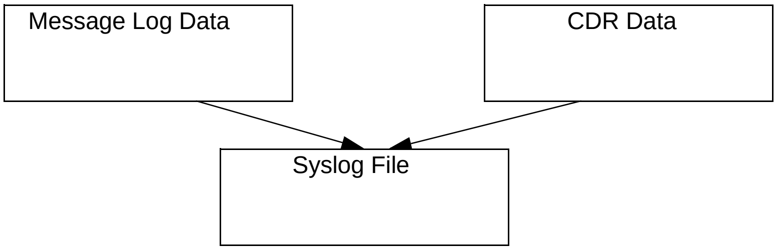
The window includes the fields described in Table 3-4.

Table 3-6. Ether Opt fields

Field	Contents
Enet I/F: UTP	The type of Ethernet connection.
Adr0	MAC Address of the first Ethernet interface of the Pipeline.
Addr1	MAC Address of the second Ethernet interface of the Pipeline.

Syslog

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



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

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

The Message Log provides the data for level 4 (warning) and level 5 (informational) syslog messages. Level 4 and level 5 messages appear in the following format:

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

where:

- *`slot-n port-n | line-n`* is the device address (slot, port or line, and channel). The device address is suppressed when it is not applicable or unknown.
- *text-1* specifies information about the reason for the syslog message. The messages are similar to those shown in the message log window.
- *text-2* specifies the system name, IP address, or MAC address of the remote end of a session for the messages.

Level 5 (notice) syslog messages

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

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

where:

- *call-event-ID* specifies the event ID in the CDR display.
- *event-description* is a description of the CDR event.
- *slot-n port-n* is the address of the AIM port, which is not included in the message if the address is not applicable or not known.
- *data-svcK* indicates the data service in use.
- *phone-n* is the phone number.

Examples

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

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

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

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

This example shows three messages for the system `marcsmax`.

Terminal-server command-line interface

The terminal-server command-line interface provides commands for checking routing tables, Frame Relay connections, and other configuration parameters. To access the terminal-server command-line interface, you must have administrative privileges. (See “About Pipeline passwords” on page 3-7).

You can use any of the following methods to open the terminal-server command-line interface:

- From the Main Edit menu, select System > Sys Diag > Term Serv, press Enter.
- In the Main Edit menu, press Ctrl-D to open the DO menu in the Main Edit menu, the select E=Termsrv.
- Enter the following keystroke sequence (Escape key, left square bracket, Escape key, zero) in rapid succession:

  ```
  <Esc> [ <Esc> 0
  ```

If you have sufficient privileges to access the command line, the Pipeline displays the command-line prompt. For example:

```
** Ascend terminal-server **
```

```
ascend%
```

To display the list of terminal-server commands, either enter a question mark:

```
ascend% ?
```

or the Help command:

```
ascend% help
```

The system responds by listing the terminal-server commands, with brief explanations:

```
?                   Display help information
help                   "     "        "
quit                Closes terminal-server session
hangup                 "      "       "       "
test                test <phone-number> [ <frame-count> ]
local               Go to local mode
remote              remote <station>
set                 Set various items. Type ’set ?’ for help
show                Show various tables. Type ’show ?’ for help
iproute             Manage IP routes.  Type ’iproute ?’ for help
```

```
dnstab              Manage local DNS table.  Type ’dnstab ?’ for help
slip                SLIP command
cslip               Compressed SLIP command
ppp                 PPP command
menu                Host menu interface
telnet              telnet [ -a|-b|-t ] <host-name> [ <port-number> ]
tcp                 tcp <host-name> <port-number>
ping                ping <host-name>
ipxping             ipxping <server-name>
traceroute          Trace route to host.  Type ’traceroute -?’ for help
kill                kill <session ID>
```

Exiting the terminal server interface

The following commands close the terminal-server command-line interface and return the cursor to the VT100 menus.

- `Quit`
- `Hangup`
- `Local`

Commands not supported on the Pipeline

The following terminal-server commands are not supported on the Pipeline:

- `Test`
- `Remote`
- `Slip`
- `CSlip`
- `PPP`
- `Show ISDN`
- `Show Pools`

Commands for use by terminal-server users

The following commands initiate a session with a host, or toggle to a different interface that displays a menu selection of Telnet hosts.

Set command

The Set command takes several arguments. To display them, enter the Set command with a question mark:

```
ascend% set ?
```

```
set ?               Display help information
set all             Display current settings
set term            Sets the telnet/rlogin terminal type
set password        Enable dynamic password serving
set fr              Frame Relay datalink control
set circuit         Frame Relay Circuit control
```

The Set All command displays current settings. For example:

```
ascend% set all
```

```
term = VT100
dynamic password serving = disabled
```

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

The Set Password command applies only when using security card authentication. It 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:

```
ascend% set password
```

```
Entering Password Mode...

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

In password mode, the terminal-server 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: 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. For details about dynamic password serving, see the *Pipeline Security Supplement*.

The Set Circuit command enables you to `turn off` traffic going through a Frame Relay circuit without disabling the circuit endpoints. This command prevents traffic from going between endpoints without disrupting the state of the DLCI. To display the support options, enter the Set Circuit command with a question mark:

```
ascend% set circuit ?
```

```
set circuit ?       Display help information
set circuit active [name]  Set the CIRCUIT to active
set circuit inactive [name]  Set the CIRCUIT to inactive
```

To allow data to flow through a circuit, use the active parameter. For example:

```
ascend% set circuit active circuit-1
```

To turn off data flow without disrupting the state of the DLCIs, use the inactive parameter. For example:

```
ascend% set circuit inactive circuit-2
```

Show command

The Show command takes several arguments. To display them, enter the Show command with a question mark:

```
ascend% show ?
```

```
show ?          Display help information
show arp        Display the Arp Cache
show icmp       Display ICMP information
show if         Display Interface info. Type ’show if ?’ for help.
show ip         Display IP information. Type ’show ip ?’ for help.
show udp        Display UDP information. Type ’show udp ?’ for help.
show igmp       Display IGMP information. Type ’show igmp ?’ for help.
show mrouting   Display MROUTING information.Type ‘show mrouting ?’
show ospf       Display OSPF information. Type 'show ospf ?' for help.
show tcp        Display TCP information. Type 'show tcp ?' for help.
show dnstab     Display local DNS table. Type 'show dnstab ?' for help.
show netware    Display IPX information. Type 'show netware ? ' for
show isdn       Display ISDN events.  Type 'show isdn <line number>'
show fr         Display Frame relay info. Type 'show fr ?' for help.
show pools      Display the assign address pools.
show uptime     Display system uptime.
show revision   Display system revision.
show users      Display concise list of active users
show sessid     Display current and base session id
```

Note: Not all displayed Show commands apply to the Pipeline. See this section for specific information.

Displaying the ARP cache

To display the ARP cache, enter the Show ARP command. For example:

```
ascend% show arp
```

```
entry typ ip address      ether addr    if rtr pkt   insert
    0 DYN 10.65.212.199  00C07B605C07   0   0   0   857783
    1 DYN 10.65.212.91   0080C7C4CB80   0   0   0   857866
    2 DYN 10.65.212.22   080020792B4C   0   0   0   857937
    3 DYN 10.65.212.3    0000813DF048   0   0   0   857566
    4 DYN 10.65.212.250  0020AFF80F1D   0   0   0   857883
    5 DYN 10.65.212.16   0020AFEC0AFB   0   0   0   857861
    6 DYN 10.65.212.227  00C07B5F14B6   0   0   0   857479
    7 DYN 10.65.212.36   00C07B5E9AA5   0   0   0   857602
    8 DYN 10.65.212.71   0080C730041F   0   0   0   857721
    9 DYN 10.65.212.5    0003C6010512   0   0   0   857602
   10 DYN 10.65.212.241  0080C72ED212   0   0   0   857781
   11 DYN 10.65.212.120  0080C7152582   0   0   0   857604
   12 DYN 10.65.212.156  0080A30ECE6D   0   0   0   857901
   13 DYN 10.65.212.100  00C07B60E28D   0   0   0   857934
   14 DYN 10.65.212.1    00000C065D27   0   0   0   857854
   15 DYN 10.65.212.102  08000716C449   0   0   0   857724
   16 DYN 10.65.212.33   00A024AA0283   0   0   0   857699
   17 DYN 10.65.212.96   0080C7301792   0   0   0   857757
   18 DYN 10.65.212.121  0080C79BF681   0   0   0   857848
   19 DYN 10.65.212.89   00A024A9FB99   0   0   0   857790
   20 DYN 10.65.212.26   00A024A8122C   0   0   0   857861
   21 DYN 10.65.212.6    0800207956A2   0   0   0   857918
   22 DYN 10.65.212.191  0080C75BE778   0   0   0   857918
   23 DYN 10.65.212.116  0080C72F66CC   0   0   0   857416
   24 DYN 10.65.212.87   0000813606A0   0   0   0   857666
   25 DYN 10.65.212.235  00C07B76D119   0   0   0   857708
   26 DYN 10.65.212.19   08002075806B   0   0   0   857929
```

In the output:

- `Entry` is a unique identifier for each ARP table entry.
- `Typ` specifies how the address was learned, dynamically (DYN) or statically (STAT).
- `IP Address` indicates the address contained in ARP requests.
- `Ether Addr` indicates the MAC address of the host with that IP address.
- `IF` specifies the interface on which the Pipeline received the ARP request.
- RTR is the next-hop router on the specified interface.

Displaying ICMP packet statistics

To view the number of ICMP packets received intact, received with errors, and transmitted, enter the Show ICMP command. For example:

```
ascend% show icmp
```

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

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

Displaying interface statistics

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

```
ascend% show if ?
```

```
show if ?           Display help information
show if stats       Display Interface Statistics
show if totals      Display Interface Total counts
```

To display the status and packet count of each active WAN link and of the local and loopback interfaces, enter the Show IF Stats command. For example:

```
ascend% show if stats
```

```
Interface    Name    Status  Type     Speed    MTU   InPackets    Out-
packet
ie0        ethernet    Up     6     10000000   1500     107385     85384
wan0                 Down     1            0   1500      0          0
wan1                 Down     1            0   1500      0          0
wan2                 Down     1            0   1500      0          0
wanidle0               Up     6     10000000   1500      0          0
lo0       loopback     Up    24     10000000   1500      0          0
```

In the output:

- `Interface` specifies the interface name (see the *Pipeline 220 Interface Configuration Guide*)
- `Name` is the name of the profile or a text name for the interface
- Status indicates either Up (the interface is functional), or Down.
- `Type` specifies 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` is the data rate in bits per second.
- `MTU` is the maximum packet size allowed on the interface. MTU stands for Maximum Transmission Unit.
- `InPackets` is the number of packets the interface has received.
- `OutPackets` is the number of packets the interface has transmitted.

To display the packet count at each interface, broken down by type of packet, enter the Show IF Totals command. For example:

```
ascend% show if totals
```

```
Name  --Octets----Ucast-- -NonUcast- Discard -Error- Unknown -Same IF-
ie0  i:   7813606   85121     22383       0        0       0        0
     o: 101529978   85306       149       0        0       0        0
wan0 i:         0       0         0       0        0       0        0
     o:         0       0         0       0        0       0        0
wan1 i:         0       0         0       0        0       0        0
     o:         0       0         0       0        0       0        0
wan2 i:         0       0         0       0        0       0        0
     o:         0       0         0       0        0       0        0
wanidle0 i:     0       0         0       0        0       0        0
         o:     0       0         0       0        0       0        0
lo0  i:         0       0         0       0        0       0        0
     o:         0       0         0       0        0       0        0
```

In the output:

- `Name` is the interface name (see the *Pipeline 220 Interface Configuration Guide*)
- `Octets` is the total number of bytes processed by the interface.
- `Ucast` is the number of packets with a unicast destination address.
- `NonUcast` is the number of packets with a multicast address or a broadcast address.
- `Discard` is the number of packets that the interface could not process.
- `Error` is the number of packets with CRC errors, header errors, or collisions.
- `Unknown` is the number of packets the Pipeline forwarded across all bridged interfaces because of unknown or unlearned destinations.
- `Same IF` is the number of bridged packets whose destination is the same as the source.

Displaying IP statistics and addresses

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

```
ascend% show ip ?
```

```
show ip ?           Display help information
show ip stats       Display IP Statistics
show ip address     Display IP Address Assignments
show ip routes      Display IP Routes
```

To display statistics about IP activity, including the number of IP packets the Pipeline has received and transmitted, enter the Show IP Stats command. For example:

```
ascend% show ip stats
```

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

To view IP interface address information, enter the Show IP Address command. For example:

```
ascend% show ip address
```

```
Interface  IP Address    Dest Address   Netmask         MTU     Status
ie0        10.2.3.4      N/A            255.255.255.224   1500      Up
wan0       0.0.0.0       N/A            0.0.0.0           1500    Down
wan1       13.1.2.0      13.1.2.128     255.255.255.248   1500    Down
wan2       0.0.0.0       N/A            0.0.0.0           1500    Down
wan3       0.0.0.0       N/A            0.0.0.0           1500    Down
lo0        127.0.0.1     N/A            255.255.255.255   1500      Up
rj0        127.0.0.2     N/A            255.255.255.255   1500      Up
bh0       127.0.0.3     N/A            255.255.255.255   1500      Up
```

Displaying UDP statistics and listen table

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

```
ascend% show udp ?
```

```
show udp ?          Display help information
show udp stats      Display UDP Statistics
show udp listen     Display UDP Listen Table
```

To display the number of UDP packets received and transmitted, enter the Show UDP Stats command. For example:

```
ascend% show udp stats
```

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

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 the Show UDP Listen command. For example:

```
ascend% show udp listen

Socket       Local Port      InQLen
     0              520            0
     1                7            0
     2              123            0
     3              514            0
     4              161            0
     5              162            0
```

Viewing multicast interfaces

For viewing multicast interfaces, the Pipeline supports Internet Group Management Protocol (IGMP) commands and multicast routing (mrouting) commands.

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

```
ascend% show igmp ?

show igmp ?         Display help information
show igmp stats     Display IGMP Statistics
show igmp groups    Display IGMP groups Table
show igmp clients   Display IGMP clients
```

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

```
ascend% show mrouting ?

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

Displaying the multicast forwarding table

To display active multicast group addresses and clients (interfaces) registered for each group, enter the Show IGMP Groups command. For example:

```
ascend% show igmp groups

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
```

In the output:

- `Hash` is an index to a hash table (displayed for debugging purposes only).

- `Group address` indicates the IP multicast address used in this packet.

  Note: The IP multicast address being monitored is marked with an asterisk, meaning that this address is joined by local application.

- `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. Periods in this field indicate that this membership never expires.
- `Counts` is 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 appears for debugging purposes).

Listing multicast clients

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

```
ascend% show igmp clients
IGMP Clients

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

In the output:

- `Client` indicates the interface ID on which the client resides. 0 represents the Ethernet. Other numbers are 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) indicates percentage of bandwidth currently utilized across the interface. If bandwidth utilization is high, some IGMP packet types will not be forwarded.
- `ALU` (Average Line Utilization) indicates percentage of bandwidth utilized across the interface. If bandwidth utilization is high, some IGMP packet types will not be forwarded.

Displaying multicast activity

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

```
ascend% show igmp stats
       46 packets received.
        0 bad checksum packets received.
        0 bad version packets received.
        0 query packets received.
```

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

Viewing Multicast Routing statistics

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

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

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

Monitoring OSPF

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

```
ascend% show ospf ?
show ospf ?              Display help information
show ospf errors         Display OSPF errors
show ospf areas          Display OSPF areas
show ospf general        Display OSPF general info
show ospf interfaces     Display OSPF interfaces
show ospf lsdb           Display OSPF link-state DB
show ospf lsa            Display OSPF link-state advertisements
show ospf nbrs           Display OSPF neighbors
show ospf rtab           Display OSPF routing tab
show ospf io             Display OSPF io
```

Viewing OSPF errors

To view OSPF errors, enter the Show OSPF Errors command. For example:

```
ascend% show ospf errors
ERRORS from:                       boot
   0: IP: Bad OSPF pkt type             0: IP: Bad IP Dest
   0: IP: Bad IP proto id               1: IP: Pkt src = my IP addr
   0: OSPF: Bad OSPF version            0: OSPF: Bad OSPF checksum
   0: OSPF: Bad intf area id            0: OSPF: Area mismatch
   0: OSPF: Bad virt link info          0: OSPF: Auth type != area type
   0: OSPF: Auth key != area key        0: OSPF: Packet is too small
   0: OSPF: Packet size > IP length     0: OSPF: Transmit bad
   0: OSPF: Received on down IF         0: Hello: IF mask mismatch
   0: Hello: Unknown Virt nbr           0: Hello: Unknown NBMA nbr
   0: DD: Unknown nbr                    0: DD: Nbr state low
   0: DD: Nbr's rtr = my rtrid           0: DD: Extern option mismatch
   0: Ack: Unknown nbr                   0: Ack: Nbr state low
   0: Ls Req: Nbr state low              0: Ls Req: Unknown nbr
   0: Ls Req: Empty request              0: LS Req: Bad pkt
   0: LS Update: Nbr state low           0: Ls Update: Unknown nbr
   0: Ls Update: Newer self-gen LSA      0: Ls Update: Bad LS chksum
```

The output lists all error messages related to OSPF, with each message preceded by the number of times it has been generated since the Pipeline powered up. Immediately following the number is a field indicating the packet type:

- IP (IP packets)
- OSPF (OSPF packets)
- Hello (Hello packets)
- DD (Database Description packets, which are exchanged periodically between neighbors)
- Ack (every DD packet must be acknowledged)
- LS Req (Link-state request— a request for an updated database)
- LS Update (An exchange to update databases)

Viewing OSPF areas

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

```
ascend% show ospf areas
```

```
Area ID: 0.0.0.0
Auth Type: Simple Passwd  Import ASE: On  Spf Runs: 23
Local ABRs: 0  Local ASBRs: 5  Inter LSAs: 7  Inter Cksum sum: 0x2ee0e
```

In the output:

- `Area ID` specifies the area number in dotted-decimal format.
- `Auth Type` indicates the type of authentication, Simple or Null.
- `Import ASE` specifies route calculation method. In effect, it specifies whether the router is an ABR or not. This functionality is always ON in the Pipeline.
- `Spf Runs` is the number of times the SPF calculation was run. The calculation is performed every time the router notes a topology change or receives an update from another router.
- `Local ABRs` is the number of ABRs the router knows about and the number of areas. Zero (0) indicates the router knows about the backbone area only.
- `Local ASBRs` is the number of ASBRs the router knows about.
- `Inter LSAs` shows the number of entries in the link-state database.
- `Inter Cksum sum` shows the checksum to indicate if a database has changed.

Viewing OSPF general info

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

```
ascend% show ospf general
```

```
Rtr ID: 10.5.2.154
    Status: Enabled Version: 2 ABR: Off ASBR: On
    LS ASE Count: 8 ASE Cksum sum: Ox4c303 Tos Support: TOS 0 Only
    New LSA Originate Count: 13  Rx New LSA Count: 498
```

In the output:

- `Rtr ID field` is the IP address assigned to the Pipeline Ethernet interface.
- `Status` shows whether OSPF is enabled or disabled.
- `Version` is the version of the OSPF protocols running.
- `ABR` can be On or Off, depending on where the Pipeline is situated on the network. If ABR is on, the Pipeline performs additional calculations related to external routes.
- `ASBR` is always displayed as On in the Pipeline. Although the Pipeline cannot function as an IGP gateway, it does import external routes (for example, when it establishes a WAN link with a caller that does not support OSPF) and the ASBR calculations are always performed.
- `LS ASE count` is the number of link-state database entries that are external.
- `ASE Cksum sum` specifies a checksum used to note that ASE routes in the database have changed.
- `TOS Support` indicates the level of TOS support in the router.
- `New LSA Originate Count` is the number of LSAs this router created.
- `Rx New LSA Count` is the number of LSAs this router received from other OSPF routers.

To display the OSPF interfaces, enter the Show OSPF Interfaces command. For example:

```
ascend% show ospf interfaces
Area     IP Address  Type   State      Cost Pri DR          BDR
----------------------------------------------------------------------
0.0.0.0  10.5.2.154  Bcast  BackupDR   1    5   10.5.2.155  10.5.2.154
0.0.0.0  10.5.2.154  PtoP   P To P     10   5   None        None
0.0.0.0  10.5.2.154  PtoP   P To P     10   5   None        None
```

In the output:

- `Area field` shows the area ID (0.0.0.0 is the backbone).
- `IP Address` is the address assigned to the Pipeline’s Ethernet interface. To identify WAN links, use the Type and Cost fields.
- `Type` can be broadcast or point-to-point. WAN links are point-to-point.
- `State` shows how far along the router is in the election process of a DR or BDR. The state can be 1-way (indicating that the election process has begun), 2-way (indicating that the router has received notification), BackupDR, or DR.
- `Cost` is the metric assigned to the link. The default cost for Ethernet is 1.
- `Pri` shows the designated router election priority assigned to the Pipeline.
- `DR` identifies the designated router.
- `BDR` identifies the backup designated router.

Viewing the OSPF link-state database

To view the router’s link-state database, enter the Show OSFP LSDB command. For example:

```
ascend% show ospf lsdb
LS Data Base:
Area         LS Type Link ID       Adv Rtr       Age  Len Seq #    Metric
----------------------------------------------------------------------
0.0.0.0      STUB    10.5.2.146    10.5.2.146    3600 24  0        0
0.0.0.0      STUB    10.5.2.154    10.5.2.154    3600 24  0        0
0.0.0.0      STUB    10.5.2.155    10.5.2.155    3600 24  0        0
0.0.0.0      STUB    10.5.2.162    10.5.2.162    3600 24  0        0
0.0.0.0      STUB    10.5.2.163    10.5.2.163    3600 24  0        0
0.0.0.0      RTR     10.5.2.146    10.5.2.146    659  72  8000003e 0
0.0.0.0      RTR     10.5.2.154    10.5.2.154    950  84  8000000a 0
0.0.0.0      RTR     10.5.2.155    10.5.2.155    940  60  80000005 0
0.0.0.0      RTR     10.5.2.162    10.5.2.162    980  84  8000003b 0
0.0.0.0      RTR     10.5.2.163    10.5.2.163    961  60  80000005 0
0.0.0.0      NET     10.5.2.155    10.5.2.155    940  32  80000003 0
0.0.0.0      NET     10.5.2.163    10.5.2.163    961  32  80000003 0
0.0.0.0      ASE     10.5.2.16     10.5.2.163    18   36  80000098 3
0.0.0.0      ASE     10.5.2.18     10.5.2.163    546  36  80000004 10
0.0.0.0      ASE     10.5.2.144    10.5.2.146    245  36  80000037 1
0.0.0.0      ASE     10.5.2.152    10.5.2.154    536  36  80000006 1
0.0.0.0      ASE     10.5.2.152    10.5.2.155    526  36  80000004 1
0.0.0.0      ASE     10.5.2.152    10.5.2.163    18   36  80000097 9
0.0.0.0      ASE     10.5.2.155    10.5.2.163    17   36  80000097 9
0.0.0.0      ASE     10.5.2.160    10.5.2.162    568  36  80000037 1
```

In the output:

- `Area field` specifies the area ID.
- `LS Type` indicates the type of link as defined in RFC 1583:

  Type 1 (RTR) are router-LSAs that describe the collected states of the router's interfaces.

  Type 2 (NET) are network-LSAs that describe the set of routers attached to the network.

  Types 3 and 4 (STUB) are summary-LSAs that describe point-to-point routes to networks or AS boundary routers.

  Type 5 (ASE) are AS-external-LSAs that describe routes to destinations external to the Autonomous System. A default route for the Autonomous System can also be described by an AS-external-LSA.
- `Link ID` is the target address of the route.
- `Adv Rtr` is the address of the advertising router.
- `Age` is the age of the route in seconds.
- `Len` is the length of the LSA.
- `Seq #` is a number that begins with 80000000 and increments by one for each LSA received.
- `Metric` is the cost of the link, not of a route. The cost of a route is the sum of all intervening links, including the cost of the connected route.

Note: You can expand each entry in the link-state database to view additional information about a particular LSA. See “Viewing OSPF link-state advertisements” on page 3-29.

Viewing OSPF link-state advertisements

To specify a link-state advertisement to be expanded, use the following format for the Show OSPF LSA command:

```
show ospf lsa area ls-type ls-id adv-rtr
```

The command requires that you include the first four fields of the LSA as listed in the database. You can select the first four fields and paste them in after typing the command, for example, to view an expanded view of the last entry in the link-state database shown in the previous section. For example:

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

```
LSA  type: ASE ls id: 10.5.2.160 adv rtr: 110.5.2.162 age: 568
          len: 36 seq #: 80000037 cksum: 0xfffa
          Net mask: 255.255.255.255 Tos 0 metric: 10 E type: 1
          Forwarding Address: 0.0.0.0 Tag: c0000000
```

Viewing OSPF neighbors

To view adjacencies, enter the Show OSPF NBRS command. For example:

```
ascend% show ospf nbrs
```

```
Area      Interface    Router Id    Nbr IP Addr   State    Mode   Pri
----------------------------------------------------------------------
0.0.0.0   10.5.2.154   10.5.2.155   10.5.2.155    Full     Slave  5
0.0.0.0   10.5.2.154   10.5.2.146   10.5.2.146    Full     Master 5
0.0.0.0   10.5.2.154   10.5.2.162   10.5.2.162    Full     Slave  5
```

In the output:

- `Area` is the area ID.
- `Interface` shows the address assigned to the interface. In the Pipeline, the IP address is always the address assigned to the Ethernet interface.
- `Router Id` is the IP address of the router used to reach a neighbor. This is often the same address as the neighbor itself.
- `Nbr IP Addr` is the IP address of the neighbor.
- `State` indicates the state of the link-state database exchange. Full means that the databases are fully aligned between the Pipeline and its neighbor.
- `Mode` indicates whether the neighbor is functioning in master or slave mode. The master sends Database Description packets (polls) which are acknowledged by Database Description packets sent by the slave (responses).
- `Pri` indicates the designated router election priority assigned to the Pipeline.

Viewing the OSPF routing table

To view the OSPF routing table, enter the Show OSPF rtab command. For example:

```
ascend% show ospf rtab
```

```
SPF algorithm run 24 times since                       boot
Dest         D_mask          Area    Cost E Path Nexthop    AdvRtr
----------------------------------------------------------------------
Nets:
```

```
10.5.2.163   255.255.255.248  0.0.0.0  10  3 EXT  10.5.2.163 10.5.2.16
10.5.2.163   255.255.255.255  0.0.0.0  20  0 EXT  10.5.2.163 10.5.2.16
10.5.2.146   255.255.255.248  0.0.0.0  20  1 EXT  10.5.2.154 10.5.2.14
10.5.2.146   255.255.255.255  0.0.0.0  20  0 STUB 10.5.2.154 10.5.2.14
10.5.2.155   255.255.255.248  0.0.0.0  10  0 INT  10.5.2.154 10.5.2.15
10.5.2.154   255.255.255.255  0.0.0.0  21  0 STUB 10.5.2.163 10.5.2.15
10.5.2.155   255.255.255.255  0.0.0.0  20  9 STUB 10.5.2.155 10.5.2.15
10.5.2.163   255.255.255.248  0.0.0.0  11  1 INT  10.5.2.163 10.5.2.16
10.5.2.162   255.255.255.255  0.0.0.0  20  0 STUB 10.5.2.163 10.5.2.16
10.5.2.163   255.255.255.255  0.0.0.0  10  0 STUB 10.5.2.163 10.5.2.16
```

In the output:

- `Dest field` shows the destination address.
- `D_mask` is the destination netmask.
- `Area` is the area ID.
- `Cost` is the cost of the route.
- `E` is the cost of the link. (The cost of a route is the sum of the cost of each intervening link, including the cost to the connected route.)
- `Path` specifies the type of link: EXT (exterior), INT (interior), or STUB (a default).
- `Next hop` specifies the target address from this router.
- `Adv Rtr` is the advertising router. Sometimes a router will advertise routes for which it is not the gateway.

Viewing OSPF protocol I/O

To display information about packets sent and received by the OSPF protocol, enter the Show OSPF IO command. For example:

```
ascend% show ospf io
```

```
IO stats from:                       boot
>> RECEIVED:
       0: Monitor request
     785: Hello
      13: DB Description
       6: Link-State Req
    1387: Link-State Update
      64: Link-State Ack
>> SENT:
     794: Hello
      15: DB Description
       6: Link-State Req
    1017: Link-State Update
     212: Link-State Ack
```

Displaying TCP statistics and connections

To display the commands available for showing TCP statistics and connections, enter the Show TCP command with a question mark:

```
ascend% show tcp ?
```

```
show tcp ?          Display help information
show tcp stats      Display TCP Statistics
show tcp connection Display TCP Connection Table
```

To display the number of TCP packets received and transmitted, enter the Show TCP Stats command. For example:

```
ascend% show tcp stats
```

```
     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 a TCP session that the Pipeline initiated. A passive open is a TCP session that the Pipeline did not initiate.

To display current TCP sessions, enter the Show TCP Connections command. For example:

```
ascend% show tcp connection
```

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

Displaying IPX packet statistics

To display IPX packet statistics, enter the Show NetWare Stats command. For example:

```
ascend% show netware stats
```

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

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

Displaying the IPX service table

To display the IPX service table, enter the Show NetWare Servers command. For example:

```
ascend% show netware servers
```

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

In the output:

- `IPX Address` is the address of the server. The address uses the following format:

  network number:node number:socket number
- `Type` indicates the type of service available (in hexadecimal format). For example, 0451 designates a file server.
- `Server Name` is the first 35 characters of the server name.

Displaying the IPX routing table

To display the IPX routing table, enter the Show NetWare Networks command. For example:

```
ascend% show netware networks

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

The output includes the following fields:

- 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.

Monitoring Frame Relay connections

To display the commands available for showing Frame Relay statistics and connections, enter the Show FR command with a question mark:

```
ascend% show fr ?

show fr ?           Display help information
show fr stats       Display Frame relay information
show fr lmi         Display Frame relay LMI information
show fr dlci [name] Display all DLCI information or just for [name]
show fr circuits    Display the FR Circuit table
```

Displaying Frame Relay statistics

To display Frame Relay statistics, enter the Show FR Stats command. For example:

```
ascend% show fr stats

Name         Type   Status    Speed    MTU     InFrame     OutFrame
fr1          DCE    Down     64000    1532          0            1
fr1-temp     DCE      Up     64000    1532          0            1
fr1-temp-9   DCE      Up     64000     1532         0            0
```

In the output:

- `Name` is the name of the Frame Relay profile associated with the interface.
- `Type` indicates the type of interface.
- `Status` indicates the status of the interface. `Up` shows the interface is functional, but is not necessarily handling an active call. `Down` shows the interface is not functional.
- `Speed` is the data rate in bits per second.
- MTU is the maximum packet size allowed on the interface.
- `InFrame` is the number of frames the interface has received.
- `OutFrame` is the number of frames transmitted.

Displaying link management information

To display Link Management Information (LMI) for each link activated by a Frame Relay profile, enter the Show FR LMI command. For example:

```
ascend% show fr lmi

T1_617D LMI for fr1
  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 Enqs Sent        0  Num Status Msgs Rcvd     0
  Num Update Status Rcvd      0  Num Status Timeouts   2779
LMI is not on for fr1-temp
LMI is not on for fr1-temp-9
```

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.)

Displaying DLCI status

To display the status of each DLCI, enter the Show FR DLCI command. For example:

```
ascend% show fr dlci

DLCIs for fr1
DLCIs for fr1-temp
eng-lab-236-Cir   DLCI =   17    Status = ACTIVE
        input pkts               0        output pkts              0
        input octets             0        output octets            0
        input FECN               0        input DE                 0
        input BECN               0
last time status changed: 03/05/1997  14:44:17
DLCIs for fr1-temp-9
eng-lab-236-Cir-9  DLCI =   16    Status = ACTIVE
        input pkts               0        output pkts              0
        input octets             0        output octets            0
        input FECN               0        input DE                 0
        input BECN               0
last time status changed: 03/05/1997  14:45:07
DLCIs not assigned
```

In the output:

- `DLCI` is the DLCI number.
- `Status` indicates ACTIVE if the connection is up or INACTIVE if not.
- `Input Pkts` is the number of frames the interface has received.
- `Output Pkts` is the number of frames the interface has transmitted.
- `Input Octets` is the number of bytes the interface has received.
- `Output Octets` is the number of bytes the interface has transmitted.
- `FECN Pkts` is the number of packets received with the FECN (Forward Explicit Congestion Notification) bit set. This field always includes a 0 (zero) because congestion management is not currently supported.

- `BECN Pkts` is the number of packets received with the BECN (Backward Explicit Congestion Notification) bit set. This field always includes a 0 (zero) because congestion management is not currently supported.
- `DE Pkts` is the number of packets received with the DE (Discard Eligibility) indicator bit set.
- `Last Time Status Changed` indicates the last time the DLCI state changed.

Displaying circuit information

To display the Frame Relay profile name, DLCI, and status of configured circuits, enter the Show FR Circuits command. For example:

```
ascend% show fr circuits

cir-9 User Setting Up
fr1-temp-9                    16            Up
fr1-temp                      17            Up
```

Show Uptime

To view how long the Pipeline has been running, enter the Show Uptime command. For example:

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

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

Show Revision

To display the software load and version number currently running in the Pipeline, enter the Show Revision command. For example:

```
ascend% show revision
techpubs-lab-17 system revision: ebiom.m40 5.0A
```

Show Users

To display the number of active sessions:

```
ascend% show users

I Session    Line: Slot: Tx    Rx    Service      Host          User
O ID         Chan  Port  Data  Rate  Type[mpID]   Address       Name
O 245761821 32459:2:1   n/a   n/a   Frame relay   10.10.212.10   corp
```

In the output:

- `IO` indicates either I (incoming call) or O (outgoing call).
- `Session ID` is the unique session-ID.
- `Line:Channel` shows the line and channel of the established session.
- `Slot:Port` shows the slot and port of the service being used by the session, which can be the number of a slot containing a modem card and the modem on that card, or the

virtual slot of the Pipeline unit's bridge/router, with port giving the virtual interfaces to bridge/router starting with 1 for the first session of a multichannel session.

- `Data Rate` indicates the bearer capacity or modem speed as appropriate to the session type.
- `Service Type` specifies the type of session, either `Termsrv` or a protocol name.

  The special values Initial and Login document the progress of a session. Initial identifies sessions that do not yet have a protocol assigned.
- `Host Address` shows the network address of the host originating the session.

  In some cases, this field might be N/A.
- `User Name` specifies the station name associated with the session. Initially, this value is Answer. This is usually replaced with the name of the remote host.

Show Sessid

The Show Revision command displays the current internal session identification number available for the Pipeline to assign to the next connection. The Pipeline assigned the saved base value to the first connection after its last reboot. Subsequent connections are assigned new numbers, incremented one from the previous number. For example:

```
ascend% show sessid
Session ID current 243975689, saved base 243975685
```

IPRoute command

The terminal-server IProute commands display the routing table and enable you to add or delete routes. The changes you make to the routing table using the IProute command last only until the Pipeline unit resets. To view the supported commands, enter the IPRoute command with a question mark:

```
ascend% iproute ?

iproute ?      Display help information
iproute add    iproute add <destination/size> <gateway> [ pref ] [ m ]
iproute delete iproute delete <destination/size> <gateway> [ proto ]
iproute show   displays IP routes (same as "show ip routes" command)
```

Displaying the routing table

Note that the IProute Show command and the Show IP Routes command have identical output. To view the IP routing table, enter the IPRoute Show command. For example:

```
ascend% iproute show

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

In the output:

- `Destination` is 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` is the address of the next hop router that can forward packets to the given destination. Direct routes (without a gateway) no longer show a gateway address in the gateway column.
- `IF` indicates the name of the interface through which a packet addressed to this destination will be sent.

  ie0 is the Ethernet interface

  lo0 is the loopback interface

  `wanN` specifies each of the active WAN interfaces

  `wanidle0` is the inactive interface (the special interface for any route whose WAN connection is down).
- `Flg` contains the following flag values:
  - C (A directly connected route such as Ethernet)
  - I (ICMP Redirect dynamic route)
  - N (Placed in the table via SNMP MIB II)
  - O (A route learned from OSPF)
  - R (A route learned from RIP)
  - r (A RADIUS route)
  - S (A static route)
  - ? (A route of unknown origin, which indicates an error)
  - G (An indirect route via a gateway)
  - P (A private route)
  - T (A temporary route)
  - * (A hidden route that will not be used unless another better route to the same destination goes down)
- `Pref` indicates 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 can be set independently.
- `Metric` shows the RIP-style metric for the route, with a valid range of 0-16. Routes learned from OSPF show a RIP metric of 10. OSPF Cost infinity routes show a RIP metric of 16.
- `Use` is 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` is the age of the route in seconds. It is used for troubleshooting, to determine when routes are changing rapidly or flapping.

The first route in the default route (destination 0.0.0.0/0), which is pointing through the active Connection profile:

```
0.0.0.0/0          10.0.0.100     wan0     SG   1     1     0     20887
```

In the following example, the IP Route profile for the default route specifies a Preference of 1, so this route is preferred over dynamically learned routes. The next route is specified in a Connection profile that is inactive:

```
10.207.76.0/24     10.207.76.1    wanidle0 SG   100   7     0     20887
```

The next route in the table is a static route that points through an inactive gateway:

```
10.207.77.0/24     10.207.76.1    wanidle0 SG   100   8     0     20887
```

The static route is followed by the loopback route:

```
127.0.0.1/32       -              lo0      CP   0     0     0     20887
```

The loopback route says that packets sent to this special address will be handled internally. The C flag indicates a Connected route, while the P flag indicates that the router will not advertise this route.

The next route is specified in a Connection profile that is currently active:

```
10.0.0.0/24        10.0.0.100     wan0     SG   100   1     21387 20887
```

These are followed by the connection to the Ethernet interface. It is directly connected, with a Preference and Metric of zero.

```
10.1.2.0/24        -              ie0      C    0     0     19775 20887
```

The last two routes are a private loopback route, and a private route to the broadcast address:

```
10.1.2.1/32        -               lo0      CP   0     0      389   20887
255.255.255.255/32 -              ie0      CP   0     0     0     20887
```

The private loopback route is a host route with our Ethernet address. It is private, so it will not be advertised. The private route to the broadcast address is used in cases where the router will want to broadcast a packet but is otherwise unconfigured. It is typically used when trying to locate a server on a client machine to handle challenges for a token security card.

Displaying the routing table when using OSPF

The OSPF routing table includes routes built from the router’s link-state database, and those added by external routing protocols such as RIP. You can also add routes statically, for example, to direct traffic destined for a remote site through one of several possible border routers. For details about adding static routes, for example, if you want to force the use of one route over those learned from OSPF, see the *Pipeline 220 Interface Configuration Guide*.

To view the IP routing table with added OSPF information, enter the IPROUTE SHOW command with the –l option:

```
   ascend% iproute show -l
```

In addition to the standard routing-table fields, which are described in the *Pipeline 220 Interface Configuration Guide* the following three columns are specific to OSPF and are displayed only when you use the –l option. For example, the following OSPF-specific columns are displayed on the far right of each entry in the routing table:

```
...     Cost        T        Tag
...     1           0        0xc0000000
...     9           1        0xc8000000
...     10          0        0xc0000000
...     9           1        0xc8000000
...     1           1        0xc0000000
...     3           1        0xc8000000
...     9           1        0xc8000000
...     4           1        0xc8000000
...     5           1        0xc8000000
...     3           1        0xc8000000
...     3           1        0xc8000000
...     3           1        0xc8000000
```

In the output:

- `Cost` is the he cost of an OSPF route. The interpretation of this cost depends on type of external metric type, displayed in the next column. If the Pipeline is advertising Type 1 metrics, OSPF can use the specified number as the cost of the route. Type 2 external metrics are an order of magnitude larger.
- `T` is the ASE-type of metric to be advertised for an external route. 0 in this column means that it is an external-type-1 or an OSPF internal route. If this column shows a 1, it means that the route is an external-type-2 route.
- `Tag` is this column specifies a 32-bit hexadecimal number attached to each external route to *tag* it as external to the AS. This number can be used by border routers to filter this record.

Multipath routing

A Pipeline running OSPF can alternate between two equal cost gateways. When OSPF detects more than one equally good gateway, in terms of routing costs, each equal-cost gateway is put on an equal-cost list. The router will alternate between all the gateways on the list. This is called equal-cost multipath routing.

For example, if a router A has two equal-cost routes to example.com, one via router B and the other via router C. For example:

```
Destination       Gateway         IF     Flg  Pref  Met    Use      Age
10.174.88.0/25    10.174.88.12   wan2   OGM   10   10      52      19
10.174.88.0/25    10.174.88.13   wan3   OGM   10   10      52      19
10.174.88.12/32    10.174.88.12  wan2   OG    10   10       0      28
10.174.88.13/32    10.174.88.13  wan3   OG    10   10       0      28
192.168.253.0/24    -            ie0    C      0    0       1      49
192.168.253.6/32    -            lo0    CP     0    0      53      49
223.1.1.0/24       10.174.88.12  wan2   OG    10   10       0      19
223.5.1.0/24       10.174.88.12  wan2   OG    10   10       0      19
223.12.9.0/24      10.174.88.12  wan2   OG    10   10       0      19
255.255.255.255/32  -            ie0    CP     0    0       0      49
```

Note that the *M* in the Flags column indicates an equal-cost multipath. For example, following is a Traceroute from A to example.com:

```
ascend% traceroute -q 10 example.com
```

```
traceroute to example.com (10.174.88.1), 30 hops max, 0 byte packets
```

```
1  C.example.com (10.174.88.13)  20 ms B .example.com (10.174.88.12)
20 ms C.example.com (10.174.88.13)  20 ms B .example.com
(10.174.88.12)  20 ms  20 ms C.example.com (10.174.88.13)  60 ms  20 ms
```

```
B .example.com (10.174.88.12)  20 ms C.example.com (10.174.88.13)  20
ms B .example.com (10.174.88.12)  20 ms
```

```
2  example.com (10.174.88.1)  20 ms  20 ms  20 ms  20 ms  30 ms  20 ms
20 ms  30 ms  20 ms  30 ms
```

Note: Notice the alternating replies. The replies are statistically dispatched to B and C, with roughly 50% of the packets sent through each gateway. For background information about the routing table and about the Traceroute command, see the *Pipeline 220 Interface Configuration Guide*.

Third-party routing

A Pipeline routing OSPF can advertise routes to external destinations on behalf of another gateway (a third-party). This is commonly known as advertising a forwarding address. Depending on the exact topology of the network, it might be possible for other routers to use this type of LSA and route directly to the forwarding address without involving the advertising Pipeline, increasing the total network throughput.

Third-party routing requires that all OSPF routers know how to route to the forwarding address. This will usually mean that the forwarding address must be on an Ethernet that has an OSPF router acting as the forwarding router, or that designated router is sending LSAs for that Ethernet to any area that sees the static route's forwarding address LSAs.

How OSPF adds RIP routes

When the Pipeline establishes an IP routing connection with a caller that does not support OSPF, it imports the AS-external route from the Connection profile and adds it to the routing table. The Pipeline does not have to run RIP to learn these routes. RIP should be turned off when the Pipeline is running OSPF.

To enable OSPF to add the RIP-v2 routes to its routing table, configure RIP-v2 normally in this Connection profile. OSPF will import all RIP routes as Type-2 ASEs. The reason why RIP routes are imported with Type-2 metrics by default is that RIP metrics are not directly comparable to OSPF metrics. To prevent OSPF from interpreting RIP metrics, we assign the imported ASE route a Type-2 metric, which means that it is so large compared to OSPF costs that the metric can be ignored.

Route preferences

Route preferences provide additional control over which types of routes take precedence over others. They are necessary in a router which speaks multiple routing protocols, largely because RIP metrics are not comparable with OSPF metrics.

For each IP address and netmask pair, the routing table holds one route per protocol, where the protocols are defined as follows:

- Connected routes, such as Ethernet, have a Preference=0.
- Routes learned from ICMP Redirects have a Preference=30.
- Routes placed in the table by SNMP MIB II have a Preference=100.
- Routes learned from OSPF have a default Preference=10.
  You can modify the default in Ethernet > Mod Config > Route Pref.

- Routes learned from RIP have a default Preference=100.
  You can modify the default in Ethernet > Mod Config > Route Pref.
- A statically configured IP Route or Connection profile has a default Preference=100.
  You can modify the default in the Connection or IP Route profile.

When choosing which routes should be put in the routing table, the router first compares the Preference 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.

If multiple routes exist for a given address and netmask pair, the route with the lower Preference is better. If two routes have the same Preference, then the lower Metric is better. The best route by these criteria is actually used by the router. The others remain latent or *hidden*, and are used in case the best route was removed.

Adding an IP route

To add a static route to the Pipeline's routing table that will be lost when the Pipeline resets, enter the IProute Add command in the following format:

```
iproute add <destination> <gateway> [<metric>]
```

where <destination> is the destination network address, <gateway> is the IP address of the router that can forward packets to that network, and <metric> is the virtual hop count to the destination network (default 8). For example:

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

The Pipeline adds 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.

Deleting an IP route

To remove a route from the Pipeline's routing table, enter the IProute Delete command in the following format:

```
iproute delete <destination> <gateway>
```

For example:

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

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.

DNSTab command

The DNSTab command displays DNS-related information. To use the command, include one of two modifiers. To display the supported commands, enter the DNSTab command with a question mark:

```
ascend% dnstab ?
dnstab ?              Display help information
dnstab show           Display local DNS table
dnstab entry          Display local DNS table entry
dnstab edit         Start editor for local DNS table
```

Monitoring the DNS table

The DNSTab Show command displays the Pipeline's DNS table. The command is identical to Show DNSTab. For example:

```
ascend% dnstab show

Local DNS Table
Name                   IP Address   # Reads   Time of last read
______________________ _____________ _________ _________________
1: ""                  ------           -------
2: "server.corp.com."  200.0.0.0             2   Feb 10 10:40:44
3: "boomerang"         221.0.0.0             2   Feb 10  9:13:33
4: ""                  ------           -------
5: ""                  ------           -------
6  ""                  ------           -------
7: ""                  ------           -------
8: ""                  ------           -------
```

Displaying specific DNS entries

The DNSTab Entry command displays a list of information about a specific entry in the local DNS table. Enter the DNSTab Entry command in the following format:

```
dnstab entry n
```

where *n* is the number of a DNS-table entry displayed by the DNSTab Show command.

The list includes the entry and all the IP addresses stored for that entry, up to a maximum specified by the List Size parameter.

If you set List Attempt to No, no list appears.

Creating the local DNS table

Use `DNSTAB edit` to create a local DNS table. The Pipeline disables DNS updates while you use the `DNSTab edit` command.

The following procedure defines a table entry as one of the eight table indexes, which include the host name, IP address (or addresses), and information fields.

1 From the terminal server, enter:

   ```
   ascend% dnstab edit
   ```

   When the system first powers up, the table is empty. When the editor first starts up, it displays zeros for each of the eight entries in the table. To exit the table editor without making an entry, press Return.

2 Type an entry number and press Enter.

A warning appears if you type an invalid entry number. If the entry exists, the current name for that entry appears in the prompt.

3 Type the name for the current entry.

If the name is validated it is entered into the table and a prompt requests the IP address for the name that you just entered.

You can find a list of restrictions you must follow in naming entries in the DNS table at the end of this section.

4 Do one of the following:

Type the IP address for the entry.

The IP address is checked for format. If the format is correct, the address is entered into the table and the editor prompts for another entry.

5 When you are finished making entries, type `0` and press Return when the editor prompts you for another entry.

Editing the local DNS table

This procedure defines a table entry as one of the eight table indexes, which include the host name, IP address (or addresses), and information fields.

1 From the terminal server, enter:

```
ascend% dnstab edit
```

If the table has already been created, the number of the entry last edited appears in the prompt.

2 Type an entry number or press Return to edit the entry number currently displayed.

A warning appears if you type an invalid entry number. If the entry exists, the current value for that entry appears in the prompt.

3 Do one of the following and press Enter.

– Type the new name for the current entry.

If the name is accepted it is entered into the table and a prompt requests the IP address for the name that you just entered.

You can find a list of restrictions you must follow in naming entries in the DNS table at the end of this section.

– Press Return to accept the current name.

– Clear the name by pressing the space bar and then Return.

If you clear an entry name and do not replace it with a new name, all information in all fields for that entry is discarded.

4 Do one of the following:

– If you are changing the name of the entry but not the IP address, press Return.

– To change the IP address, type the new IP address

The IP address you enter is checked for format. If the format is correct, the address is entered into the table and the editor prompts for another entry.

5 When you are finished making entries, type `0` and press Return when the editor prompts you for another entry.

Deleting an entry from the local DNS table

To delete an entry from the local DNS table:

1 To display the table, from the terminal server, enter:

```
ascend% dnstab edit
```

2 Type the number of the entry you want to delete and press Return.

3 Press the space bar and then press Return.

Note: Restrictions for names in the local DNS table:

- Names must be unique in the table.
- Names must start with an alphabetic character, either upper- or lower-case. (from A to Z or a to z).
- Names must be less than 256 characters
- Dots (periods) at the end of names are ignored.
- Names can be local names or fully qualified names that include the domain name. The Pipeline will automatically add the local domain name before it is qualified (or the secondary domain name, if the qualification with the domain name fails) from the DNS submenu of the Ethernet Profile.

Menu command

The Menu command invokes the terminal-server menu mode, which lists up to four Telnet hosts as configured in Ethernet > Mod Config > TServ Options. For example:

Table 3-7. Sample terminal-server menu

Up to 16 lines of up to 80 characters each will be accepted. Long lines will be truncated. Additional lines will be ignored
1. host1.abc.com 2. host2.abc.com 3. host3.abc.com 4. host4.abc.com Enter Selection (1-4, q)

To return to the command-line, press 0. Terminal-server security must be set up to allow the operator to toggle between the command line and menu mode, or the Menu command has no effect.

Telnet command

The Telnet command initiates a login session to a remote host. Use the following format:

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

If DNS is configured in the Ethernet profile, you can specify a hostname. For example:

```
ascend% telnet myhost
```

If DNS is not configured, you must specify the host's IP address instead. There are also several options in Ethernet > Mod Config > TServ Options that affect Telnet; for example, if Def Telnet is set to Yes, you can just type a hostname to open a Telnet session to that host. For example:

```
ascend% myhost
```

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
```

When the Pipeline displays the Telnet prompt, `telnet>`, you can enter any of the Telnet commands described in "Telnet session commands" on page 3-45. You can quit the Telnet session at any time by typing quit at the Telnet prompt:

```
telnet> quit
```

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.

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 | –b | –t

  (Optional.) You can specify -a, -b, or -t on the Telnet command line to indicate ASCII, Binary, or Transparent mode. A specification on the command line overrides the setting of the Telnet Mode parameter.

  – In ASCII mode, the Pipeline uses standard 7-bit mode.

  – In Binary mode, the Pipeline tries to negotiate 8-bit Binary mode with the server at the remote end of the connection.

  – In Transparent mode, the user can send and receive binary files, and use 8-bit file transfer protocols, without having to be in Binary mode.
- <port-number>

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

Telnet session commands

The commands in the following 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:

```
telnet> ?
```

To open a Telnet connection after invoking Telnet, use the Open command; 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 view a list of Set commands, enter the Set command with a question mark:

```
telnet> set ?
```

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

```
telnet> close
```

Telnet error messages

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

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

TCP command

The TCP command initiates a login session to a remote host. Use the following format:

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

For example:

```
ascend% tcp myhost
```

The arguments to the TCP 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.
- [<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.

If a raw TCP connection fails, the Pipeline returns one of the following 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.)

Ping command

The terminal-server Ping command is useful for verifying that the transmission path is open between the Pipeline and another station. It sends an ICMP echo_request packet to the specified station. It the station receives the packet, it returns an ICMP echo_response packet. For example, to ping the host `techpubs`:

```
ascend% ping techpubs
```

```
PING techpubs (10.65.212.19): 56 data bytes
64 bytes from 10.65.212.19: icmp_seq=0 ttl=255 time=0 ms
64 bytes from 10.65.212.19: icmp_seq=3 ttl=255 time=0 ms
^C
--- techpubs ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 0/0/0 ms
```

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

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

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

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.

IPXPING command

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. Use the following format:

```
ipxping [-c <count>] [-i <delay>] [-s <packetsize>] <hostname>
```

The arguments to the IPXping command are:

- <hostname>: The IPX address of the host, or if the host is a NetWare server, its hostname.
- [-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.

where <hostname> 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 the following 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
```

The output includes the following information:

- The IPX address of the source and destination nodes.
- The byte counts of the request and response packets.
- The ping ID of the command. (The ping Request # replied to by target host.)
- The number of milliseconds required to send the IPXping and receive a response.

- The number of packets transmitted and received.
- Duplicate or damaged packets, if applicable.
- Average round-trip times for the ping request and reply.

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

To display statistics related to the IPXping command, type:

```
ascend% show netware pings
InPing Requests/OutPing Replies OutPing Requests/InPing Replies
      10            10                  18            18
```

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

Traceroute command

The Traceroute command is useful for locating slow routers or diagnosing IP routing problems. It traces the route an IP packet follows by launching UDP probe packets with a low TTL (Time-To-Live) value and then listening for an ICMP `time exceeded` reply from a router. The format of the Traceroute command is as follows:

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

All flags are optional. The only required parameter is the destination hostname or IP address.

- -n

  Prints hop addresses numerically rather than symbolically and numerically (this eliminates a name server address-to-name lookup for each gateway found on the path).
- -v

  Verbose output. 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.
- host

  The destination host by name or IP address.
- 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).

For example, to trace the route to the host `techpubs`:

```
ascend% traceroute techpubs
```

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

Probes start with a TTL of one and increase by one until of the following conditions occurs:

- The PipelinePipeline receives an ICMP `port unreachable` message.

  The UDP port in the probe packets is set to an unlikely value, such as 33434, because the target host is not intended to process the packets. A `port unreachable` message indicates that the packets reached the target host and were rejected.
- The TTL value reaches the maximum value.

  By default, the maximum TTL is set to 30. You can specify a different TTL by using the –m option; for example:

```
ascend% traceroute -m 60 techpubs
```

```
traceroute to techpubs (10.65.212.19), 60 hops max, 0 byte packets
 1  techpubs.eng.abc.com (10.65.212.19)  0 ms  0 ms  0 ms
```

Three probes are sent at each TTL setting. The second line of command output shows the address of the router and round trip time of each probe. If the probe answers come from different gateways, the address of each responding system will be printed. If there is no response within a 3 second timeout interval, the command output is an asterisk. The following annotations might be included after the time field in a response:

- !H (Host reached.)
- !N (Network unreachable.)
- !P (Protocol unreachable.)
- !S (Source route failed. This might indicate a problem with the associated device.)
- !F (Fragmentation needed. This might indicate 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.

Kill command

The Kill command enables you to clear the nailed connection. Disconnect using the session ID. The disconnect code that results is identical to the RADIUS disconnect code, allowing you to track all administrative disconnects. Use the following format:

```
kill <session ID>
```

where <session ID> is the session ID as displayed by the Show Users command described in the preceding section. The reported disconnect cause is DIS_LOCAL_ADMIN. The active Security profile must have Edit All Calls=Yes. If Edit All Calls=No, the Pipeline displays the following message when you issue the kill command:

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

When the session is properly terminated, the PipelinePipeline displays the following message:

```
Session 216747095 killed.
```

Pipeline Diag Command Reference

4

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

This reference covers these topics:

Sys Diag commands

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

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

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

Restore Cfg

This command restores a Pipeline configuration that was 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.

Follow these instructions to restore your configuration from backup:

1 Verify that the Upload and Edit Security permissions are enabled in the active Security profile.

2 Verify that the Term Rate parameter in the System profile is set to 9600.

3 Verify that your terminal emulation program has a disk capture feature and an autotype feature, and that its data rate is set to 9600 baud.

4 Connect the backup device to the Pipeline unit’s Control port.

5 Highlight Restore Cfg and press Enter.

6 When the ‘Waiting for upload data” prompt appears, turn on the autotype function on your emulator and supply the filename of the saved Pipeline data.

7. 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.

Save Cfg

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

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

Follow these instructions to save your configuration:

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

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

Sys Reset

This command restarts the Pipeline and clears all sessions 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 Pipeline to the switch will be incorrect.

To perform a system reset, follow these steps:

1. Highlight System Reset and press Enter.

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

   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. These messages may be displayed:

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

```
SYSTEM IS UP:  Index: 100   Revision: 5.0a
   Date: 03/04/1997.       Time: 22:33:00
```

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

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

3 Press any key to display the Main Edit menu.

Term Serv

This command starts a terminal server session. The system displays the terminal-server command-line prompt (by default, “ascend%”).

Type a question mark at the command line to display a list of available commands. (For complete information about the terminal-server interface see the *Pipeline 220 Interface Configuration Guide*.)

Upd Rem Cfg

This command is not supported on the Pipeline.

Pipeline Profile Reference

A

This chapter shows the configuration profiles in the VT100 interface and example values for each parameter contained in those profiles. For details on the parameters listed here, see Chapter 2, “Pipeline Alphabetic Parameter Reference.” For details on the diagnostic commands, see Chapter 4, “MAX Diag Command Reference.”

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

How the Pipeline profiles are organized

The following is an example Main Edit Menu at the top level, which shows the nailed T1 option configured.

```
Main Edit Menu
   00-000 System
   10-000 Serial Port T1-CSU
   20-000 Ethernet
```

The Pipeline comes with a built-in T1/E1 line or a V.35 serial port for WAN access. You can configure the type of WAN interface in the System menu.

The numbers in the VT00 menus relate to slot numbers in the Pipeline unit, which may be an actual expansion slot or a “virtual” slot on the unit’s motherboard.

- The system itself is assigned slot number 0 (menu 00-000). The System menu contains the following profiles and submenus, which are all related to system-wide configuration and maintenance:

  ```
  00-000 System
     00-100 Sys Config
     00-200 Sys Diag
     00-300 Security
     00-400 Feature Codes
  ```

- The WAN interface (either nailed T1/E1 or serial WAN port is slot 1 (menu 10-000).
- The Ethernet is slot 2 (menu 20-000). The Ethernet menu contains submenus and profiles related to the local network, routing and bridging, and WAN connections.

System profiles

These profiles reside below the System menu at the top level of the VT100 menus. The settings in these profiles affect how the Pipeline functions system-wide.

System profile (Sys Config)

```
System
   Sys Config
      Name=gateway-1
      Location=east-bay
      Contact=thf
      Date=2/20/97
      Time=10:00:29
      Term Rate=9600
      Console=Standard
      Remote Mgmt=Yes
      Excl Routing=No
      Auto Logout=No
      Idle Logout=0
      High BER=10 ** -3
      High BER Alarm=No
      No Trunk Alarm=No
      NewNASPortID=No
      WAN interface=T1-CSU
      Edit=00-000
      Status 1=10-100
      Status 2=20-200
      Status 3=20-100
      Status 4=00-200
      Status 5=20-300
      Status 6=20-400
      Status 7=00-100
      Status 8=20-700
```

System diagnostics (Sys Diag)

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

Security profiles

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

Feature Codes profile

```
System
   Feature Codes
      IP Security=
```

Profiles for WAN lines and ports

Serial Port T1-CSU

```
Serial Port T1-CSU
   Mod Config
      Nailed-T1 Group=1
      Activation=Enabled
      Framing Mode=D4
      Encoding=AMI
      FDL=None
      Buildout=0 db
      Clock Source=Yes
      Number of DS0 Channels=4
```

Serial Port E1-Nailed

```
Serial Port E1-Nailed
   Mod Config...
     Nailed-E1 Group=1
     Activation=Enabled
     Framing Mode=G.703
     Clock Source=Yes
     Ending DS0 Channel=31
     Enable Channel 16=Yes
```

Serial WAN port

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

Network profiles

Answer profile

```
Ethernet
   Answer
      Use Answer as Default=No
      Profile Reqd=Yes
      Framed Only=No

      Encaps...
         PPP=Yes
         FR=Yes
         X.75=Yes
         TCP-CLEAR=Yes

      IP options...
         Metric=7

      PPP options...
         Route IP=Yes
         Route IPX=Yes
         Route Appletalk=Yes
         Bridge=Yes
         Recv Auth=Either
         MRU=1524
         LQM=No
         LQM Min=600
         LQM Max=600
         Link Comp=Stac
         VJ Comp=Yes
         Disc on Auth Timeout=Yes

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

      Session options...
         RIP=Off
         Data Filter=5
         IPX SAP Filter=1

      TCP-Clear options...
         Detect End of Packet=No
         End of Packet Pattern=N/A
         Packet Flush Length=N/A
         Packet Flush Time=N/A
```

Bridge Adrs profile

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

Connection profile

```
Ethernet
   Connections
      Station=device-name
      Active=Yes
      Route IP=Yes
      Route IPX=No
      Route Appletalk=Yes
      Framed Only=No
      Bridge=No

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

      Encaps=FR
      Encaps options...
         FR Prof=
         DLCI=16
        Circuit=N/A

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

      Encaps=TCP-CLEAR
      Encaps options...
         Recv PW=localpw
         Login Host=techpubs
         Login Port=23
         Detect End of Packet=No
         End of Packet Pattern=N/A
         Packet Flush Length=N/A
         Packet Flush Time=N/A

      IP options...
         LAN Adrs=0.0.0.0/0
         WAN Alias=0.0.0.0/0
         IF Adrs=0.0.0.0/0
         Preference=100
         Metric=7
         DownPreference=120
         DownMetric=7
         Private=No
         RIP=Off
         Multicast Client=No
         Multicast Rate Limit=5
         Client Pri DNS=0.0.0.0
         Client Sec DNS=0.0.0.0
         Client Assign DNS=Yes
         Client Gateway=0.0.0.0

      IPX options...
         IPX RIP=None
         IPX SAP=Send
         IPX Net#=cfff0003
         IPX Alias#=00000000
         Handle IPX=None
         SAP HS Proxy Net#1=ccff0f03
         SAP HS Proxy Net#2=
         SAP HS Proxy Net#3=
         SAP HS Proxy Net#4=
         SAP HS Proxy Net#5=
         SAP HS Proxy Net#6=

      Appletalk options...
         Zone Name=
         Net Start=
         Net End=

      Session options...
         Data Filter=5
         IPX SAP Filter=0
         BackUp=
         Block calls after=0
         Blocked duration=0
         ATMP Gateway=N/A
         MAX ATMP Tunnels=
         FR Direct=No
         FR Prof=N/A
         FR DLCI=N/A


      OSPF options…
         RunOSPF=Yes
         Area=0.0.0.0
         AreaType=Normal
         HelloInterval=40
         DeadInterval=120
         Priority=5
         AuthType=Simple
         AuthKey=ascend0
         Cost=10
         DownCost=1000
         ASE-type=Type1
         ASE-tag=c0000000
         TransitDelay=5
         RetransmitInterval=20

      Telco options...
         Group=1
         FT1 Caller=N/A
         Data Svc=56KR

      Accounting...
         Acct Type=None
         Acct Host=N/A
         Acct Port=N/A
         Acct Timeout=N/A
```

```
         Acct Key=N/A
         Acct-ID Base=N/A
```

Ethernet profile (Mod Config)

```
Ethernet
   Mod Config
      Module Name=

      Ether1 options...
         IP Adrs=10.65.212.100/24
         2nd Adrs=0.0.0.0/0
         RIP=Both-v1
         Ignore Def Rt=Yes
         Proxy Mode=Off
         Filter=5
         IPX Frame=None
         IPX Enet#=N/A
         IPX SAP Filter=N/A
         Handle IPX Type20=N/A

      Ether2 options...
         IP Adrs=10.67.224.101/24
         2nd Adrs=0.0.0.0/0
         RIP=Both-v1
         Ignore Def Rt=Yes
         Proxy Mode=Off
         Filter=5
         IPX Frame=None
         IPX Enet#=N/A
         IPX SAP Filter=N/A
         Handle IPX Type20=N/A

      SNMP options...
         Read Comm=Ascend
         R/W Comm Enable=Yes
         R/W Comm=write
         Security=Yes
         RD Mgr1=10.0.0.1
         RD Mgr2=10.0.0.2
         RD Mgr3=10.0.0.3
         RD Mgr4=10.0.0.4
         RD Mgr5=10.0.0.5
         WR Mgr1=10.0.0.11
         WR Mgr2=10.0.0.12
         WR Mgr3=10.0.0.13
         WR Mgr4=10.0.0.14
         WR Mgr5=10.0.0.15
         Queue Depth=0

      OSPF options...
         RunOSPF=Yes
         Area=0.0.0.0
         AreaType=Normal
         HelloInterval=10
         DeadInterval=40
         Priority=5
         AuthType=Simple
         AuthKey=ascend0
         Cost=1
         ASE-type=Type1
         ASE-tag=c0000000
         TransitDelay=1
         RetransmitInterval=5
      OSPF global options...
         Enable ASBR=Yes
      Route Pref…
         Static Preference=100
         Rip Preference-100
         RIP Queue Depth=50
         RipAseType-Type2
         Rip Tag=c8000000
         OSPF Preference=10
         OSPF ASE Preference=150
      TServ options...
         TS Enabled=Yes
         Passwd=Ascend
         Banner=** Ascend Terminal Server **
         Login Prompt=Login:
         Passwd Prompt=Password:
         Prompt=gateway-1>
         Prompt Format=No
         Term Type=vt100
         Telnet =Yes
         Def Telnet=Yes
         Clear Call=Yes
         Telnet mode=ASCII
         Initial Scrn=Cmd
         Toggle Scrn=No
         Security=Full
         3rd Prompt=
         3rd Prompt Seq=N/A
         Remote Conf=No
         Host #1 Addr=0.0.0.0
         Host #1 Text=
         Host #2 Addr=0.0.0.0
         Host #2 Text=
         Host #3 Addr=0.0.0.0
         Host #3 Text=
         Host #4 Addr=0.0.0.0
         Host #4 Text=
         Telnet Host Auth=No
         Clr Scrn=Yes
         Packet Wait time=0
         Packet characters=0
         Login Timeout=300
         IP Netmask Msg=Netmask:
         IP Gateway Addr Msg=Gatewa+
      Bridging=Yes
      IPX Routing = No
      AppleTalk=Yes
      Shared Prof=No
      Telnet PW=Ascend
      RIP Policy=Split Horzn
      RIP Summary = Yes
```

```
ICMP Redirects = Ignore
NAT Routing=No
NAT Profile=N/A

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

DHCP Spoofing...
   DHCP Spoofing=Yes
   DHCP PNP Enabled=Yes
   Renewal Time=10
   Become Def. Router=No
   Dial if Link Down=No
   Always Spoof=No
   IP Group 1=192.1.32.1/24

DNS...
   Domain Name=abc.com
   Sec Domain Name=
   Pri DNS=10.65.212.10
   Sec DNS=12.20 7.23.51
   Allow As Client DNS=Yes
   Pri WINS=0.0.0.0
   Sec WINS=0.0.0.0
   List Attempt=No
   List Size=N/A
   Client Pri DNS=0.0.0.0
   Client Sec DNS=0.0.0.0
   Enable Local DNS Table=No
   Loc.DNS Tab Auto Update=No

Multicast...
   Forwarding=Yes
   Membership Timeout=360
   Mbone Profile=
   Client=No
   Rate Limit=5
   HeartBeat Addr=224.0.1.1
   HeartBeat Udp Port=123
   HeartBeat Slot Time=10
   HeartBeat Slot Count=10
   Alarm threshold=3
   Source Addr=128.232.0.0
   Source Mask=0.0.0.0

Auth...
   Auth=None
   Auth Host #1=N/A
   Auth Host #2=N/A
   Auth Host #3=N/A
   Auth Port=N/A
   Auth Src Port=N/A
   Auth Timeout=N/A
   Auth Key=N/A
   Auth Pool=N/A
   Auth TS Secure=N/A
   Auth Send Attr. 6,7=N/A
   Local Profiles First=N/A
```

```
         Timeout Busy=No
         APP Server=No
         APP Host=N/A
         APP Port=N/A
         Sess Timer=N/A
         Framed Addr Start=No
         Auth Reset Timeout=N/A
      Log...
         Syslog=Yes
         Log Host=10.65.212.12
         Log Port=514
         Log Facility=Local0
         LogCallInfo=EndofCall

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

      AppleTalk...
        Zone Name=engnet
        Appletalk Router=Yes
        Net Start=
        Net End=
        Default Zone=
        Zone Name # 1=
        Zone Name # 2=
        Zone Name # 3=
.
.
.
        Zone Name # 31=

      SNTP Server...
         SNTP Enabled=Yes
         Time zone-UTC+0000
         SNTP host#1=0.0.0.0
         SNTP host#2=0.0.0.0
         SNTP host#3=0.0.0.0

      UDP Cksum=No
      TCP Timeout=0
      Adv Dialout Routes=Always
```

Filter profile

```
Ethernet
   Filters
      Name=filter-name
      Input filters...
         In filter 01—12
            Valid=Yes
            Type=GENERIC
            Generic...
               Forward=No
               Offset=14
               Length=8
               Mask=ffffffffffffffff
               Value=aaaa0300000080f3
               Compare=Equals
               More=No

            Ip...
               Forward=No
               Src Mask=255.255.255.192
               Src Adrs=192.100.50.128
               Dst Mask=0.0.0.0
               Dst Adrs=0.0.0.0
               Protocol=0
               Src Port Cmp=None
               Src Port #=N/A
               Dst Port Cmp=None
               Dst Port #=N/A
               TCP Estab=N/A

            Ipx...
               Forward=No
               Src Network Adrs=00000000
               Dst Network Adrs=00000000
               Src Node Adrs=000000000000
               Dst Node Adrs=000000000000
               Src Socket #=N/A
               Src Socket Cmp=None
               Dst Socket #=N/A
               Dst Socket Cmp=None

      Output filters...
         Out filter 01—12
            Valid=Yes
            Type=GENERIC
            Generic...
               Forward=No
               Offset=14
               Length=8
               Mask=ffffffffffffffff
               Value=aaaa0300000080f3
               Compare=Equals
               More=No

            Ip...
               Forward=No
               Src Mask=255.255.255.192
               Src Adrs=192.100.50.128
               Dst Mask=0.0.0.0
               Dst Adrs=0.0.0.0
               Protocol=0
               Src Port Cmp=None
               Src Port #=N/A
               Dst Port Cmp=None
               Dst Port #=N/A
               TCP Estab=N/A

            Ipx...
               Forward=No
               Src Network Adrs=00000000
               Dst Network Adrs=00000000
               Src Node Adrs=000000000000
```

```
               Dst Node Adrs=000000000000
               Src Socket #=N/A
               Src Socket Cmp=None
               Dst Socket #=N/A
               Dst Socket Cmp=None
```

Firewall profiles

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

Frame Relay profile

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

IPX Routes profile

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

IPX SAP Filter profile

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

NAT profile

```
20-B00 NAT
   20-B01 NAT..
      Routing=Yes
      Profile=
      FR address=0.0.0.0
       Static Mappings...
         Static Map 01
            Valid=Yes
            Dst Port #=0
            Protocol=TCP
            Loc Port #=0
            Loc Adrs=0.0.0.0
      Def Server=0.0.0.0
      Reuse last addr=No
      Reuse addr timeout=N/A
```

SNMP Traps profile

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

Static Rtes profile (IP routes)

```
Ethernet
   Static Rtes
      Name=SITEBGW
      Active=Yes
      Dest=10.2.3.0/24
      Gateway=10.2.3.4
      Metric=2
      Preference=100
      Private=No
      Ospf=Cost=1
      LSA-type=ExternalType1
      NSSA-ASE7=Type1
      ASE=tag=c0000000
      Third-Party=No
```

Index