Pipeline 25-Fx Administrator's Guide

Ascend Communications

Part Number 7820-0287-002 September 17, 1996

Important Safety Instructions

The following safety instructions apply to the Pipeline 25-Fx:

1 Read and follow all warning notices and instructions marked on the Pipeline 25-Fx or included in the manual.

2 The maximum recommended ambient temperature for the Pipeline 25-Fx is 104° Fahrenheit (40° Celsius). Care should be given to allow sufficient air circulation or space between units when the Pipeline 25-Fx is installed in a closed or multi-unit rack assembly, because the operating ambient temperature of the rack environment might be greater than room ambient.

3 The connections and equipment that supply power to the Pipeline 25-Fx should be capable of operating safely with the maximum power requirements of the Pipeline 25-Fx. In the event of a power overload, the supply circuits and supply wiring should not become hazardous. The input rating of the Pipeline 25-Fx is printed on its label.

4 Do not allow anything to rest on the power cord and do not locate the product where persons will walk on the power cord.

5 Do not attempt to service this product yourself, as opening or removing covers may expose you to dangerous high voltage or other risks. Refer all servicing to qualified service personnel.

6 General purpose cables are provided with this product. Special cables, which may be required by the regulatory inspection authority for the installation site, are the responsibility of the customer.

7 When installed in the final configuration, the product must comply with the applicable safety standards and regulatory requirements of the country in which it is installed. If necessary, consult with the appropriate regulatory agencies and inspection authorities to ensure compliance.

In addition, take the following precautions when dealing with telecommunications circuits:

- Never install telephone wiring during a lightning storm.
- Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.
- Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
- Use caution when installing or modifying telephone lines.
- Avoid using equipment connected to telephone lines (other than a cordless telephone) during an electrical storm. There is a remote risk of electric shock from lightning.
- Do not use a telephone or other equipment connected to telephone lines to report a gas leak in the vicinity of the leak.

Contents

Figures

Tables

About This Guide

This guide provides comprehensive information about Pipeline configuration settings and network management. It is written for primarily for network administrators.

To learn how to install your Pipeline and configure it with settings provided by a network service provider or system administrator, see the *Pipeline 25-Fx User's Guide* included with your Pipeline.

What is in this guide?

This guide contains these chapters:

- Chapter 1, "Getting Acquainted with the Pipeline," introduces the Pipeline 25-Fx and explains some Pipeline 25-Fx terminology.
- Chapter 2, "Navigating the User Interface," explains how to navigate the Pipeline 25-Fx configuration interface.
- Chapter 3, "Configuring WAN Connections," shows you how to configure the Pipeline 25-Fx for various types of WAN connectivity.
- Chapter 4, "Configuring the Pipeline as a Bridge," explains how to configure the Pipeline 25-Fx for bridging.
- Chapter 5, "Configuring the Pipeline as an IP Router," explains how to configure the Pipeline 25-Fx for IP routing.
- Chapter 6, "Configuring the Pipeline as an IPX Router," explains how to configure the Pipeline 25-Fx for IPX routing.
- Chapter 7, "Pipeline System Security," explains how to configure the Pipeline 25-Fx security.

- Chapter 8, “Using Filters,” explains how filters work and how to define filters.
- Chapter 9, “Pipeline System Administration,” explains how to perform administrative tasks on the Pipeline 25-Fx.
- Chapter 10, “Using the Command Mode,” explains how to use the Pipeline terminal server to perform diagnostic and system maintenance tasks.
- Chapter 11, “Reference,” provides complete descriptions of the Pipeline configuration parameters and DO menu commands.
- Chapter 12, “Status Menu Reference,” describes the contents of the Pipeline status menus.
- Appendix A, “Troubleshooting,” helps you correct problems that can occur during or after configuration.
- Appendix B, “System Event Messages,” lists all the possible event messages that can appear in the status windows.
- Appendix C, “ISDN Cause Codes,” lists ISDN diagnostic codes that appear in the System Events status window.
- Appendix D, “Upgrading Pipeline Software,” explains how to install new versions of the Pipeline software.
- Appendix E, “Pipeline 25-Fx Specifications,” lists hardware and software specifications for the Pipeline.

The guide also includes a glossary and an index.

What you should know

This guide is intended for the person who will configure and maintain the Pipeline 25-Fx. To configure the Pipeline 25-Fx, you need to understand the following:

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

Documentation conventions

This section shows the documentation conventions used in this guide.

Convention	Meaning
`Monospace text`	Monospace text represents information that you enter exactly as shown, and it identifies onscreen text, such as, statistical information.
[]	Square brackets indicate an optional attribute that you append to a command. To include an attribute, type only the information inside the brackets. Do not type the brackets unless they appear in bold type.
italics	Italics represent variable information. Do not enter the words themselves in the command; enter the information they represent.
Key1-Key2	Keys displayed next to each other represent combination keystrokes. To enter combination keystrokes, press one key and hold it down while you press one or more other keys. Release all the keys at the same time.
|	The | symbol separates command choices that are mutually exclusive.
Note:	A note signifies important additional information.
 **Caution:**	A caution means that a failure to follow the recommended procedure could result in a loss of data or damage to equipment.
 **Warning:**	A warning means that a failure to take appropriate safety precautions could result in physical injury.

Getting Acquainted with the Pipeline

1

This chapter contains:

Pipeline features

Welcome to the Pipeline —Ascend's affordable home office and telecommuting solution. The Pipeline provides full internetworking and high-speed multimedia communications from your home office.

In a single modem-sized box, the Pipeline supports these features:

- ISDN Basic Rate Interface (BRI) interface
- Protocol-independent bridging
- Bandwidth-on-Demand
- Inverse multiplexing for 128 Kbps throughput
- Security features (dial-up security, PAP, CHAP, security cards)
- Unicast and Multicast packet filtering
- PPP (Point-to-Point Protocol) and MPP (Multichannel Point-to-Point)
- Flash memory for simple software upgrades
- Data compression for maximum throughput (up to 512 Kbps)
- Optional IP routing software for accessing TCP/IP-based networks, such as the Internet or a company network that has Unix computers
- Optional IPX routing software for connecting to a company network that includes NetWare servers

Network connection features

The Pipeline uses profiles— named configurations that contain the settings needed for a particular purpose or connection.

System profiles are located below the System menu. These profiles set parameters related to the device itself, security, and administration.

Network profiles are accessed below the Ethernet menu. Network profiles set parameters related to network conditions and connections. These network profiles are supported in the Pipeline:

- Connections (incoming and outgoing connections)

- Bridge Adrs (physical addresses for remote devices)
- Static Routes (IP routing table)
- Filters (packet filters)
- Answer (incoming connections from unknown networks)
- IPX Routes (static IPX routes to far-end servers) *IPX routing only*
- IPX SAP Filters (NetWare Service Advertising Protocol filters) *IPX routing only*
- Mod Config (local Ethernet configuration)

Connection Profiles

Each of the Connection Profiles is related to a specific destination and is used to establish outgoing and incoming connections with that network.

The first Connection Profile is automatically created when you set the parameters in the Configure Profile. The Configure Profile sets many parameters that are specific to one remote network. However, the Configure Profile also lets you specify a hostname for the Pipeline and configure its ISDN characteristics—settings which apply globally to all connections.

How sessions are initiated

A session is an active connection. Packets sent or received by the Pipeline initiate a session automatically, as soon as there is a need for one. However, you can also manually start up a session by using the Pipeline DO menu or by using your communications software.

The Pipeline negotiates a session with a remote device by dialing it up (or accepting a dial-in call) and then exchanging information to ensure that communication can occur. The information that's exchanged as a sort of initial handshaking between devices can include the following:

- Telephone company options
- Encapsulation options (agreeing on how data will be exchanged)
- Authentication and data compression
- Bridging and/or routing information

Note: Typically, the Pipeline starts up a connection with a remote network "on demand," based on active traffic (packets sent to or received from a remote network). It's possible for routine traffic to start up connections, causing unnecessary connection costs. You can prevent this from happening by using a filter.

Telco options

Most of the Telco (telephone company) options related to ISDN have default values set for calls within North America and have to do with the type of data service supported on your ISDN line.

By default, the Pipeline assumes a full 64K data service on each of its ISDN channels, which requires that the phone company as well as the complete path between your local device and the far-end device must support 64K data service. The complete path to some European or Pacific Rim countries cannot guarantee 64K service, in which case you need to configure the Pipeline to use 56K instead.

Encapsulation

The Pipeline connects to remote sites by using PPP (Point-to-Point Protocol). The remote site must support PPP for a connection to occur.

The Pipeline supports both standard PPP and a multichannel version of the protocol called MPP (Multichannel Point-to-point Protocol), which supports inverse multiplexing, dynamic bandwidth allocation, and channel monitoring and replacement. These features have configuration options associated with them, so you can fine-tune when and how they occur.

If you configure the Pipeline to use MPP (the default) and the remote network it connects to doesn't support MPP, the device negotiates for a Multilink PPP connection, and failing that, reverts to standard PPP.

Authentication

Authentication is an important part of negotiating a session. Many sites require a password before accepting a session. "Security features" on page 1-11 describes the security supported on the Pipeline in more detail.

Data compression

The Pipeline supports STAC compression (with an optional hardware module) and Van Jacobsen compression.

STAC compression refers to a compression algorithm, developed by STAC Electronics, Inc., which modifies the standard LZS compression algorithm to optimize for speed (as opposed to optimizing for compression). If you configure the device to use STAC compression and the far-end network also supports STAC compression, it is one of the parameters negotiated when setting up a PPP connection.

Van Jacobsen compression refers to a header compression algorithm, originally developed for TCP/IP but extended to include both TCP/IP and IPX, which reduces the size of packet headers and increases the efficiency of line utilization.

Bridging and routing

Depending on your Pipeline model, you can either route IP or IPX, as well as bridge. Protocol-independent bridging is used to handle protocols other than IP or IPX. Routing and bridging may be used simultaneously over any link.

When you configure a routing connection, remember that *both sides* of the connection must be configured with routing information. Remote network information is configured in the Connection Profile for that destination network. Network information for the local Ethernet is configured in the Ethernet Profile.

Bridge Adrs Profiles

If the Dial Broadcast feature is disabled in a Connection Profile, the Pipeline does not initiate dialing for broadcast requests (for example, when a local application sends out a broadcast looking for a server). Instead, it relies on Bridge Adrs Profiles.

Static Rtes Profiles

When the Pipeline is configured to route IP protocols it relies on Static Rtes Profiles to determine where to send packets.

Filter Profiles

The most common use of Filter Profiles is to filter out packets that don't need to go over the ISDN connection, so unnecessary connections aren't activated. Because the Pipeline automatically (and silently) initiates a connection based on network activity, routine network traffic such as broadcast traffic can bring a connection up or keep a connection up unnecessarily. A filter can screen out routine broadcast or multicast traffic on the network to keep those packets from maintaining the connection. A filter used in this way is called a call filter. The Pipeline comes with two predefined call filters for NetWare, or TCP/IP connections. Filters can also be used to screen out certain kinds of data on the local or ISDN interface, or to drop incoming packets that are addressed to particular hosts. A filter used in that way is called a data filter.

Answer Profile

When the Pipeline receives an incoming data call, it first verifies that the incoming call supports the required authentication (if any). Required authentication is set in the Answer Profile.

The Pipeline then looks for a Connection Profile that matches the incoming call identification. If it finds a Connection Profile for the incoming call, the Pipeline uses the configuration settings in the Connection Profile for the call.

If the Pipeline doesn't find a Connection Profile for the call, it tries to use the configuration settings in the Answer Profile.

IPX Routes Profiles (IPX routing only)

IPX Routes Profiles contain all the information necessary to reach a specific IPX service on the far-end network. IPX Routes Profiles are typically required for IPX networks where it may take a long time for clients to find a server (to prevent timeouts), and we recommend that you configure at least one IPX Routes Profile whenever IPX routing is in use.

IPX SAP Filter Profiles (IPX routing only)

In NetWare 4.0 and later, built-in directory services eliminates the need for SAP. Services are located through directory services instead.

In NetWare 3.*x*, however, NetWare servers broadcast SAP packets every 60 seconds to make sure that all routers and bridges know about available services.

Like other IPX routers, the Pipeline builds a service table based both on statically configured IPX routes and information contained in SAP broadcast packets. In an active IPX environment that includes many servers and many types of servers, the resulting service table can be very large. IPX SAP Filters enables Pipeline to restrict the service table to a manageable size and provide more control for the network administrator.

Ethernet Profile

The local Ethernet network has certain defaults set by the Configure Profile, but can be configured with IP or IPX routing parameters, information about message logging, and other local options. If you are connecting to remote IP or IPX networks, you must specify the near-end IP or IPX parameters in this profile.

Voice features of the Pipeline

An ISDN telephone line can carry data, voice, or both at once. The Pipeline includes two telephone ports, Phone 1 and Phone 2, that let you use standard telephones, fax machines, or other analog telephone equipment on the same ISDN line you use for data.

Throughout this manual, the term analog device refers to any conventional telephone device, such as a telephone or fax machine, that you connect to one of the Phone ports of the Pipeline. The term analog port refers to either of the Phone ports.

How your ISDN service affects voice features

The voice features that are available on your Pipeline are determined in part by the type of ISDN service your telephone company provides and by the telephone switching equipment, known as a switch, that it uses to provide that service. For example, most types of residential ISDN service can include two telephone numbers, known as directory numbers. Because each voice call requires its own directory number, you need two directory numbers to make or receive two different voice calls at the same time, such as when making a voice call at the same time you receive a fax. In contrast, one type of ISDN service, AT&T Custom Point-to-Point, includes only one directory number.

The sections that follow note differences in voice features for certain types of ISDN service and for certain switches. Because standardized ISDN services, such as National ISDN-1 (NI-1), are becoming more common, these differences are becoming less frequent. A separate document, "Ordering ISDN Service for the Ascend Pipeline 25 and 75," explains how to order ISDN Basic Rate Interface (BRI) service—the affordable ISDN service for which the Pipeline is designed—and lists advantages and dissuasiveness of different types of BRI service. If your telephone company offers more than one type of BRI service, you can use the lists of advantages and dissuasiveness to determine which type is best for you.

Note: The voice features of the Pipeline 75 are identical to those of the Pipeline 25, and so are the switch settings the telephone company uses to support them. Because the Pipeline 25 is widely used, most telephone companies know the switch settings that are necessary. When ordering ISDN service for a Pipeline 75, you can say simply that you are using a Pipeline 25. If your telephone company does not know the proper settings, you can copy and send them the recommended settings listed in Th. document "Ordering ISDN Service for the Ascend Pipeline 25 and 75." These settings are necessary for the voice features to work as described in the following sections.

How outgoing voice calls are handled

An ISDN Basic Rate Interface (BRI) line has up to two bearer (B) channels. When configured properly for the Pipeline, each channel can carry either voice or data. When a B channel is used for voice, it can carry a single voice call. When a B channel is used for data, it normally carries the data at a rate of 64Kbps

(kilobits per second). Two B channels used for data can be combined to carry 128Kbps to the same location.

The voice-handling features of the Pipeline make it easy to make outgoing voice calls:

- If neither B channel is currently in use, you can make a voice call by picking up the receiver of a telephone connected to either analog port.
- If a single B channel is currently in use, you can make a voice call by picking up the receiver of a telephone connected to either analog port. The other B channel is used for the call.
  - Exception: If the switch is a Northern Telecom DMS-100 and the value of the Phone Num Binding parameter is Yes, you cannot make the call if the currently used B channel and the analog port to which the phone is connected both use the same directory number.
  - Exception: If the type of ISDN service is AT&T Custom Point-to-Point, there can be only one voice call at a time.
- If both B channels are used for a data call to the same location, you can make a voice call by picking up the receiver of a telephone connected to either analog port. The Pipeline automatically preempts one of the B channels for the voice call. This feature, known as *outgoing call preemption*, works on all types of ISDN service and all switches.

If both B channels are used in use for any other combination of calls—for two voice calls, for one voice call and one data call, or for two data calls to different locations—you cannot make another voice call.

In general, the directory number used for a voice call is the directory number assigned to the analog port from which the call is made. See "The voice-handling features of the Pipeline also make it easy to receive incoming voice calls. In the most common configuration, where each analog port is assigned to a different directory number, incoming voice calls are handled as follows:" on page 1-10 to learn how to assign a directory number to an analog port.

- Exception: If the switch is a Northern Telecom DMS-100, a currently used B channel and the analog port to which the phone is connected both use the same directory number, and the value of the Phone Num Binding parameter is No, the other directory number is used for the call.

Because AT&T Custom Point-to-Point service includes only one directory number, all outgoing voice calls use that number.

How incoming voice calls are handled

The voice-handling features of the Pipeline also make it easy to receive incoming voice calls. In the most common configuration, where each analog port is assigned to a different directory number, incoming voice calls are handled as follows:

- If neither B channel is currently in use, you can receive a voice call on either directory number.
- If a single B channel is currently used for a data call, you can receive a voice call on either directory number. The other B channel is used for the voice call. The call is routed to the analog port assigned to the directory number.
  - Exception: If the switch is a Northern Telecom DMS-100, the caller receives a busy signal if the incoming call is for the same directory number used by the data call.
- If a single B channel is currently used for a voice call, you can receive a voice call for the directory number not used by the current voice call. The call is routed to the analog port assigned to the directory number.
- If a single B channel is currently used for a voice call, and there is an incoming call to the same directory number as the current call, the caller receives a busy signal.
- If both B channels are used for a data call to the same location, you can receive a voice call to either directory number. The Pipeline automatically preempts one B channel for the voice call, and the call is routed to the analog port assigned to the directory number. This feature is known as incoming call preemption.
  - Exceptions: AT&T Custom Multipoint service and AT&T Custom Point-to-Point service do not support incoming call preemption. With these services, callers receive a busy signal whenever both B channels are in use.
- If both B channels are used in use for any other combination of calls—for two voice calls, for one voice call and one data call, or for two data calls to different locations—the Pipeline cannot handle another voice call, and callers to either directory number receive a busy signal.

Incoming voice calls are handled differently with AT&T Custom Point-to-Point service. Because this service includes only one directory number, it can handle only one voice call at a time.

- If a single B channel is currently used for a data call, you can receive a voice call. The call is routed to the Phone 1 port.
- If a B channel is currently used for a voice call, a caller to the directory number receives a busy signal.
- If both B channels are in use, a caller to the directory number receives a busy signal.

Note: In certain cases, a voice call can be used to carry data. The technique used for this, known as Data Over Voice Bearer Service (DOVBS), is described. If a Pipeline receives an incoming voice call for one of its directory numbers, neither analog port is assigned to the directory number, and a B channel is available, the Pipeline assumes that DOVBS is being used, converts the voice to data, and routes the data to the local-area network.

Security features

The Pipeline software includes several security features. They are described in more detail in Chapter 7, “Pipeline System Security.”

- PAP and CHAP

  The Pipeline supports both PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol).
- Restricted incoming calls

  You can configure the Pipeline to reject incoming calls from any unrecognized network. Restricting network access to the Pipeline provides a high level of secure control against unauthorized access from remote sites.
- Call-back security

  When call-back is enabled in a Connection Profile, the Pipeline hangs up after receiving an incoming call and then dials back to the remote end. Call-back security provides the highest level of control in assuring that incoming calls are coming from a known network.
- Security cards and passwords

A security card is a hand-held device the shape and size of a credit card, such as those provided by Engima Logic or Security Dynamics. If the administrator of the far-end network assigns you a security card, you can configure the Pipeline to respond to password challenges.

- Multi-level user access password security

  The Pipeline provides multi-level password security to allow different levels of access to critical operations. Access security is defined in Security Profiles.

- Filters used for security purposes

  Filtering can provide the most robust form of security available in a dial-up internetworking environment. You can tailor a filter on a per-connection basis to allow or deny packets from any combination source and destination address, protocol discriminator, source and destination port, and TCP sessions.

Administrative features

The Pipeline software contains these management features:

- Windows configuration utility

  If you have a Windows PC you can use the Windows Configuration program included with your Pipeline to configure your unit. This program guides you through the configuration of your unit and provides detailed online help.

- FLASH memory software upgrades

  The Pipeline FLASH EEPROM enables software upgrades in the field without opening the unit or changing memory chips. The Pipeline can be upgraded through the serial Control port.

- The DO menu

  Pressing Ctrl-d while a configuration menu is open displays the DO menu. A common use of this menu is to manually dial or clear a call, or to change security levels in the Pipeline.

- Remote management

  Using bandwidth between sites over the management subchannel established by the MP+ protocol, any Ascend unit can control, configure, and obtain statistical and diagnostic information about any other Ascend unit both locally

and remotely. Multi-level password security ensures that unauthorized personnel do not have access to remote management functions.

- System diagnostic commands

  The Pipeline provides commands for rebooting the device, saving or restoring configuration information, and performing other administrative functions.

- The command mode interface

  You can invoke a command-line interface where you can test a connection, check routing tables and other configuration parameters, or enable remote configuration of the Pipeline.

- Status windows

  The status windows in the system software provide information about what is currently happening in the Pipeline. For example, one status window displays up to 31 of the most recent system events that have occurred since the Pipeline was powered up, and another displays statistics about the currently active session. There are also a few active functions you can perform in the status window, such as manually clearing an active connection.

Navigating the User Interface

2

This chapter contains these sections:

Using the configuration menus

You can access the Pipeline configuration menus in a VT100 emulation window from a computer connected to the Terminal port. Refer to the installation instructions in the *Pipeline 25-Fx User's Guide* for information on connecting your computer to the Control port. When you see the configuration menus, you have established a Console session.

You can also use the Rem Mgmt command to enable a caller at the far end of an MPP call to access the Pipeline configuration menus.

The main edit menu

The configuration interface consist the Main Edit Menu and eight status windows. The left part of the screen is the Main Edit Menu, which is used to configure the Pipeline. See Figure 2-1.

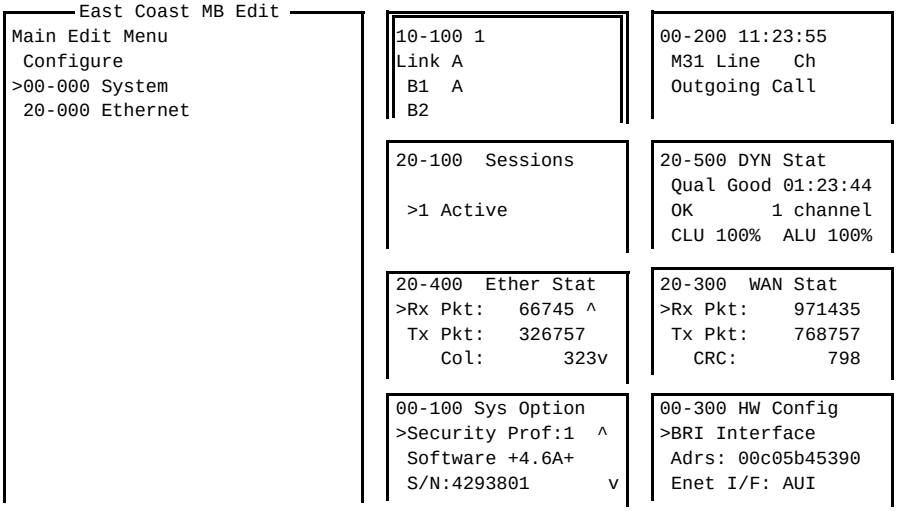


Figure 2-1. Pipeline configuration menus and status windows

How the configuration menus are organized

Figure 2-1 shows how the menus and profiles are organized in the Pipeline with IP routing.

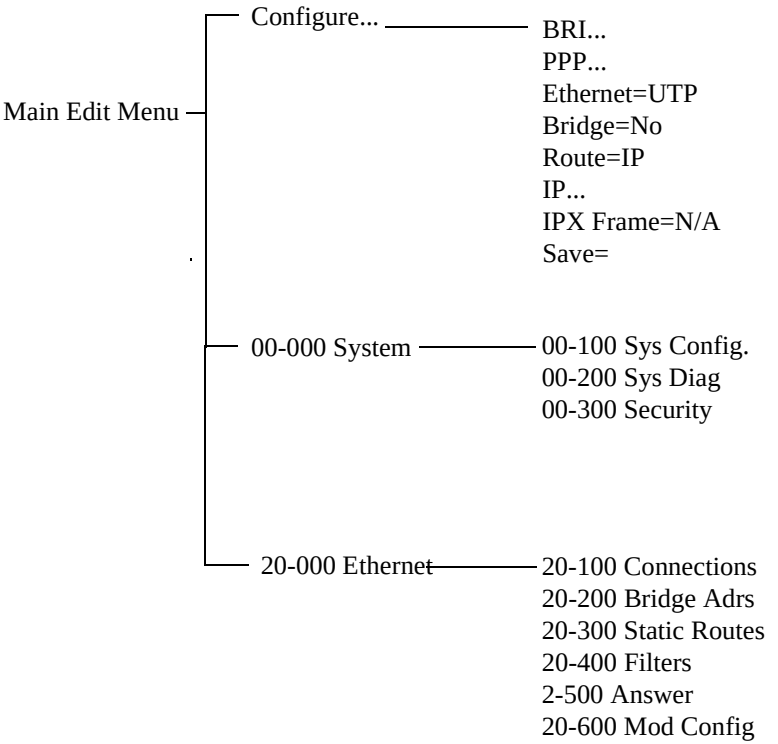


Figure 2-2. Menu and profile organization in the Pipeline with IP routing

Figure 2-3 shows how the menus and profiles are organized in the Pipeline with IPX routing.

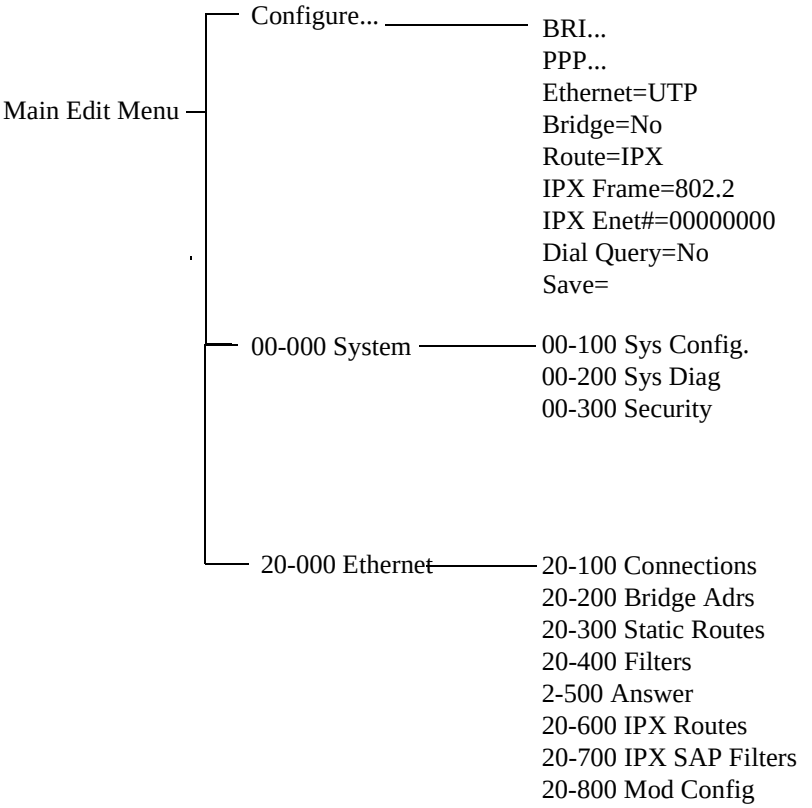


Figure 2-3. Menu and profile organization in the Pipeline with IPX routing

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.

In Figure 2-1, the 10-100 status display is active (near the top-middle of the screen).

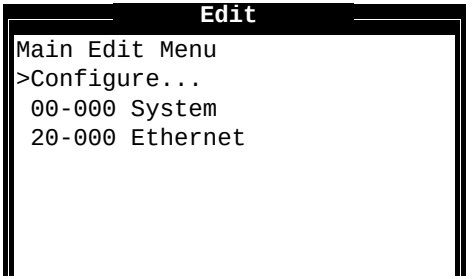
If you press the Tab key, the thick double lines move to 00-200, the next screen to the right. If you continue pressing the Tab key, you activate each window from

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.

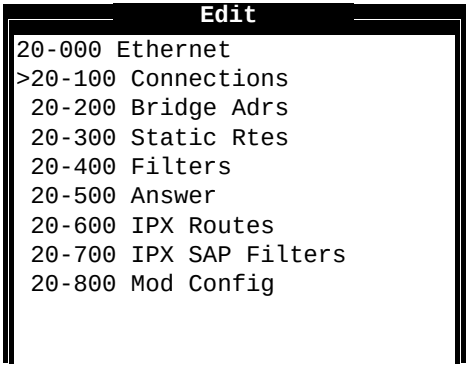
Opening menus and profiles

The Main Edit Menu contains a list of menus, each of which can contain profiles and submenus.

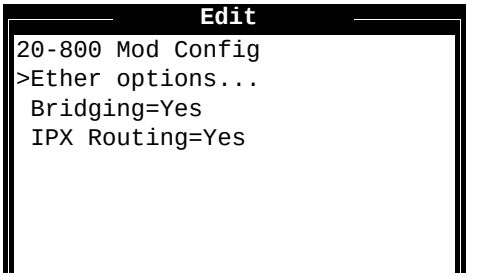
In the menu that is currently open, he cursor character (>) points to one item in the menu. to move the cursor down, press Ctrl-N (next) or the down-arrow key. To move it up, press Ctrl-P (previous) or the up-arrow key. (Some VT100 emulators do not support the use of arrow keys.)



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 20-000 Ethernet, and press Enter. The Ethernet menu opens.



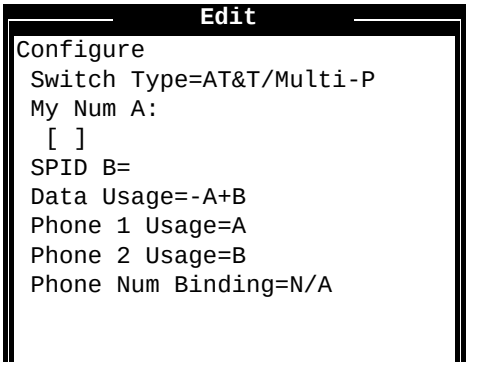
The Ethernet menu contains submenus and profiles related to network functionality, such as bridging, routing, WAN connections, and so forth. The Mod Config Profile in this menu relates to the configuration of the Ethernet interface itself, as shown next.



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 My Num A parameter, next.



Note that while the edit field is open, the menu item directly below the parameter you are setting is temporarily obscured.

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.

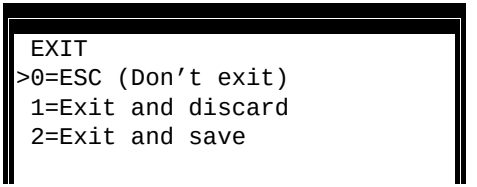
To close the edit field and accept the new text, press Enter.

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

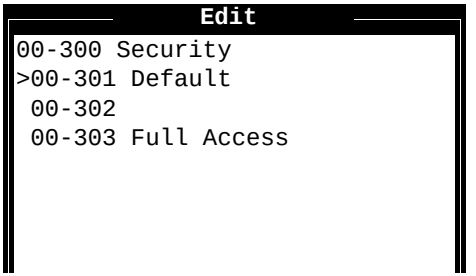
When you exit a profile, you are prompted to confirm that you want to save changes.



You can save the profile values by choosing the Exit and Save option and pressing Enter, or by pressing 2.

About Pipeline passwords

The Pipeline has up to three security levels, each of which is defined in a Security Profile. When shipped from the factory, all 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.



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. 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. This is an important four-step process:

1 Open the Default Security Profile and set the Operations privilege to No.

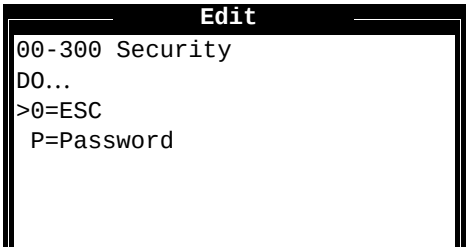
2 Assign a password to the Full Access Security Profile. (Do not restrict privileges in the Full Access Profile.)

3 Activate the Full Access Security Profile and proceed to configure the Pipeline.

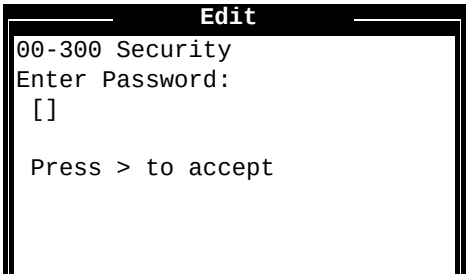
See Chapter 7, “Pipeline System Security,” for full details on modifying Security Profiles and assigning passwords.

Caution: If you reset or power-cycle the Pipeline, it activates the new, restrictive Default profile. You will not be able to perform any configuration tasks until you activate and supply the password for the Full Access Profile, described next. The default password for the Full Access Profile is Ascend.

To activate the Full Access Security Profile, press Ctrl-D. A context-sensitive menu, called the DO menu, is displayed.



In the DO menu, press P (or select P=Password). The list of Security Profiles will be displayed. Select Full Access and press Enter. The Pipeline prompts for that profile's password.



Type the password and press Enter to accept it. (We recommend that you modify the Full Access Profile to assign a password other than the default "Ascend" as soon as possible.)

A message states that the password was accepted and the Pipeline is using the new security level, or if the password you entered is incorrect, you are prompted again to enter the password.

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 it is truncated 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 display.

Table 2-1. Special purpose keys for Control Monitor display

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.
Delete	Delete the character under the cursor.
Backspace	Delete the character to the left of the cursor.
Ctrl-D	Open the DO menu.
Ctrl-L	Refresh the VT-100 screen.
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.

Where to go next?

Now that you understand the Pipeline user interface, proceed to the next chapter to finish the configuration of your Pipeline or use the list below to determine where to go next:

- Refer to Chapter 3, “Configuring WAN Connections,” for information about configuring your WAN interfaces.
- Refer to Chapter 4, “Configuring the Pipeline as a Bridge,” for information about configuring the Pipeline for bridging.
- Refer to Chapter 5, “Configuring the Pipeline as an IP Router,” for information about configuring the Pipeline for IP routing.
- Refer to Chapter 6, “Configuring the Pipeline as an IPX Router,” for information about configuring the Pipeline for IPX routing.

Configuring WAN Connections

3

This chapter covers these topics:

Note: This chapter does not explain how to configure connections for IP routing, IPX routing, or protocol-independent bridging. Those topics are covered in their own chapters later in this guide.

Introduction to WAN connections

This chapter describes how to set up required parameters that enable a dial-in or dial-out connection with a particular destination. It focuses on issues related to the connection's link encapsulation and telephone options, not on the transfer of data packets via IP routing, IPX routing, or protocol-independent bridging. Those topics are handled in their own chapters later in this guide.

This chapter also does not discuss security issues such as PAP and CHAP authentication. For details on connection security, see Chapter 7, "Pipeline System Security."

MP+ and PPP

The Pipeline supports MP+ and PPP link encapsulation.

An MP+ connection uses PPP encapsulation and supports multi-channel calls. Standard PPP uses a single channel, so the main benefit of MP+ is increased bandwidth.

MP+ calls are typically network-to-network calls involving an IP, IPX, or other type of networking connection. You can configure bandwidth management and inverse multiplexing to provide very high performance for the connection.

Types of profiles

Typically, a Connection Profile contains all parameters specific to a particular destination. Before the Pipeline even answers an incoming call, it checks the settings in its Answer Profile for information about what to do with the call. If the call does not include the information required by the Answer Profile (such as a name and password), the Pipeline hangs up. Some sites allow the Pipeline to build a connection based on the parameters in the Answer Profile, although this is considered very low security. For details on connection security, see Chapter 7, "Pipeline System Security."

What happens when a connection is established

After the Pipeline has established an incoming connection, it removes the link encapsulation from the inbound data stream and routes the packets internally. When it receives an outbound data stream destined for the remote end of the link, it adds the appropriate link encapsulation to those packets.

Typically, MP+ and PPP encapsulated connections form a link between the Pipeline unit's internal bridge/router and a bridge/router device at the far-end of the call. When it's a bridging connection, the packets received at either end of the link are simply forwarded from the link to each bridge's LAN. When it's an IP or IPX routing connection, the destination addresses in the packets determine where they are forwarded.

Inverse multiplexing

Inverse multiplexing is a method of combining individually dialed channels into a single, higher-speed data stream. Each end of the connection must use an inverse multiplexer, or inverse mux.

For call types that do not involve inverse multiplexing, the Pipeline simply connects to the remote device over the channel or channels whose phone number is dialed, without synchronizing the channels.

For multichannel MP+ calls involving inverse multiplexing, the Pipeline connects to the remote end over a single channel, and then uses information stored in the remote inverse multiplexer to dial multiple channels to the same destination based on the total amount of bandwidth requested.

For MP+ and frame relay data connections, the inverse mux in the Pipeline performs its function at the packet level. One data packet goes over the first circuit, the next goes over the second circuit, and so on, until all the data packets are distributed over all the available circuits. The receiving end adjusts for network-induced delay and reassembles the data packets into their proper order. This inverse multiplexing technique is also referred to as load balancing. Telecommuting applications use packet-level inverse multiplexing.

Enabling link types

To enable the Pipeline to send and receive calls for the various link encapsulation types described in this chapter, you must set the parameters listed in Table 3-1.

Table 3-1. Answer and Connection Profile link encapsulation types

Location	**Parameters**
Ethernet→Connections→*any Connection Profile*	Encaps=MPP Encaps=PPP
Ethernet→Answer→PPP options...	Route IP=Yes (*for IP routing only)* Route IPX=Yes (*for IPX routing only)* Bridge=Yes Recv Auth=Either MRU=1524 LQM=No LQM Min=600 LQM Max=600 Link Comp=Stac VJ Comp=Yes Dyn Alg=Quadratic Sec History=15 Add Pers=5 Sub Pers=10 Min Ch Count=1 Max Ch Count=1 Target Util=70 Idle Pct=0

To set parameters enabling the Pipeline to inbound calls using any of the link encapsulation methods:

1. Open the Ethernet Profile.
2. Open the Connection profile.
3. Set the Encaps parameter to the encapsulation type you plan to use.
   For example:

Encaps=MPP or
Encaps=PPP

4 Close the Connection Profile, saving your changes.

Setting PPP parameters in the Answer Profile

The PPP parameters in the Answer Profile determine the basic parameters that will be required of all incoming MP+ and PPP calls. The bandwidth parameters are used to establish the base channel of incoming MP+ calls and are immediately superseded by the settings in the Connection Profile as soon as that profile is used.

To set PPP parameters in the Answer Profile:

1 Open the Answer Profile.

2 Open the PPP Options submenu.

3 Set Route IP=Yes. (*for IP routing only)*

If this parameter is set to No, all incoming PPP IP routing connections are rejected.

4 Set Route IPX=Yes. (*for IPX routing only)*

If this parameter is set to No, all incoming PPP IPX routing connections are rejected.

5 Set Bridge=Yes.

If this parameter is set to No, all incoming PPP bridging connections are rejected.

6 Set Recv Auth=Either.

Or, set it to PAP or CHAP.

When this parameter is set to None, incoming MP+ or PPP calls are not required to provide a password. Setting it to Either ensures that all of these calls will require their own Connection Profile that specifies a Recv Password, and that either PAP or CHAP encryption is acceptable.

7 Leave the default bandwidth settings.

The bandwidth settings in the Answer Profile apply to incoming calls for which no Connection Profile exists; if a Connection Profile exists, the settings in that profile take precedence.

In this case, since Connection Profiles will be required, you don't need to change the default bandwidth parameters for MP+ calls in the Answer Profile.

8 Close the Answer Profile, saving your changes.

Configuring MP+ connections

MP+ (Multilink Protocol Plus) can combine up to 4 individual channels into a single high-speed connection. Both the dialing side and the answering side of the link must support MP+. If only one side supports MP+, the connection uses MP or standard single-channel PPP.

Understanding bandwidth algorithms

Once an MP+ connection has been established, the protocol can increase the bandwidth of the connection "on demand" by adding channels as they are needed and then dropping channels as bandwidth requirements decrease without terminating the link. This feature is called dynamic bandwidth allocation.

Do you need Dynamic Bandwidth Allocation?

If you use a circuit between two locations to capacity 24 hours per day, using a nailed-up line is more cost effective than using a switched line. However, if you need the circuit only sporadically, or if the circuit is sometimes underutilized, it often makes more sense to lease a smaller amount of nailed-up bandwidth and then supplement it with additional switched bandwidth as traffic requirements dictate.

For example, you might establish some connections only when you need to transfer data, and a single circuit can accommodate low traffic levels. However, if traffic levels grow beyond the capacity of the circuit (such as during a large file transfer), Dynamic Bandwidth Allocation automatically adds additional switched channels. When traffic levels subside, Dynamic Bandwidth Allocation automatically removes the channels from the connection. The bandwidth and connection costs are thereby reduced. You pay only for bandwidth when you need it.

To determine when to add or subtract channels, the Pipeline uses a specified time period as the basis for calculating average line utilization (ALU), and then compares the ALU to a target percentage threshold. When the ALU exceeds the threshold for a specified period of time, the Pipeline attempts to add channels. When ALU falls below the threshold for a specified period of time, the Pipeline attempts to remove channels.

Table 3-2 shows the parameters used for these calculations and automatic bandwidth adjustments.

Table 3-2. MP+ bandwidth management parameters

Location	Parameters
Ethernet→Connections→*any profile* (Connection Profile)	Encaps=MPP
Ethernet→Connections→*any profile*→ Encaps options...	Base Ch Count=1 Min Ch Count=1 Max Ch Count=1 Inc Ch Count=1 Dec Ch Count=1 Dyn Alg=Quadratic Sec History=15 Add Pers=5 Sub Pers=10 Target Util=70 Idle Pct=0
Ethernet→Connections→*any profile*→ Session options...	Idle=120 Preempt=60

How the Pipeline calculates average line utilization

This Dyn Alg parameter specifies which algorithm to use for calculating average line utilization (ALU) for the time period specified by the Sec History parameter.

Figure 3-1 illustrates the differences between the algorithms you can choose.

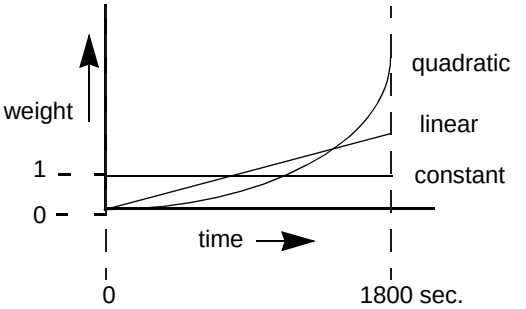


Figure 3-1. Bandwidth algorithms for MP+ calls

- Linear gives more weight to recent samples of bandwidth usage than to older samples taken during the historical period specified by the Sec History parameter. The weighting grows at a linear rate.
- Quadratic (the default for MP+ calls) gives more weight to recent samples of bandwidth usage than to older samples taken during the historical period specified by the Sec History parameter. The weighting grows at a quadratic rate.
- Constant gives equal weight to all samples taken during the historical time period specified by the Sec History parameter. When you select this option, older historical samples have as much impact on the decision to change bandwidth allocation as do more recent samples.

How the Pipeline uses the calculated ALU

The Pipeline compares the calculated ALU to the percentage specified in the Target Util parameter. When ALU exceeds the threshold defined by Target Util for a period of time greater than the value of the Add Pers parameter, the Pipeline attempts to add the number of channels specified by the Inc Ch Count parameter. (Channels must be available, and the addition cannot cause the number of channels to exceed the value specified by the Max Ch Count parameter.)

When ALU falls below the threshold defined by Target Util for a period of time greater than the value of the Sub Pers parameter, the Pipeline attempts to remove the number of channels specified by the Dec Ch Count parameter. It will never remove the base channel of the connection, cause the number of channels to fall

below the value specified by the Min Ch Count parameter, or cause the ALU to exceed the value of Target Util.

Guidelines for setting bandwidth parameters

When configuring dynamic bandwidth allocation parameters, keep these recommendations in mind:

- The values for the Sec History, Add Pers, and Sub Pers parameters should smooth out spikes in bandwidth utilization that last for a shorter time than it takes to add capacity.

  Over ISDN lines, the Pipeline 50 can add bandwidth in less than five seconds.

- Once the Pipeline adds bandwidth, there is typically a minimum usage charge; thereafter, billing is time sensitive.

  The Sub Pers value should be at least equal to the minimum duration charge plus one or two billing time increments. Typically, billing is done to the next multiple of six seconds, with a minimum charge for the first thirty seconds. Your carrier representative can help you understand the billing structure of their switched tariffs.

- Avoid adding or subtracting channels too quickly (less than 10-20 seconds apart).

  Adding or subtracting channels very quickly leads to many short duration calls, each of which incur the carrier's minimum charge. In addition, adding or subtracting channels too quickly can affect link efficiency, since the devices on either end have to retransmit data when the link speed changes.

Managing idle calls and channels

Bandwidth utilization parameters manage active calls. To clear inactive calls and reallocate their bandwidth, you can use the Idle Pct, Idle, and Preempt parameters. For details on filtering out broadcasts and other routine traffic that might keep a connection active for no real reason, see Chapter 8, “Using Filters.”

Clearing a call based on idle time

The Idle parameter specifies the number of seconds the Pipeline waits before clearing a call when a session is inactive. If the timer expires, the Pipeline clears the call. For information on preventing certain types of routine traffic from resetting the timer, see Chapter 7, “Pipeline System Security.”

If you specify 0 (zero), the Pipeline does not enforce a time limit. (However, if the Idle Pct parameter is non-zero, it will clear an inactive session based on bandwidth utilization.)

Clearing a call based on idle bandwidth

The Idle Pct parameter specifies a percentage of bandwidth utilization below which an MP+ call is cleared. Bandwidth utilization must fall below this percentage on *both sides* of the connection before the Pipeline clears the call. If the device at the remote end of the link enters an Idle Pct setting lower than the value you specify, the Pipeline does not clear the call until bandwidth utilization falls below the lower percentage.

The default value for Idle Pct is 0, which causes the Pipeline to ignore bandwidth utilization when determining whether to clear a call and use the Idle timer instead.

Reallocating idle channels

The Preempt parameter specifies the number of idle seconds the Pipeline waits before using one of the channels of an idle link for a new call. You can specify a number between 0 and 65535. The Pipeline sets no time limit if you enter 0 (zero). The default setting is 60.

An example MP+ connection

This example shows how to configure the MP+ link encapsulation, bandwidth, and authentication parameters. It does not show bridging or routing configurations, which are described in their own chapters later in this guide.

Note: For details on enabling MP+ calls in the Answer Profile, see "Enabling link types" on page 3-4. This example presumes that the Answer Profile has been configured as described in that section.

These are the parameters set in this example:

Table 3-3. MP+ configuration parameters

Location	Parameters
System→Sys Config (System Profile)	Name=localdevice
Ethernet→Connections→*any profile* (Connection Profile)	Station=remotedevice Active=Yes Encaps=MPP
Ethernet→Connections→*any profile*→ Encaps options...	Base Ch Count=1 Min Ch Count=1 Max Ch Count=1 Inc Ch Count=1 Dec Ch Count=1 Dyn Alg=Quadratic Sec History=15 Add Pers=5 Sub Pers=10 Target Util=70 Idle Pct=0
Ethernet→Connections→*any profile*→ Session options...	Idle=5 Preempt=60

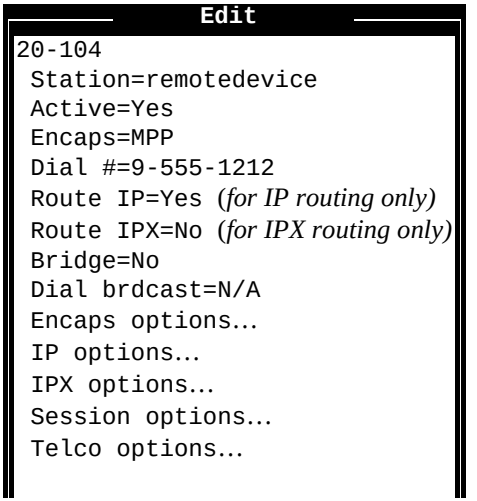
To set the Pipeline system name:

1. Open the System Profile.
2. Specify a name for the Pipeline unit in the Name parameter.
   This parameter is required if Send Auth=PAP or Send Auth=CHAP.
3. Close the System Profile.

To create a Connection Profile that specifies MP+ encapsulation:

1. Open a Connection Profile.
2. Assign a name to the profile.

   When a call is authenticated using PAP or CHAP, the caller must specify both a login name and password. The login name must match the Connection Profile name exactly.
3. Set Active=Yes.
4. Set Encaps=MPP.



To configure the MP+ bandwidth and authentication options:

1. Open the Encaps Options submenu.
2. Turn data compression on.

   For example:

   Link Comp=Stac
   VJ Comp=Yes
3. Set the appropriate authentication parameters.

   For example:

   Send Auth=CHAP
   Send PW=*SECURE*
   Recv PW=*SECURE*

See the Chapter 7, “Pipeline System Security,” for details.

4 Set the bandwidth parameters.

For example:

Base Ch Count=1
Min Ch Count=1
Max Ch Count=4
Inc Ch Count=1
Dec Ch Count=1
Dyn Alg=Quadratic
Sec History=15
Add Pers=5
Sub Pers=10
Target Util=70
Idle Pct=0

5 Close the Encaps Options submenu.

To configure the Idle and Preempt timers:

1 Open the Session Options submenu.

2 Set the Idle and Preempt parameters.

For example:

Idle=30
Preempt=60

This value is the number of seconds a call or channel can be idle before being cleared. See Chapter 8, “Using Filters,” for related information.

3 Close the Session Options submenu.

4 Exit the Connection Profile.

ISDN subaddressing

You can use ISDN subaddressing to control how the Pipeline routes calls that are received on the BRI lines. When ISDN subaddressing is used, incoming calls include a subaddress number as part of the phone number. The subaddress is preceded by a comma in the phone number, for example:

510-555-1212,5

Configuring ISDN subaddressing

Table 3-4 shows Pipeline system parameter that affects ISDN subaddressing.

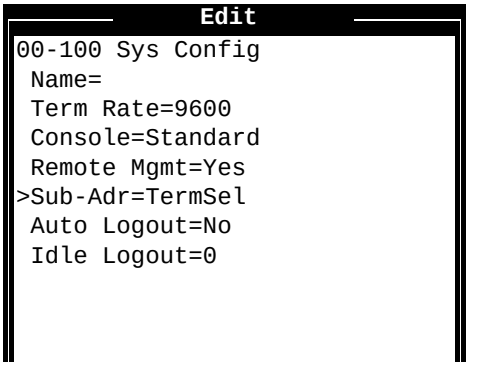
Table 3-4. System-level WAN configuration parameters

Location	Parameters with default values
System→Sys Config (System Profile)	Sub-Adr=None

For details on this parameter, see Chapter 11, “Reference.”

To configure ISDN subaddressing:

1 Open the System Profile.



2 Set Sub-Adr=TermSel.

Termsel specifies that the Pipeline must use an ISDN subaddress to determine whether a call is answered.

The called-party number must have a subaddress. Otherwise, the Pipeline ignores the call. If the Pipeline accepts the call, the subaddress becomes part of the incoming phone number.

3 Exit the System Profile.

Where to go next?

Refer to Chapter 4, “Configuring the Pipeline as a Bridge,” for information about configuring your Pipeline as a bridge.

Chapter 5, “Configuring the Pipeline as an IP Router,” for information about configuring your Pipeline as IP router.

Chapter 6, “Configuring the Pipeline as an IPX Router,” for information about configuring your Pipeline as IPX router.

Configuring the Pipeline as a Bridge 4

This chapter covers these topics:

Ascend bridging parameters

Table 4-1 shows configuration parameters related to protocol-independent bridging.

Table 4-1. Bridging configuration parameters

Location	Parameter with default value
System→Sys Config (System Profile)	Name=[]
Ethernet→Connections→*any profile* (Connection Profile)	Station=[] Bridge=No Dial Brdcast=N/A
Ethernet→Connections→*any profile*→ Encaps options...	Send Auth=None Recv PW=N/A Send PW=N/A
Ethernet→Bridge Adrs→*any profile* (Bridge Profile)	Enet Adrs=000000000000 Net Adrs=0.0.0.0 Connection #=0
Ethernet→Answer→PPP options... (Answer Profile)	Bridge=No Recv Auth=None
Ethernet→Mod Config (Ethernet Profile)	Bridging=Yes

For detailed descriptions of each parameter, see the Chapter 11, “Reference.”

For information about how the authentication parameters are used (Send Auth, Recv PW, Send PW, and Recv Auth), see “How a bridging connection is established” on page 4-5.

For information about filters for bridging connections, see Chapter 8, “Using Filters.”

Introduction to Ascend bridging

This section provides an overview of packet bridging and when to use bridging instead of a routing configuration. It also explains how the Pipeline brings up a bridging connection.

When to use bridging

Bridges are used primarily to provide connectivity for protocols other than IP and IPX. Because a bridging connection forwards packets at the hardware address level (link layer), it does not distinguish between protocol types and it requires no protocol-specific network configuration.

The most common uses of bridging in the Pipeline are:

- To provide AppleTalk or other non-routed protocol connectivity with another site
- To link any two sites so that their nodes appear to be on the same LAN
- To support protocols that depend on broadcasts to function, such as BOOTP

Bridges run in promiscuous mode; that is, they examine all packets on the LAN, so they incur greater processor and memory overhead than routers do. On heavily loaded networks, this increased overhead can result in slower performance.

In addition to the performance benefit of routing, routers have other advantages over bridging as well. Because they examine packets at the network layer (instead of the link layer), you can filter on logical addresses, providing enhanced security and control. In addition, routers support multiple transmission paths to a given destination, enhancing the reliability and performance of packet delivery.

Globally enabling bridging

The Pipeline has a global Bridging parameter that must be enabled for bridging to be supported. Setting Bridging=Yes in the Ethernet Profile puts the Ethernet controller in the Pipeline 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.

Table 4-2. Global bridging parameter

Location	Parameter
Ethernet→Mod Config (Ethernet Profile)	Bridging=Yes

How a bridging connection is initiated

The Pipeline handles dial-in and dial-out aspects of WAN connections, and bridges packets between networks. At the appropriate point in a session negotiation, the Pipeline begins passing packets to its bridging/routing software. The bridging/routing module in the Pipeline then operates like a regular LAN bridge with ports on two different Ethernet segments.

When the Pipeline is configured to bridge, it accepts all packets on the network. It brings up a connection to a remote network when the destination address in a packet is one of the following:

- A physical address that is not on the local Ethernet segment (the segment to which the Pipeline is connected)
- A broadcast address

The important thing to remember about bridging connections is that they operate on physical and broadcast addresses, not on logical (network) addresses.

Physical addresses and the bridge table

A physical address is a unique hardware-level address associated with a specific network controller. A device's physical address is also called its Media Access Control (MAC) address. On Ethernet, the physical address is a six-byte hexadecimal number assigned by the Ethernet hardware manufacturer, for example:

```
0000D801CFF2
```

If the Pipeline receives a packet whose destination MAC address is not on the local network, it first checks its internal bridge table (see "Transparent bridging" on page 4-9).

If it finds the packet's destination MAC address in its bridge table, the Pipeline dials the connection and bridges the packet.

If the address is *not* specified in its bridge table, the Pipeline checks for active sessions that have bridging enabled. If there is one or more active bridging links, the Pipeline forwards the packet across *all* active sessions that have bridging enabled.

Note: The Pipeline cannot dial a connection for packets that are not on the local network and not specified in its bridge table, because it has no way of finding the proper Connection Profile. See "Creating and maintaining the bridge table" on page 4-9 for more details.

Broadcast addresses and Dial Brdcast

A broadcast address is recognized by multiple nodes on a network. For example, the Ethernet broadcast address at the physical level is:

```
FFFFFFFFFFFF
```

All devices on the same network accept packets with that destination address.

If the Pipeline receives a packet whose destination MAC address is a broadcast address, it forwards the packet across all active sessions that have bridging enabled and initiates a session for all Connection Profiles in which the Dial Brdcast parameter is set to Yes.

Note: A special case is made for Address Resolution Protocol (ARP) packets that contain an IP address specified in the bridge table (see "Setting Bridge Profile parameters" on page 4-16 for details). 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 that profile. In effect, the Pipeline as a proxy for the node that actually has that address.

How a bridging connection is established

The Pipeline uses station names and passwords to sync up a bridging connection, as shown in Figure 4-1.

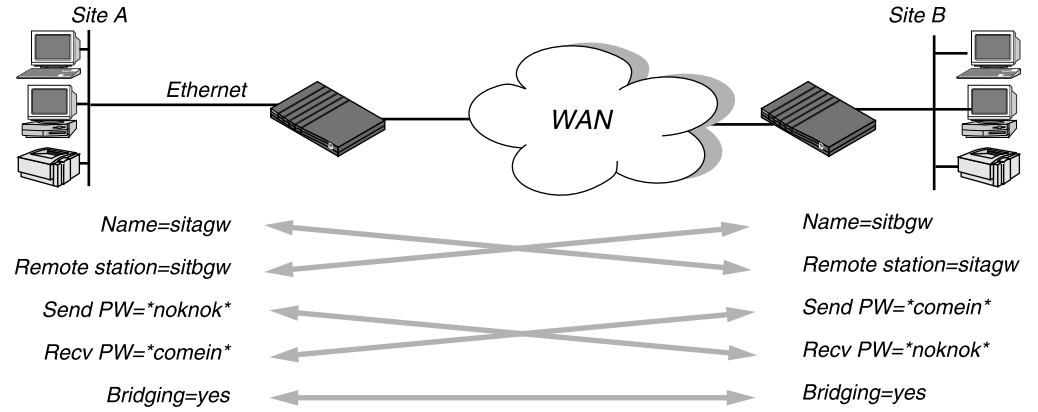


Figure 4-1. Negotiating a bridge connection (PPP encapsulation)

The system name assigned to the Pipeline in the Name parameter of the Sys Config Profile must *exactly* match the device name specified in the Connection Profile on the remote bridge, including case changes. Similarly, the name assigned to the remote bridge must exactly match the name specified in the Station parameter of that Connection Profile, including case changes.

Note: The most common cause of trouble when initially setting up a PPP bridging connection is that the wrong name is specified for the Pipeline or the remote device. Often case changes are not specified, or a dash, space, or underscore is not entered.

Using bridging and routing on the same link

When IP routing is enabled in a Connection Profile, IP packets are *always* routed and never bridged across that connection.

- If Route IP=Yes and Bridge=No in the Connection Profile, only IP packets will be forwarded; all other packets are dropped.
- If Route IP=Yes and Bridge=Yes in the Connection Profile, IP packets are routed and all other packets are bridged across that connection.

When IPX routing is enabled for a connection, the Pipeline can route only one packet frame type for IPX packets across that connection. For example, if the IPX frame type is set to 802.3, only 802.3 packets can be routed. If some

NetWare servers on the local network use a different frame type, such as 802.2, the disposition of those packets depends on the Bridge setting in the Connection Profile.

- If IPX Frame=802.3, and Route IPX=Yes and Bridge=No in the Connection Profile, only 802.3 IPX packets are routed; all other packets are dropped.
- If IPX Frame=802.3, and Route IPX=Yes and Bridge=Yes in the Connection Profile, 802.3 IPX packets are routed and the Pipeline attempts to bridge all other packet types, including IPX packets in other frame types.

  For example, if the Pipeline receives an IPX packet in the 802.2 packet frame, it uses the physical address in that packet to bridge it across all active bridging sessions.

IPX client bridging

Note: Like all options in the IPX Options submenu, the Handle IPX parameter is set to N/A if an IPX frame type is not specified in the Ethernet Profile. If Route IPX is set to Yes in the Connection Profile, the Handle IPX parameter is set to N/A, but acts as if set to Server.

If the local network supports NetWare clients *and no NetWare servers*, you want to enable a client to bring up the WAN connection by querying (broadcasting) for a NetWare server on a remote network. To do this when Route IPX=No, use the Connection Profile settings shown in Table 4-3.

Table 4-3. IPX bridging for local clients only

Location	Parameter
Ethernet→Connections→*any profile* (Connection Profile)	Route IPX=No Bridge=Yes Dial Brdcast=Yes

The IPX Frame type must be configured in the Ethernet Profile, and Bridging must be globally enabled, as described in “Globally enabling bridging” on page 4-3.

IPX server bridging

If the local network supports NetWare servers (or a combination of clients and servers) and the remote network supports NetWare clients only, you want to enable the Pipeline to respond to NCP watchdog requests for remote clients, but to bring down inactive connections whenever possible. To do this when Route IPX=No, use the Connection Profile settings shown in Table 4-4.

Table 4-4. IPX bridging for local servers

Location	Parameter
Ethernet→Connections→*any profile* (Connection Profile)	Route IPX=No Bridge=Yes Dial Brdcast=No
Ethernet→Connections→*any profile*→ IPX options...	NetWare t/o=30

The IPX Frame type must be configured in the Ethernet Profile, and Bridging must be globally enabled, as described in "Globally enabling bridging" on page 4-3.

The Pipeline uses the value specified in the "NetWare t/o" parameter as the time limit for responding to NCP watchdog requests on behalf of clients on the other side of the bridge, a process called "watchdog spoofing."

Note: The Pipeline can perform watchdog spoofing only for the IPX frame type specified in the Ethernet Profile. For example, if IPX Frame=802.3, only connections to servers using that packet frame type will be spoofed.

For details, see Chapter 6, "Configuring the Pipeline as an IPX Router."

Servers on both sides of the connection

If NetWare servers are supported on both sides of the WAN connection, we strongly recommend that you use an IPX routing configuration instead of bridging IPX. If you bridge IPX in that type of environment, client-server logins will be lost when the Pipeline brings down an inactive WAN connection.

Creating and maintaining the bridge table

To forward bridged packets to the right destination network, the Pipeline uses a bridge table that associates end nodes with a particular connection. It builds this table dynamically, as described in the next section. It also incorporates information found in its Bridge Profiles. Bridge Profiles let you explicitly specify up to 8 destination nodes and their connection information.

Transparent bridging

The Pipeline is a transparent bridge (also called a learning bridge). It keeps track of where a particular address is located and the Connection Profile needed to bring up that interface. As it forwards a packet, it notes the packet's source address and creates a bridge table that associates node addresses with a particular interface.

For example, Figure 4-2 shows the physical addresses of some nodes on the local Ethernet and at a remote site. The Pipeline at site A is configured as a bridge.

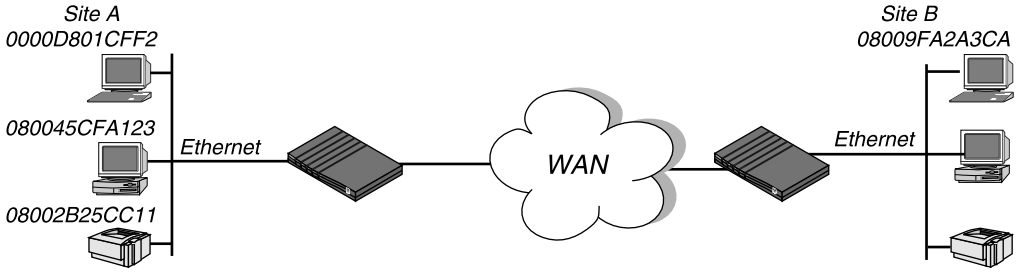


Figure 4-2. How the Pipeline creates a bridging table

The Pipeline at site A gradually "learns" addresses on both networks by looking at each packet's source address, and it develops a bridge table like this:

```
0000D801CFF2      SITEA
080045CFA123      SITEA
08002B25CC11      SITEA
08009FA2A3CA      SITEB (Connection Profile #4)
```

A Connection Profile is associated with a bridging link either because it was used to dial the link or because it matched an incoming call.

Entries in its bridge table must be relearned within a fixed aging time limit; otherwise they are removed from the table.

Static bridge table entries

As administrator of the Pipeline, you can configure up to 8 Bridge Profiles, each of which specifies the physical address of one remote device and the number of the Connection Profile used to establish a connection with that device. See "Setting Bridge Profile parameters" on page 4-16 for details.

When a Connection Profile is listed in a Bridge Profile, you can turn off Dial Brdcast in that Connection Profile. Dial Brdcast is a very convenient way of bridging packets if the Pipeline has only a few bridging connections, but it can be expensive in an environment where many profiles support bridging (see "Broadcast addresses and Dial Brdcast" on page 4-5).

If Dial Brdcast is turned off in a Connection Profile, the Pipeline does not initiate dialing for that connection based on broadcast requests. Instead, it relies on its bridge table to recognize which Connection Profile to use.

Note: If you turn off Dial Brdcast and the Pipeline does not have a bridge table entry for a destination address, the Pipeline will not bring up that connection.

Planning a bridging connection

This section describes how to get the local information you need, and shows how to plan a bridging configuration using PPP encapsulation. See "Configuring a bridging connection" on page 4-13 for a step-by-step example.

In this example, site A wants to set up a Connection Profile that enables a user at site B to open an AppleTalk Remote Access (ARA) connection into the site A network. Both site A and site B support the Challenge Handshake Authentication Protocol and require passwords for entry.

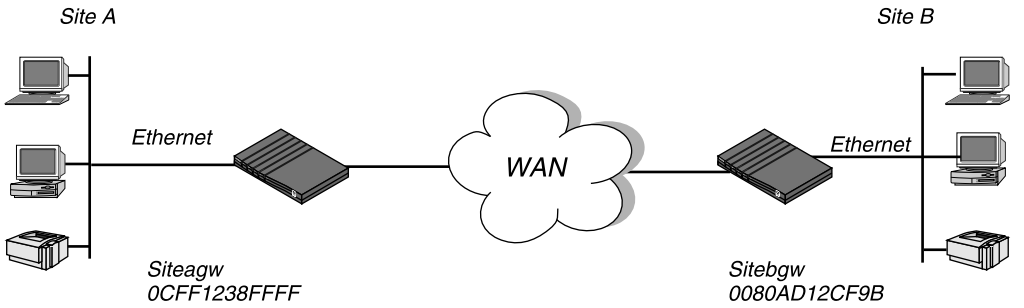


Figure 4-3. An example bridge connection

The site A Pipeline bridging configuration is shown in Table 4-5.

Table 4-5. Bridging configuration for site A

Location	**Parameter**
System→Sys Config (System Profile)	Name=SITEAGW
Ethernet→Connections→20-104 (Connection Profile)	Station=SITEBGW Active=Yes Encaps=PPP (or MPP) Bridge=Yes Dial Brdcast=No
Ethernet→Connections→20-104→ Encaps options...	Send Auth=CHAP (or PAP) Recv PW=*SECURE* (a password) Send PW=*SECURE* (a password)
Ethernet→Bridge Adrs→*any profile* (Bridge Profile)	Enet Adrs=0080AD12CF9B Net Adrs=0.0.0.0 Connection #=4
Ethernet→Answer→PPP options... (Answer Profile)	Bridge=Yes PPP=Yes (or MPP=Yes) Recv Auth=Either (or PAP or CHAP)

Table 4-5. Bridging configuration for site A (continued)

Location	Parameter
Ethernet→Mod Config (Ethernet Profile)	Bridging=Yes

The configuration for the site B unit is shown in Table 4-6

Table 4-6. Bridging configuration for site B

Location	Parameter
System→Sys Config (System Profile)	Name=SITEBGW
Ethernet→Connections→20-102 (Connection Profile)	Station=SITEAGW Active=Yes Encaps=PPP (or MPP) Bridge=Yes Dial Brdcast=No
Ethernet→Connections→20-102→ Encaps options...	Send Auth=CHAP (or PAP) Recv PW=*SECURE* (a password) Send PW=*SECURE* (a password)
Ethernet→Bridge Adrs→*any profile* (Bridge Profile)	Enet Adrs=0CFF1238FFFF Net Adrs=0.0.0.0 Connection #=2
Ethernet→Answer→PPP options... (Answer Profile)	Bridge=Yes PPP=Yes (or MPP=Yes) Recv Auth=Either (or PAP or CHAP)
Ethernet→Mod Config (Ethernet Profile)	Bridging=Yes

Configuring a bridging connection

This section shows how to configure bridging for a Pipeline connecting to a remote site. This example configuration does not show the link-specific settings (such as Telco options, or MP+ configuration), or additional routing settings that may be appropriate at your site. It focuses only on bridging.

Setting Ethernet Profile parameters

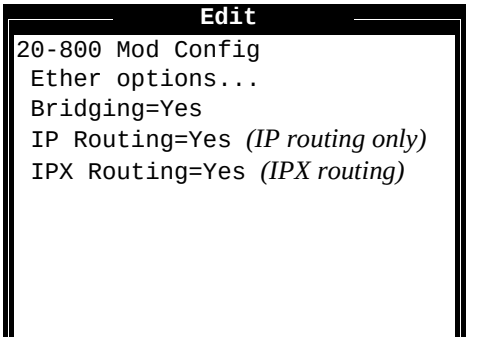
The Ethernet parameters specify information about the local network (on the Ethernet to which the Pipeline is directly connected). These parameters are always required. In effect, they turn on the bridging capability.

To set Ethernet Profile parameters for a bridging connection:

1 Open the Ethernet Profile.

2 Set Bridging=Yes.

See "Globally enabling bridging" on page 4-3 for an explanation of how this parameter turns on the bridging capability.



3 If IPX bridging is required, open the Ether Options submenu and set the IPX Frame type.

4 Exit the Ethernet Profile and save the changes you made.

Setting Answer Profile parameters

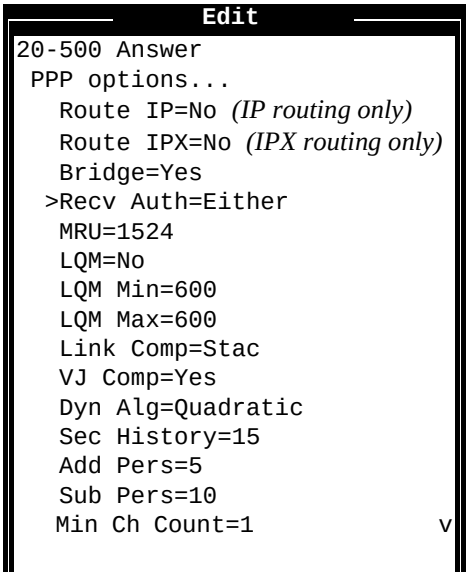
Bridge must be set to Yes in the Answer Profile to enable the Pipeline to bridge packets.

Note: If you are configuring a frame relay IPX connection, these parameters do not apply.

To set Answer Profile parameters for a bridging connection:

1. Open the Answer Profile.
2. Set PPP=Yes (or MPP=Yes).
3. Open the PPP Options submenu.
4. Set Bridge to Yes.

   Bridging must be enabled on both the answering and dialing side of a PPP or MP+ session link; otherwise the link cannot bridge packets. Bridge is set to N/A if the Bridging parameter in the Ethernet Profile has not been set.



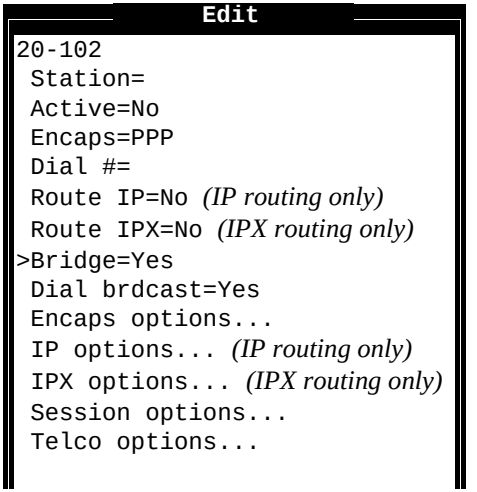
5. Set Recv Auth to Either (or PAP or CHAP). Authentication is required for bridging connections.

6 Exit the Answer Profile and save the changes you made.

Setting Connection Profile parameters

To set Connection Profile parameters for a bridging connection:

1 Open a Connection Profile.



2 Type the name of the answering device in the Station parameter.

The most common cause of trouble when initially setting up a bridging connection is that the wrong name is specified for the Pipeline or the remote device. Often case changes are not specified correctly, or a dash or underscore is entered incorrectly. Make sure you type the name exactly as it appears in the remote device.

3 Set Active to Yes.

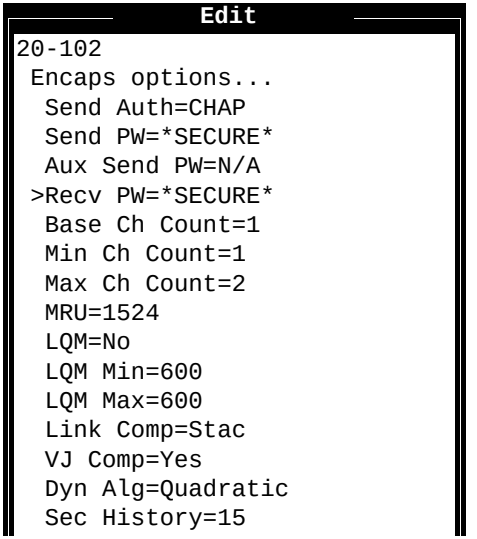
4 Set Encaps to PPP (or MPP).

5 Set Bridge to Yes.

6 For the purposes of this example, set Dial Brdcast to No. In this example, a Bridge Profile will be used to bring up the connection.

See “How a bridging connection is initiated” on page 4-4 if you are not sure about which setting to use.

7 Select Encaps options and press Enter to open this submenu:



8 Set Send Auth to CHAP (or PAP, as appropriate for the connection).

9 Specify the password expected by the remote device in the Send PW parameter.

10 Specify the incoming password in the Recv PW parameter.

11 Exit the Connection Profile, saving the changes you made.

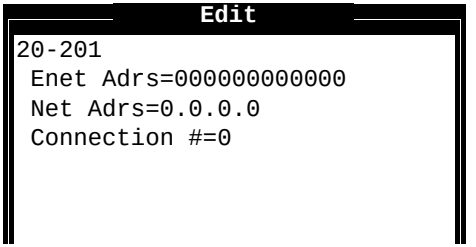
Setting Bridge Profile parameters

In this example, Dial Brdcast is set to No in the Connection Profile, so the Pipeline does not initiate dialing for that connection based on broadcast requests. Instead, it relies on its bridge table to recognize which Connection Profile to use.

Note: If you turn off Dial Brdcast and the Pipeline does not have a bridge table entry for a destination address, the Pipeline will not bring up that connection.

To set Bridge Profile parameters for this connection:

1 Open a Bridge Profile.



2 Type the Ethernet (hardware) address of the answering device in the Enet Adrs parameter, for example:

```
0080AD12CF9B
```

See “Physical addresses and the bridge table” on page 4-4 if you need more details. You must get this address from the administrator of the far-end device.

3 For the purposes of this example, leave the Net Adrs parameter set to zero.

This is an optional parameter that enables the Pipeline to respond to ARP requests for the specified address.

4 Type the last digit of the Connection Profile number used to access this remote device in the Connection # parameter, for example:

```
2
```

5 Exit the Bridge Profile, saving your changes.

Configuring the Pipeline as an IP Router

5

This chapter covers these topics:

Ascend IP router parameters

Table 5-1 shows configuration parameters related to IP routing.

Table 5-1. IP configuration parameters

Location	Parameter with default value
Ethernet→Connections→*any profile* (Connection Profile)	Route IP=No
Ethernet→Connections→*any profile*→ IP options…	LAN Adrs=0.0.0.0 WAN Alias=0.0.0.0 Metric=1 Private=No
Ethernet→Connections→*any profile*→ Session options…	Call Filter=0
Ethernet→Static Rtes→*any profile* (IP Route Profile)	Name= Active=No Dest=0.0.0.0 Gateway=0.0.0.0 Metric=1 Private=Yes
Ethernet→Answer→PPP options…	Route IP=No
Ethernet→Mod Config (Ethernet Profile)	ICMP Redirects=Accept
Ethernet→Mod Config→Ether options…	IP Adrs=0.0.0.0 Ignore Def Rte=No Proxy Mode=Off

For details on each parameter, see Chapter 11, “Reference.”

Overview of IP routing

The Pipeline implements these protocols in the TCP/IP suite:

- IP (Internet Protocol)
- TCP (Transmission Control Protocol)
- UDP (User Datagram Protocol)
- ICMP (Internet Control Message Protocol)
- ARP (Address Resolution Protocol)

The Pipeline supports TCP/IP over any type of WAN connection, and is fully interoperable with non-Ascend products that support TCP/IP.

Note: This chapter does not explain basic TCP/IP concepts. It assumes that you have an existing IP network and a domain name.

When to use IP routing

Use IP routing in the Pipeline to connect two sites that both have an IP address. The most common uses for IP routing in the Pipeline are:

- To enable many independent connections to the Internet (Internet Service Providers)
- To integrate multiple IP subnets that are geographically distributed (telecommuting hubs)

The Pipeline can be configured as a bridge, a router, or both. However, you cannot both bridge and route TCP/IP packets across the same connection. When you configure the Pipeline as an IP router, IP packets are no longer bridged at the link layer. They are *always* routed at the network layer. All other protocols continue to be bridged unless you turn off bridging.

See Chapter 4, “Configuring the Pipeline as a Bridge,” for more information about bridging.

How an IP routing connection is initiated

The Pipeline handles dial-in and dial-out aspects of WAN connections, and routes packets between networks. At the appropriate point in a session negotiation, the Pipeline begins passing packets to its bridging/routing software. The bridging/routing module in the Pipeline then operates as a regular IP router, with two interfaces on two different networks or subnets.

An IP routing connection can be network-to-network or host-to-network.

Typically, a network-to-network connection is initiated when a user starts up a TCP/IP application, such as a World-Wide Web browser or Telnet, and enters a URL, hostname, or IP address that is not on the local network. This creates an outbound IP packet (a packet whose destination address is not on that network). The calling device places the call and the answering device picks it up. If the session is negotiated successfully, the IP packet is passed to the bridging/routing software and routed appropriately.

A host-to-network connection is usually initiated by a user starting up PPP and calling the Pipeline . The calling host may be connected to a modem or wireless communication device.

Enabling IP routing in the Pipeline

For the Pipeline to operate as an IP router across the WAN, the Pipeline must have its own IP address on the local Ethernet and IP routing must be enabled in the Answer Profile as well as the Connection Profile for a particular destination.

In the Answer Profile, Route IP must be set to Yes to enable the Pipeline to negotiate a session based on the IP address of the caller. In a Connection Profile, the Route IP parameter is used as described in “Setting an IP address for a far-end device” on page 5-7.

Table 5-2. Parameters required to enable IP routing

Location	Parameters
Ethernet→Connections→*any profile* (Connection Profile)	Route IP=Yes

Table 5-2. Parameters required to enable IP routing (continued)

Location	Parameters
Ethernet→Answer→PPP options… (Answer Profile)	Route IP=Yes
Ethernet→Mod Config→Ether options… (Ethernet Profile)	IP Adrs=10.2.3.1

Host requirements

IP hosts, such as UNIX systems, Windows or OS/2 PCs, or Macintosh systems, must have appropriately configured TCP/IP software. A remote host calling into the local IP network must also have PPP software.

UNIX systems typically include a TCP/IP stack, DNS software, and other software, files, and utilities used for Internet communication. UNIX network administration documentation describes how to configure these programs and files.

PCs running Windows or OS/2 need the TCP/IP networking software or "stack." The stack is included with Windows 95, but the user may need to purchase and install it separately if the computer has a previous version of Windows or OS/2.

Macintosh computers need MacTCP or Open Transport software for TCP/IP connectivity. MacTCP is included with all Apple system software including and after Version 7.1. To see if a Macintosh has the software, the user should open the Control Panels folder and look for MacTCP or MacTCP Admin.

For any platform, the TCP/IP software must be configured with the host's IP address, subnet mask, and default gateway (that is, of the Pipeline). If a DNS server is supported on your local network, you should also configure the host software with the DNS server's address.

Configuring IP addresses

You must configure the IP address of a remote device the Pipeline connects to using a Connection Profile. An IP address in a Connection Profile is permanent and is always associated with the same device.

Ascend format for IP addresses

In Ascend units, IP addresses must be specified in decimal (not hexadecimal) format, and can include a netmask modifier in Ascend format, such as:

```
198.5.248.40/30
```

where /30 specifies the number of bits to be interpreted as the network portion of the IP address. The number must be greater than the default netmask shown in Table 5-3. If no netmask is specified in an IP address, the following default netmasks are assumed:

Table 5-3. IP address classes and default netmasks

Class	Address range	Netmask bits
Class A	0.0.0.0 → 127.255.255.255	8
Class B	128.0.0.0 → 191.255.255.255	16
Class C	192.0.0.0 → 223.255.255.255	24
Class D	224.0.0.0 → 239.255.255.255	N/A
Class E (reserved)	240.0.0.0 → 247.255.255.255	N/A

The example address is a class C address, so the default netmask is 24 bits. If the address ends with a subnet specification, such as this:

```
198.5.248.40/30
```

the /30 specification indicates that an additional 6 bits of the address will be interpreted as a subnet number. That is, the first 24 bits of the address are interpreted as the IP network number (standard for Class C), the next 6 bits are

the subnet number, and only 2 bits are available for host number assignment. A 2-bit host portion allows only four hosts on that subnet.

Note: If the Pipeline is connected to a local subnet and will connect to a remote subnet of the *same* IP network, both sides of the connection must use the same subnet mask.

Setting the Pipeline IP address on Ethernet

The host address of the Pipeline on its Ethernet interface must be both unique and consistent with other addresses on the same IP network. To assign the Pipeline an IP address on your local Ethernet, open the Ether Options submenu of the Ethernet Profile.

Table 5-4. Pipeline IP address on Ethernet

Location	Parameter
Ethernet→Mod Config→Ether options… (Ethernet Profile)	IP Adrs=10.2.3.1/22

After you have configured the IP address, you can ping the Pipeline from a local host to verify that it is up and running on the network.

Setting an IP address for a far-end device

The IP address of a far-end device, whether it is a router or a host, is specified in the Connection Profile for that connection. The address of the remote device may be one of the following:

- On a separate, unique IP network

  If the far end is a router (which may be an Ascend unit or similar calling device), you must specify the router's IP address. If the far-end router's address includes a subnet mask, you must specify that as well, or the entire far-end network is assumed to be accessible.

  If the far end is a host, you must specify a host route. A host route is an IP address with a subnet mask of /32. An IP address followed by a /32 netmask specification is called a "host route." Host routes are used for a host-to-net-

work connection where the remote host has an IP address on a separate network but there is no IP router at the far end.

- On a subnet of the local IP network

  If the far end will be a subnet of the local IP network, you must specify the IP address of the remote router (which may be an Ascend unit or similar calling device) on that subnet. If the Pipeline is also on a subnet, both sides of the connection must use the same subnet mask.

- On the local IP network

  If the far end is a host, such as a PC with PPP software, you can specify an IP address on the local network.

For example, Figure 5-1 shows site A (the Pipeline) and site B as two separate IP networks.

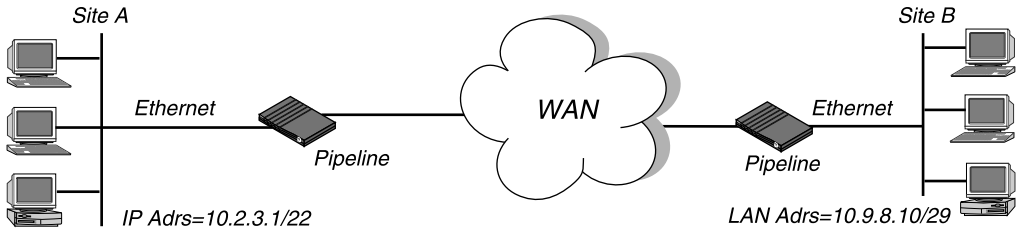


Figure 5-1. Connection to a separate IP network

In this example connection, when site B initiates a connection, the Pipeline answers the call and looks for the caller's Connection Profile. If the Pipeline finds the caller's Connection Profile and it has a non-zero IP address, it compares that address to the one offered by the caller. If the addresses are the same, the connection is established; otherwise, the Pipeline hangs up.

Table 5-5. IP parameters in a Connection Profile

Location	**Parameter**
Ethernet→Connections→*any profile* (Connection Profile)	Route IP=Yes
Ethernet→Connections→*any profile*→ IP options…	LAN Adrs=10.9.8.10/29

If the Pipeline does not find the caller's Connection Profile and a profile is not required (if Profile Reqd=No in the Answer Profile), it checks that Route IP=Yes in the Answer Profile and uses the IP address offered by the caller in the PPP negotiation. If Profile Reqd=Yes in the Answer Profile and the Connection Profile is not found, the Pipeline hangs up.

A similar session negotiation occurs in the other direction if a local device at site A initiates a connection to site B.

Creating and maintaining the IP routing table

When Route IP is enabled, the Pipeline creates a routing table during initialization.

Each entry in the routing table specifies at least two pieces of information: a destination network address, and the router used to forward a packet toward that destination. The routing table contains entries that you have configured using either Connection Profiles or Static Rtes Profiles (static routes). See "Static routes" on page 5-12 for information about static routes.

When a packet's destination is not on the local IP network, the Pipeline scans its routing table to determine where to forward the packet. If two possible routes exist for forwarding the outbound packet, the Pipeline uses the route with the lower metric. If no routes exist, it forwards the packet to the default route (see "The default route" on page 5-13).

For applications such as Telnet and Ping, which require that packets be transmitted in both directions, both the calling and answering devices must have appropriate routes.

Dialing non-Ascend routers

When the Pipeline answers a PPP call, it examines the IP source address, assumes the source is a router, and builds a temporary route back to the source network. Since the source subnet mask is not given, the Pipeline assumes the network address is class A, B, or C, based on the source IP address. If you have dialed a non-Ascend router that does not build this initial temporary route, you may have to use static routes to build a route back.

Dynamic IP routing

The Pipeline uses these TCP/IP routing protocols to build its routing table:

- ICMP, which can dynamically redirect packets to a more efficient route, and
- ARP, which enables the Pipeline to respond to address queries with its own physical address ("proxy ARP").

RIP

Some networks use Routing Information Protocol (RIP) is on the Ethernet interface if other routers (such as a Cisco router or a UNIX system running the route daemon) are connected to the local IP network. Many sites turn off RIP on the WAN interface, because it tends to cause very large local routing tables.

The Pipeline does not use RIP to build its routing table.

These are the parameters that affect how the Pipeline uses RIP:

Table 5-6. RIP parameters

Location	Parameter
Ethernet→Connections→*any profile*→ IP options… (Connection Profile)	Private=N/A
Ethernet→Mod Config→Ether options…	Ignore Def Rte=Yes

For details on each of these parameters, see Chapter 11, "Reference."

ICMP Redirects

ICMP dynamically determines the best route to a destination network or host and can use ICMP Redirect packets to redirect packets to a more efficient route. You should accept ICMP redirects only when the Pipeline has a single default route to another device because the possibility of receiving counterfeit ICMP Redirects poses a security threat. The following parameter affects ICMP Redirect packets:

Table 5-7. ICMP Redirects

Location	Parameter
Ethernet→Mod Config (Ethernet Profile)	ICMP Redirects=Ignore

ARP and proxy ARP

ARP (Address Resolution Protocol) broadcasts requests for a MAC address associated with a known IP address. It works like this:

- A user on an IP host FTPs to another host by name (for example).
- The host software obtains the IP address for that hostname via DNS.
- The FTP software asks the TCP/IP software to establish a connection to that address.
- If the IP address is on the local IP network, the host software broadcasts ARP requests to every host on the Ethernet, saying: "If you are the owner of this IP address, please reply with your physical address." IP packets are then sent directly to the responding host.

If the IP address is *not* on the local network, the host software doesn't ARP. Typically, the host software is configured with the IP address of the Pipeline as its default router, and packets destined for remote networks are always forwarded to the default router.

However, in host-to-network connections where the remote host is assigned an IP address on the local network, local TCP/IP software sees the IP address as local and sends out ARP requests. In those cases, the Pipeline can use Proxy Mode to respond with its own MAC address for non-local IP addresses.

A remote host can be assigned an IP address on the local network through the Connection Profile used to reach the remote host. In this case, the Pipeline knows that it must route packets destined for the remote host across the WAN, but local hosts see the IP address as local.

In this situation, set Proxy Mode=Always.

You can disable Proxy Mode by setting it to Off in the Ether Options submenu of the Ethernet Profile.

Table 5-8. Proxy ARP

Location	Parameter
Ethernet→Mod Config→Ether options… (Ethernet Profile)	Proxy Mode=Off

Static routes

The Pipeline relies on static routes to reach a destination. These static routes can be created using Static Route Profiles or Connection Profiles.

Static Route Profiles

Table 5-9 shows the parameters contained in a static route and example values.

Table 5-9. Static route parameters

Location	Parameter
Ethernet→Static Rtes→*any profile* (IP Route Profile)	Name=*profile-name* Active=Yes Dest=10.210.1.30/12 Gateway=10.9.8.10 Metric=2 Private=No

This example IP Route Profile states that the path to the destination subnet is through the IP router at 10.9.8.10. Provided that the Pipeline has a Connection Profile for 10.210.1.30 (so it can bring up that connection), it will route packets addressed to that subnet to the device at the far end of that connection.

When the Dest parameter has a subnet specification, the remote router is seen as a gateway to that subnet, rather than to a whole remote network. To specify the entire remote network, you would use a network address such as this:

```
Dest=10.0.0.0
```

The default route

If no routes exist for the destination address of a packet, the Pipeline forwards the packet to the default route. If the Pipeline is

If the first Static Rte Profile is configured, that is the default route. The name of that profile is always Default, and its destination is always 0.0.0.0 (you cannot change these values). If the first Static Rte Profile is *not* configured, the Pipeline has no default route.

Note that if you are using the Pipeline to connect a single host to a central LAN or an ISP, you can use the default route to specify the IP address of the remote device.

Some sites use the default route to specify a local IP router (such as a Cisco router or a UNIX host running the route daemon). For example, this profile specifies a local router at 10.2.3.12:

Table 5-10. Default route parameters

Location	Parameter
Ethernet→Static Rtes→*first profile*	Name=Default Active=Yes Dest=0.0.0.0 Gateway=10.2.3.12 Metric=1 Private=Yes

How Connection Profiles work as static routes

Each Connection Profile defines a static route. For example, in the network diagram shown in Figure 5-2, the Connection Profile itself is a static route to the subnet specified in the LAN Adrs parameter (10.9.8.10/22). With this LAN Adrs parameter, the implied static route is defined with these addresses:

- Dest=10.9.8.10/22
- Gateway=10.9.8.10

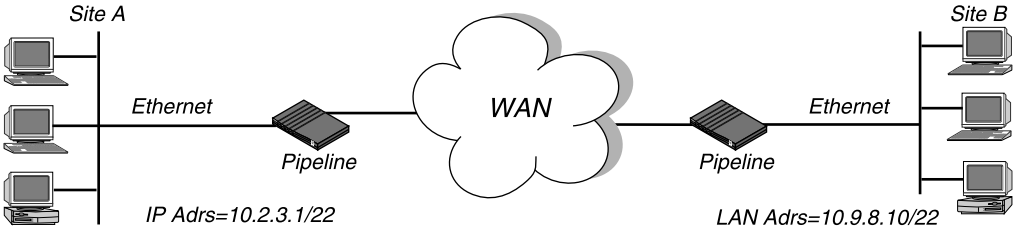


Figure 5-2. A connection serving as a static route

How Connection Profiles and Static Rte Profiles work together

If the Pipeline is connected to a device on the remote LAN (such as a Pipeline 50) that has disabled RIP, the local Pipeline must rely on a static route to route to other networks through that connection. Figure 5-3 shows an example network diagram.

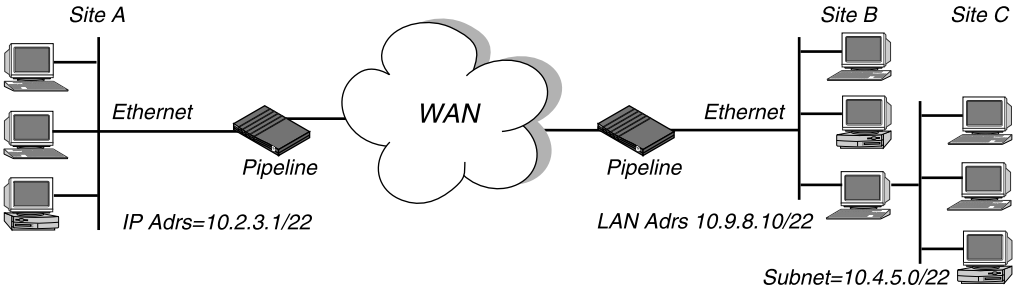


Figure 5-3. Static route required to reach other networks

In the example network shown in Figure 5-3, if RIP is turned off for site B, the Pipeline must have the Static Rte Profile shown below to route to site C:

Table 5-11. Static route to site C

Location	Parameter
Ethernet→Static Rtes→*any profile*	Name=sitec-net Active=Yes Dest=10.4.5.6/22 Gateway=10.9.8.10 Metric=2 Private=Yes

Interface-based routing

The Pipeline implements what is referred to as system-based or box-based routing. With system-based routing, the entire box is addressed with a single IP address. For systems that have a single backbone connection, system-based routing is by far the simplest form of routing from both a configuration and trouble-shooting perspective. The alternative form of routing is referred to as interface-based routing. With interface-based routing, each physical or logical interface on the box has its own IP address.

However, there are some applications that the Pipeline is used for in which it might be useful to "number" some of the interfaces— in other words, to have the Pipeline operate as a partially system-based router and partially interface-based router. Reasons for using numbered interfaces include troubleshooting leased point-to-point connections and forcing routing decisions between two links going to the same final destination. More generally, interface-based routing allows the Ascend product to operate more nearly the way a multi-homed Internet host behaves, should that be desired.

This feature allows the user to configure each link as "numbered" (interface-based) or "unnumbered" (system-based). If no interfaces are specified as numbered, then the box will operate exactly as has previously. Interface numbering is accomplished via the Connection profile.

System behavior with a numbered interface

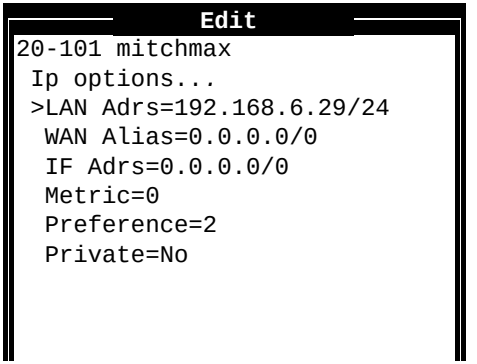
If a Pipeline is using a numbered interface, the following differences in operation should be noted, compared to unnumbered (system-based) routing:

- IP packets generated in the Pipeline and sent to the remote address will have an IP source address corresponding to the numbered interface, not to the default (Ethernet) address of the Pipeline.
- During authentication of a call placed from a Pipeline using a numbered interface, the Pipeline will report the address of the interface as its IP address.
- The Pipeline will add to its routing table host routes all numbered interfaces listed in Connection Profiles.
- The Pipeline will accept IP packets whose destination is a numbered interface listed in a Connection profile, considering them to be destined for the Pipeline itself. (The packet may actually arrive over any interface, and the numbered interface corresponding to the packet's destination address need not be in the active state.)

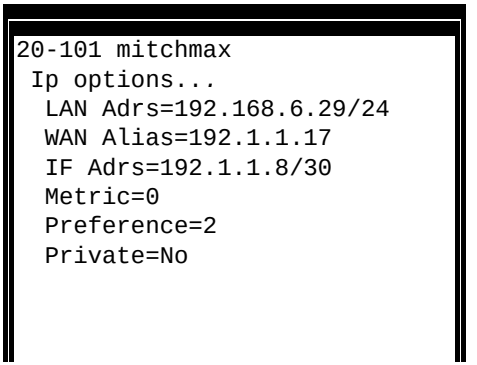
Using the IF Adrs parameter

Configuration of a numbered link takes place in a Connection profile, under the IP Options submenu. You use the IF Adrs to specify the IP address of the interface. If the field is left at its default value (0.0.0.0/0), then the interface will be treated as unnumbered.

The screen below shows a typical screen for an unnumbered interface. The new IF Adrs field is not used for an unnumbered interface.



The screen below shows settings for a numbered interface. The WAN Alias parameters has been filled in with the address of the remote end of the link, and the new IF Adrs parameter contains the number of the interface at the near end of the link.



Specifying the remote interface address

This section provides some guidelines on using interface-based routing.

If both the system and interface addresses are known

If interface-based routing is being added to a system which has already been set up using system-based routing, the easiest way to specify the remote interface address is by using the WAN Alias parameter in the Connection profile. WAN Alias is used to identify the remote end of the link. If a WAN Alias is set, the following will take place:

- Host routes will be created to both the Lan Adrs and the WAN Alias; the WAN Alias will be listed in the routing table as a gateway (next hop) to the Lan Adrs.
- A route will be created to the remote system's subnet, showing the WAN Alias as the next hop.
- Incoming PPP/MPP calls must report their IP addresses as the WAN Alias (rather than the Lan Adrs). That is, the caller must be using a numbered interface, and its interface address must agree with the WAN Alias on the receiving side.

If you want to create static routes to hosts at the remote end, you can use the WAN Alias address as the “next hop” (gateway) field. (The Lan Adrs address will also work, as would be used for system-based routing.)

If only the interface address is known

It is also permissible to omit the remote side’s system address from the profile and use interface-based routing exclusively. This is an appropriate mechanism if, for example, the remote system is on a backbone net which may be periodically reconfigured by its administrators, and you want to refer to the remote system only by its mutually agreed-upon interface address.

In this case, the remote interface address is entered in the Lan Adrs parameter, and the WAN Alias is left as default (0.0.0.0). Note that Lan Adrs must always be filled in, so if the only known address is the interface address, it must be placed in the Lan Adrs parameter rather than the WAN Alias parameter.

If the remote interface address is placed in the Lan Adrs parameter, the following will take place:

- A host route will be created to the Lan Adrs (interface) address.
- A net route will be created to the subnet of the remote interface.

- Incoming PPP/MPP calls must report their IP addresses as the Lan Adrs (interface) address.

If the remote interface address is not specified

If interface-based routing is in use and the local interface is numbered, the remote address will usually be known (in practice, the subnet must be agreed upon by administrators of both sites.) It is possible, but not recommended, to number the local interface, omitting the interface address of the remote site and using only its system or LAN address. In that case, do not use the (supposedly unknown) remote interface address in any static routes.

The fallback behavior when a local interface is numbered but no corresponding remote interface address is set, is the following:

- The remote interface must have an address on the same subnet as the local, numbered interface. Incoming PPP will be rejected if the Connection Profile numbers the local interface and the (remote) caller supplies an address not on the same subnet.

Planning an IP routing configuration

This section shows how to plan two different kinds of IP configuration. See “Configuring an IP routing connection” on page 5-21 for a step-by-step example.

Note: The most common cause of trouble in initially establishing an IP connection is incorrect configuration of the IP address or subnet specification for the remote host or calling device.

An example network-to-network connection

In this example, the Pipeline connects its local network to another remote IP network. Figure 5-4 shows an example network diagram.

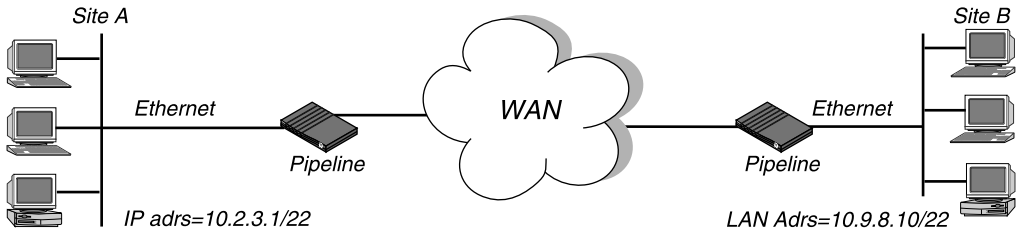


Figure 5-4. Network-to-network connection

The site A Pipeline configuration is shown in Table 5-12. (All other IP parameters use the default values.)

Table 5-12. IP configuration for site A

Location	Parameter
Ethernet→Connections→SITEB (Connection Profile)	Route IP=Yes
Ethernet→Connections→SITEB→ IP options…	LAN Adrs=10.9.8.10/22
Ethernet→Answer→PPP options… (Answer Profile)	Route IP=Yes
Ethernet→Mod Config→ Ether options… (Ethernet Profile)	IP Adrs=10.2.3.1/22

The site B Ascend unit configuration is shown in Table 5-13. (All other IP parameters can use the default values.)

Table 5-13. IP configuration for site B

Location	Parameter
Ethernet→Connections→SITEA (Connection Profile)	Route IP=Yes

Table 5-13. IP configuration for site B (continued)

Location	Parameter
Ethernet→Connections→SITEA→ IP options…	LAN Adrs=10.2.3.1/22
Ethernet→Answer→PPP options… (Answer Profile)	Route IP=Yes
Ethernet→Mod Config→Ether options… (Ethernet Profile)	IP Adrs=10.9.8.10/22

Configuring an IP routing connection

This section shows how to configure an IP routing connection.

This example configuration does not show the link-specific settings, such as Telco options or MP+ configuration, or additional bridging and IP settings that may be appropriate at your site. It focuses only on IP routing.

Note: The example shows a network-to-network connection with static addressing. Some settings would be different for another type of connection, addressing, or routing.

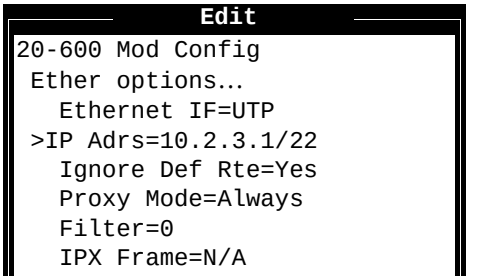
Setting Ethernet Profile parameters

The Ethernet parameters specify information about the local IP network (on the Ethernet to which the Pipeline is directly connected). These parameters are always required. In effect, they turn on the IP routing capability.

To set Ethernet Profile parameters for an IP routing connection:

1 Open the Ethernet Profile.

2 Open the Ether Options submenu.



3 Set IP Adrs to a valid host address on the local Ethernet IP net.

4 Set Ignore Def Rte to Yes (recommended).

5 Set Proxy Mode to Always (recommended).

6 Exit the Ethernet Profile and save the changes you made.

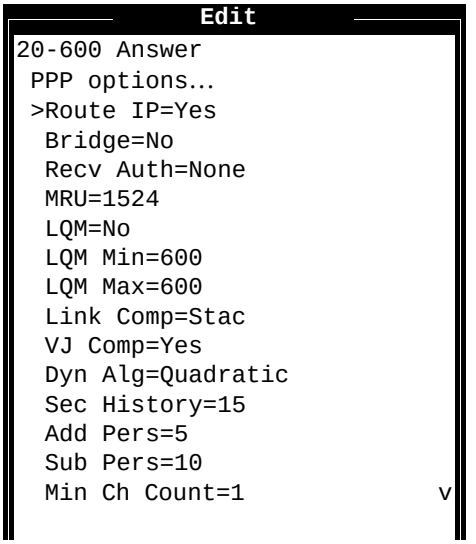
Setting Answer Profile parameters

Route IP must be set to Yes in the Answer Profile to enable the Pipeline to negotiate a session using the IP address of a caller.

To set Answer Profile parameters for an IP routing connection:

1 Open the Answer Profile.

2 Open the PPP Options submenu.



3 Set Route IP to Yes.

4 Exit the Answer Profile and save the changes you made.

Setting Connection Profile parameters

IP configuration in a Connection Profile is fairly simple. Most of the IP options have default values that work for many sites, and there is a predefined “IP Call” filter that keeps inbound data packets from resetting the Idle Timer.

To set Connection Profile parameters for an IP routing connection:

1 Open a Connection Profile.

2 Set Route IP=Yes.

```
Edit
20-104
 Station=brian-gw
 Active=Yes
 Encaps=MPP
 Dial #=1-510-555-1212
>Route IP=Yes
 Bridge=No
 Dial brdcast=N/A
 Encaps options...
 IP options...
 Session options...
 Telco options...
```

3 Open the IP Options submenu.

4 Specify the IP address (including the netmask, if needed) of the remote device in the LAN Adrs parameter.

```
Edit
20-104 brian-gw
 IP options...
 >LAN Adrs=10.9.8.10/22
  WAN Alias=0.0.0.0
  Metric=2
  Private=No
```

5 Leave WAN Alias set to zero, unless it is required by the far-end router.

If the far-end router is an Ascend unit, this parameter is not required. See WAN Alias in Chapter 11, “Reference,” for details.

6 Set Metric to the appropriate number of hops between the local and remote networks.

7 Exit the Connection Profile, saving the changes you made.

BOOTP Relay

The Bootstrap Protocol (BOOTP) defines how a computer on a TCP/IP network can get from another computer its Internet Protocol (IP) address and other information it needs to start up. The computer that requests startup information is called the BOOTP client, and the computer that supplies the startup information is called the BOOTP server. A request for startup information sent from a BOOTP client to a BOOTP server is called a BOOTP request, and the BOOTP server's response is called a BOOTP reply.

When the BOOTP client and BOOTP server are not on the same local-area network, the BOOTP request must be relayed from one network to another. This task, known as BOOTP relay, can be performed by a Pipeline.

A device that relays BOOTP requests to another network is known as a BOOTP relay agent. In addition to delivering BOOTP requests to servers, a BOOTP relay agent is responsible for delivering BOOTP replies to clients. In most cases, the agent is a router that connects the networks, such as a Pipeline.

Using BOOTP relay

By default, a Pipeline does not relay BOOTP requests to other networks. To enable the BOOTP relay feature for BOOTP clients connected to your Pipeline, follow these steps:

1 Get the IP addresses the BOOTP server or servers to be used.
You can specify up to two BOOTP servers, as described later in this section.

2 Open the configuration windows if they are not already open.

3 Open the Ethernet-->Mod Config menu.
For the location of this menu, see the manual for your Pipeline.

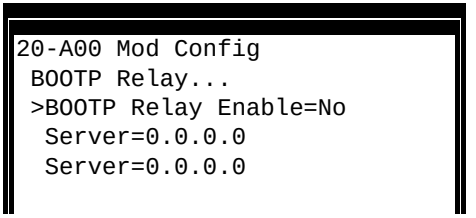
4 Make sure DHCP Spoofing is disabled by following these steps:

- Move the marker to DHCP Spoofing and then press the Return key.
  The DHCP Spoofing menu appears.
- Move the marker to DHCP Spoofing if it isn't already there.
- If the value of DHCP Spoofing is Yes, press the Return key to change it to No.

DHCP Spoofing makes it possible to use the Dynamic Host Configuration Protocol (DHCP), another protocol for getting startup information from a server. You can use only one protocol for getting startup information. If both DHCP Spoofing and BOOTP relay are enabled, you will receive an error message.

5 Move the marker to BOOTP Relay and then press the Return key.

The BOOTP Relay menu appears.



6 Move the marker to BOOTP Relay Enable.

7 Press the Return key repeatedly until the value Yes appears.

8 Move the marker to the first menu item named Server and then press the Return key.

9 In the text box that appears, enter the IP address of a BOOTP server.

10 Press Return to close the text box.

11 If there is another BOOTP server available, move the marker to the second menu item named Server and then press the Return key.

You are not required to specify a second BOOTP server.

Note: 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.

12 In the text box that appears, enter the IP address of the second BOOTP server.

13 Press Return to close the text box.

TCP/IP-related commands

The Pipeline terminal server interface supports a number of administrative commands for viewing information about TCP/IP/UDP. For details about these commands and related configurations, see Chapter 10, “Using the Command Mode.”

The Pipeline can be configured or managed from a remote location if both ends of the connection are using MPP encapsulation. A network manager at one location can create a remote session and perform all of the configuration, diagnostic, management, and other functions that could be performed from a locally attached computer.

Configuring the Pipeline as an IPX Router

6

This chapter covers these topics:

Ascend IPX router parameters

Table 6-1 shows configuration parameters related to IPX routing

Note: You must select an IPX Frame type (in the Configure Profile or in the Ethernet, Mod Config, Ether Options submenu before you can set any of the IPX parameters.

Table 6-1. IPX configuration parameters

Location	Parameter with default value
System→Sys Config (System Profile)	Name=[]
Ethernet→Connections→*any profile* (Connection Profile)	Station=[] Route IPX=No
Ethernet→Connections→*any profile*→ Encaps options...	Recv PW=None Send PW=None Send Auth=None
Ethernet→Connections→*any profile*→ IPX options...	Peer=Router Dial Query=No IPX Net#=00000000 IPX Alias#=00000000 Netware t/o=30
Ethernet→Connections→*any profile*→ Sessions options…	IPX SAP Filter=0
Ethernet→Answer→PPP options... (Answer Profile)	Route IPX=No Recv Auth=None
Ethernet→Answer→Sessions options...	IPX SAP Filter=0

Table 6-1. IPX configuration parameters (continued)

Location	Parameter with default value
Ethernet→IPX Routes→*any profile* (IPX Route Profile)	Server Name=[] Active=No Network=00000000 Node=000000000001 Socket=0000 Server Type=0000 Hop Count=2 Tick Count=12 Connection #=0
Ethernet→IPX SAP Filters→*any profile* (IPX SAP Filter Profile)	Name=[] Input filters... Output filters...
Ethernet→IPX SAP Filters→*any profile*→ Input filters→01 to 12 Ethernet→IPX SAP Filters→*any profile*→ Output filters→01 to 12	Valid=No Type=Exclude Server Type=0 Server Name=[]
Ethernet→Mod Config (Ethernet Profile)	IPX Routing=Yes
Ethernet→Mod Config→Ether options...	IPX Frame=None IPX Enet #=N/A IPX Pool #=N/A IPX SAP Filter=0

For detailed descriptions of each parameter, see Chapter 11, “Reference.” See also “Ascend extensions to standard IPX” on page 6-5.

Note: The Station parameter and authentication parameters (Recv PW, Send PW, Send Auth, and Recv Auth) are not used in establishing a connection if IP routing is also configured for that connection (see “Deciding on authentication for IPX incoming calls” on page 6-14).

For information about packet filters for IPX connections, see Chapter 8, "Using Filters."

Introduction to Ascend IPX routing

Ascend IPX routing works with Novell NetWare version 3.11 or newer.

The Pipeline (and Ascend Pipeline products) supports IPX routing over PPP and MP+. Support for both the IPXWAN and PPP IPXCP protocols make the Pipeline fully interoperable with non-Ascend products that conform to these protocols and associated RFCs. IPX routing can be configured along with protocol-independent bridging and IP routing in any combination.

Note: This chapter does not explain basic IPX concepts. It assumes that you are adding the Pipeline to an existing Novell LAN. If you are not familiar with NetWare or IPX routing, we recommend that you read the applicable Novell documentation.

When to use Ascend IPX routing

Use Ascend IPX routing to connect a local Novell LAN to another site that supports NetWare. The most common uses are:

- To allow geographically remote NetWare clients to access your local NetWare servers. See "Planning a connection with servers on one side of the link only" on page 6-14.
- To integrate your local NetWare servers and clients with remote sites to form an interconnected wide-area network.

  See "Planning a connection with servers on both sides of the link" on page 6-17.

Note: You may choose to bridge IPX packets at the link level instead (see Chapter 4, "Configuring the Pipeline as a Bridge," for more information).

Standard IPX routing using RIP

All IPX routers periodically broadcast IPX RIP (Routing Information Protocol) packets that inform other routers about available networks. IPX RIP is similar to the routing information protocol in the TCP/IP protocol suite, but it is a different protocol. (In this chapter, RIP always refers to IPX RIP.)

Most IPX routers, including the bridge/router module in the Pipeline, use RIP broadcasts to create and update their internal routing table. When an IPX router receives an IPX packet, it consults its routing table to see where to forward the packet. In the Pipeline, the routing table affects which connection(s) are brought up.

The Pipeline recognizes network number –2 (0xFFFFFFFE) as the IPX RIP default route and uses that route appropriately. When it receives a packet for an unknown destination, it forwards the packet to the IPX router advertising the default route. If more than one IPX router is advertising the default route, a routing decision is made based on Hop and Tick count.

For example, if the Pipeline receives an IPX packet destined for network 77777777 and it does not have a routing table entry for that destination, the Pipeline forwards the packet towards network number FFFFFFFE, if available, instead of simply dropping the packet.

Because entries in a routing table age and expire when updates are not renewed frequently enough (for example, if a connection has not been up for a while), the Ascend extensions are also necessary for reliable IPX routing.

Ascend extensions to standard IPX

NetWare uses dynamic routing and service location, so clients expect to be able to locate a server dynamically, regardless of where it is physically located. This scheme was not designed for WAN operations, and Ascend provides these extensions to standard IPX for enhancing WAN functionality:

- IPX Route Profiles
- Dial Query
- Watchdog spoofing

IPX Route Profiles

An IPX Route Profile adds one remote NetWare server to the routing table. Each profile contains all of the information needed to reach one server. When an outbound packet is received for a remote server, the Pipeline consults its routing table to forward the packet. If there is no active session to the server's network, the Pipeline locates the appropriate Connection Profile, and dials the connection.

To configure an IPX Route Profile, open a profile below the IPX Routes menu (See "Configuring an IPX Route Profile" on page 6-25 for details). Table 6-2 shows the parameters associated with the IPX Route Profile.

Table 6-2. IPX Route Profile

Location	Parameter
Ethernet→IPX Routes→*any profile* (IPX Route Profile)	Server Name=*server-name* Active=Yes Network=CC1234FF Node=000000000001 Socket=0000 Server Type=0004 Hop Count=2 Tick Count=12 Connection #=0

Using IPX Route Profiles when there are servers on both sides of the WAN helps to limit the number of unwanted connections. Once you have specified an IPX Route Profile, the routing table is not empty, so Dial Query is canceled.

Dial Query

Dial Query in a Connection Profile instructs the Pipeline to bring up that connection when a NetWare client on the local network queries for a server and the Pipeline unit's routing table is empty. To enable Dial Query, set Dial Query=Yes in the IPX Options submenu of a Connection Profile.

Table 6-3. Dial Query parameter

Location	Parameter
Ethernet→Connections→*any profile*→ IPX options... (Connection Profile)	Dial Query=Yes

Note: If there are any servers in the Pipeline unit's routing table, either from an IPX Route Profile or dynamic routes (RIP), Dial Query has no effect.

Watchdog spoofing

NetWare servers send out NCP watchdog packets to monitor client connections. Clients that respond to watchdog packets remain logged into the server. If a client does not respond for a certain amount of time, the server logs the client out.

Repeated watchdog packets would cause a WAN connection to stay up, but if the Pipeline simply filtered those packets, client logins would be dropped by the remote server. To prevent repeated client logouts while allowing WAN connections to be brought down in times of inactivity, the Pipeline responds to NCP watchdog requests as a proxy for clients on the other side of an offline IPX routing or IPX bridging connection. Responding to these requests is commonly called watchdog spoofing. To the server, a spoofed connection looks like a normal, active client login session.

The "NetWare t/o=" parameter in the IPX Options submenu of a Connection Profile determines how long the Pipeline performs watchdog spoofing after a WAN connection has been brought down. Its default value is 30 minutes.

Table 6-4. Netware t/o parameter

Location	Parameter
Ethernet→Connections→*any profile*→ IPX options... (Connection Profile)	Netware t/o=30

The timer begins counting down as soon as the link goes down. At the end of the selected time, the client-server connections may be released by the server. If there is a reconnection of the WAN session before the end of the selected time, the timer is reset.

Dial-in NetWare clients

The Pipeline allows individual NetWare clients that are not connected to an Ethernet to dial in and be assigned to an IPX network. The client must be running PPP client software to connect to an IPX network through the Pipeline.

Support for this feature uses these two parameters:

Table 6-5. IPX for dial-in clients

Location	Parameter
Ethernet→Connections→*any profile*→ IPX options... (Connection Profile)	Peer=Dialin
Ethernet→Mod Config→Ether options... (Ethernet Profile)	IPX Pool #=CFCF1234

In the Connection Profile for the incoming call, set the Peer parameter to Dialin rather than its default (Router). When Peer=Router, the Pipeline expects to exchange routing information with the other side of the connection. When Peer=Dialin, the Pipeline assigns the IPX Pool # network number to the connection and treats the other side of the connection as a single node. It does not send RIP and SAP advertisements across the connection and ignores RIP and SAP advertisements received from the far end. However, it does respond to RIP and SAP queries received from dial-in clients.

In the Ether Options submenu of the Ethernet Profile, set the IPX Pool # to a unique 32-bit hexadecimal IPX network number. During PPP negotiation, the Pipeline assigns this network number to the dial-in client. If the client does not provide its own unique node number, the Pipeline assigns a unique node number to the client as well. The Pipeline continuously advertises the route to the Pool network.

Note: The network number you specify in the IPX Pool# field must be unique within the IPX routing domain.

Managing the NetWare server table

In NetWare 3.*x*, NetWare servers broadcast SAP (Service Advertising Protocol) packets every 60 seconds to make sure that all routers and bridges know about available services. n NetWare 4.0 and later, built-in directory services eliminates the need for SAP. Services are located through directory services instead.

Like other IPX routers, the Pipeline builds a server table based both on statically configured IPX routes and information contained in SAP broadcast packets. In an active IPX environment that includes many servers and many types of servers, the resulting server table can be very large. IPX SAP Filters enable the Pipeline to restrict the server table to a manageable size and provide more control for the network administrator.

Table 6-6 shows IPX SAP filter parameters.

Table 6-6. IPX SAP filter parameters

Location	Parameters
Ethernet→Connections→*any profile*→ Sessions options… (Connection Profile)	IPX SAP Filter=0
Ethernet→Answer→Sessions options... (Answer Profile)	IPX SAP Filter=0
Ethernet→IPX SAP Filters→*any profile* (IPX SAP Filter Profile)	Name=*filter-name* Input filters... Output filters...
Ethernet→IPX SAP Filters→*any profile*→Input filters→01 to 12 Ethernet→IPX SAP Filters→*any profile*→Output filters→01 to 12	Valid=No Type=Exclude Server Type=*service-type* Server Name=*server-name*

Table 6-6. IPX SAP filter parameters (continued)

Location	Parameters
Ethernet→Mod Config→Ether options… (Ethernet Profile)	IPX SAP Filter=0

Note: IPX SAP filters control which services are added to the local server table or passed on in SAP response packets across IPX routing connections (*not* IPX bridging connections). They do not manage connectivity costs, like filters that prevent periodic RIP and SAP broadcasts from keeping a connection up unnecessarily.

IPX SAP proxy mode

The Service Advertising Protocol (SAP) allows service-providing nodes such as file servers or print servers to advertise their services and addresses. Through SAP, routers create and maintain a database of internetwork service information. This allows NetWare clients to determine what services are available on the network and obtain the internetwork address of the servers providing those services.

Figure 6-1 shows a WAN connection between a large IPX network and a small branch or home office that supports only NetWare clients (and no servers). In this situation, the Pipeline typically forwards SAP broadcasts to the Pipeline at Site B at connection time. The Pipeline then creates a SAP table listing services and server addresses at Site A. If the corporate IPX network is large and supports many NetWare services, the service table created by the Pipeline can become very large and unmanageable.

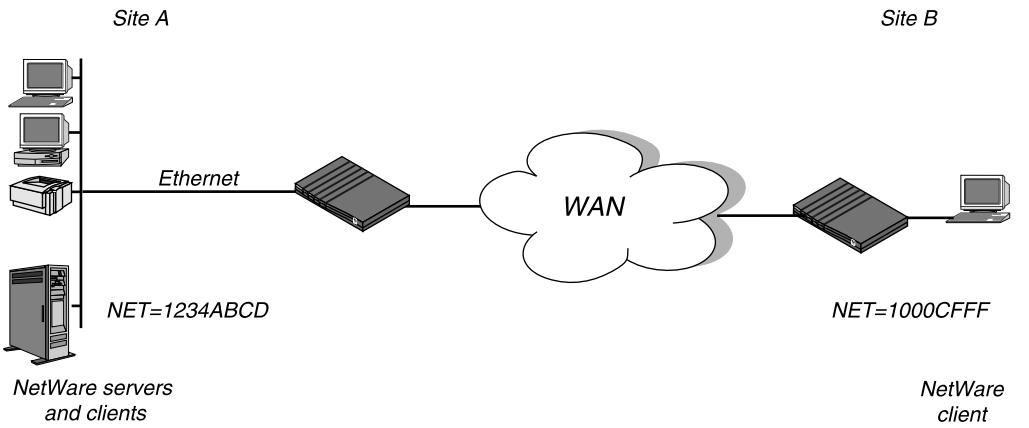


Figure 6-1. Example IPX network

If the small NetWare site supports only NetWare clients (not servers) and uses a Pipeline to connect to the corporate network, the Pipelines can be configured to run in SAP proxy mode. In SAP proxy mode, the Pipelines do not create a SAP table. They simply drop all SAP broadcasts received from the corporate network and handle individual SAP queries as they are received from their local NetWare clients by forwarding the query across the WAN link.

Note: SAP proxy mode is recommended when only NetWare clients are on the Ethernet side of Pipeline. If the Pipeline running in SAP proxy mode has a NetWare server on its Ethernet, it stores the relevant SAP entries for that server and advertises it across the WAN interface as a normal SAP broadcast.

Planning an IPX WAN connection

This section describes how to get the local IPX information you need, and shows how to plan two common IPX WAN configurations.

- A connection with servers on one side of the link only
- A connection with servers on both sides of the link

See “Configuring an IPX connection” on page 6-20 for a step-by-step example.

Making the Pipeline compatible with the local IPX network

The IPX configuration for the Ethernet interface of the Pipeline must be consistent with other NetWare servers connected to the same Ethernet segment.

- The Pipeline must use the same IPX network number as NetWare servers on the Ethernet.
- The Pipeline must be configured with the same IPX frame type used by the NetWare servers.

To find out the IPX configuration of an existing NetWare server, type Load Install at the server's console to view the AUTOEXEC.NCF file.

IPX network number

Note: The Pipeline can learn the right IPX network number on Ethernet by listening to other routers. Leave the IPX network number at zero to allow this learning behavior. If you enter a value other than zero, the Pipeline becomes a "seeding" router and other routers can learn their number from the Pipeline. For more details about seeding routers, see the Novell documentation.

In a NetWare server's AUTOEXEC.NCF file, look for two lines similar to this:

```
internal network 1234
Bind ipx ipx-card net=CF0123FF
```

The first line specifies the internal network number of the server. If you are not familiar with internal network numbers, see the Novell documentation. Ascend products do not require internal network numbers.

The BIND line specifies the network number for the Ethernet. When you configure the local Ethernet IPX number in the Ethernet Profile, you must specify this number. Or, you can set the Pipeline unit's IPX network number to zero to cause it to learn its network number from other routers on the Ethernet.

Note: IPX network numbers on each network segment and internal network within a server on the *entire WAN* must have a unique network number. So, you need to know both the external and internal network numbers in use at all sites.

IPX frame type

In a NetWare server's AUTOEXEC.NCF file, look for a line similar to this:

```
Load 3c509 name=ipx-card frame=ETHERNET_8023
```

This line specifies the packet frame being used by this server's Ethernet controller (in this example, 802.3 frames). If you are not familiar with the concept of packet frames, see the Novell documentation.

Note: The Pipeline can route only one packet frame type, and it routes and spoofs IPX packets only if they are encapsulated in that frame. If bridging is enabled in the same Connection Profile as IPX routing, the Pipeline will attempt to bridge any other IPX packet frame types. For more information see Chapter 4, "Configuring the Pipeline as a Bridge."

Checking local NetWare configurations

NetWare clients on a wide-area network do not need special configuration in most cases. These are some issues that sometimes affect the IPX routing environment:

- Preferred servers

  If the local IPX network supports NetWare servers, configure NetWare clients with a preferred server on the local network, not at a remote site. If the local Ethernet does not support NetWare servers, configure local clients with a preferred server on the network that requires the least expensive connection costs.

- Local copy of LOGIN.EXE

  Try to use the WAN primarily for transferring files, not for executing programs. We recommend that you put LOGIN.EXE on each client's local drive.

- Packet Burst (NetWare 3.11)

  Packet Burst lets servers send a data stream across the WAN before a client sends an acknowledgment. It is included automatically in server and client software for NetWare 3.12 or later. If local servers are running NetWare 3.11, the servers should have PBURST.NLM and PC clients should have BNETX.COM. Refer to your Novell documentation for more information.

- Macintosh or UNIX clients

Both Macintosh and UNIX clients can use IPX to communicate with servers. However, both types of clients also support native support using AppleShare (Macintosh) or TCP/IP (UNIX).

If Macintosh clients must access NetWare servers across the WAN by using AppleShare client software (rather than MacIPX), the WAN link must support bridging. Otherwise, AppleTalk packets will not make it across the connection.

If UNIX clients will access NetWare servers via TCP/IP (rather than UNIXWare), the Pipeline must also be configured as a bridge or IP router. Otherwise, TCP/IP packets will not make it across the connection.

Deciding on authentication for IPX incoming calls

Unlike an IP routing configuration, where the Pipeline uniquely identifies the calling device by its IP address, an IPX routing configuration does not include a built-in way to identify incoming callers. For that reason, password authentication using PAP or CHAP is required unless IP routing is configured in the same Connection Profile.

If a connection requires both IPX and IP routing, you are not required to configure incoming password authentication. The Pipeline uses station names and passwords to sync up the connection with the remote device.

Planning a connection with servers on one side of the link only

In this configuration, the Pipeline is connected to a local IPX network that supports both servers and clients. To plan a connection that allows one or more NetWare clients on a geographically remote network to access the local NetWare servers, read this section.

Note: When the Pipeline will connect to an existing Novell LAN, you need to work with the administrator of that network to obtain network numbers and server-specific information.

Figure 6-2 shows an example network diagram.

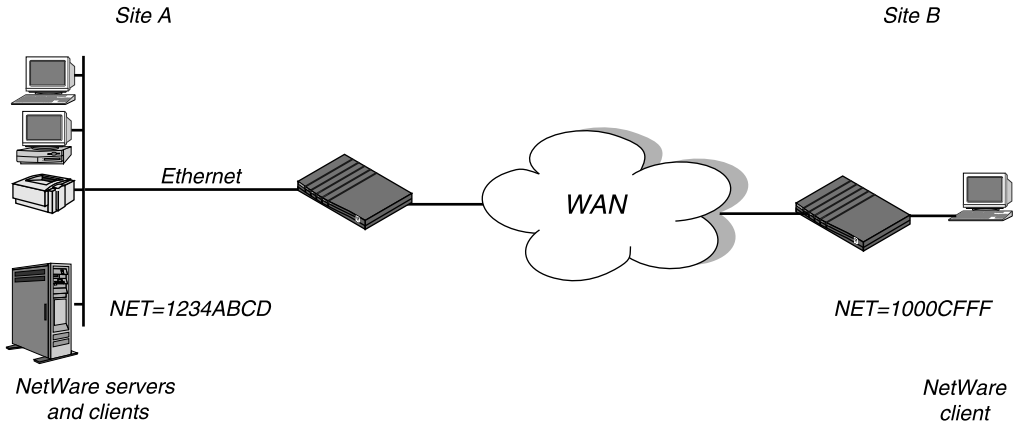


Figure 6-2. Servers on one side of the connection only

In this example, site A supports NetWare 3.12 servers, NetWare clients, and a Pipeline. The NetWare server at site A is configured with this information:

```
Name=SERVER-1
internal net CFC12345
Load 3c509 name=ipx-card frame=ETHERNET_8023
Bind ipx ipx-card net=1234ABCD
```

Site B is a home office that consists of one PC and a Pipeline. It is not an existing Novell LAN, so the Pipeline configuration creates a new IPX network (1000CFFF in this example).

Note: The new IPX network number assigned to site B in this example cannot be in use *anywhere* on the entire IPX wide-area network. (It cannot be in use at site A or any network to which site A connects.)

The site A Pipeline configuration is shown in Table 6-7. (All other IPX parameters can use the default values.)

Table 6-7. IPX configuration for site A with NetWare servers and clients

Location	Parameter
System→Sys Config (System Profile)	Name=SITEAGW

Table 6-7. IPX configuration for site A with NetWare servers and clients (continued)

Location	Parameter
Ethernet→Connections→*any profile* (Connection Profile)	Station=SITEBGW Route IPX=Yes
Ethernet→Connections→*any profile*→ Encaps options...	Send AUTH=PAP (or CHAP) Recv PW=*SECURE* (a password) Send PW=*SECURE* (a password)
Ethernet→Connections→*any profile*→ IPX options...	Netware t/o=30 (default)
Ethernet→Answer→PPP options... (Answer Profile)	Route IPX=Yes Recv AUTH=Either (or PAP or CHAP)
Ethernet→Mod Config (Ethernet Profile)	IPX Routing=Yes
Ethernet→Mod Config→Ether options...	IPX Frame=802.3 IPX Enet #=1234ABCD

Note: If one of the calling units is set to answer only, only the incoming authentication parameters are needed. If a unit is configured to call only, only the outbound authentication is used.

The site B Pipeline configuration is shown in Table 6-8. (All other IPX parameters can use the default values.)

Table 6-8. IPX configuration for site B with NetWare clients only

Location	Parameter
System→Sys Config (System Profile)	Name=SITEBGW
Ethernet→Connections→*any profile* (Connection Profile)	Station=SITEAGW Route IPX=Yes

Table 6-8. IPX configuration for site B with NetWare clients only (continued)

Location	Parameter
Ethernet→Connections→*any profile*→ Encaps options...	Send AUTH=PAP (or CHAP) Recv PW=*SECURE* (a password) Send PW=*SECURE* (a password)
Ethernet→Connections→*any profile*→ IPX options...	Dial Query=Yes
Ethernet→Answer→PPP options... (Answer Profile)	Route IPX=Yes Recv AUTH=Either (or PAP or CHAP)
Ethernet→Mod Config (Ethernet Profile)	IPX Routing=Yes
Ethernet→Mod Config→Ether options...	IPX Frame=802.3 IPX Enet #=1000CFFF

See "Configuring an IPX connection" on page 6-20 for more details.

Planning a connection with servers on both sides of the link

In this type of IPX WAN configuration, the Pipeline is connected to an IPX network that supports both servers and clients and will connect with a remote site that also supports both servers and clients. See Figure 6-3.

Note: When the Pipeline will connect to an existing Novell LAN, you need to work with the administrator of that network to obtain network numbers and service-specific information.

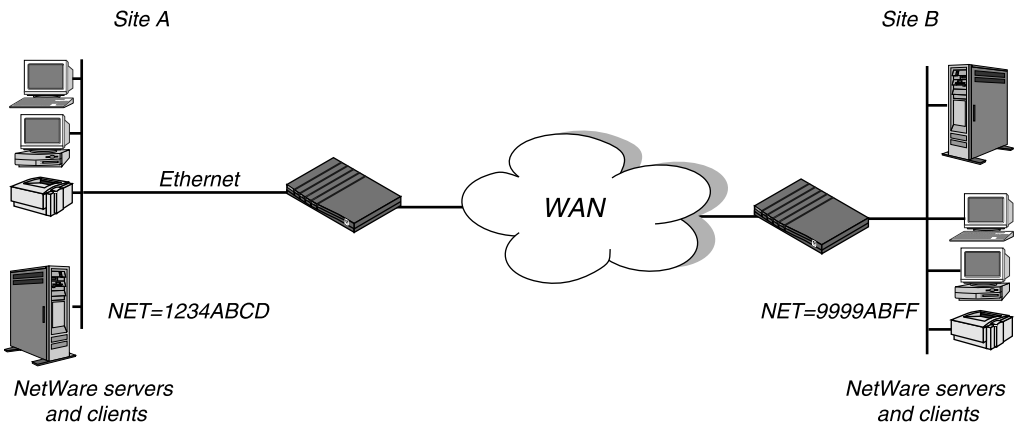


Figure 6-3. Servers on both sides of the connection

In this example, site A and site B are both existing Novell LANs that support NetWare 3.12 and NetWare 4 servers, NetWare clients, and a Pipeline. The NetWare server at site A is configured with this information:

```
Name=SERVER-1
internal net CFC12345
Load 3c509 name=ipx-card frame=ETHERNET_8023
Bind ipx ipx-card net=1234ABCD
```

The NetWare server at site B (Figure 6-3) is configured this information:

```
Name=SERVER-2
internal net 013DE888
Load 3c509 name=net-card frame=ETHERNET_8023
Bind ipx net-card net=9999ABFF
```

The site A Pipeline configuration is shown in Table 6-9. (All other IPX parameters can use the default values.)

Table 6-9. IPX configuration for site A with both servers and clients

Location	Parameter
System→Sys Config (System Profile)	Name=SITE1GW

Table 6-9. IPX configuration for site A with both servers and clients (continued)

Location	Parameter
Ethernet→Connections→x0-105 (Connection Profile #5)	Station=SITE2GW Route IPX=Yes
Ethernet→Connections→x0-105→Encaps options...	Send AUTH=PAP (or CHAP) Recv PW=*SECURE* (a password) Send PW=*SECURE* (a password)
Ethernet→Answer→PPP options... (Answer Profile)	Route IPX=Yes Recv Auth=Either
Ethernet→IPX Routes→*any profile* (IPX Route Profile)	Server Name=SERVER-2 Active=Yes Network=013DE888 Node=000000000001 Socket=0451 Server Type=0004 Connection #=5
Ethernet→Mod Config (Ethernet Profile)	IPX Routing=Yes
Ethernet→Mod Config→Ether options...	IPX Frame=802.3 IPX Enet #=1234ABCD

Note: If one of the calling units is set to answer only, only the incoming authentication parameters are needed. If a unit is configured to call only, only the outbound authentication is used.

The site B gateway configuration is shown in Table 6-10. (All other IPX parameters can use the default values.)

Table 6-10. IPX configuration for site B with both servers and clients

Location	Parameter
System→Sys Config (System Profile)	Name=SITE2GW
Ethernet→Connections→x0-102 (Connection Profile #2)	Station=SITE1GW Route IPX=Yes
Ethernet→Connections→x0-102→Encaps options...	Send AUTH=PAP (or CHAP) Recv PW=*SECURE* (a password) Send PW=*SECURE* (a password)
Ethernet→Answer→PPP options... (Answer Profile)	Route IPX=Yes Recv Auth=Either
Ethernet→IPX Routes→*any profile* (IPX Route Profile)	Server Name=SERVER-1 Active=Yes Network=CFC12345 Node=000000000001 Socket=0451 Server Type=0004 Connection #=2
Ethernet→Mod Config (Ethernet Profile)	IPX Routing=Yes
Ethernet→Mod Config→Ether options...	IPX Frame=802.3 IPX Enet #=9999ABFF

Configuring an IPX connection

This section shows how to configure IPX routing for a Pipeline connecting to a remote site where both servers and clients are supported.

This example configuration does not show the system configuration (such as the name assigned to the Pipeline), link-specific settings (such as Telco options or

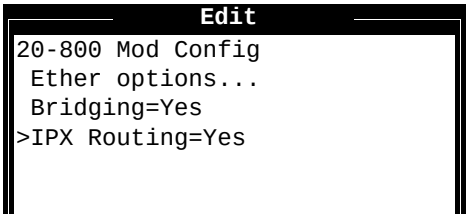
MP+ configuration), or additional bridging and IP settings that may be appropriate at your site. It focuses only on IPX routing.

Configuring the Ethernet Profile

The Ethernet parameters specify information about the local IPX network (on the Ethernet to which the Pipeline is directly connected). These parameters are always required. In effect, they turn on the IPX routing capability.

To enable IPX routing:

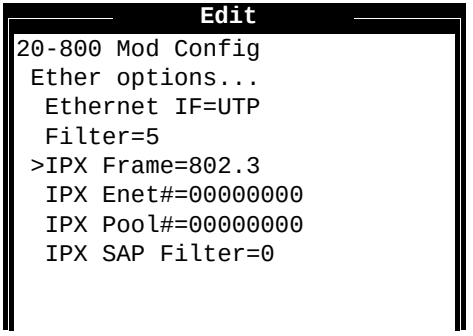
1 Open the Ethernet Profile.



2 IPX Routing is set to Yes by default.

3 Open the Ether Options submenu.

4 Set IPX Fram**e** to the appropriate IPX frame type for the local Ethernet.
See “IPX frame type” on page 6-13.



5 Set IPX Enet# to the unique network number for this Ethernet interface.

Or, if there are other IPX routers on this Ethernet, leave this value at zero to have this Pipeline learn the IPX network number from other routers. See "IPX network number" on page 6-12.

6 Exit the Ethernet Profile and save the changes you made.

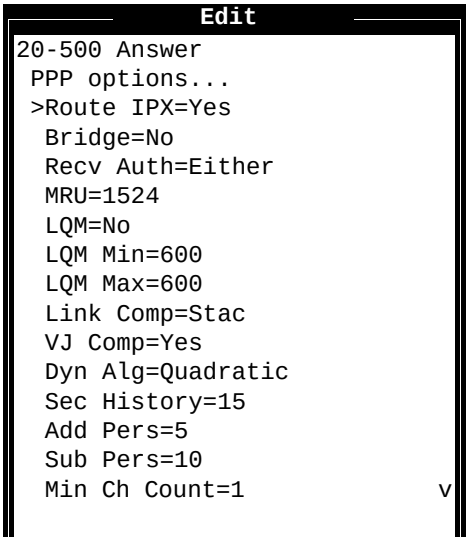
Configuring the Answer Profile

Route IPX must be enabled on both the answering and dialing side of a connection; otherwise the session cannot route IPX. See "Deciding on authentication for IPX incoming calls" on page 6-14 for details about authentication for IPX routing.

Note: If you are configuring a frame relay IPX connection, these parameters do not apply.

1 Open the Answer Profile.

2 Open the PPP Options submenu.



3 Set Route IPX to Yes.

Route IPX must be enabled on both the answering and dialing side of a PPP or MP+ session link; otherwise the link cannot route IPX. Route IPX is set to N/A if the IPX parameters in the Ethernet Profile have not been set.

4 Set Recv Auth to Either (or PAP or CHAP, as appropriate for your site).

5 Exit the Answer Profile and save the changes you made.

Configuring the Connection Profile

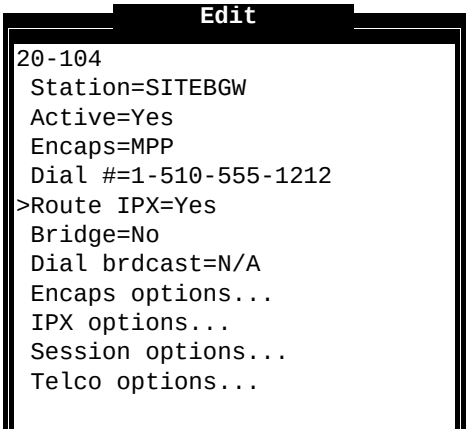
IPX configuration in a Connection Profile is fairly simple. Most of the IPX options have default values that work for many NetWare sites.

1 Open a Connection Profile.

2 Set the Station name of the remote device.

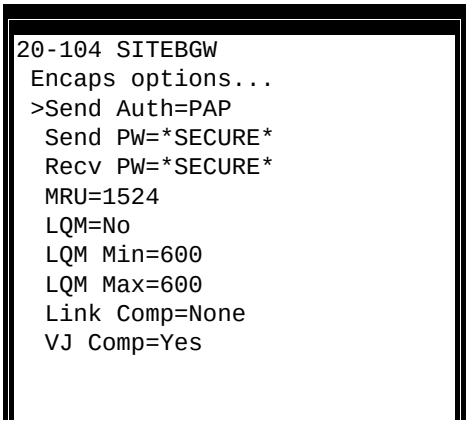
Make sure that it matches the name of the remote device exactly, including case changes.

3 Set Route IPX=Yes.



Route IPX is N/A if the IPX frame type has not been set (see “Configuring the Ethernet Profile” on page 6-21).

4 Open the Encaps Options submenu.



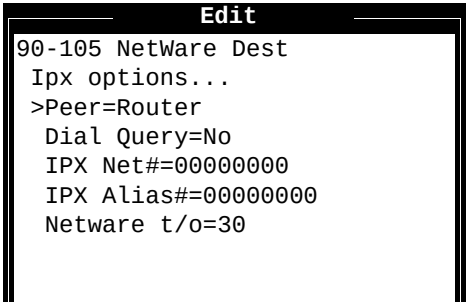
5 Specify the appropriate Send authentication (PAP or CHAP).

6 Enter the password expected by the remote network in the Send PW parameter.

7 Enter the password expected by the Pipeline for incoming callers in the Recv PW parameter.

8 Press Escape to return to the Connection Profile, and then open the IPX Options submenu.

The IPX Options submenu has default values that work for this connection, but the next few steps show how to use those parameters. See Chapter 11, “Reference,” for more detail on each parameter.



9 Leave Peer=Router.

See “Dial-in NetWare clients” on page 6-8.

10 Leave Dial Query set to No.

See “Dial Query” on page 6-6.

11 Leave the IPX Net # and IPX Alias # parameters set to zero.

If you specify an address in the IPX Net # parameter, the Pipeline creates a static route to that network. This is not usually required or useful.

When routing from a Pipeline to another Ascend unit, an IPX Alias # is not required. It is used only if the far-end router uses numbered interfaces.

12 Leave the “NetWare t/o=” parameter set to the default 30 minutes.

See “Watchdog spoofing” on page 6-7.

13 Exit the Connection Profile, saving the changes you made.

Note: If there is an active session for this profile, you must terminate the session and start it up again for the new settings in the Connection Profile to take effect.

Configuring an IPX Route Profile

The IPX Routes menu lets you define 2 profiles in the Pipeline. Each profile contains all of the information needed to reach one NetWare server on a remote network. When the Pipeline receives an outbound packet for that server, it finds the referenced Connection Profile and dials the connection.

The main advantage of an IPX Route Profile is that it prevents timeouts when a client takes a long time to locate a server on the WAN. However, when the specified server goes down or is otherwise inaccessible, the Pipeline continues to look for the server.

Note: You do not need to create IPX Routes to servers that are on the local Ethernet.

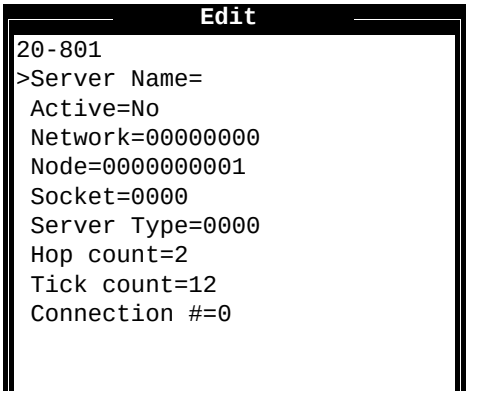
Most sites configure only a few IPX routes and rely on RIP for most other connections. If you have servers on both sides of the WAN connection, we recommend that you define at least one IPX Route Profile at each site, even if your environment requires dynamic routes. If you have one IPX Route Profile that points to a “master” NetWare server on a remote network,

NetWare workstations can learn about other remote services by connecting to the "master" NetWare server.

Note: Remember that static IPX routes are manually administered, so they must be updated if there is a change to the network configuration. For this reason, static routes can increase the administration cost of the network and possibly lead to confusion after configuration changes.

To create an IPX Routes Profile:

1 Open an unnamed IPX Route Profile below the IPX Routes menu.



2 Set Server Name to the name of the remote NetWare server (such as SERVER-1).

3 Set Active to Yes.

4 Set the Network to the remote server's internal network number, for example:

```
ABC01FFF
```

5 Set the Node number to the remote server's node number, for example, the default 0000000000001.

This is typically the node number for Novell file servers.

6 Specify the remote service's socket number, for example, 0451.

Typically, Novell file servers use socket 0451. The number you specify must be a well-known socket number. Services that use dynamic socket numbers may use a different socket each time they load and will not

work with IPX Route Profiles. To bring up a connection to a remote service that uses a dynamic socket number, specify a "master" server on that network that uses a well-known socket number.

7 Specify the SAP Service Type; for example, file servers are type 0004.

8 Set Hop Count to the distance (in hops) to the destination network.

Usually the default of 2 is appropriate.

9 Set Tick Count to the distance to the destination network in IBM PC clock ticks.

In most cases, the default of 12 is appropriate.

10 Specify the number of the Connection profile through which the remote network will be accessed.

Make sure you specify the right profile to reach this server.

11 Exit the IPX Route Profile and save the changes you made.

Defining an IPX SAP filter

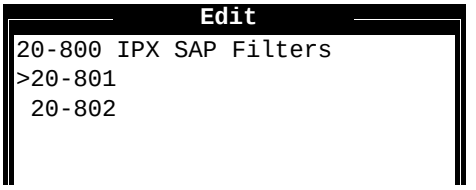
IPX SAP filters include or exclude specific NetWare services from the server table maintained by the Pipeline. You can exclude or explicitly include up to 12 services in each IPX SAP Filter Profile.

IPX SAP Filter Profiles are organized like regular Ascend Filter Profiles. If you are unfamiliar with Filter Profiles, see Chapter 8, "Using Filters."

To define an IPX SAP filter that excludes a NetWare 3.x file server named "SERVER-1," follow these steps:

1 Open the IPX SAP Filters menu.

At the top level, you'll see a list of defined IPX SAP Filter Profiles.



2 Open a Filter Profile.

When you open an IPX SAP Filter Profile, you assign the profile a name and choose Input or Output filters.

```
Edit
20-801 File Server
>Name=File Server
 Input filters...
 Output filters...
```

Input filters apply to all SAP packets received by the Ascend unit. Input filters screen advertised services and exclude them from its server table (or include them) as specified in the filters.

Output filters apply to SAP response packets transmitted by the Ascend unit. If the Ascend unit receives a SAP request packet, it applies Output filters before transmitting the SAP response, and excludes services from the response packet (or includes them) as specified in the filters.

Input and Output filters are identical in structure: each one contains up to 12 sets of conditions.

3 Open the list of Input filters.

```
Edit
20-801 File Server
 Input filters...
 >In filter 01
  In filter 02
  In filter 03
  In filter 04
  In filter 05
  In filter 06
  In filter 07
  In filter 08
  In filter 09
  In filter 10
  In filter 11
  In filter 12
```

These filters are applied in the order in which they are listed: In filter 01 followed by In filter 02, and so forth.

4 Open an In filter by selecting it and pressing Enter.

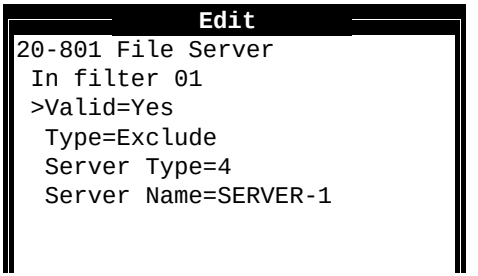
5 Set the Valid parameter to Yes

6 Set the filter type to Exclude.

7 Specify the service type (a hexadecimal number).

File servers are service type 4.

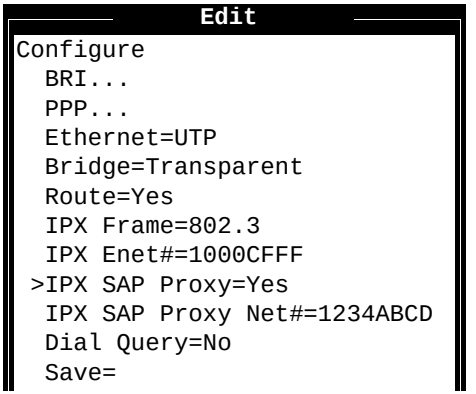
8 Specify the NetWare server's name (for this example, SERVER-1).



Configuring a Pipeline to run in SAP proxy mode

To configure a Pipeline to drop SAP broadcasts and forward SAP requests in proxy mode:

1 Open the Configure Profile.



2 Set IPX SAP Proxy to Yes.

3 Set the IPX SAP Proxy Net # to the remote IPX network number.
For example, for the Pipeline shown in Figure 6-1 on page 11:
IPX SAP Proxy Net#=1234ABCD

4 Close and save the Configure Profile.

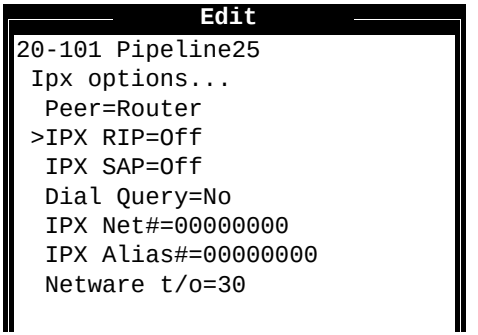
Note: You must configure a static IPX route to the remote site.

Configuring IPX RIP and SAP for a WAN connection

When a Pipeline establishes a connection with the remote Pipeline, it sends out all of its RIP and SAP broadcasts on the WAN link. If the RIP or SAP tables are large, this behavior can lead to the Pipeline running out of memory. To configure the Pipeline to prevent this overload in the remote Pipeline:

1 Open the Connection Profile for the remote Pipeline.

2 Open the IPX Options submenu.



3 Set IPX RIP=Off.

4 Set IPX SAP=Off.

5 Close the Connection Profile.

Similarly, you could configure the Pipeline's Connection Profile to the Pipeline to turn off IPX RIP and SAP or to send RIP and SAP packets but not receive them.

Note: When RIP is turned off, you must configure a static IPX route to the remote device. When SAP is turned off, the remote device must have a service table and static route that enables NetWare clients to locate services on the large IPX network.

Checking IPX statistics

The terminal server interface has a suite of "show netware" commands. For details on all of these commands, see Chapter 10, "Using the Command Mode."

To check NetWare statistics:

1 Invoke the terminal server from the System:Sys Diag menu.

By default, the terminal server is a shell interface with an "Ascend" prompt.

```
ascend%
```

2 To view IPX packet activity, type this command at the Ascend prompt:

`show netware stat`

This command displays packets received, forwarded, dropped, and outbound packet information.

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

3 To view information about known servers, type:

`show netware servers`

You'll see a list like this:

```
       IPX address                  type        server name
EE000001:000000000001:0040          026b     ASCEND__________
EE000001:000000000001:4510          0004     NOVL1
EE000001:000000000001:4005          0278     ASCEND__________
A30E0A04:000000000001:8060          0047     EPS_0E0A04
A30E1347:000000000001:8060          0047     EPS_0E1347
A30E0EB8:000000000001:8060          0047     EPS_0E0EB8
A30EB294:000000000001:8060          0047     EPS_04B294
```

4 To see the Pipeline IPX routing table, type:

`show netware networks`

```
network      next router       hops    ticks    origin
22222222     000000000000      2       12       nov12-m2       S
A30E0A04     0080A30E0A04      1       3        Ethernet
A30E1347     0080A30E1347      1       3        Ethernet
A30E0EB8     0080A30E0EB8      1       3        Ethernet
A304B294     0080A304B294      1       3        Ethernet
EE000001     00608CB24081      1       3        Ethernet
AA000002     000000000000      0       1        Ethernet       S
```

Pipeline System Security

7

This chapter covers these topics:

Pipeline Security overview

The Pipeline provides the following security options for securing it against unauthorized users:

- System security
  This includes enabling the MP+ Remote Management and configuring Security Profiles.
- Connection security
  This includes configuring callback, filtering, rejection of unknown users, and security card authentication.

Introduction to system security

System security protects the Pipeline itself from unauthorized access. The following configuration parameters are related to system security:

Table 7-1. System security parameters

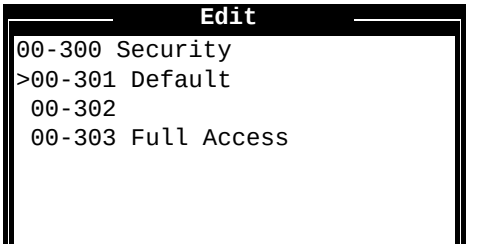
Location	Parameter with default value
System→Sys Config	Remote Mgmt=Yes
System→Security→*any profile*	Name=[] Passwd=[] Operations=Yes Edit Security=Yes Edit System=Yes Field Service=Yes

For details on each of these parameters, see Chapter 11, “Reference.”

Note: All passwords are initially null except for the Full Access Profile password, which has the default password “Ascend”. We recommend that you change these defaults as soon as possible. See “Setting up security profiles” on page 7-3 for more information.

Setting up security profiles

The Pipeline has up to three security levels, which are defined in Security Profiles. Security Profiles are located below System→Security in the Pipeline configuration menus.



When the Pipeline is shipped from the factory, all levels are set with full privileges. A profile must have a name to be activated, so only the Default and Full Access Profiles can be activated initially.

Note: We strongly recommend that you follow the instructions in "Modifying the Default Profile" on page 7-4 and "Assigning a password to the Full Access Profile" on page 7-5. These instructions result in two security levels, one that is totally restrictive (Default) and one that is totally open (Full Access). If you need additional security levels, you can define them in the remaining Security Profile.

Parameters in a Security Profile

The parameters in a Security Profile are listed below. For more details on each of these parameters, see Chapter 11, "Reference."

Table 7-2. Parameters in a Security Profile

Parameter	Description
Name	A Security Profile name can be up to 16 characters. Initially, only two of the Security Profiles have a name (Default and Full Access). A profile must have a name for users to select it.

Table 7-2. Parameters in a Security Profile (continued)

Parameter	Description
Passwd	A password can be up to 20 characters. The Default profile has no password. The default password for the Full Access Profile is “Ascend”.
Operations	When set to Yes, an operator can view configuration profiles and change the value of any parameter that is not restricted by other settings. Setting this to No sets all other privileges in the profile to N/A. In addition, when this privilege is set to No, an operator cannot access most DO commands. Only DO Esc, and DO password are available to them.
Edit Security	When set to Yes, an operator can edit Security Profiles and access all other operations by enabling them in his or her active Security Profile. This is the most powerful privilege, because it enables users to modify their own privileges.
Edit System	When set to Yes, an operator can edit the System Profile and the IP routing table (in the terminal server interface). If Edit System=No, an operator cannot edit the System Profile, or the IP routing table.
Field Service	When set to Yes, an operator can perform Ascend-provided field service operations, such as uploading new system software.

Modifying the Default Profile

The first profile in the Security menu is named Default. The password assigned to this profile is null, and the profile’s name and password cannot be changed. The Pipeline activates this profile whenever it is powered on or reset, and for every new login session.

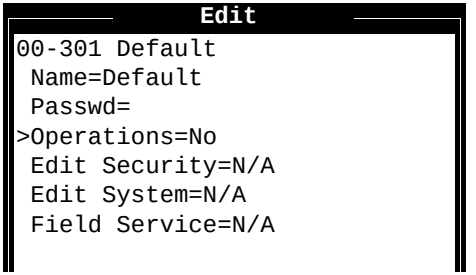
Note: Although the Default Profile is set initially with full privileges, it is intended to be very restrictive, because every user who logs in via Telnet, the Control port, or remote management, is granted the privileges specified there.

To edit the Default Profile to make it appropriately restrictive:

1 Open the Default Profile.

The first two parameters in the Default Profile cannot be changed—the name is always Default and the password is always null.

2 Set Operations to No.



All other parameters are set to N/A when Operations=No.

Operators will be able to view settings but will not be able to change anything, and all passwords (including the null password) will be hidden by the string *SECURE* in the Pipeline user interface.

3 Exit the Default Profile, saving your changes.

Assigning a password to the Full Access Profile

The last profile in the Security menu is named Full Access. The default password assigned to this profile is “Ascend”.

The Full Access Profile is intended to remain totally open, with all privileges set to Yes. It is important to change the default password as soon as possible. It is also important *not* to turn off the Edit Security privilege in the Full Access Profile, or you will be unable to edit privileges when Full Access has been activated.

To assign a password protecting the Full Access Profile:

1 Open the Full Access Profile.

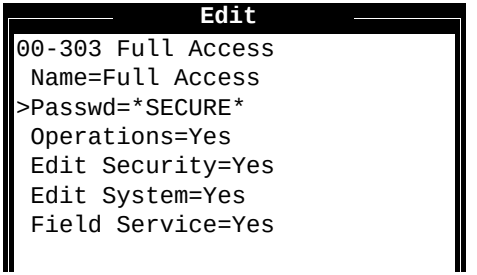
2 When you are prompted for the password, type:

Ascend

Passwords are case sensitive. You must enter the password exactly as shown.

3 Select the Passwd parameter and press Enter to open a text field.

4 Type a new password for this profile.



5 Leave all other privileges enabled.

Do not turn off the Edit Security privilege!

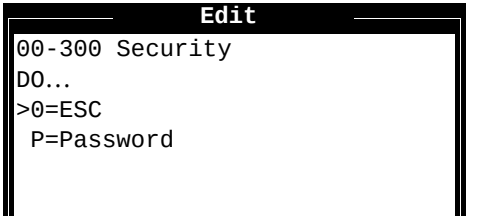
6 Exit the Full Access Profile, saving your changes.

Although the Pipeline does not prevent you from turning off privileges in the Full Access Profile, most sites leave all privileges enabled in this profile and define additional Security Profiles to handle slightly more restrictive privileges.

Activating a new security level

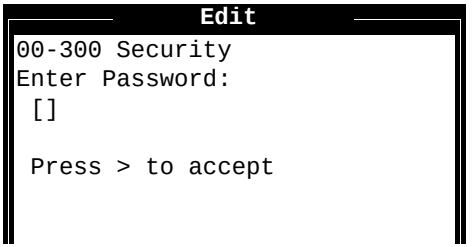
To activate a new security level:

1 Press Ctrl-D to open the DO menu, and then press P (or select P=Password).



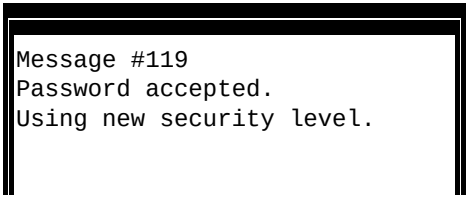
2 In the list of Security Profiles that opens, select the profile you want to activate.

The Pipeline then prompts for that profile's password.



3 Type the password you assigned to the profile and press Enter to accept it.

If you enter the right password, a message states that the password was accepted and the Pipeline is using the new security level.



If the password you enter is incorrect, you are prompted again to enter the password.

Restricting operator access

There are several access methods that enable an operator to log into the Pipeline or to access information about it. Each of these access methods must be considered when you're setting up system security in the Pipeline.

Note: An operator is assigned the default security level at login. Without a password to the Full Access Profile or another "open" Security Profile, the operator can view information but cannot change anything.

This section describes how to restrict an MP+ remote management access from a remote Ascend unit.

An operator of a remote Ascend unit can use the DO menu (DO-8) to begin a remote management session on an MP+ call.

Disabling remote management access

To prevent an operator from accessing the Pipeline from a remote Ascend unit using MPP remote management, open the System Profile and set the Remote Mgmt parameter to No.

Table 7-3. Remote management parameter

Location	Parameter
System→Sys Config	Remote Mgmt=No

For related information on remote management, see the Chapter 9, "Pipeline System Administration."

Introduction to connection security

The Pipeline includes several security mechanisms for controlling dial-in access, including the following features:

- Authentication protocols for PPP (point-to-point protocol) encapsulated calls

  The Pipeline supports both PAP (password authentication protocol) and CHAP (challenge handshake authentication protocol).

- Callback

  When callback is enabled in a profile and an incoming call matches that profile, the Pipeline hangs up and dials back using the dial number specified in the profile. Callback security provides the highest level of control in assuring that incoming calls are coming from a known network.

- Rejecting unknown callers

  When password authentication is not in use, you can configure the Pipeline to reject all incoming bridging or routing calls for which a matching profile is not found.

- Filters

  Filtering can provide a robust form of security available in a dial-up internetworking environment. You can tailor a filter on a per-connection basis to

allow or deny packets from any combination source and destination address, protocol discriminator, source and destination port, and TCP sessions.

For details on filter security, see Chapter 8, "Using Filters."

- Integration with ACE or SAFEWORD servers using personal security cards

  A security card is a hand-held device the shape and size of a credit card, such as those provided by Enigma Logic or Security Dynamics. You can configure the Pipeline to work with a remote network's security card authentication. Once the Pipeline has been authenticated by the remote network, all users dialing into the Pipeline have access to the remote network.

This section does not describe the details of how IP addresses are validated or assigned to incoming callers dynamically, although that process may be part of caller authentication. See Chapter 5, "Configuring the Pipeline as an IP Router."

This section does not describe how to configure the Pipeline to work with ACE or SAFEWORD servers. For details on that topic, see "How Security Card Authentication works" on page 7-14.

The configuration parameters shown in Table 7-1 are related to connection authentication:

Table 7-4. Connection authentication parameters

Location	**Parameter with default value**
System→Sys Config	Name=[]
Ethernet→Connections→*any profile*	Station=[] Dial #=[]
Ethernet→Connections→*any profile*→ IP options...	LAN Adrs=0.0.0.0
Ethernet→Connections→*any profile*→ Encaps options...	Send Auth=None Send PW=[] Aux Send PW=N/A Recv PW=[]
Ethernet→Connections→*any profile*→ Telco options...	Callback=No AnsOrig=Both

Table 7-4. Connection authentication parameters

Location	Parameter with default value
Ethernet→Answer	Profile Reqd=No
Ethernet→Answer→PPP options...	Recv Auth=None
Ethernet→Mod Config→Auth...	APP Server=No APP Host=N/A APP Port=N/A
Ethernet→Mod Config→DHCP Spoofing...	DHCP Spoofing=No Spoof Adr=N/A Renewal Time=N/A

Authenticating calls

The Pipeline authenticates incoming calls based on the type of call and the authentication settings related to that call type. These are the basic types of incoming call:

- PPP and MP+ calls

  Most sites require PAP or CHAP authentication of PPP calls. If the incoming PPP call does not include a source IP address, PAP or CHAP authentication is required.

You can use callback to increase the security of your local network against intrusion based on any type of incoming call.

Using callback security

Callback security instructs the Pipeline to hang up and call back when it receives an incoming call. You can require callback to ensure that the connection is made with the number specified in the Dial # parameter.

To set callback security, use the parameters shown in Table 7-5.

Table 7-5. Callback parameters

Location	Parameter
Ethernet→Connections→*any profile*	Dial #=555-1415
Ethernet→Connections→*any profile*→ Telco options...	Callback=Yes AnsOrig=Both

If you set Callback=Yes, you must also set the parameter AnsOrig=Both, because the Connection Profile must both answer the call and call back the device requesting access. Similarly, the calling device must be able to both dial out to and accept incoming calls from the Pipeline.

Requiring a Connection Profile

The Profile Reqd parameter in the Answer Profile affects how the Pipeline handles bridging and routing calls for which it could find no Connection Profile. This parameter does not affect terminal server calls. The Profile Reqd parameter is shown in Table 7-6.

Table 7-6. Profile required parameter

Location	Parameter
Ethernet→Answer	Profile Reqd=Yes

If the Pipeline doesn't find a matching Connection Profile for the incoming call, it checks the Answer Profile.

If the call is PPP-encapsulated and Recv Auth is *not* set to None, the call is rejected.

If the call is PPP-encapsulated and both Recv Auth=None and Profile Reqd=No, the Pipeline attempts to set up the parameters of the session using the information specified in the Answer Profile.

PPP authentication using PAP or CHAP

PPP and MP+ calls can use PAP or CHAP authentication provided that both sides of the connection support the same protocol (PAP, CHAP, or both).

PAP provides a simple way for a peer to establish its identity in a two-way handshake when initially establishing a link. It sends passwords unencrypted, so it is not a very strong authentication method. PAP provides baseline security when your system interoperates with non-Ascend equipment.

CHAP is a stronger authentication method than PAP. During the establishing of the initial link, CHAP verifies the identity of a peer through a three-way handshake. It sends passwords encrypted by means of a one-way hash function. CHAP's use of an incrementally changing identifier and a variable challenge value protects against playback attack.

Table 7-7 lists the parameters related to authentication of incoming PPP calls in a Connection Profile.

Table 7-7. Authentication parameters for incoming PPP or MP+ calls

Location	Parameter
Ethernet→Connections→*any profile*	Station=[] Encaps=PPP or MP+
Ethernet→Connections→*any profile*→ IP options...	LAN Adrs=0.0.0.0
Ethernet→Connections→*any profile*→ Encaps options...	Recv PW=[]
Ethernet→Connections→*any profile*→ Telco options...	AnsOrig=Both (or Ans Only)
Ethernet→Answer	Profile Reqd=Yes
Ethernet→Answer→PPP options...	Recv Auth=Either (or PAP or CHAP)

For an incoming PPP or MP+ call, the Pipeline attempts to match the caller's name and password to the Station and Recv PW parameters in a Connection Profile. If it does not find a matching profile, it checks the caller's source IP address and attempts to match it to the LAN Adrs parameter in a Connection Profile.

If Recv Auth is set to PAP or to CHAP, the Pipeline tries to authenticate the call using the specified protocol. It completes the initial handshake for that protocol, compares the password to the Recv PW parameter, and hangs up if authentication fails. If Recv Auth=Either, the Pipeline first tries to use CHAP and if the far end of the connection doesn't support CHAP, the Pipeline uses PAP instead.

The AnsOrig parameter specifies whether the Pipeline can initiate calls, receive them, or both. The Pipeline will not accept an incoming call if this parameter is set to Call Only.

Table 7-8 lists the parameters related to authentication in outbound PPP calls.

Table 7-8. Authentication parameters for outbound PPP or MP+ calls

Location	**Parameter**
System→Sys Config	Name=[]
Ethernet→Connections→*any profile*	Encaps=PPP or MP+
Ethernet→Connections→*any profile*→ Encaps options...	Send Auth=PAP (or CHAP) Send PW=[] Aux Send PW=N/A
Ethernet→Connections→*any profile*→ Telco options...	AnsOrig=Both (or Call Only)

The strings specified in the Name and Send PW parameters are the name and password used to authenticate the call. These strings must match the Station and Recv PW parameters on the answering device.

The AnsOrig parameter specifies whether the device can initiate calls, receive them, or both. If this parameter is set to Ans Only, no outbound calls will be made.

How Security Card Authentication works

A secure network site can be set up to change its password very frequently, many times a day. For these secure sites, the Ascend MAX is a network access server (NAS). The NAS is the device that requests a RADIUS service, such as authenticating a user.

In the context of a security card environment, a user attempting to open a connection to the remote network through the security hub (such as an Ascend MAX) is a client of your Pipeline, your Pipeline is a client of the RADIUS server, and the RADIUS server is a client of an external authentication server, such as a Security Dynamics (ACE) or Enigma Logic (SAFEWORD) server.

The ACE or SAFEWORD server syncs up with hand-held personal security cards (devices the size and shape of a credit card) to provide users with the current password in real-time. The LCD on the users' security cards displays the current, one-time-only password required to gain access at that moment to the secure network.

An example security card environment is shown in Figure 7-1. It includes a calling unit, such as an Ascend Pipeline, a NAS (the MAX), a RADIUS server, and an ACE or SAFEWORD server.

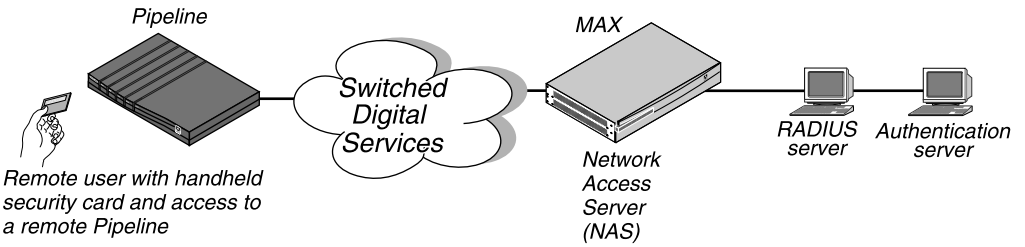


Figure 7-1. Security card environment

This is how security-card passwords are authenticated:

1 A connection is initiated from a calling unit, such as an Ascend Pipeline, to a NAS (such as an Ascend MAX).

2 The NAS requests authentication of the call from the RADIUS server.

3 The RADIUS server forwards the request to the ACE or SAFEWORD server.

4 The ACE or SAFEWORD server sends a challenge message (which may confirm a null challenge) back through the RADIUS server and the NAS to the Pipeline that's dialing in.

5 A user on the dialing network, who may be at the Pipeline console in a terminal server session or using the APP Server utility at a Unix or Windows host, sees the challenge message and obtains the current password from his or her security card.

6 The user enters the current password obtained from the security card in response to the challenge message.

If 60 seconds or more pass without a response, the call is dropped.

If the user enters the correct password, network access is established.

If the user enters an incorrect password, the ACE or SAFEWORD server returns another challenge (a maximum of three challenges is possible) and the user has another 60 seconds to enter the correct password. After three incorrect entries, or if 60 or more seconds pass per challenge without a response, the call is terminated.

Supporting outbound security card calls

You can configure the Pipeline to use a security card to call out to a NAS at a secure site. The instructions in this section explain how to configure the Pipeline unit as the calling unit, and how to respond to password challenges from an ACE or SAFEWORD server on the remote network.

Note: Configuring security card calls requires close cooperation with the network administrator of the remote site.

Setting an authentication mode in the Pipeline

The authentication mode configured in the Pipeline affects how the token passwords are transmitted and how the dial-in user is affected by channels being added to an established session. The Pipeline requests the authentication mode

with which it is configured, but the RADIUS profile in the answering NAS determines which mode will actually be used.

Configuring PAP-TOKEN mode

PAP-TOKEN is the default authentication mode used when the RADIUS profile has a password of ACE or SAFEWORD. See “Setting an authentication mode in the Pipeline” on page 7-15 for information about additional conditions that must be specified on the server for any other type of authentication mode.

PAP-TOKEN is an extension of PAP authentication.

The Pipeline prompts the user for a dynamic password obtained from the security card, possibly along with a challenge key. The password is sent in the clear (via PAP), but because it’s a one-time-only password, this is not a serious security risk.

The response to the initial password challenge authenticates the base channel of the call. If bandwidth requirements cause another channel to come up, the user is challenged for a password whenever a channel is added to a call.

These are the parameters to configure in the Pipeline for PAP-TOKEN:

Table 7-9. PAP-TOKEN parameters

Location	Parameter
Ethernet→Connections→*any profile* → Encaps options...	Send Auth=PAP-TOKEN Send PW=*SECURE* (a password)

The Send Auth parameter specifies the authentication mode requested by the caller. The Send PW password is sent as part of the initial session negotiation. If the session presents a password challenge, the user types in their current one-time-only password obtained from the security card in response to that challenge.

Configuring PAP-TOKEN-CHAP mode

You can configure PAP-TOKEN-CHAP in the calling unit, but it is the RADIUS configuration on the answering side that determines which mode will actually be

used. If the RADIUS profile is not set up for PAP-TOKEN-CHAP, PAP-TOKEN will be used instead.

PAP-TOKEN-CHAP authenticates additional channels using CHAP.

The Pipeline prompts the user for a dynamic password obtained from the security card, possibly along with a challenge key. The initial password response (from the Send PW parameter) is used to authenticate the base channel of the call. It is sent unencrypted (via PAP).

When the Pipeline adds additional channels to the base channel of the call, PAP-TOKEN-CHAP uses CHAP authentication for the new channels. CHAP sends encrypted passwords, so it can take the password from the Aux Send PW parameter and transmit it securely.

These are the parameters to configure in the Pipeline for PAP-TOKEN-CHAP:

Table 7-10. PAP-TOKEN-CHAP parameters

Location	Parameter
Ethernet→Connections→*any profile* → Encaps options...	Send Auth=PAP-TOKEN-CHAP Send PW=*SECURE* (a password) Aux Send PW=*SECURE* (a password)

The Send Auth parameter specifies the authentication mode requested by the caller. See “Setting an authentication mode in the Pipeline” on page 7-15 for related information.

The Send PW password is sent as part of the initial session negotiation. If the session presents a password challenge, the user types in their current one-time-only password obtained from the security card in response to that challenge.

The Aux Send PW parameter is sent via CHAP for authenticating additional channels.

Configuring CACHE-TOKEN

CACHE-TOKEN uses CHAP and stores (“caches”) the initial password.

These are the parameters to be configured in the calling unit:

Table 7-11. CACHE-TOKEN parameters

Location	Parameter
Ethernet→Connections→*any profile* → Encaps options...	Send Auth=CACHE-TOKEN Send PW=*SECURE* (a password)

The Send Auth parameter specifies the authentication mode requested when initiating a security card authenticated connection (see "Setting an authentication mode in the Pipeline" on page 7-15).

The Send PW password is sent as part of the initial session negotiation. The password supplied by the user in response to the initial password challenge is used to authenticate the base channel of the call via CHAP. If the RADIUS server has been configured correctly, it caches that encrypted password for the specified period, or for the specified amount of idle time during the connection. When channels are added to the call or when a new call is made, it uses the cached password to authenticate them.

Using DHCP spoofing

For LAN-based computers, Dynamic Host Configuration Protocol (DHCP) is a standards-based protocol for dynamically allocating and managing IP addresses. DHCP runs between individual computers and a DHCP server to allocate and assign IP addresses to the computers as well as limit the time for which the computer can use the IP address. When the computer's "lease" is up on the address, it must communicate with the DHCP server again to obtain the IP address.

Using standard PAP or CHAP authentication and standard bridging protocols, DHCP can also be used across a dial-up connection just as if the DHCP server were on the local network. In a dial-up environment, a remote PC's request for an IP address causes the Pipeline to bring up a connection. The connection is authenticated and established before the DHCP server receives the request and responds accordingly.

Note: The Pipeline brings up a connection to the DHCP server because the Connection Profile to the DHCP server is a dial-on-broadcast type and the DHCP request is a broadcast packet. That is, Bridging=Yes in the Ethernet Profile, Mod Config submenu; and Route IP=No, Bridge=Yes, and Dial Brdcast=Yes in the Connection Profile.

An added complexity occurs in a dial-up environment when card-based security and the Ascend Password Protocol (APP) for Windows is in use. In such an environment, the call to the DHCP server occurs only after APP authentication. However, the Windows APP authentication requires an IP address, which the DHCP server is supposed to supply. In such a case, set up DHCP spoofing on the Pipeline.

DHCP spoofing works like this:

- If there is no authenticated dial-up session and the Pipeline receives a DHCP Discover packet, it responds with a DHCP Offer packet containing the configured (spoofed) IP address, netmask, and renewal time. This is quickly verified by an exchange between the client and the Pipeline. The renewal time is limited to a few seconds to ensure that the computer gets its *real* address from the remote DHCP server as soon as possible.
- The APP Server utility can run using only broadcast addresses, so that the Pipeline does not need a real IP address and the temporary "spoofed" address is not relied upon. See "APP Host" in Chapter 11, "Reference," for details.
- As soon as an authenticated dial-up link exists, the Pipeline refuses to renew the spoofed address, forcing the computer to get its real address from the remote DHCP server.

To enable DHCP spoofing, you need to configure the parameters shown in Table 7-12.

Table 7-12. DHCP spoofing parameters

Location	Parameter
Ethernet→Mod Config→DHCP Spoofing	DHCP Spoofing=Yes Spoof Adr=181.53.211.5 Renewal Time=10

Table 7-12. DHCP spoofing parameters

Location	Parameter
Ethernet→Mod Config	Bridging=Yes
Ethernet→Connections→*Connection Profile that dials the network with the DHCP server*	Bridge=Yes

- DHCP Spoofing

  When DHCP spoofing=Yes, the Pipeline can spoof a DHCP server for one IP address for the specified amount of time (Renewal Time).

- Spoof Adr

  Spoof Adr sets up the IP address and netmask assigned to the DHCP client when Pipeline performs DHCP spoofing. It must be a valid IP address on the local network.

- Renewal Time

  Renewal Time sets the lease time of the spoofed IP address. Enter a time in seconds from 3 to 65535. The default is 10.

Invoking password mode in the terminal server

A user can bring up a connection to the secure site in the usual way: by invoking a program that requires a connection to a host on that remote network, by using the DO menu in the Pipeline, or by dialing the remote NAS via modem.

Note: If the connection is brought up by modem, the process of responding to password challenges begins at Step 2, below.

Users can invoke password mode in a terminal server session by following these steps:

1. At the terminal server prompt, the user types:

   ```
   set password
   ```

   The following message is displayed:

   ```
   Entering Password Mode...
   ```

The prompt changes to the following:

```
[^C to exit] Password Mode>
```

2. The user brings up the connection.
3. While the connection is being negotiated, the remote NAS returns a challenge prompt that looks like this:

   ```
   From: hostname
   0-Challenge: challenge
   Enter next password:
   ```

4. The user enters the password obtained from his or her security card at the challenge prompt.

   A user has 60 seconds to enter the password correctly. If the password is entered correctly, the connection is established to the secure network. If the password is not entered within 60 seconds, the login attempt times out. If the password is entered incorrectly, the challenge prompt is displayed again up to three times.

   hostname is the name of the NAS called, such as an Ascend MAX, and it is optional on some systems. If the Send Auth parameter is configured incorrectly, no challenge prompt appears, or the user sees and error message such as this:

   ```
   From: hostname
   Received unexpected PAP Challenge!... check PPP Auth Mode
   ```

5. To return to normal terminal server operations, the user presses CTRL-C at the Password Mode prompt.

Configuring a connection with a local APP Server utility

To allow users to supply token passwords from a PC or UNIX host on the local network, you must configure the Pipeline to communicate with the APP Server utility on that host. APP is a UDP protocol whose default port is 7001. The communication between the Pipeline and the host running the APP Server may be unicast (when both the Pipeline and the host have an IP address) or broadcast (when the host may not have an IP address).

The APP parameters are shown in Table 7-13.

Table 7-13. APP Server-specific parameters

Location	Parameter
Ethernet→Mod Config→Auth...	APP Server=Yes APP Host=10.65.212.1 APP Port=7001

- APP Server

  Set this parameter to yes to enable the Pipeline to communicate password challenges to the host running the APP Server utility.

- APP Host

  Specify the IP address of the host running the APP Server utility on the local IP network. If the host obtains its address at boot time from a BOOTP or DHCP server, or if it has no IP address, you can specify the IP broadcast address in this parameter (255.255.255.255).

- APP Port

  Use the default UDP port number, 7001, unless it is already in use. If you change this number, you must specify the new UDP port number in the APP Server utility (DOS), the WIN.INI file (Windows), or /etc/services (UNIX). The Pipeline and the host running the APP Server utility must agree about the UDP port number.

Enabling users to respond to password challenges

Users can respond to the password challenges presented by an ACE or SAFEWORD server from a Windows or Unix host running the APP Server utility. One session window on the calling side displays password challenges and allows the user to type in the appropriate response. Only one host on the network can run the APP Server utility.

Using the APP Server on a UNIX host

The APP Server utility for UNIX enables a user to respond to token password challenges received from a remote NAS. You can download this utility from ftp.ascend.com.

This section describes how to install and run the APP Server utility on a UNIX host. When a user on the LAN starts an application that requires a connection to a host on a secure network, the Pipeline initiates a call transparently (as usual). After the initial session negotiation, the remote NAS returns a password challenge that looks similar to this:

```
From: hostname
0-Challenge: challenge (or null challenge, depending on
your setup)
Enter next password:
```

This prompt is displayed in the APP Server screen on the UNIX host. A user has 60 seconds to obtain the current dynamic password from the security card and enter it correctly. If the password is entered correctly, the connection is established to the secure network. If the password is not entered within 60 seconds, the login attempt times out. If the password is entered incorrectly, the challenge prompt is displayed again up to three times.

To install and run the APP Server utility on a UNIX host:

1 Download the APP Server files from ftp.ascend.com to the UNIX host.

2 Decompress (gunzip) and separate (tar) the files.

3 Edit the Makefile appropriately for your operating system and compiler.

4 Compile the appsrvr source file (make).

5 Add a line to /etc/services assigning UDP port 7001 to the appServer.

If you can use the default port 7001 (if it is not already assigned), add this line to /etc/services to document that the port is now in use:

appServer<tab>7001/udp

If port 7001 is already assigned to a different purpose, you can use a different port for the APP Server utility by adding a line such as this to the services file:

appServer<tab>*nnn*/udp

where *nnn* is the port number to be used. Make sure that the Pipeline configuration agrees with this number (see “Configuring a connection with a local APP Server utility” on page 7-21).

6 If the UNIX host has an IP address, you can run the utility in unicast mode by typing this command at the UNIX prompt:

./appsvr

When you run the utility in unicast mode, it transmits packets on the specified UDP port with the source address set to its own IP address. When the Pipeline receives those packets on the specified UDP port, it returns packets to that IP address.

7 If the UNIX host does *not* have an IP address (for example, if it obtains its address from a BOOTP or DHCP server), run the utility in broadcast mode instead by typing this command:

./appsrvr –b

The –b option sets a socket option to allow broadcast transmissions and inhibits the utility's complaints about receiving invalid APP frame types when it receives when it receives its own transmissions.

Note: On some UNIX systems, you need root privileges to run the APP Server utility in broadcast mode. (Some hosts disallow broadcast transmissions without root privileges.) If you are running the utility in broadcast mode, make sure that the Pipeline is configured with the broadcast address in the APP Host parameter (APP Host=255.255.255.255).

Note: If your Pipeline does not have an IP address, set IP Adrs=0.0.0.0/0 and Bridging=Yes (in the Ethernet Profile, Mod Config submenu) and set Route IP=No, Dial Brdcast=Yes, and Bridge=Yes (in the Connection Profile used to reach the DHCP server.

Using the APP Server utility on a DOS or Windows host

The APP Server utility for Windows or DOS enables a user to respond to token password challenges received from a remote NAS. You can download the utility from ftp.ascend.com.

This section describes how to install and run the APP Server utility on a PC running Windows or DOS. When a user on the LAN starts an application that requires a connection to a host on the secure network, the Pipeline initiates a call transparently (as usual). After the initial session negotiation, the remote NAS returns a password challenge.

If the PC is running DOS, the password challenge looks similar to this:

```
Ascend Password Server Module vX.X
Requester: hostname
Request: challenge (or null challenge, depending on your
setup)
```

```
Enter password:
```

If the PC is running Windows, the challenge is displayed in the AppServer window. It has the same fields as the DOS prompt shown immediately above, but it is in a graphic format.

Two APP Server executables are available for PC-compatible systems:

- APPSRVR1.EXE

  This program provides a “one-shot” authentication mechanism that occurs only when the PC is booted. It does not require an IP address or TCP/IP stack in the DOS system.

  APPSRVR1.EXE is executed from AUTOEXEC.BAT as part of system startup. It can be used to authenticate a connection that has begun transparently or it can bring up a connection to the remote NAS.

  APPSRVR1.EXE builds an IP header and sends broadcast packets via the ODI driver to the Pipeline, passing it the name and IP address of a Connection Profile. The Pipeline must be configured with the broadcast address in the APP Host parameter (APP Host= 255.255.255.255).

  Note: If your Pipeline does not have an IP address, set IP Adrs=0.0.0.0/0 and Bridging=Yes (in the Ethernet Profile, Mod Config submenu) and set Route IP=No, Dial Brdcast=Yes, and Bridge=Yes (in the Connection Profile used to reach the DHCP server.

- APPSRVR2.EXE

  This program is a Windows application. It can be used to authenticate a connection that has begun transparently or it can bring up a connection to the remote NAS.

  APPSRVR2.EXE is typically launched at system startup and remains open on the Windows system. You can launch it manually by double-clicking its icon, or include it in the Startup group. It has a Connect button for initiating a connection, and will prompt for a password when it is needed.

Installing the APP Server utility for DOS

To provide authentication from a DOS system, install only APPSRVR1.EXE. Users must reboot the PC to initiate a connection to the secure network.

Note: APPSRVR1.EXE does not require an IP stack or IP address, but it does require an ODI driver.

1. Create an \ASCEND directory below the root directory.
2. Copy APPSRVR1.EXE into that directory.
3. Open AUTOEXEC.BAT and add a command line invoking APPSRVR1.EXE.

   The command line for APPSRVR1.EXE must be positioned after the line invoking the network ODI driver and *before* the network protocol stack (TCIP or IPX or other supported protocol). For example:

```
C:\NOVELL\LSL.COM
C:\NOVELL\XXXODI.COM
C:\ASCEND\APPSRVR1.EXE
REM Protocol Stack is loaded next
```

The APPSRVR1.EXE command line can include the options shown in Table 7-14.

Table 7-14. Options for the APPSRVR1.EXE command line

Option	Effect
`/tss`	Set seconds between connection attempts, where *ss*=number of seconds (example: t135; default: 20 secs.)
`/ykk`	Set number of times the PC attempts to connect before timeout, where *kk*=number of attempts (example: y4)
`/mxx`	Set host MAC address in decimal format, where *xx*=MAC address in decimal format of the PC running appsrv1 (default: zero)
`/pmm`	Set UDP port number (mm—default: 7001). See the note below.
`/bnn`	Set UDP port number (nn) broadcast at startup (default: same port as APPSRVR1.EXE). See the note below.
`/cyy`	Sets name of Connection Profile called on startup. If the Connection Profile is not specified in AUTOEXEC.BAT by using this option, the utility prompts the user for the name of the profile.
`/f`	Suppress call on startup (default: force call on startup)
`/d`	Disconnect call
`/?`	Display APPSRVR1.EXE help screen.

Note: The PC sends a broadcast UDP packet that has the destination and the source port 7001 unless you specify otherwise with the /p or /b options. If you specify a number other than 7001 in the APP Port parameter, you must use one of these options to specify the same port.

Installing the APP Server utility for Windows

To provide authentication under Windows, you can install one or both of the APPSRVR utilities.

- Install APPSRVR1.EXE…

  If the Windows PC does not have a TCP/IP stack, install only APPSRVR1.EXE. Do not install APPSRVR2.EXE, which requires IP.

  You may want to install APPSRVR1.EXE even if the PC has a stack, to enable a user to authenticate a call before Windows has been started.

- Install APPSRVR2.EXE…

  Install this program if the Windows PC has a TCP/IP stack.

Note: If the Windows PC has an IP stack without an IP address, see "Using DHCP spoofing" on page 7-18 or install APPSRV1.EXE.

To install both programs on the Windows PC:

1. Create an \ASCEND directory below the root directory.
2. Copy APPSRVR1.EXE, APPSRVR2.EXE, and CTL3D.DLL into that directory.

   If you have decided not to install APPSRVR1.EXE, don't copy it into the directory and skip the next step.
3. Open AUTOEXEC.BAT and add a command line invoking APPSRVR1.EXE.

   See "Installing the APP Server utility for DOS" on page 7-25 for details.
4. Create a new program group in your Program Manager.

   Choose File→New→Program Group and type "Ascend".
5. Create an icon for APPSRVR2.EXE in your Program Manager.

   Choose File→New→Program Item.
6. To launch the APP Server utility when you start Windows, place the APPSRVR2.EXE icon in your Startup group.

If you prefer not to add the APP Server utility to your Startup group, you can launch the utility manually by double-clicking its icon.

Specifying banner text

You can specify banner text that the Windows or DOS APP Server displays when a user is prompted for a password.

To specify the text, you must modify the ASCI I text file called APPSRVR.INI using any DOS or Windows editor. You can enter up to 200 characters; different portions of the text can appear on different lines, separated by line feeds. The file can reside in either the current directory or the Windows directory. DOS looks for the file in the current directory; if it cannot find the file there, it looks for it in the Windows directory. Windows always looks for the file in the Windows directory.

In Windows, the file is read during initialization and the text is displayed in a dialog box with the password prompt. In the DOS version, the text is simply displayed before the password prompt.

Using Filters

8

This chapter covers these topics:

Ascend filter parameters

Table 8-1 shows configuration parameters related to filters.

Table 8-1. Filter configuration parameters

Location	Parameters with default values
Ethernet→Connections→*any profile*→Session options…	Call Filter=0 Data Filter=0 Idle=120
Ethernet→Filters→*any filter*	Name=[] Input filters... Output filters...
Ethernet→Filters→*any profile*→Input filters→ 01 to 12 Ethernet→Filters→*any profile*→Output filters→ 01 to 12	Valid=No Type=GENERIC Generic... Ip...
Ethernet→Filters→*any profile*→Input filters→ 01 to 12→Generic Ethernet→Filters→*any profile*→Output filters→ 01 to 12→Generic	Forward=No Offset=0 Length=0 Mask=0000000000000000 Value=0000000000000000 Compare=Equals More=No

Table 8-1. Filter configuration parameters

Location	Parameters with default values
Ethernet→Filters→*any profile*→Input filters→ 01 to 12→Ip Ethernet→Filters→*any profile*→Output filters→ 01 to 12→Ip	Forward=No Src Mask=0.0.0.0 Src Adrs=0.0.0.0 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
Ethernet→Answer→Sessions options...	Call Filter=0 Data Filter=0 Idle=120
Ethernet→Mod Config→Ether options…	Filter=0

For details on each parameter, see Chapter 11, "Reference."

Introduction to Ascend filters

Ascend packet filtering allows for independent filters on a per-connection and per-interface basis for call establishment and clearing, as well as transmit and receive data. Each Filter Profile associated with an interface consists of an ordered list of Output or Input filters (or both) that will be applied to every packet sent or received by the Pipeline on that interface.

Note: For information about IPX SAP filters, which affect which NetWare services the Pipeline adds to its service table, see Chapter 6, "Configuring the Pipeline as an IPX Router."

Call filters for managing costs

The Pipeline has an Idle Timer that can be set in the Session Options submenu of a Connection Profile and the Answer Profile. By default, the Idle Timer is set to two minutes. It is restarted by active traffic. If the configured amount of idle time elapses without any active traffic on that connection, the Pipeline clears the call. Table 8-2 shows the Idle Timer parameters.

Table 8-2. Idle Timer parameters

Location	Parameters
Ethernet→Connections→*any profile*→ Sessions options…	Idle=120
Ethernet→Answer→Session options...	Idle=120

Call filters let you define which packets will not restart the Idle Timer, so only valid traffic keeps a connection up. Packets defined in a call filter cannot restart the Idle Timer or initiate a call.

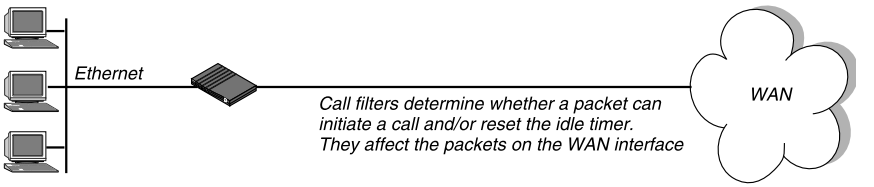


Figure 8-1. Call filters

To apply a call filter to the WAN interface, specify the Filter Profile number in the Session Options submenu of a Connection Profile or Answer Profile. Table 8-3 shows the parameters for applying a call filter.

Table 8-3. Applying a call filter

Location	Parameters
Ethernet→Connections→*any profile*→ Sessions options…	Call Filter=1
Ethernet→Answer→Session options...	Call Filter=2

The Call Filter parameters "plug in" a filter that defines which packets will initiate a call or reset the idle timer once a call across the WAN has been established. If it is set to zero, no filter is applied. To apply a filter, specify its number (between 1 and 12) in the Filters parameter. See "How a Filter Profile is organized" on page 8-6 for an example.

Note: When you apply a filter to the WAN interface, the filter takes effect only when the connection goes from an offline state to a call-placed state.

Data filters for affecting the data stream

Filters can also be applied to the data stream on the Ethernet or WAN interface, for example, to drop packets addressed to particular hosts or to prevent broadcasts from going across the WAN. A filter used in that way is called a data filter.

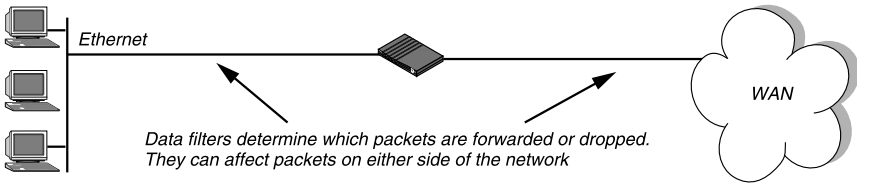


Figure 8-2. Data filters

To apply a data filter to the WAN interface, specify the Filter Profile number in the Session Options submenu of a Connection Profile or Answer Profile. To apply a data filter to the Ethernet interface, specify its number in the Ether Options submenu of the Ethernet Profile. Table 8-4 lists the parameters for applying a data filter.

Table 8-4. Applying a data filter

Location	Parameters
Ethernet→Connections→*any profile*→ Sessions options…	Data Filter=5
Ethernet→Answer→Sessions options...	Data Filter=7
Ethernet→Mod Config→Ether options…	Filter=1

Note: A data filter in a Connection Profile does not affect the answering process.

When you apply a filter to the WAN interface (Connection or Answer Profile), the filter takes effect only when the connection goes from an offline state to a call-placed state. However, when you apply a filter to the Ethernet interface, it takes effect immediately. If you change the Filter Profile definition, the new filters apply as soon as you save the Filter Profile.

How a Filter Profile is organized

Figure 8-3 shows how filters are organized in the menu interface, and the terminology used to describe each part of a filter.

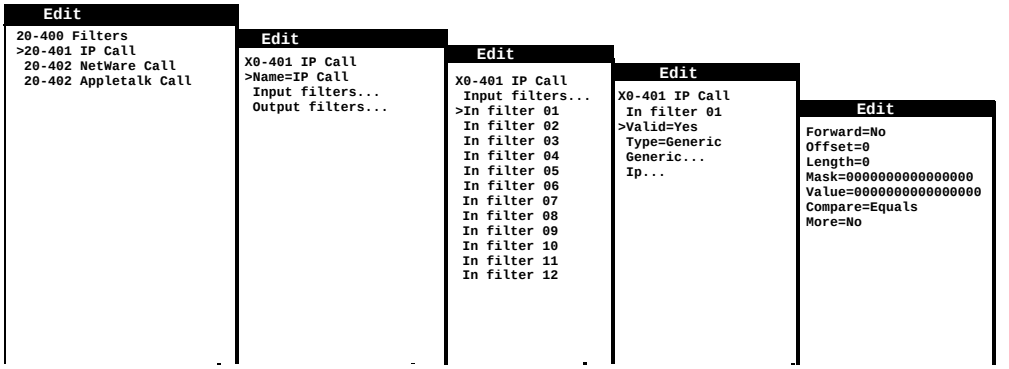


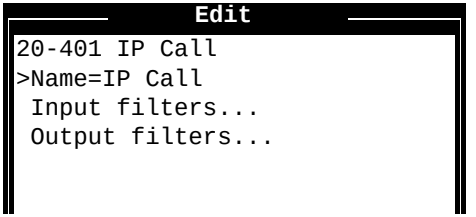
Figure 8-3. Filter terminology

The Filters menu contains a list of Filter Profiles, which are numbered from 1 to 12. When applying a filter, you identify it by number, not by its name in this list. For example, to apply the IP Call filter, specify number 1.

Each Filter Profile has these components:

- Input or output filters (or both)
- Generic or IP filters (or both)

At the top level of a Filter Profile, you can assign a name and choose between Input or Output filters.

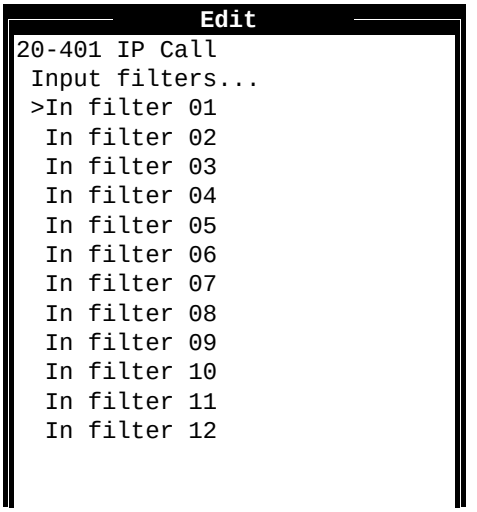


Input or output filters

Each Filter Profile can include both Input filters (which are applied only to inbound packets) and Output filters (which are applied only to outbound packets).

Input filters applied to the Ethernet interface block packets from the Ethernet *into* the Pipeline; Output filters applied to the Ethernet interface block packets from the Pipeline *out* to the Ethernet. Similarly, Input filters applied on the WAN side (in a Connection or Answer Profile) block packets from the WAN into the Pipeline; Output filters applied to the WAN side block packets from the Pipeline *out* to the WAN.

Input filters and Output filters are identical in structure: up to 12 filters can be defined and these filters are applied in the order in which they appear (01 followed by 02, and so forth).



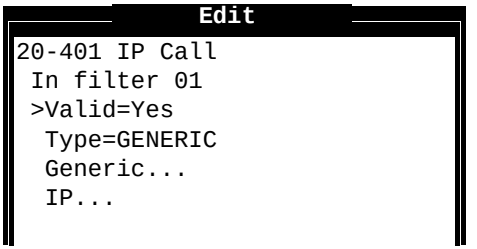
You can define each filter to either *forward* or *block* packets, or to allow/prevent a call to be placed or maintained.

The filters you define are applied to a packet in the order in which they appear in this list, provided that each filter has the Valid parameter set to Yes. Setting the Valid parameter to No in a filter prevents it from being applied.

If only Input filters are defined, the default action for Output filters is to forward all packets or to allow all packets to reset the timer. The same is true in the other direction, if you define only Output filters, the default action for inbound packets is to forward them and allow them to reset the timer.

Generic or IP filters

When you open a filter, you can set the Valid parameter to Yes and select the type of the packet conditions to be defined (Generic or IP).



- Generic filters define bits and bytes within a packet.
  Generic filters can apply to any packet type, including TCP or IP.
- IP filters define conditions related to the TCP/IP/UDP protocol suite only.

Generic filters

If the Type parameter in a filter is set to GENERIC, you can define generic conditions, which can occur in any type of packet. Table 8-5 shows the filter conditions you may specify in a generic filter.

Table 8-5. Generic filter conditions

Location	Parameters
Ethernet→Filters→*any profile*→Input filters→ 01 to 12→Generic Ethernet→Filters→*any profile*→Output filters→ 01 to 12→Generic	Forward=No Offset=0 Length=0 Mask=0000000000000000 Value=0000000000000000 Compare=Equals More=No

For details on these parameters, see Chapter 11, "Reference."

The Forward parameter determine whether the Pipeline will forward a packet if it matches the definition (Forward=Yes) or drop the packet if it matches (Forward=No).

The Offset, Length, Mask, and Value parameters are used to define the location and contents of certain bytes within a packet.

The Compare parameter specifies how a packet's contents are compared to the value specified in this filter. After applying the Offset, Mask, and Length values to reach the appropriate location in a packet, the contents of that location are compared to the Value parameter. If Compare is set to Equals (the default), the filter is applied if the packet data are identical to the specified value. If Compare is set to NotEquals, the filter is applied if the packet data are not identical.

The More parameter specifies whether the current filter is linked to the one immediately following it. If More=Yes, the filter can examine multiple non-contiguous bytes within a packet, by "marrying" the current filter to the next one, so that the next filter is applied before the Forward decision is made. The match occurs only if *both* non-contiguous bytes contain the specified values. If More=No, the Forward decision is based on whether the packet matches the definition in this one filter.

IP filters

If the Type parameter is set to IP, you can define filter conditions related only to TCP/IP/UDP data packets (including bridged packets). An IP filter examines source addresses, destination addresses, IP protocol type and port, or a combination of these. Table 8-6 shows the filter conditions you may specify in an IP filter.

Table 8-6. IP filter conditions

Location	Parameters
Ethernet→Filters→*any profile*→Input filters→ 01 to 12→Ip Ethernet→Filters→*any profile*→Output filters→ 01 to 12→Ip	Forward=No Src Mask=0.0.0.0 Src Adrs=0.0.0.0 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

For details on these parameters, see Chapter 11, “Reference.”

The Forward parameter determines whether the Pipeline will forward a packet if it matches the definition (Forward=Yes) or drop the packet if it matches (Forward=No).

The source and destination Mask and Adrs parameters specify the contents of the source or destination fields in a packet. You can use the Mask parameter to mask out portions of the source or destination address, for example, to mask out the host number.

The Protocol parameter is used to identify a specific TCP/IP protocol; for example, 6 specifies TCP packets. 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. A list of the most common protocol numbers is also listed in Chapter 11, “Reference.”

- 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

The source and destination Port Cmp and Port # parameters specify whether to compare the protocol ports, which identify the application running over TCP/IP.

The TCP Estab parameter can be set to match a packet only if a TCP session is already established.

An example: Defining a filter

This section shows how to define a data filter and apply it to a WAN connection. The purpose of this data filter is to prevent “spoofing” of IP addresses. “Spoofing” IP addresses—not to be confused with watchdog or DHCP spoofing described elsewhere in this manual—is a technique whereby outside users pretend to be from the local network in order to obtain unauthorized access to the network.

This example data filter contains three Input filters (applied to inbound packets) and one Output filter (applied to outbound packets).

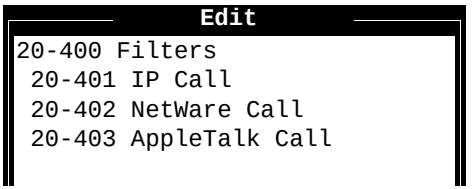
The Input filters specify the local IP network and the loopback (127.0.0.0) network address. In effect, these filters say: "If you see an inbound packet with one of these source addresses, drop the packet." The third Input filter then defines every other source address (0.0.0.0) and specifies "Forward everything else to the local network."

The Output filter defines the local IP network address and specifies: "If the outbound packet has a source address on the local network, forward it; otherwise, drop it." All outbound packets with a non-local source address will be dropped.

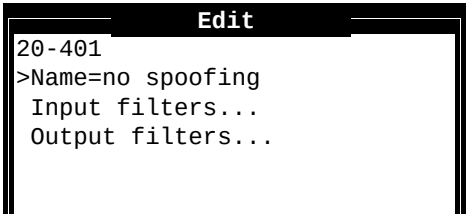
Note: This example assumes a local IP network address of 192.100.50.128, with a subnet mask of 255.255.255.192. Of course, you should use your own local IP address and netmask when defining a Filter Profile.

1 Select an Filter Profile in the Filters menu and press Enter, for example, IP Call.

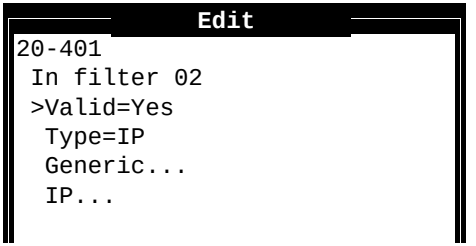
Note: Because the Pipeline only supports 3 filters, this example modifies the predefined IP Call filter. See "Predefined Filter Profiles" on page 8-17 for information about predefined filters.



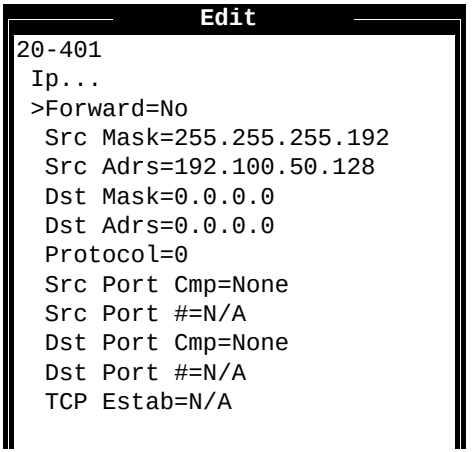
2 Assign a name to the Filter Profile, for example, Name="no spoofing".



3 Select Input Filters and then open In filter 02.



4 Set Valid=Yes and Type=IP, and then open the IP submenu. and specify the following conditions:



This filter prevents packets with a local IP address from coming into the Pipeline from the WAN. It does so by specifying the local net mask and IP address in the Src Mask and Src Adrs fields. If an incoming packet has the local address, it will not be forwarded onto the Ethernet. The destination address of incoming packets is not screened.

5 Exit the current Input filter, saving your changes. Then, select In filter 03.

6 Set Valid=Yes and Type=IP, and then open the IP submenu and specify the following conditions:

```
Edit
20-401
 Ip...
 >Forward=No
  Src Mask=255.0.0.0
  Src Adrs=127.0.0.0
  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
```

This filter prevents incoming packets with the loopback address (the "local host" net address). Like the first filter, it uses only the Src Mask and Src Adrs fields to do so.

7 Exit the current Input filter, saving your changes. Then, select In filter 04.

8 Set Valid=Yes and Type=IP, and then open the IP submenu and specify the following conditions:

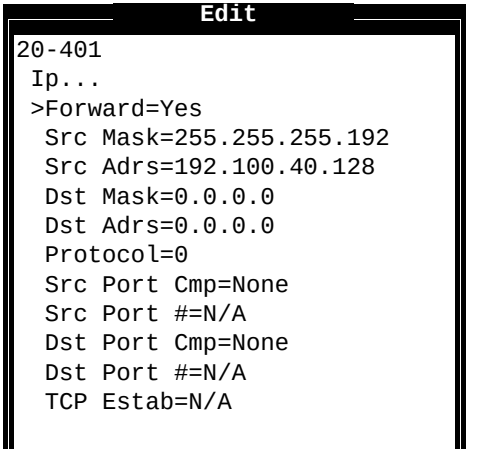
```
Edit
20-401
 Ip...
 >Forward=Yes
  Src Mask=0.0.0.0
  Src Adrs=0.0.0.0
  Dst Mask=0.0.0.0
  Dst Adrs=0.0.0.0
  Protocol=0
  Src Port Cmp=None
  Src Port #=N/A
  Dst Port Cmp=None
  Dst Port #=N/A
  TCP Estab=N/A
```

This third filter allows all other incoming IP packets to be forwarded to the Ethernet interface.

9 Press Esc, saving your changes, and return to the top level of the "no spoofing" Filter Profile.

10 Open the Output filters menu, and select Out filter 02.

11 Set Valid=Yes and Type=IP, and then open the IP submenu and specify the following conditions:



This filter forwards all outbound packets with the local IP address as the source address.

12 Press Esc as necessary to return to the Ethernet menu, saving your changes.

13 Open a Connection Profile in which you want to apply the new filter. Open the Session Options submenu in that Connection Profile.

14 Set Data Filter=4 (or whatever filter number you choose).

15 Save the modified Connection Profile.

Now you must hang up the connection and let it re-establish for the filter to take effect. You can do this when the Connection Profile is open by pressing Ctrl-D to open the DO menu, and then selecting "2 Hang Up." Then, press Ctrl-D again and select "1 Dial."

Predefined Filter Profiles

The Pipeline ships with three predefined Filter Profiles, one for each commonly used protocol suite. These predefined filters are intended as call filters, to help keep connectivity costs down. They provide a base that you can build on to fine-tune how the Pipeline handles routine traffic on your network.

NetWare Call filter

The predefined NetWare Call filter is designed to prevent SAP (Service Advertising Protocol) packets originating on the local IPX network from resetting the Idle Timer or initiating a call.

Note: In NetWare 4.0 and later, built-in directory services eliminates the need for SAP. Services are located through directory services instead.

In NetWare 3.x, NetWare servers broadcast SAP packets every 60 seconds to make sure that all routers and bridges know about available services. To prevent these packets from keeping a connection up unnecessarily, apply the predefined NetWare Call filter in the Session Options submenu of Connection Profiles in which IPX routing is configured.

Output filters in NetWare Call

The predefined NetWare Call filter contains six Output filters, which identify outbound SAP packets and prevent them from resetting the Idle Timer or initiating a call.

```
Out filter 01...Generic...Forward=No
Out filter 01...Generic...Offset=14
Out filter 01...Generic...Length=3
Out filter 01...Generic...Mask=ffffff000000000000
Out filter 01...Generic...Value=e0e0030000000000
Out filter 01...Generic...Compare=Equals
Out filter 01...Generic...More=Yes

Out filter 02...Generic...Forward=No
Out filter 02...Generic...Offset=27
Out filter 02...Generic...Length=8
```

```
Out filter 02...Generic...Mask=ffffffffffff
Out filter 02...Generic...Value=fffffffffff0452
Out filter 02...Generic...Compare=Equals
Out filter 02...Generic...More=Yes

Out filter 03...Generic...Forward=No
Out filter 03...Generic...Offset=47
Out filter 03...Generic...Length=2
Out filter 03...Generic...Mask=ffff000000000000
Out filter 03...Generic...Value=0002000000000000
Out filter 03...Generic...Compare=Equals
Out filter 03...Generic...More=No

Out filter 04...Generic...Forward=No
Out filter 04...Generic...Offset=12
Out filter 04...Generic...Length=4
Out filter 04...Generic...Mask=fc00ffff00000000
Out filter 04...Generic...Value=0000ffff00000000
Out filter 04...Generic...Compare=Equals
Out filter 04...Generic...More=Yes

Out filter 05...Generic...Forward=No
Out filter 05...Generic...Offset=24
Out filter 05...Generic...Length=8
Out filter 05...Generic...Mask=ffffffffffffffff
Out filter 05...Generic...Value=fffffffffff0452
Out filter 05...Generic...Compare=Equals
Out filter 05...Generic...More=Yes

Out filter 06...Generic...Forward=No
Out filter 06...Generic...Offset=44
Out filter 06...Generic...Length=2
Out filter 06...Generic...Mask=ffff000000000000
Out filter 06...Generic...Value=0002000000000000
Out filter 06...Generic...Compare=Equals
Out filter 06...Generic...More=No
```

Extending the predefined filter for RIP packets

To extend the NetWare Call filter to also prevent IPX RIP packets from resetting the Idle Timer or initiating a call, you can define the following additional Output filters:

```
Out filter 07...Generic...Forward=No
Out filter 07...Generic...Offset=0
Out filter 07...Generic...Length=6
Out filter 07...Generic...Mask=ffffffffffff0000
Out filter 07...Generic...Value=ffffffffffff0000
Out filter 07...Generic...Compare=Equals
Out filter 07...Generic...More=Yes

Out filter 08...Generic...Forward=No
Out filter 08...Generic...Offset=24
Out filter 08...Generic...Length=8
Out filter 08...Generic...Mask=ffffffffffff
Out filter 08...Generic...Value=ffffffffffff0453
Out filter 08...Generic...Compare=Equals
Out filter 08...Generic...More=No

Out filter 09...Generic...Forward=No
Out filter 09...Generic...Offset=0
Out filter 09...Generic...Length=6
Out filter 09...Generic...Mask=ffffffffffff0000
Out filter 09...Generic...Value=ffffffffffff0000
Out filter 09...Generic...Compare=Equals
Out filter 09...Generic...More=Yes

Out filter 10...Generic...Forward=No
Out filter 10...Generic...Offset=27
Out filter 10...Generic...Length=8
Out filter 10...Generic...Mask=ffffffffffffffff
Out filter 10...Generic...Value=ffffffffffff0453
Out filter 10...Generic...Compare=Equals
Out filter 10...Generic...More=No

Out filter 11...Generic...Forward=Yes
Out filter 11...Generic...Offset=0
Out filter 11...Generic...Length=0
Out filter 11...Generic...Mask=0000000000000000
Out filter 11...Generic...Value=0000000000000000
Out filter 10...Generic...Compare=Equals
Out filter 11...Generic...More=No
```

Defining a SNEP data filter for Ethernet

NetWare's copy-protection scheme makes use of SNEP (Serialization Number Exchange Protocol) packets, which are sent and received by all servers on the network. SNEP packets occur as request/response pairs between servers. When NetWare servers are supported on both sides of the WAN, these packet exchanges can keep an IPX connection active unnecessarily.

This example SNEP filter is intended to be applied as a data filter on the Ethernet interface. To create a SNEP data filter for the Ethernet interface of the Pipeline, create a new Filter Profile and define the following Input filters:

```
In filter 01...Generic...Forward=No
In filter 01...Generic...Offset=30
In filter 01...Generic...Length=2
In filter 01...Generic...Mask=ffff000000000000
In filter 01...Generic...Value=0457000000000000
In filter 01...Generic...Compare=Equals
In filter 01...Generic...More=No

In filter 02...Generic...Forward=No
In filter 02...Generic...Offset=33
In filter 02...Generic...Length=2
In filter 02...Generic...Mask=ffff000000000000
In filter 02...Generic...Value=0457000000000000
In filter 02...Generic...Compare=Equals
In filter 02...Generic...More=No

In filter 03...Generic...Forward=Yes
In filter 03...Generic...Offset=0
In filter 03...Generic...Length=0
In filter 03...Generic...Mask=0000000000000000
In filter 03...Generic...Value=0000000000000000
In filter 03...Generic...Compare=Equals
In filter 03...Generic...More=No
```

If you have enough Output filters available in the NetWare Call filter (for example, if you don't extend the filter to include RIP as described in "Extending the predefined filter for RIP packets" on page 8-18), or if you're using NetWare 4.0 or higher and you don't need the predefined SAP filters, you could choose instead to include these SNEP filters as Output filters in the Call Filter.

IP Call filter

The predefined IP Call filter prevents inbound packets from resetting the Idle Timer. It does not prevent any type of outbound packets from resetting the timer or placing a call.

Input and Output filters

The IP Call filter contains one Input filter, which defines all inbound packets, and one Output filter, which defines all outbound packets (all outbound packets destined for the remote network specified in the Connection Profile in which the filter is applied.)

```
In filter 01...Generic...Forward=No
In filter 01...Generic...Offset=0
In filter 01...Generic...Length=0
In filter 01...Generic...Mask=0000000000000000
In filter 01...Generic...Value=0000000000000000
In filter 01...Generic...Compare=Equals
In filter 01...Generic...More=No

Out filter 01...Generic...Forward=Yes
Out filter 01...Generic...Offset=0
Out filter 01...Generic...Length=0
Out filter 01...Generic...Mask=0000000000000000
Out filter 01...Generic...Value=0000000000000000
Out filter 01...Generic...Compare=Equals
Out filter 01...Generic...More=No
```

Another example IP filter

This section describes an IP data filter that illustrates some of the issues you'll need to consider when writing your own IP filters. The example filter does not address fine points of network security. You may want to use this example filter as a starting point and augment it to address your security requirements.

In this example, the local network supports a Web server and the administrator needs to provide dial-in access to the server's IP address while restricting dial-in traffic to all other hosts on the local network. However, many local IP hosts need to dial out to the Internet and use IP-based applications such as Telnet or FTP,

which means that their response packets need to be directed appropriately to the originating host. In this example, the Web server's IP address is 192.9.250.5.

This filter would be applied as a data filter in Connection Profiles.

```
In filter 01...Ip...Forward=Yes
In filter 01...Ip...Src Mask=0.0.0.0
In filter 01...Ip...Src Adrs=0.0.0.0
In filter 01...Ip...Dst Mask=255.255.255.255
In filter 01...Ip...Dst Adrs=192.9.250.5
In filter 01...Ip...Protocol=6
In filter 01...Ip...Src Port Cmp=None
In filter 01...Ip...Src Port #=N/A
In filter 01...Ip...Dst Port Cmp=Eql
In filter 01...Ip...Dst Port #=80
In filter 01...Ip...TCP Estab=No

In filter 02...Ip...Forward=Yes
In filter 02...Ip...Src Mask=0.0.0.0
In filter 02...Ip...Src Adrs=0.0.0.0
In filter 02...Ip...Dst Mask=0.0.0.0
In filter 02...Ip...Dst Adrs=0.0.0.0
In filter 02...Ip...Protocol=6
In filter 02...Ip...Src Port Cmp=None
In filter 02...Ip...Src Port #=N/A
In filter 02...Ip...Dst Port Cmp=Gtr
In filter 02...Ip...Dst Port #=1023
In filter 02...Ip...TCP Estab=No

In filter 03...Ip...Forward=Yes
In filter 03...Ip...Src Mask=0.0.0.0
In filter 03...Ip...Src Adrs=0.0.0.0
In filter 03...Ip...Dst Mask=0.0.0.0
In filter 03...Ip...Dst Adrs=0.0.0.0
In filter 03...Ip...Protocol=17
In filter 03...Ip...Src Port Cmp=None
In filter 03...Ip...Src Port #=N/A
In filter 03...Ip...Dst Port Cmp=Gtr
In filter 03...Ip...Dst Port #=1023
In filter 03...Ip...TCP Estab=No
```

```
In filter 04...Ip...Forward=Yes
In filter 04...Ip...Src Mask=0.0.0.0
In filter 04...Ip...Src Adrs=0.0.0.0
In filter 04...Ip...Dst Mask=0.0.0.0
In filter 04...Ip...Dst Adrs=0.0.0.0
In filter 04...Ip...Protocol=1
In filter 04...Ip...Src Port Cmp=None
In filter 04...Ip...Src Port #=N/A
In filter 04...Ip...Dst Port Cmp=None
In filter 04...Ip...Dst Port #=N/A
In filter 04...Ip...TCP Estab=No
```

The first Input filter specifies the Web server's IP address as the destination and sets IP forward to Yes, so all IP packets received with that destination address will be forwarded.

The second Input filter specifies TCP packets (Protocol=6) *from* any address and *to* any address and forwards them if the destination port is greater than the source port. For example, Telnet requests go out on port 23 and responses come back on some random port greater than port 1023. So, this filter defines packets coming back to respond to a user's request to Telnet (or to other requests using the TCP protocol) to a remote host.

The third Input filter specifies UDP packets (Protocol=17) with exactly the same situation as described above for Telnet. For example, a RIP packet is sent out as a UDP packet to destination port 520. The response to this request also is sent to a random destination port greater than 1023.

Finally, the fourth Input filter specifies unrestricted pings and traceroutes. ICMP does not use ports like TCP and UDP so, so a port comparison would be meaningless.

AppleTalk Call filter

The AppleTalk Call filter instructs the Pipeline to place a call and reset the Idle Timer based on AppleTalk activity on the LAN, but to prevent inbound packets or AppleTalk Echo (AEP) packets from resetting the timer or initiating a call. It includes one Input filter and five Output filters.

The Input filter prevents inbound AppleTalk packets from resetting the Idle Timer or initiating a call.

The first two Output filters identify the AppleTalk Phase II AEP protocol, and the next two Output filters identify AppleTalk Phase I AEP protocol. Because More is set to Yes in the first and No in the second filter of these two pairs, a packet has to meet the criteria defined in both filters to be considered a match.

The last Output filter tells the Pipeline to allow all other outbound packets to reset the Idle Timer or initiate a call.

```
In filter 01...Generic...Forward=No
In filter 01...Generic...Offset=0
In filter 01...Generic...Length=0
In filter 01...Generic...Mask=0000000000000000
In filter 01...Generic...Value=0000000000000000
In filter 01...Generic...Compare=Equals
In filter 01...Generic...More=No

Out filter 01...Generic...Forward=No
Out filter 01...Generic...Offset=14
Out filter 01...Generic...Length=8
Out filter 01...Generic...Mask=ffffff000000ffff
Out filter 01...Generic...Value=aaaa03000000809b
Out filter 01...Generic...Compare=Equals
Out filter 01...Generic...More=Yes

Out filter 02...Generic...Forward=No
Out filter 02...Generic...Offset=33
Out filter 02...Generic...Length=2
Out filter 02...Generic...Mask=ffff0000000000000
Out filter 02...Generic...Value=0404000000000000
Out filter 02...Generic...Compare=Equals
Out filter 02...Generic...More=No

Out filter 03...Generic...Forward=No
Out filter 03...Generic...Offset=12
Out filter 03...Generic...Length=2
Out filter 03...Generic...Mask=ffff000000000000
Out filter 03...Generic...Value=809b000000000000
Out filter 03...Generic...Compare=Equals
Out filter 03...Generic...More=Yes
```

```
Out filter 04...Generic...Forward=No
Out filter 04...Generic...Offset=24
Out filter 04...Generic...Length=3
Out filter 04...Generic...Mask=ffffff0000000000
Out filter 04...Generic...Value=0404040000000000
Out filter 04...Generic...Compare=Equals
Out filter 04...Generic...More=No

Out filter 05...Generic...Forward=yes
Out filter 05...Generic...Offset=0
Out filter 05...Generic...Length=0
Out filter 05...Generic...Mask=0000000000000000
Out filter 05...Generic...Value=0000000000000000
Out filter 05...Generic...Compare=Equals
Out filter 05...Generic...More=No
```

Pipeline System Administration

9

This chapter covers these topics:

Ascend administration parameters

Table 9-1 shows parameters and commands related to Pipeline system administration.

Table 9-1. System administration parameters

Location	Parameters with default values
System→Sys Config	Name=[] Term Rate=9600 Console=Standard Remote Mgmt=Yes
System→Sys Diag	Restore Cfg Save Cfg Sys Reset Cmd Mode

For detailed descriptions of each command or parameter, see Chapter 11, "Reference."

The System Profile (Sys Config menu) contains additional parameters that are not shown in Table 9-1 and are not described in this chapter. Those parameters are related to bandwidth and WAN configuration, and are described in Chapter 3, "Configuring WAN Connections," as well as in Chapter 11, "Reference."

For details on security, see Chapter 7, "Pipeline System Security."

Introduction to Ascend administration

This chapter explains how to manage the Pipeline.

Status information

The status windows in the standard configuration interface provide information about what is currently happening in the Pipeline. For example, one status

window displays up to 31 of the most recent system events that have occurred since the Pipeline was powered up, and another displays statistics about the currently active session. You can also perform DO commands, for example, clear an active connection, using the status windows.

See "Working with status and log messages" on page 9-7.

Administration commands and security levels

The Pipeline has password security to stop unauthorized personnel from performing administration tasks. Typically, the "Full Access" Profile is reserved for administrators. To activate the Full Access security level, use the DO menu (see "Activating the Full Access security level" on page 9-5).

For details on Security Profiles, see the *Pipeline Security Supplement.*

- DO commands

  Pressing Ctrl-D in the Control Monitor displays the DO menu, which contains commands for changing security levels in the Pipeline, or manually dialing or clearing a call. When full access (or another appropriate security level) has been activated, you can perform all DO commands as well as other administrative operations.

  See "DO commands for security and manual tasks" (the next section).

- System reset and configuration management

  The Pipeline provides commands for rebooting the device, saving or restoring configuration information, and performing other administrative functions. The Pipeline enables software upgrades in the field without opening the unit or changing memory chips, a process that also makes use of the configuration management commands.

  See "System administration operations" on page 9-10.

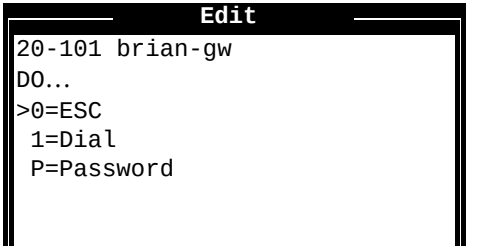
- Terminal server commands

  The Pipeline unit's command-line interface provides commands for testing a connection, checking routing tables and other configuration parameters, or configuring far-end Ascend units across the WAN. Many of these commands are related to system administration.

  See Chapter 10, "Using the Command Mode.".

DO commands for security and manual tasks

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:



To type a DO command, press and release the Control Monitor's 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 VT-100 monitor is equivalent to the DO key or Ctrl-D.

Table 9-2 lists the DO commands.For details on these commands, see Chapter 11, "Reference."

Table 9-2. DO commands

Command	Description
DO Beg/End Rem Mgm (DO 8)	Begin/End remote management.
DO Contract BW (DO 5)	Decrease bandwidth.
DO Dial (DO 1)	Dial the selected or current profile.
DO ESC (DO 0)	Abort and exit the DO menu.
DO Hang Up (DO 2)	Hang up from a call in progress.

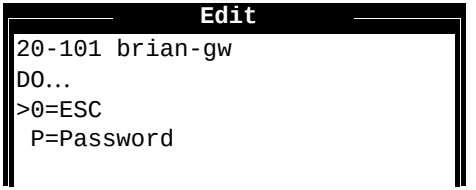
Table 9-2. DO commands

Command	Description
DO Save (DO S)	Save parameter values into the specified profile.
DO Password (DO P) 9	Log into or out of the Pipeline.

Activating the Full Access security level

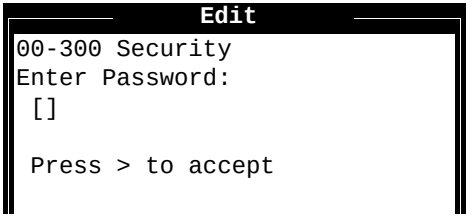
To activate the Full Access Profile, which enables you to perform administrative operations:

1 Press Ctrl-D to display the DO menu.



2 Press P (or select P=Password) to invoke Password command.

3 A menu of Security Profiles opens. Select Full Access. The Pipeline prompts for the password for the Full Access Profile.



4 Type the password and press Enter to accept it.

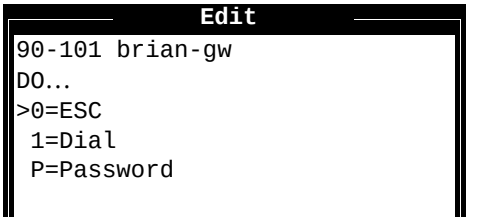
If you enter the right password, a message states that the password was accepted and the Pipeline is using the new security level. If the password you enter is incorrect, you are prompted again to enter the password.

Manually placing and clearing calls

This section shows how to use a few more DO commands. To manually place a call, the Connection Profile for that call must be open or selected in the list of Profiles. To clear a call, you can either open the Connection Profile for the active connection, or tab over to the status window in which that connection is listed (see “Working with status and log messages” on page 9-7).

For example, to manually place a call:

1. Select or open the Connection Profile for the destination you want to call.
2. Press Ctrl-D to invoke the DO menu.

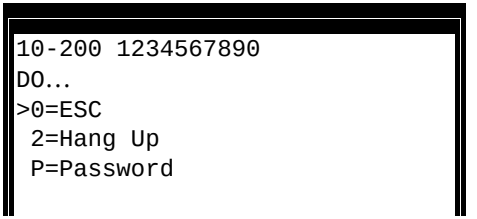


3. Press 1 (or select 1=Dial) to invoke the Dial command.
4. Watch the information in Sessions status window. You should see the number being called followed by a message that the network session is up.

To manually clear a call:

1. Open the Connection Profile or tab over to the status window that displays information about the active session you want to clear.
2. Press Ctrl-D to open the DO menu.

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



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

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

Working with status and log messages

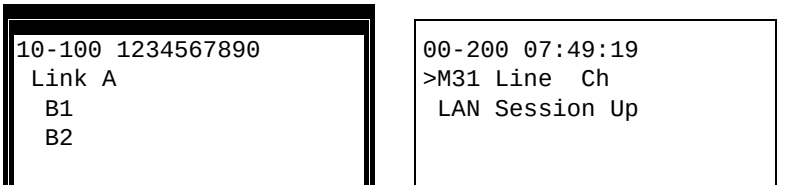
Eight status windows are displayed on the right side of the screen in the Pipeline configuration interface (Figure 9-1). These status windows provide a great deal of read-only information about what is currently happening in the Pipeline.

A thick border around a window indicates that it is active. To make a status window active, press Tab until it is highlighted by a border. Pressing Tab moves through the windows in sequence from left to right, top to bottom, and then returns to the main configuration menus.

Flashing questions marks mean there is no WAN connection. For example, the line might be down or unplugged from the back of the Pipeline.

Note: Some of the status windows contain more information than can be displayed in the small window. If a lowercase v appears in the lower-right corner of a window, it means there is more information available. To scroll through additional information in a window, use the Tab key to move to that window, then use the arrow keys or Ctrl-P or Ctrl-N to scroll through the remaining entries.

For detailed explanation of the Status window contents, refer to Appendix B, “System Event Messages.”



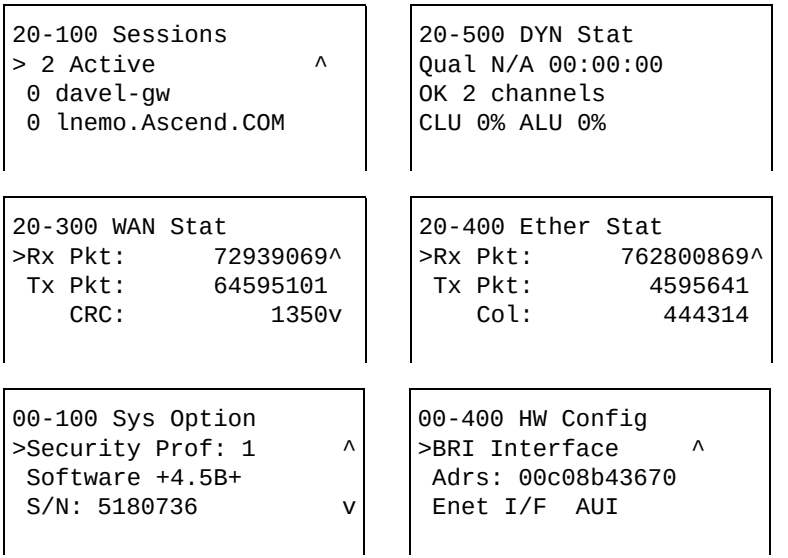


Figure 9-1. Status windows

Displaying the software load name

The name of the software load is displayed in the Sys Options status window and in fatal error messages. The load name is an important aid to troubleshooting error conditions.

Ascend software releases are distributed in software *loads*, which vary according to the functionality and target platform for the binary.

The load appears in the Sys Options status window, for example:

```
00-100 Sys Option
>Pipeline 25     ^
 Load: p25ip
 Switched
Installed     v
```

The load name is also displayed in fatal error messages. For example:

```
> fat
WARNING: Index: 201 Load: p25ip Revision: 4.6ci1
       Date: 06/03/1996.       Time: 13:04:48
       Location: b0149048 b013f6c0 b014915c b0073450
00000000 b2807400
```

Configuring local management information

To set parameters that affect how the Pipeline operates, its system name, who to contact in an error condition, and other administrative information, open the System Profile (Sys Config menu) below the System menu This profile contains global parameters that to how the Pipeline operates.

Table 9-3. Local management information

Location	Parameters
System→Sys Config	Name=*host-name* Term Rate=9600 Console=Standard Remote Mgmt=Yes

With the exception of the Name parameter, which affects authentication of incoming calls, the first few parameters in the System Profile (Sys Config menu) are related to local management.

- The system name

  The Pipeline must have its own system name in the System Profile. This name identifies the Pipeline and is sent to the far-end device whenever a PPP session/link is established.

- Term Rate

  The Term Rate parameter controls the data transfer rate on the Pipeline Control port. For a local control monitor, set it to 9600.

- Console

  The Console parameter determines the configuration interface.

- Remote Management

  The Remote Mgmt parameter allows or does not allow a device at the far end of an MP+ call to operate the Pipeline remotely.

System administration operations

The commands shown in Table 9-4 perform system administration operations:

Table 9-4. Administration commands

Location	Commands
System→Sys Diag	Restore Cfg Save Cfg Sys Reset Cmd Mode

For details on the Cmd Mode command, see Chapter 10, "Using the Command Mode."

See Appendix D, "Upgrading Pipeline Software," for related information.

Backing up the Pipeline configuration

If you have set a security level that restricts field service, you may need to set a different security level or supply a password before saving your configuration.

Note: When you backup the Pipeline configuration, the configuration data is written to a text file on the disk of the accessing host (the computer connected to the Pipeline Control port). *Passwords are not saved.* Send and Recv passwords, Security Profile passwords, and passwords specified in the Ethernet Profile (Mod

Config menu), are all set to the null password when you restore a configuration from a saved file. We strongly recommend that you record these passwords off-line if you need to restore them.

Before you start the backup, verify that your terminal emulation program has a disk capture feature. Disk capture allows your emulator to capture to disk the ASCII characters it receives at its serial port. You should also verify that the data rate of your terminal emulation program is set to 9600 baud or lower and that the Term Rate parameter in the System Profile (Sys Config menu) is also set to 9600. Higher speeds might cause capture errors.

You can cancel the backup process at any time by typing Ctrl-C.

To save the Pipeline configuration (except passwords) to disk:

1 In the Sys Diag menu, select Save Config and press Enter.

The following message appears:

```
Ready to download - type any key to start...
```

2 Turn on the Capture feature of your communications program and supply a filename for the saved profiles.

Consult the documentation for your communications program if you have any questions about how to turn on the Capture feature.

3 Press any key to start saving your configured profiles.

Rows of configuration information are displayed on the screen as the file is downloaded to your hard disk. When the file has been downloaded to your hard disk, your communications program displays a message indicating the download is complete.

4 Turn off the Capture feature of your communications program.

5 Print a copy of your configured profiles for later reference.

Note: If you examine the saved Pipeline data file, notice that some of the lines begin with *START=* and other lines begin with *END=*. These START/STOP lines and the block of data contained between them constitute a profile. If a parameter in a profile is set to its default value, it does not appear. In fact, you can have profiles with all parameters at their defaults and the corresponding START/STOP blocks would be empty.

Restoring the Pipeline configuration

If you have set a security level that restricts field service, you may need to set a different security level or supply a password before saving your configuration.

Before you start the restore procedure, verify that your terminal emulation program has an autotype (or ASCII file upload) feature. Autotype allows your emulator to transmit a text file over its serial port. You should also verify that the data rate of your terminal emulation program is set to 9600 baud or lower and that the Term Rate parameter in the System Profile (Sys Config menu) is also set to 9600. Higher speeds might cause transmission errors.

You can use the Restore Cfg command to restore a full configuration that you saved by using the Save Cfg command, or to upload more specific configuration information obtained from Ascend, for example, a single filter stored in a special configuration file. To load configuration information from disk, first connect the backup device to the Pipeline Control port. Then:

1 In the Sys Diag menu, select Restore Cfg and press Enter.

The following message appears:

```
Waiting for upload data...
```

2 Use the Send ASCII File feature of the communications software to send the Pipeline the configuration file.

If you have any questions about how to send an ASCII file, consult the documentation for your communications program. When the restore has been completed, the following message appears:

```
Restore complete - type any key to return to menu
```

3 Press any key to return to the configuration menus.

If you restored a complete configuration, the passwords used in your Security profiles have been wiped out. To reset them:

1 Press Ctrl-D to invoke the DO menu, select Password, and choose the Full Access profile.

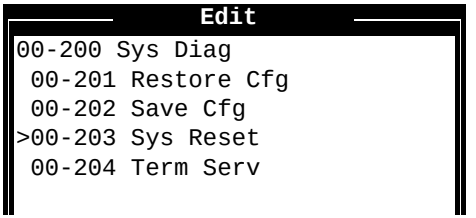
2 When you are prompted to enter the password, press Enter (the null password).

After you have restored your privileges by entering the null password, we recommend that you immediately open the Connection Profiles, Security

Profiles, and Ethernet Profile (Mod Config menu) and reset the passwords to their previous values.

Resetting the Pipeline

The Sys Reset command in the Sys Diag menu restarts the Pipeline and clears all calls.



To reset, choose Sys Reset in the Sys Diag menu. The Pipeline asks you to verify that you want to reset. When you confirm, the Pipeline clears active connections and runs its Power-On Self Test (POST), just as it would if the power were cycled. If you do not see the POST display, press Ctrl-L.

While the Connection LED on the front panel is ON, the Pipeline checks its memory, configuration, and lines. If any of the tests fail, the Connection LED remains on or blinking.

While the POST is running you see this message:

```
Pipeline
Power-On Self Test
Running
```

Press any key to display the Main Edit Menu.

Using the Command Mode

10

You can use the Pipeline command mode to perform diagnostic and system maintenance tasks.

This chapter contains these sections:

Using the command mode

To use the command mode:

1. Open the Pipeline configuration menus in the usual way. (You can open the menus from a PC on the Pipeline unit's Control port using vt100 emulation software across the serial connection.)
2. When the configuration menus are visible, activate the appropriate Security Profile.
3. Open the Sys Diag menu below the System menu, select Cmd Mode, and press Enter.

   The command mode prompt appears.

   ```
   ascend%
   ```

To display a list of the commands available in the command mode, enter a question mark (?) or HELP at the terminal server prompt. This list appears:

```
?            Display help information

help         "             "

quit         Closes terminal server session

hangup       "              "           "

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

local        Goes 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
```

The rest of this chapter describes how to use these commands.

Terminating a session

The following commands terminate the terminal server session and return you to the Pipeline configuration menus:

```
quit
hangup
local
```

Self-test calls using the TEST command

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

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

For example:

```
test 555-1212
```

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

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

Command arguments

The arguments to the TEST command are as follows:

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

[<frame-count>]	(Optional.) The number of frames to send during the test. You can specify a number from 1 to 65535. The default is 100.
[data-svc=<data-svc>]	For data-svc, enter a data service identical to any of the values available for the Data Svc parameter of the Connection Profile. For a list of valid values, see Chapter 11, "Reference." If you do not specify a value, the default value is the one specified for the Data Svc parameter.

TEST error messages

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

`bad digits in phone number`	The phone number you specified contained a character other than the numbers 0 through 9 and the characters ()[]-.
`call failed`	The Pipeline did not answer the outgoing call. This error can indicate a wrong phone number or a busy phone number. Use the SHOW ISDN command to determine the nature of the failure.
call terminated <N1> packets sent <N2> packets received	This message indicates the number of packets sent (<N1>) and received (<N2>).
`can't handshake`	The Pipeline answered the outgoing call, but the two sides did not properly identify themselves. This error can indicate that the phone number was incorrect.
`frame-count must be in the range 1-65535`	The number of frames requested exceeded 65535.

`no phone number`	You did not specify a phone number on the command line.
`test aborted`	The test was terminated (Ctrl-C).
`unit busy`	You attempted to start another self-test when one was already in progress. You can run only a single self-test at a time.
`unknown items on command line`	The command line contained unknown items. Inserting one or more spaces in the telephone number can generate this error.
unknown option <option>	The command line contained the option specified by `<option>`, which is invalid.
unknown value `<value>`	The command line contained the value specified by <value>, which is invalid.
`wrong phone number`	A device other than the Pipeline answered the call; therefore, the phone number you specified was incorrect.

Remote management with the REMOTE command

The REMOTE command starts a remote management session with the device at the remote end of an MP+ connection. During the remote management session, the user interface of the remote device replaces your local user interface. Enter the command in this format:

```
remote <station>
```

You can enter Ctrl-\ at any time to terminate the remote management session. Note that either end of an MP+ link can terminate the remote management session by hanging up all channels of the connection.

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

Bringing up the connection

To bring a connection online before beginning a remote management session, you can use the DO DIAL command.

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

Note: Remote management works best at higher terminal speeds.

Management privileges

At the beginning of a remote management session, you have privileges set by the default Security Profile at the remote end of the connection. To have other security privileges, log into a Security Profile with the privileges you require using the DO PASSWORD command.

Remote error messages

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

not authorized	Your current security privileges are insufficient for beginning a remote management session. To assign yourself the required privileges, log in with the DO PASSWORD command to a Security Profile whose Edit System parameter is set to Yes.

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

Setting items using the SET command

The SET command can be used to specify a terminal type or to enable dynamic password serving. To display all SET commands and their syntax, type:

```
set ?
```

The SET ALL command displays current settings, for example:

```
set all
```

```
term = vt100
dynamic password serving = disabled
```

The SET TERM command sets the terminal type (default vt100). Enter the command in this format:

```
set term=<termtype>
```

The SET PASSWORD command enables password mode, where a third party ACE or SAFEWORD server can display password challenges dynamically.

Displaying internal tables using the SHOW command

The SHOW command displays various tables stored in the Pipeline unit's memory. To see your choices, type:

```
show ?
```

This list is displayed:

`show ?`	`Display help information`	
`show arp`	`Display the Arp Cache`	IP only
`show icmp`	`Display ICMP information`	IP only
`show if`	`Display Interface info. Type 'show if ?' for help.`	
`show ip`	`Display IP info. Type 'show ip ?' for help.`	IP only
`show udp`	`Display UDP info. Type 'show udp ?' for help.`	IP only
`show tcp`	`Display TCP info. Type 'show tcp ?' for help.`	
`show netware`	`Display NetWare IPX info. Type 'show netware ?' for help.`	IPX only
`show isdn`	`Display ISDN events info. Type 'show isdn <line number>'`	

```
show uptime   Display how long the Pipeline 25-Fx has been
              running. Type 'show uptime'
```

Note: When a SHOW command displays statistics, the statistics always indicate the count since the Pipeline was last reset or switched on.

How interfaces are labeled

The following interface names are used in displaying information for any SHOW command:

- ie0 means the Ethernet interface.
- wan0 means the first bridge/router session.
- wan1 means the second bridge/router session.
- wan2... means the next bridge/router session.
- wanidle0 means the interface of all inactive links or sessions waiting for an active link.
- lo0 means the loopback interface (127.0.0.0).

Displaying the ARP cache (IP only)

The SHOW ARP command displays the ARP (Address Resolution Protocol) cache, which associates IP addresses with physical network addresses. Enter the command in this format:

```
show arp
```

The SHOW ARP command displays statistics about the current ARP cache, using these fields:

IP Address	The IP address in an ARP request.
Hardware Address	The MAC address in an ARP request.
Type	Dynamic or static, indicating how the address was obtained.

Interface	The interface on which the Pipeline received the ARP packet (see “How interfaces are labeled” on page 10-9).
Ref Count	The number of times the address was used.

Displaying ICMP statistics (IP only)

The SHOW ICMP command shows the number of ICMP (Internet Control Message Protocol) packets received intact, received with errors, and transmitted. Enter the command in this format:

```
show icmp
```

The SHOW ICMP command displays statistics about ICMP packets, showing these fields:

<#> packets received	The number of ICMP packets received.
<#> packets received with errors	The number of ICMP packets received with an error condition.
Input histogram	The number of ICMP packets received in each category.
<#> packets transmitted	The number of ICMP packets transmitted.
<#> packets not transmitted due to lack of resources	The number of ICMP packets not transmitted due to a lack of resources.
Output histogram	The number of ICMP packets transmitted in each category.

Displaying interface statistics

The SHOW IF STATS and SHOW IF TOTALS commands display interface information.

To display the status and packet count of each bridge/router, frame relay session, Ethernet interface, and software loopback, type:

```
show if stats
```

The SHOW IF STATS command displays statistics about the packets sent and received at each interface, using these fields:

Interface	The interface name (see "How interfaces are labeled" on page 10-9).
Name	The name of the Connection Profile or Frame Relay Profile associated with the interface.
Status	The status of the interface. A status of Up indicates that the interface is functional, but is not necessarily handling an active call. A status of Down indicates that the interface is not functional.
Type	The type of application being used on the interface, as specified in RFC 1213 (MIB-2).
Speed	The data rate in bits per second.
MTU	The maximum packet size allowed on the interface. MTU stands for Maximum Transmission Unit.
InPackets	The number of packets the interface has received.
OutPackets	The number of packets the interface has transmitted.

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

```
show if totals
```

The SHOW IF TOTALS command displays statistics about packet types and counts, using these fields:

Name	The interface name (see “How interfaces are labeled” on page 10-9).
Octets	The total number of bytes processed by the interface.
Ucast	Packets with a unicast destination address.
NonUcast	Packets with a multicast address or a broadcast address.
Discard	The number of packets that the interface could not process.
Error	The number of packets with CRC errors, header errors, or collisions.
Unknown	The number of packets the Pipeline forwarded across all bridged interfaces because of unknown or unlearned destinations.
Same IF	The number of bridged packets whose destination is the same as the source.

Displaying IP information (IP only)

The SHOW IP STATS, SHOW IP ADDRESS, and SHOW IP ROUTES commands provide IP (Internet Protocol) information.

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

```
show ip stats
```

The screen displays the total count of IP packets received and transmitted by the Pipeline, for example:

```
33 packets received.
0 packets received with header errors.
0 packets received with address errors.
6 packets forwarded.
```

```
0 packets received with unknown protocols.
0 inbound packets discarded.
27 packets delivered to upper layers.
65 transmit requests.
0 discarded transmit packets.
2 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 display the IP address of each bridge/router session, as well as the IP address of the Ethernet interface, enter this command:

```
show ip address
```

The SHOW IP ADDRESS command displays source and destination IP addresses of each session, using these fields:

Interface	The interface for each address. ie0 is set by the IP Adrs parameter. For more details, see “How interfaces are labeled” on page 10-9.
IP Address	The IP address of the interface.
Dest IP Address	The IP address of the remote router. (This field applies only to an interface with an active link that is routing IP.)
Netmask	The netmask in use on the interface.
MTU	The maximum packet size allowed on the interface.
Status	The status of the interface. (“Up” means that the interface is functional, but is not necessarily handling an active call. “Down” means that the interface is not functional.)

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

```
show ip routes
```

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

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

where <hostname> is a hostname or IP address.

The SHOW IP ROUTES command lists the routing table, using these fields:

Destination	The destination of the route (an IP address and subnet mask).
Gateway	The address of the closest router.
Interf	The interface associated with the route (see "How interfaces are labeled" on page 10-9).
Flags	One of the following characters: S=Static Route D=Dynamic Route G=Gateway Route H=Host Route P=Private U=Up *=Hidden A hidden route is one that has been superseded by a dynamic route.
Metric	The number of hops to the destination.
Use	The number of packets that have used the route.
Ref	The number of current users of the route.

The Pipeline displays exactly the same information it displays when you enter the IPROUTE SHOW command (see "Working with IP routes using the IPROUTE command (IP only)" on page 10-20).

Displaying UDP information (IP only)

The SHOW UDP STATS and SHOW UDP LISTEN commands provide UDP (User Datagram Protocol) information.

To display the number of UDP packets received and transmitted, enter this command:

```
show udp stats
```

These UDP statistics appear:

```
0 packets received.
0 packets received with no ports.
0 packets received with errors.
32 packets transmitted.
```

To display a table of the current UDP ports on which the Pipeline is listening, enter this command:

```
show udp listen
```

The SHOW UDP LISTEN command displays information about the socket number, UDP port number and the number of packets queued for each UDP port, using these fields:

Socket	The socket number associated with the port.
Local Port	The UDP port on which the Pipeline is listening.
InQLen	The input queue length for the port.

Displaying TCP information

The SHOW TCP STATS and SHOW TCP CONNECTION commands provide TCP (Transmission Control Protocol) information.

To display the number of TCP packets received and transmitted, enter this command:

```
show tcp stats
```

These TCP statistics are displayed:

```
0 active opens.
0 passive opens.
0 connect attempts failed.
0 connections were reset.
0 connections currently established.
0 segments received.
0 segments transmitted.
0 segments re-transmitted.
```

Note: The message “active open” indicates an open TCP session that the Pipeline initiated. The message “passive open” indicates an open TCP session that the Pipeline did not initiate.

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

```
show tcp connection
```

The SHOW TCP CONNECTION command displays information about the socket number, TCP port number and the status of the port, using these fields:

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

Displaying IPX information (IPX only)

The SHOW NETWARE STATS, SHOW NETWARE SERVERS, and SHOW NETWARE NETWORKS commands provide information about the Pipeline as an IPX router.

To display IPX packet statistics, enter this command:

```
show netware stats
```

These statistics are displayed:

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

These statistics show the following information:

<#> packets received	The number of IPX packets the Pipeline has received.
<#> packets forwarded	The number of IPX packets the Pipeline has forwarded.
<#> packets dropped exceeding maximum hop count	The number of IPX packets the Pipeline has dropped because they had already passed through too many routers.
<N4> outbound packets with no route	The number of IPX packets handled by the Pipeline that did not have a route.

To display a list of known NetWare servers from the Pipeline unit's IPX server database, enter this command:

```
show netware servers
```

The SHOW NETWARE SERVERS command displays the server table, which contains the IPX address, service type, and server names of NetWare servers. The output uses these fields:

IPX address	The IPX address of the server. The address uses this format: <network number>:<node number>:<socket number> For example, EE000001:000000000001:0040

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

To display a list of known NetWare networks from the Pipeline unit's IPX route database, enter this command:

```
show netware networks
```

The SHOW NETWARE NETWORKS command displays IPX routing information using these fields:

network	The 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.

Displaying ISDN event information

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

```
show isdn
```

The Pipeline responds with one or more of these messages:

```
PH: ACTIVATED
PH: DEACTIVATED
```

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

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

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

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

Displaying how long the Pipeline has been running

The SHOW UPTIME command displays how long the Pipeline 25-Fx has been running since the last time it was powered on or reset. To use it, enter this command line at the command mode prompt:

```
%show uptime
```

The command returns the number of days, hours, minutes, and seconds the Pipeline has been running, as in this example:

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

Working with IP routes using the IPROUTE command (IP only)

The IPROUTE SHOW, IPROUTE ADD, and IPROUTE DELETE commands let you work with the Pipeline unit's IP routing table.

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

```
iproute show
```

Here is an example of the output:

```
Destination      Gateway      IF      Flg Pref  Met   Use   Age
0.0.0.0/0        10.0.0.100     wan0    SG   1    1    0
20887
10.207.76.0/24    10.207.76.1   wanidle0 SG   100   7    0
20887
10.207.76.1/32    10.207.76.1   wanidle0 S    100   7    2
20887
10.207.77.0/24    10.207.76.1   wanidle0 SG   100   8    0
20887
127.0.0.1/32      -            lo0      CP   0     0    0
20887
```

```
10.0.0.0/24         10.0.0.100      wan0    SG  100  1    21387
20887
10.0.0.100/32       10.0.0.100      wan0    S   100  1    153
20887
10.1.2.0/24         -               ie0     C   0    0    19775
20887
10.1.2.1/32         -               lo0     CP  0    0    389
20887
255.255.255.255/32  -               ie0     CP  0    0    0
20887
```

The routes in this table are explained as follows:

```
0.0.0.0/0       10.0.0.100      wan0      SG   1     1     0
20887
```

This is the default route, pointing through the active Connection Profile. The IP Route Profile for the default route specifies a Preference of 1, so this route is preferred over dynamically learned routes.

```
10.207.76.0/24    10.207.76.1    wanidle0 SG   100   7    0
20887
10.207.76.1/32    10.207.76.1    wanidle0 S    100   7    2
20887
```

These routes are specified in a Connection Profile. Note that there are two routes—a direct route to the gateway itself and a route to the larger network.

```
10.207.77.0/24    10.207.76.1    wanidle0 SG   100   8    0
20887
```

This is a static route that points through an inactive gateway.

```
127.0.0.1/32       -              lo0      CP   0     0     0
20887
```

This is the loopback route, which 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.

```
10.0.0.0/24    10.0.0.100 wan0      SG    100   1      21387 20887
10.0.0.100/32  10.0.0.100 wan0     S     100   1     153   20887
```

These routes are created by a Connection Profile that is currently active. These are similar to the 10.207.76.0 routes shown above, but these routes live on an active interface.

```
10.1.2.0/24     -               ie0       C     0      0      19775
20887
```

This route describes the connection to the Ethernet interface. It is directly connected, with a Preference and Metric of zero.

```
10.1.2.1/32     -               lo0       CP    0      0      389
20887
```

This is another loopback route, a host route with our Ethernet address. It is private, so it will not be advertised.

```
255.255.255.255/32 -              ie0       CP    0      0      0
20887
```

This is a private route to the broadcast address. This route 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.

Information in the routing table display

The columns in the routing table display the following information:

- Destination

  The Destination column indicates the target address of a route. To send a packet to this address, the Pipeline will use this route. Note that the router will use the most specific route (having the largest netmask) that matches a given destination.

- Gateway

  The Gateway column specifies 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

  The Interface column shows 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 where all routes point when their WAN connections are down).

- Flg

  The Flg column can contain the following flag values:

  – C=Connected (A directly connected route, for example, the Ethernet.)

  – I=ICMP (ICMP Redirect dynamic route.)

  – N=NetMgt (Pleased in the table via SNMP MIB II.)

  – O=OSPF (A route learned from OSPF.)

  – R (A RIP dynamic route.)

  – S=Local (A locally configured IP Route profile or Connection Profile route.)

  – ?=Unknown (A route of unknown error, which indicates an error.)

  – G=Gateway (A gateway is required in order to reach this route.)

  – P=Private (This route will not be advertised via RIP or OSPF.)

  – T=Temporary (This route will be destroyed when its interface goes down.)

  – *=Hidden (A hidden route means that there is a better route in the table, so this route is hidden “behind” the better route. If the better route should go away, then this route may be used.)

  Note that the H (host route) flag has been removed because it was redundant with a /32 netmask in the Destination column. The U (up) flag has also been removed. Physical interfaces are considered “up” once they have been defined in the Ascend Enterprise MIB, so the U flag was contradictory. The D (dynamic route) flag has been replaced by the I (ICMP Redirect) and R (RIP) flags, which are new.

- Pref

  The Preference column contains the preference value of the route. Note that all routes that come from RIP will have a preference value of 100, while the preference value of each individual static route may be set independently.

- Metric

The Metric column shows the RIP-style metric for the route, with a valid range of 0-16. Routes learned from OSPF show a max RIP metric of 10. OSPF Cost infinity routes show a RIP metric of 16.

- Use

  This is a count of the number of times the route was referenced since it was created. (Many of these references are internal, so this is not a count of the number of packets sent using this route.)

  Note: Unused routes are now indicated by a 0 in the Use column. They were indicated previously by a 1 in the Use column.

- Age

  This is the age of the route in seconds. It is used for troubleshooting, to determine when routes are changing rapidly or flapping.

Note: The Pipeline restores all routes listed in the Static Route Profile after a system reset.

To add a static route to the Pipeline unit's routing table, enter the IPROUTE ADD command in this 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).

Note: The IPROUTE ADD command has the same effect as adding a route to a Static Route Profile, except that any route set with IPROUTE ADD is lost whenever the Pipeline is reset. For detailed information about IP routing, see XREF-IP-CHAPTER.

For example, enter this command:

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

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

If you try to add a route to a destination that already exists in the routing table, the Pipeline replaces the existing route, but only if the existing route has a higher metric. If you get the message "Warning: a better route appears to exist", the

Pipeline rejected your attempt to add a route because the routing table already contained the same route with a lower metric.

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

```
iproute add <destination> <gateway>
```

For example:

```
iproute delete 10.1.2.0 10.0.0.3/24
```

Reference

11

This chapter provides a reference for the Pipeline 25-Fx parameters and the Pipeline DO commands.

This chapter contains these sections:

Parameter reference

Parameters are listed in alphabetical order. Each listing provides information in this format:

Parameter Name

Description: The Description text explains the parameter.

Usage: The Usage text explains how to use the parameter.

Example: The Example text shows you an example entry or setting.

Dependencies: The Dependencies text tells you what other information you need to configure and use the parameter.

Parameter Location: The Parameter Location text shows you where to find the parameter.

See Also: The See Also text points you to related parameters.

Alphabetical parameter listing

Active

Description: This parameter appears in a Connection Profile and a Static Rtes Profile. Its functionality differs depending on the profile:

- In a Connection Profile the Active parameter activates or deactivates the profile.

  If you activate a profile, it is available for use. If you deactivate a profile, it is not available for use.
- In a Static Rtes Profile, the Active parameter determines whether the route defined in the profile appears in the Pipeline 25-Fx's static routing table.

Usage: Press Enter to toggle between Yes and No.

- Yes activates the profile or specifies that the route can appear in the static routing table.

Yes is the default.

- No deactivates the profile, keeps the route from appearing in the static routing table, or removes the route if it is already in the table.

  A dash appears before each deactivated profile or route.

Parameter Location: Connection Profile, Connections
Static Rtes Profile, any profile

Add Pers

Description: This parameter specifies the number of seconds that average line utilization (ALU) for transmitted data must exceed the threshold indicated by the Target Util parameter before the Pipeline 25-Fx begins adding bandwidth to a session. The Pipeline 25-Fx determines the ALU for a session by using the algorithm specified by the Dyn Alg parameter.

When utilization exceeds the threshold for a period of time greater than the value of the Add Pers parameter, the Pipeline 25-Fx attempts to add a channel. Using the Add Pers and Sub Pers parameters prevents the system from continually adding and subtracting bandwidth, and can slow down the process of allocating or removing bandwidth.

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

When the Pipeline 25-Fx is using MP+ (Encaps=MPP), the default value is 5.

Dependencies: Keep this additional information in mind:

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

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

Parameter Location: Answer Profile, Answer/PPP options
Connection Profile, Connections/Encaps options

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

---

AnsOrig

Description: This parameter specifies whether the Pipeline 25-Fx can initiate calls, receive them, or both. The setting you choose affects calls to or from the destination specified by the Station and LAN Adrs parameters in the Connection Profile.

Usage: Press Enter to cycle through the choices.

- Both specifies that the Pipeline 25-Fx can initiate calls to the destination specified in the Connection Profile, and that the Pipeline 25-Fx can receive calls from that destination as well.

  Both is the default.
- Call Only specifies that the Pipeline 25-Fx can dial out to the destination specified in the Connection Profile, but cannot answer calls from that destination.
- Ans Only specifies that the Pipeline 25-Fx can receive calls from the destination specified in the Connection Profile, but cannot initiate calls to that destination.

Parameter Location: Connection Profile, Connection/Telco options

See Also: LAN Adrs, Station

APP Host (IP only)

Description: This parameter 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: Press Enter to open a text field. Then, type the IP address of the authentication server.

The address consists of four numbers between 0 and 255, separated by periods. Separate the optional netmask from the address using a slash. The default value is 0.0.0.0/0. The default setting specifies that no APP server is available.

Press Enter again to close the text field.

Example: `200.65.207.63/29`

Dependencies: Keep this additional information in mind:

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

Parameter Location: Ethernet Profile, Mod Config/Auth

See Also: APP Server, Send Auth

APP Port (IP only)

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

Usage: Press Enter to open a text field. Then, type a UDP port number. Valid port numbers range from 0 to 65535. The default value is 0, which indicates that no UDP port is being monitored by the APP server. Press Enter again to close the text field.

Example: `35`

Dependencies: Keep this additional information in mind:

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

Parameter Location: Ethernet Profile, Mod Config/Auth

See Also: APP Server, Send Auth

APP Server (IP only)

Description: This parameter lets you enable responses to security card password challenges by using the APP Server utility on a UNIX or Windows workstation.

Usage: Press Enter to toggle between Yes and No.

- Yes enables the Pipeline 25-Fx to respond to password challenges by using the APP Server utility.
- No disables responses from the APP Server utility.

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

Dependencies: Keep this additional information in mind:

- You must set Send Auth=PAP-Token for the APP Server parameter to have any effect.
- The APP Server utility must be running on a UNIX or Windows workstation on the local network.

Parameter Location: Ethernet Profile, Mod Config/Auth

See Also: Send Auth

Auto Logout

Description: This parameter specifies whether the Pipeline 25-Fx automatically logs out when a device disconnects from the Pipeline 25-Fx's control port or when the Pipeline 25-Fx loses power. The disconnected device can be a terminal, a VT-100, a terminal emulator, or a modem.

A terminal is a computer that does not have its own processor; it must connect to a computing device called a terminal server in order to use its CPU. VT100, ANSI, and TTY are all types of terminals.

A terminal emulator is a program that makes your computer act like a terminal so that you can connect to a terminal server. All processing takes place remotely.

A modem (MOdulator/DEModulator) is a device that takes digital data from a computer, translates (or modulates) the 1s and 0s into analog form, and sends the data over an analog communications channel. The receiving modem demodulates the analog signal into digital data and sends it to the computer to which it is attached.

Usage: Press Enter to toggle between Yes and No.

- Yes enables automatic logout.
- No disables automatic logout.
  No is the default.

Parameter Location: System Profile, Sys Config

Aux Send PW

Description: This parameter specifies the password that the Pipeline 25-Fx sends when it adds channels to a security-card MP+ call that uses PAP-TOKEN-CHAP authentication. The Pipeline 25-Fx obtains authentication of the first channel of this MP+ call from the hand-held security card.

Usage: Press Enter to open a text field. Then, type a password. This password must match the one set up for your Pipeline 25-Fx in the RADIUS users file on the NAS (Network Access Server). Press Enter again to close the text field.

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

Parameter Location: Configure Profile, Connection Profile, Connections/Encaps options

See Also: Send Auth

Base Ch Count

Description: This parameter specifies the initial number of channels the Pipeline 25-Fx sets up when originating calls for a PPP, MP+, or MP multichannel link.

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

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

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

No matter what type of link you use, the amount you specify cannot exceed the maximum channel count set by the Max Ch Count parameter.

Press Enter to close the text field.

Dependencies: Keep this additional information in mind:

- You can determine the base bandwidth of a call by multiplying the value of the Base Ch Count parameter by the value of the Data Svc parameter.

Parameter Location: Connection Profile, Connections/Encaps options

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

Bill #

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

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

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

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

The Pipeline 25-Fx uses the Bill # parameter differently depending on the type of line you use:

- Bill # for outgoing calls on an ISDN BRI line applies only to installations in Australia.

Press Enter to close the text field.

Example: These specifications are valid for Bill #:

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

Parameter Location: Connection Profile, Connections/Telco options

See Also: Calling #, Clid Auth

BOOTP Relay Enable

Description: This parameter controls whether Bootstrap Protocol (BOOTP) requests are relayed to other networks.

Usage: Press Enter to cycle through the choices.

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

No is the default.

Dependencies: You must use the Server parameter to specify the address of at least one BOOTP server. The BOOTP Relay menu also includes a second Server parameter for specifying a second BOOTP server. If you specify two BOOTP servers, the Pipeline that relays the BOOTP request determines when each server is used. The order of the BOOTP servers in the BOOTP Relay menu does not necessarily determine which server is tried first.

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

Parameter Location: Mod Config, BOOTP Relay

See Also: Server

Bridge

Description: This parameter enables or disables protocol-independent bridging at the link level. If you disable bridging, you must enable routing by setting Route IP=Yes or Route IPX=Yes in the Connection Profile.

Usage: Press Enter to cycle through the choices.

- No disables bridging. If you disable bridging, you must enable routing or you will be unable to save the profile.

  No is the default.
- Transparent enables transparent bridging. When the Pipeline is performing transparent bridging it keeps track of where a particular address is located and the Connection Profile needed to bring up that interface. As it forwards a packet, it notes the packet's source address and creates a bridge table that associates node addresses with a particular interface.
- IPX Client enables IPX smart bridging. Use this option if you support only NetWare client on the local network, not NetWare servers. The Pipeline continues to act as a protocol-independent bridge, and applies a set of internal filters that enable it to bring down and idle IPX connection without breaking IPX client-server or peer-to-peer connections.

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

Bridge and Route IP

- If Bridge=Yes and Route IP=Yes, the Pipeline 25-Fx routes IP packets, and bridges all other packets.
- If Bridge=Yes and Route IP=No, the Pipeline 25-Fx bridges all packets.
- If Bridge=No and Route IP=Yes, the Pipeline 25-Fx routes only IP packets.
- If Bridge=No and Route IP=No, an error occurs and you cannot save the profile

  You must enable bridging or routing, or both.

Bridge and Route IPX

- If Bridge=Yes and Route IPX=Yes, the Pipeline 25-Fx routes IPX packets, and bridges all other packets.
- If Bridge=Yes and Route IPX=No, the Pipeline 25-Fx bridges all packets.
- If Bridge=No and Route IPX=Yes, the Pipeline 25-Fx routes only IPX packets.
- If Bridge=No and Route IPX=No, an error occurs and you cannot save the profile.

  You must enable bridging or routing, or both.

Additional Dependencies

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

  The Connection Profile on the dialing side and the Answer Profile on the answering side must both set the Bridge parameter to Yes. Otherwise, the Pipeline 25-Fx does not bridge the packets.
- The Bridge parameter does not apply (Bridge=N/A) if you turn off bridging in the Ethernet Profile (Bridging=No).
- Bridge in the Answer Profile applies to incoming calls for which no Connection Profile exists; if a Connection Profile exists, the setting of its Bridge parameter takes precedence.
- If Profile Reqd=Yes in the Answer Profile, Bridge does not apply (Bridge=N/A) in the Answer Profile.
- If Profile Reqd=Yes in the Answer Profile, you must set Bridge=Yes in the answering Connection Profile.

- Do not confuse the Bridge parameter with the Bridging parameter.
  - The Bridge parameter in the Answer Profile applies only to connections that the Pipeline 25-Fx answers.
  - The Bridge parameter in the Connection Profile applies only to a specific connection.
  - The Bridging parameter globally enables or disables bridging.

Parameter Location: Answer Profile, Answer/PPP options
Connection Profile, Connections
Configure Profile

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

Bridging

Description: This parameter allows you to globally enable or disable bridging for all connections that the Pipeline 25-Fx answers or dials.

Usage: Press Enter to toggle between Yes and No.

- Yes globally enables bridging.

  When you choose this setting, the Pipeline 25-Fx operates in promiscuous mode. The Ethernet controller in the Pipeline 25-Fx accepts all packets and passes them up the protocol stack for a higher-level decision on whether to route, bridge, or reject them. This mode is appropriate if you are using the Pipeline 25-Fx as a bridge.

- No globally disables bridging.

  When you choose this setting, the Ethernet controller filters out all packets except broadcast packets and those explicitly addressed to the Pipeline 25-Fx. The Bridge parameter in the Connection and Answer Profiles, and all parameters exclusively associated with bridging, are set to N/A.

  This mode significantly reduces processor and memory overhead when the Pipeline 25-Fx is routing, and can result in much better performance, especially in moderate to heavily loaded networks.

  No is the default.

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

- The Bridge parameter in the Answer Profile applies only to connections that the Pipeline 25-Fx answers.
- The Bridge parameter in the Connection Profile applies only to a specific connection.
- The Bridging parameter in the Ethernet Profile globally enables or disables bridging.

Parameter Location: Ethernet Profile, Mod Config

See Also: Bridge

Callback

Description: This parameter enables or disables the callback feature.

When you enable the callback feature, the Pipeline 25-Fx hangs up after receiving an incoming call that matches the one specified in the Connection Profile. The Pipeline 25-Fx then calls back the device at the remote end of the link using the Dial # specified in the Connection Profile.

You can use this parameter to tighten security, as it ensures that the Pipeline 25-Fx always makes a connection with a known destination.

Usage: Press Enter to toggle between Yes and No.

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

  No is the default.

Dependencies: Keep this additional information in mind:

- If you set Callback=Yes, you must also set AnsOrig=Both, because the Connection Profile must both answer the call and call back the device requesting access.

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

Parameter Location: Connection Profile, Connections/Telco options

See Also: AnsOrig, Dial #

Call Filter

Description: This parameter specifies a call filter for an Answer Profile or a Connection Profile.

By default, any packet destined for the WAN causes the Pipeline 25-Fx to place a call. In addition, by default, every packet resets the idle timer, the indicator that the Pipeline 25-Fx uses to know when to clear a call. When you set up a call filter, only those packets that the call filter forwards can initiate a call or reset the Preempt or Idle parameters.

Usage: Press Enter to cycle through the choices.

- IP Call specifies the IP Call filter.
- Netware Call specifies the Netware Call filter.
- AppleTalk Call specifies the AppleTalk Call filter.
- None specifies that no filter is to be used.

When you set Call Filter to None, the Pipeline 25-Fx forwards all packets. None is the default.

Dependencies: Keep this additional information in mind:

- The Pipeline 25-Fx applies a call filter after applying a data filter; only those packets that the data filter forwards can reach the call filter.
- If IPX client bridging is in use (Bridge=IPX Client), set the Call Filter parameter to 0 (zero).
- Call Filter in the Answer Profile applies to incoming calls for which no Connection Profile exists; if a Connection Profile exists, the setting of its Call Filter parameter takes precedence.
- If Profile Reqd=Yes in the Answer Profile, Call Filter does not apply (Call Filter=N/A) in the Answer Profile.

Parameter Location: Configure Profile/PPP options
Connection Profile, Connections/Session options

See Also: Data Filter, Filter menu, Forward, More, Profile Reqd

Cmd Mode

Description: You use this parameter to open a command-line interface where you can perform diagnostic tasks, such as testing a connection, and other tasks.

Usage: Press Enter to open the command-line interface. When you do, the command-line prompt appears:

```
ascend%
```

To return to the menu interface, type “quit” at the command-line prompt and then press the Return key.

Dependencies: Some security levels prevent access to command mode.

Parameter Location: System Profile, Sys Diag

See Also: Chapter 10, “Using the Command Mode.”.

Compare

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

After applying the Offset, Mask, and Length values to reach the appropriate location in a packet, the Pipeline 25-Fx compares the packet’s contents to the Value parameter. If Compare is set to Equals (the default), the Pipeline 25-Fx applies the filter if the packet data is identical to the setting of the Value parameter. If Compare is set to NotEquals, the Pipeline 25-Fx applies the filter if the packet data is not identical to the setting of the Value parameter.

Usage: Press Enter to cycle through the choices.

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

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

Dependencies: Keep this additional information in mind:

- This feature is also provided for RADIUS servers using the following syntax:

  `GENERIC dir action offset mask value` [`==` or `!=`][`more`]

  Fields enclosed in brackets are optional. The default Equals setting (==) is assumed if != is not specified.
- Compare=N/A if the filter is not Valid or if the filter type is IP.

Parameter Location: Filter Profile, Filters

See Also: Length, Mask, Offset, Value

Connection

Description: This parameter can appear in a Bridging Profile or an IPX Route Profile. Its functionality differs depending on the profile:

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

  The IP address contained in the Connection Profile's LAN Adrs parameter corresponds to the MAC address contained in the Bridging Profile's Enet Adrs parameter. The Pipeline 25-Fx dials the Connection Profile when a node on its LAN sends a packet whose destination matches the Enet Adrs value in the profile.
- In an IPX Route Profile, this required parameter identifies the number of the Connection Profile through which you can reach the NetWare server connected by the static route.

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

Bridging Profile

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

Press Enter again to close the text field.

IPX Route Profile

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

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

Press Enter again to close the text field.

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

Bridging Profile

You must set Dial Brdcast=No if you want the Pipeline 25-Fx to use a static bridge entry. Any Connection Profile that dials on broadcast does not need a Bridging Profile.

IPX Route Profile

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

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

Parameter Location: Bridging Profile, Bridge Adrs
IPX Route Profile, IPX Routes

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

Console

Description: This parameter specifies the type of control interface established at the VT-100 port labeled Control on the back panel of the Pipeline 25-Fx.

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

The Control Monitor is a menu-based user interface for configuring, managing, and monitoring the Pipeline 25-Fx. It consists of nine windows—eight status windows and a single edit window.

Parameter Location: System Profile, Sys Config

Data Filter

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

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

When you set Data Filter to 0 (zero), the Pipeline 25-Fx forwards all data packets. Zero is the default.

Dependencies: Keep this additional information in mind:

- The Pipeline 25-Fx applies a call filter after applying a data filter; only those packets that the data filter forwards can reach the call filter.
- If IPX client bridging is in use (Bridge=IPX Client), set the Data Filter parameter to 0 (zero).
- Do not confuse the Filter parameter with the Data Filter parameter.

  The Filter parameter filters data packets on the Pipeline 25-Fx's local LAN interface; the Data Filter parameter filters data packets on the Pipeline 25-Fx's WAN interface. The WAN interface is the port on the Pipeline 25-Fx that is connected to a WAN line.

- Data Filter in the Answer Profile applies to incoming calls for which no Connection Profile exists; if a Connection Profile exists, the setting of its Data Filter parameter takes precedence.
- If Profile Reqd=Yes in the Answer Profile, Data Filter does not apply (Data Filter=N/A) in the Answer Profile.

Parameter Location: Answer Profile, Answer/Session options
Connection Profile, Connections/Session options

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

Data Svc

Description: This parameter specifies the type of data service the link uses.

A data service is provided over a WAN line and is characterized by the unit measure of its bandwidth. A data service can transmit either data or digitized voice.

Usage: Press Enter to cycle through the choices. You can specify one of the settings listed in Table 11-1.

Table 11-1. Data Svc settings

Setting	Description
56K	The call contains any type of data and connects to the Switched-56 data service. The only services available to lines using inband signaling (such as Switched-56 lines) are 56K and 56KR.
56KR	The call connects to the Switched-56 data service. The only services available to lines using inband signaling (such as Switched-56 lines) are 56K and 56KR.
64K	The call contains any type of data and connects to the Switched-64 data service.

Table 11-1. Data Svc settings

Setting	Description
Voice	This value applies only to calls made over an ISDN BRI line. The voice setting enables the Pipeline 25-Fx to instruct the network to place an end-to-end digital voice call for transporting data when a switched data service is not available. If you choose this setting, the data might become corrupted or unusable unless you meet these technical requirements: • Use only digital end-to-end connectivity; no analog signals should be present anywhere in the link. • Make sure that the phone company is not using any intervening loss plans to economize on voice calls. • Do not use echo cancellation; analog lines can echo, and the technology to take out the echoes can also scramble data in the link. • Do not make any modifications that can change the data in the link.

Dependencies: Keep this additional information in mind:

- The Voice setting only applies to switched channels.
- You can determine the base bandwidth of a call by multiplying the value of the Base Ch Count parameter by the value of the Data Svc parameter.
- Either party can request a data service that is unavailable; in this case, the Pipeline 25-Fx cannot connect the call.

Parameter Location: Connection Profile, Connections/Telco options

See Also: Encaps

Data Usage

Description: This parameter specifies which of your ISDN telephone numbers to use for incoming data calls. If your ISDN service allows data calls on only one

telephone number, you can use this parameter to specify the telephone number to use.

Usage: Press Enter to cycle through the choices.

- A allows incoming data calls to the telephone number specified by the My Num A parameter.
- B allows incoming data calls to the telephone number specified by the My Num B parameter.
- A + B allows incoming data calls to the telephone number specified by the My Num A parameter or the telephone number specified by the My Num B parameter.

Dependencies: If the value of the Switch Type parameter is AT&T/P-T-P, the Data Usage parameter is N/A. There is only one telephone number for this type of ISDN service, and this telephone number is used for all data calls.

Outside of North America, the Data Usage parameter can be set if the value of the Switch Type parameter is FRANCE, U.K, NET 3, JAPAN, BELGIUM, AUSTRALIA, SWISS, GERMAN, or MP GERMAN.

Parameter Location: Configure Profile, BRI

See Also: My Num A, My Num B, Switch Type

DBA Monitor

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

Usage: Press Enter to cycle through the choices:

- Transmit

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

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

- None
  This specifies that the Ascend unit will not monitor traffic over the link.

Dependencies: Keep this additional information in mind:

- DBA-Monitor is only supported on MPP calls (Encaps=MPP).
- If both sides of the link have DBA Monitor set to None, DBA is disabled.

Parameter Location: Ethernet, Connections/Encaps options

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

Dest

Description: This parameter specifies the IP address of the route's destination.

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

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

The Pipeline 25-Fx ignores any digits in the IP address hidden by a netmask. For example, the address 200.207.23.1/24 becomes 200.207.23.0. To specify a route to a specific host, use a mask of 32.

The default value is 0.0.0.0/0. In a Static Rtes Profile, the first route is the default route, and the Dest parameter is set to 0.0.0.0/0; this default specifies all destinations for which no other route exists.

Press Enter to close the text field.

Example: `200.207.23.1`

Dependencies: Keep this additional information in mind:

- If you do not know the right IP address to enter, you must obtain it from the network administrator.
- Do not attempt to configure an IP address by guesswork!

- The Dest parameter does not apply (Dest=N/A) if the Pipeline 25-Fx does not support IP (Route IP=No).

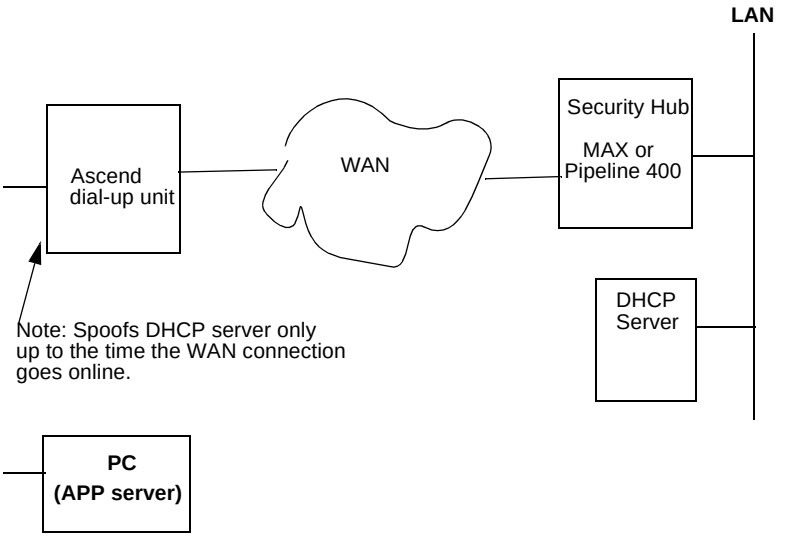
Parameter Location: Static Rtes Profile, Static Rtes

See Also: Encaps, Route IP

DHCP Spoofing (IP only)

Description: This parameter enables or disables Dynamic Host Configuration Protocol (DHCP) spoofing. When DHCP spoofing is enabled, the Pipeline 25-Fx can act as a DHCP server for one IP address.

When card-based security is used, the user must interact with the Pipeline 25-Fx to provide the card-based password. This interaction must occur over IP. However, the user doesn't have an IP address yet at the time when the password must be supplied.



To solve this "which came first" problem, the Pipeline 25-Fx supports DHCP spoofing. DHCP spoofing works like this:

1 If there is no authenticated dial-up session and the Pipeline 25-Fx receives a DHCP Discover packet, it responds with a DHCP Offer packet containing the configured IP address, netmask, and renewal time. This is quickly veri-

fied by an exchange between the client and the Pipeline 25-Fx. The renewal time is limited to a few seconds to ensure that the computer gets its *real* address from the remote DHCP server as soon as possible.

2 The APP Server utility runs using only broadcast addresses (see the discussion on the APP Server Utility and DHCP Spoofing in the *Pipeline 25-Fx User's Guide*), so that the Pipeline 25-Fx does not need a real IP address and the temporary "spoofed" address is not relied upon.

3 As soon as an authenticated dial-up link exists, the Pipeline 25-Fx refused to renew the spoofed address, forcing the computer to get its real address from the remote DHCP server.

Usage: Press Enter to toggle between Yes and No.

- Yes enables DHCP spoofing.
- No (default) disables this feature.

Parameter Location: Ethernet, Mod Config/DHCP Spoofing...

Dependencies: The Spoof Adr and Renewal Time parameters must be configured for this feature to work.

See Also: Spoof Adr, Renewal Time

Dial

Description: This parameter appears in the Configure Profile and a Connection Profile. Its functionality differs depending on the profile:

- In the Configure or Connection Profile, the Dial # parameter specifies the phone number the Pipeline 25-Fx dials to reach the bridge, router, or node at the remote end of the link.

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

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

The Pipeline 25-Fx sends only the numerical characters to place a call.

The default value is null.

Press Enter to close the text field.

Dependencies: Keep this additional information in mind:

- If Sub-Adr=Termsel (in the System, Sys Config menu) include the ISDN subaddress in the Dial #, separating it from the phone number with a comma. The characters before the comma comprise the phone number; the one or two numeric characters after the comma comprise the subaddress. Consider this example:

  `555-1212,23`

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

Parameter Location: Configure Profile
Connection Profile, Connections

See Also: Encaps, Group, Sub-Adr

Dial Brdcast

Description: This parameter specifies whether broadcast packets initiate dialing.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that the Pipeline 25-Fx dials a link if (a) the link is not online and (b) the Pipeline 25-Fx receives a frame whose MAC address is set to broadcast.

  When a device on the local Ethernet interface sends out broadcast packets that the Pipeline 25-Fx must bridge to another network, the Pipeline 25-Fx starts up a session for each Connection Profile in which Dial Brdcast=Yes. Gradually, it builds an internal bridge table based on experience; this table helps to limit the number of calls by recording the appropriate destination network for various addresses.

- No specifies that broadcast packets do not initiate dialing.

  If you choose this setting, the Pipeline 25-Fx relies on its Bridging Profiles, which contain remote physical addresses you have manually entered.

  The IP address contained in the Connection Profile's LAN Adrs parameter corresponds to the MAC address contained in the Bridging Profile's Enet Adrs parameter. The Pipeline 25-Fx dials the Connection Profile when a

node on its LAN sends a packet whose destination matches the Enet Adrs value.

No is the default.

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

Parameter Location: Connection Profile, Connections

See Also: Connection #

Dial Query (IPX only)

Description: This parameter specifies whether the Pipeline 25-Fx places a call to the location indicated in the Connection Profile when a workstation on the local IPX network looks for the nearest IPX server. More than one Connection Profile can have this parameter set to Yes. As a a result, several connections can occur at the same time.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that the Pipeline 25-Fx places a call to the location specified in the Connection Profile when a workstation looks for the nearest server.

  Note that a workstation is likely to stop attempting to find a server before the Pipeline 25-Fx establishes any connections with the Dial Query mechanism.
- No specifies that the Pipeline 25-Fx does not place a call to the location specified in the Connection Profile when a workstation looks for the nearest server.

  No is the default.

Dependencies: If there is an entry in the Pipeline 25-Fx unit's routing table for the location specified by the Connection Profile, Dial Query has no effect.

Parameter Location: Connection Profile: Ethernet→Connections→Any Connection Profile→IPX Options

Dst Adrs

Description: In a filter of type IP, this parameter specifies the destination address to which the Pipeline 25-Fx compares a packet's destination address.

Usage: Press Enter to open a text field. Then, type the destination address the Pipeline 25-Fx should use for comparison when filtering a packet. The address consists of four numbers between 0 and 255, separated by periods.

The null address 0.0.0.0 is the default. If you accept the default, the Pipeline 25-Fx does not use the destination address as a filtering criterion.

Press Enter to close the text field.

Example: `200.62.201.56`

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

Parameter Location: Filter Profile, Filters/IP

See Also: Dst Mask

Dst Mask

Description: In a filter of type IP, this parameter specifies the bits that the Pipeline 25-Fx should mask when comparing a packet's destination address to the value of the Dst Adrs parameter. The masked part of an address is hidden; the Pipeline 25-Fx does not use it for comparison with Dst Adrs. A mask hides the part of a number that appears behind each binary 0 (zero) in the mask; the Pipeline 25-Fx uses only the part of a number that appears behind each binary 1 for comparison.

The Pipeline 25-Fx applies the mask to the address using a logical AND after the mask and address are both translated into binary format.

Usage: Press Enter to open a text field. Then, type the IP mask in dotted decimal format. The value 0 (zero) hides all bits, because the decimal value 0 is the binary

value 00000000; the value 255 does not mask any bits, because the decimal value 255 is the binary value 11111111.

The null address 0.0.0.0 is the default; this setting indicates that the Pipeline 25-Fx 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 25-Fx uses for comparison.

Press Enter to close the text field.

Example: Suppose a packet has the destination address 10.2.1.1. If Dst Adrs=10.2.1.3 and Dst Mask=255.255.255.0, the Pipeline 25-Fx masks the last digit and uses only 10.2.1, which matches the packet.

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

Parameter Location: Filter Profile, Filters/IP

See Also: Dst Adrs

Dst Port

Description: In a filter of type IP, this parameter specifies the destination port number to which the Pipeline 25-Fx compares the packet's destination port number. The destination port number specifies the port on the remote device that must be "listening" for packets.

The Dst Port Cmp criterion determines how the Pipeline 25-Fx carries out the comparison.

Usage: Press Enter to open a text field. Then, type the number of the destination port the Pipeline 25-Fx should use for comparison when filtering packets. You can enter a number between 0 and 65535.

The default setting is 0 (zero). If you accept the default, the Pipeline 25-Fx does not use the destination port number as a filtering criterion.

Press Enter to close the text field.

Example: 25

Port 25 is reserved for SMTP; that socket is dedicated to receiving mail messages. Port 20 is reserved for FTP data messages, Port 21 for FTP control sessions, and Port 23 for Telnet sessions.

Parameter Location: Filter Profile, Filters/IP

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

Dst Port Cmp

Description: In a filter of type IP, this parameter specifies the type of comparison the Pipeline 25-Fx makes when using the Dst Port # parameter.

Usage: Press Enter to cycle through the choices.

- None specifies that the Pipeline 25-Fx does not compare the packet's destination port to the value specified by Dst Port #.

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

Dependencies: Keep this additional information in mind:

- This parameter works only for TCP and UDP packets.

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

Parameter Location: Filter Profile, Filters/IP

See Also: Dst Port #

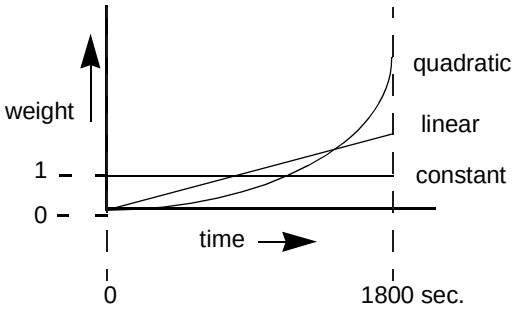
Dyn Alg

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

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

MP+ supports Dynamic Bandwidth Allocation.

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



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

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

  Quadratic is the default for MP+ calls (Encaps=MPP).

- Constant gives equal weight to all samples taken during the historical time period specified by the Sec History parameter.

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

Dependencies: Keep this additional information in mind:

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

Parameter Location: Answer Profile: Ethernet→Answer→PPP Options
Connection Profile: Ethernet→Connections→Any Connection Profile→Encaps Options

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

---

Edit Security

Description: This parameter grants or restricts privileges to edit Security Profiles.

Usage: Press Enter to toggle between Yes and No.

- Yes grants privileges.

  Yes is the default. When you choose Yes, a user is permitted to edit Security Profiles, and can access all other operations by enabling them in his or her active Security Profile.

- No restricts privileges.

Dependencies: Keep this additional information in mind:

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

Parameter Location: Security Profile, Security

Edit System

Description: This parameter grants or restricts privileges to edit the System Profile and the Ethernet Profile.

Usage: Press Enter to toggle between Yes and No.

- Yes grants privileges to edit the System Profile.
  Yes is the default.
- No restricts privileges.

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

Parameter Location: Security Profile, Security

Encaps

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

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

PPP

PPP (Point-to-Point Protocol) provides a standard means of encapsulating data packets over a single-channel WAN link that a Connection Profile sets up. It ensures basic compatibility with non-Ascend devices.

For this setting to work, both the dialing side and the answering side of the link

must support PPP.

MP

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

MPP

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

MP+ allows you to combine up to 30 individual channels into a single high-speed connection.

MP+ consists of two components: a low-level channel identification, error monitoring, and error recovery mechanism, and a session management level for supporting bandwidth modifications and diagnostics. MP+ enables the Pipeline 25-Fx to perform Dynamic Bandwidth Allocation (DBA)—that is, MP+ enables the Pipeline 25-Fx to add or remove channels without disconnecting a link as the need for bandwidth increases or decreases.

Both the dialing side and the answering side of the link must support MP+. If only one side supports MP+, the connection uses MP or standard single-channel PPP.

Dependencies: Keep this additional information in mind:

- When you select an encapsulation method, the Encaps options submenu displays a group of parameters relevant to your selection; you must set the appropriate Encaps options parameters.
- The Encaps parameter does not apply (Encaps=N/A) when the Pipeline 25-Fx answers a call.
- If Encaps=MPP the Pipeline 25-Fx adds or subtracts switched channels on the connection as required by the DBA parameters on either side of the connection.

DBA, or Dynamic Bandwidth Allocation, enables the Pipeline 25-Fx to use average line utilization (ALU) of transmitted data as the basis for adding or subtracting bandwidth from a switched connection without terminating the link. MP+ supports Dynamic Bandwidth Allocation. Each side makes its calculations based on the traffic received at that side. If the two sides of the connection disagree on the number of channels needed, the side requesting the greater number prevails.

- If Encaps=MPP, the minimum number of channels in the link is the number set by Min Ch Count.
- If Encaps=MPP the maximum number of channels in the link is the number set by Max Ch Count.

Parameter Location: Connection Profile, Connections

See Also: Encaps options submenu

Enet Adrs

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

The Pipeline 25-Fx uses the Bridging Profile to build a bridge table with corresponding MAC and IP addresses. The Enet Adrs parameter specifies the MAC address of each remote device; the Net Adrs parameter specifies the IP address of each remote device.

These parameters enable the Pipeline 25-Fx to respond to local ARP (Address Resolution Protocol) requests on behalf of a device at the remote end of the link. Whenever the Pipeline 25-Fx receives an ARP request for a MAC address corresponding to a specified IP address, it checks to see whether the IP address matches one in its bridge table. If it does, the Pipeline 25-Fx returns the MAC address corresponding to the IP address.

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

The default setting is 000000000000.

Press Enter to close the text field.

Example: `0180C2000000`

Parameter Location: Bridging Profile, Bridge Adrs

See Also: Net Adrs

Ethernet

Description: This parameter specifies which of the two Ethernet connectors on the Pipeline you use to connect to the local-area network.

Usage: Press Enter to cycle through the choices.

- AUI specifies the Thick Ethernet (10Base-5) connector.
- UTP specifies the 10Base-T (unshielded twisted pair) connector.

> **Note:** If you connect an Ethernet transceiver to either connector (such as a transceiver that converts Thick Ethernet to Thin Ethernet), choose the connector to which the transceiver is attached.

Dependencies: Changing the value of the Ethernet parameter also changes the value of the Ethernet IF parameter. These two parameters have the same purpose and values.

Parameter Location: Configure Profile

See Also: Ethernet IF

Ethernet IF

Description: You use this parameter to specify which of the two Ethernet connectors on the Pipeline you use.

Usage: Press Enter to cycle through the choices.

- AUI specifies the Thick Ethernet (10Base-5) connector.
- UTP specifies the 10Base-T (unshielded twisted pair) connector.

Note: If you connect an Ethernet transceiver to either connector (such as a transceiver that converts Thick Ethernet to Thin Ethernet), choose the connector to which the transceiver is attached.

Dependencies: Changing the value of the Ethernet IF parameter also changes the value of the Ethernet parameter. These two parameters have the same purpose and values.

Parameter Location: Ethernet Profile, Mod Config/Ether Options

See Also: Ethernet

Field Service

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

Usage: Press Enter to toggle between Yes and No.

- Yes grants privileges.
  Yes is the default.
- No restricts privileges.
  Selecting No does not disable access to any Pipeline 25-Fx operations. Field service operations are special diagnostic routines not available through Pipeline 25-Fx menus.

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

Parameter Location: Security Profile, Security

Filter

Description: This parameter specifies the number of a data filter that plugs into the Ethernet Profile. The data filter manages data flow on the Ethernet interface.

The filter examines each incoming or outgoing packet, and uses the Forward parameter to determine whether to forward or discard it.

Usage: Press Enter to open a text field. Then, type a number between 0 and 16. The number corresponds to a data filter you created in the Filters menu. When you set Filter to 0 (zero), the Pipeline 25-Fx forwards all packets.

Zero is the default.

Press Enter again to close the text field.

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

- The Filter parameter filters data packets on the Pipeline 25-Fx's local LAN interface.
- The Data Filter parameter filters data packets on the Pipeline 25-Fx's WAN interface.

  The WAN interface is the port on the Pipeline 25-Fx that is connected to a WAN line.
- The Call Filter parameter determines which packets can initiate a call or reset the idle timer.

  By default, any packet destined for the WAN causes the Pipeline 25-Fx to place a call. In addition, by default, every packet resets the idle timer, the indicator that the Pipeline 25-Fx uses to know when to clear a call. The Call Filter parameter limits the packets that can cause these events.

  The Pipeline 25-Fx applies the call filter specified by Call Filter only after applying the data filter specified by Filter or Data Filter. Only those packets that a data filter forwards reach a call filter.

Parameter Location: Ethernet Profile, Mod Config/Ether options

See Also: Forward, More

Force56

Description: This parameter specifies whether the Pipeline 25-Fx uses only the 56-kbps portion of a channel, even when all 64 kbps appear to be available.

Use this feature when you place calls to European or Pacific Rim countries and the complete path cannot distinguish between the Switched-56 and Switched-64 data services. This feature is not required if you are placing calls only within North America.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that the Pipeline 25-Fx uses only 56 kbps.
- No specifies that the Pipeline 25-Fx can use 64 kbps, if available.
  No is the default.

Parameter Location: Connection Profile, Connections/Telco options

Forward

Description: In a data filter or a call filter, this parameter specifies whether the Pipeline 25-Fx forwards or discards packets that match the filter. When you use Forward in a call filter, any forwarded data packet resets the idle timer and can initiate a call.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that the Pipeline 25-Fx forwards all packets matching the filter.
  If you have not specified any filters, Yes is the default.
- No specifies that the Pipeline 25-Fx does not forward packets matching the filter.
  If you have specified one or more filters, No is the default.

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

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

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

Parameter Location: Filter Profile, Filter/Generic and Filter/IP

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

Gateway

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

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

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

You must configure the network address of the destination station with the LAN Adrs parameter in the Connection Profile; otherwise, the Pipeline 25-Fx assumes that the router is on the same Ethernet interface.

Press Enter to close the text field.

Example: `200.207.23.1`

Dependencies: Keep this additional information in mind:

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

  Do not attempt to configure an IP address by guesswork!

- The Gateway parameter does not apply (Gateway=N/A) if the Pipeline 25-Fx does not support IP (Route IP=No).

Parameter Location: Static Rtes

See Also: Encaps, LAN Adrs, Route IP

Handle IPX Type20 (IPX only)

Description: This parameter controls whether 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 recommended by Novell) and are not forwarded over links that have less than 1 Mbps throughput. Setting this parameter to Yes allows applications to use IPX Type 20 packets to broadcast names regardless of the speed of the link.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies to use IPX Type 20 packets to broadcast names over a network.
- No specifies not to use IPX Type 20 packets to broadcast names over a network.

  No is the default.

Dependencies: This parameter is N/A if the value of the IPX Frame parameter is None.

Parameter Location: Ethernet profile-->Mod Config-->Ether Options

---

Hop Count (IPX only)

Description: This parameter specifies the distance to the destination IPX network in hops. From the Pipeline 25-Fx, the local IPX network is one hop away. The IPX network at the remote end of the route is two hops away—one hop across the WAN and one hop to the local IPX network.

Usage: Press Enter to open a text field. Then, type a valid hop count from 1 to 15. A hop count of 16 is considered unreachable and is not valid for static routes. Press Enter again to close the text field.

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

Parameter Location: IPX Route Profile, IPX Routes

See Also: Route IPX

ICMP Redirects (IP only)

Description: This parameter specifies whether the Pipeline 25-Fx accepts or ignores Internet ICMP Redirect messages.

Usage: Press Enter to cycle through the choices.

- Accept specifies that the Pipeline 25-Fx processes incoming ICMP Redirect messages.

  Accept is the default.
- Ignore specifies that the Pipeline 25-Fx drops all incoming ICMP Redirect messages.

Dependencies: Set ICMP Redirects=Ignore whenever the Pipeline 25-Fx maintains a routing table, because counterfeit ICMP Redirects pose a potential security threat. You should accept ICMP Redirects only when the Pipeline 25-Fx has a single default route to another device.

Parameter Location: Ethernet Profile, Mod Config

Idle

Description: This parameter specifies the number of seconds the Pipeline 25-Fx waits before clearing a call when a session is inactive.

Usage: Press Enter to open a text field; then, type a number between 0 and 65535. If you specify 0 (zero), Pipeline 25-Fx does not enforce a limit; an idle connection stays open indefinitely.

The default setting is 120 seconds.

Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- If MP+ encapsulation is in use and the bandwidth utilization *on both sides of the connection* drops below the value entered in the Idle Pct field, the Pipeline 25-Fx clears the call, regardless of the value you enter for the Idle parameter.
- Idle in the Answer Profile applies to incoming calls for which no Connection Profile exists; if a Connection Profile exists, the setting of its Idle parameter takes precedence.
- If Profile Reqd=Yes in the Answer Profile, Idle does not apply (Idle=N/A) in the Answer Profile.
- Because the Idle Pct is parameter is dependent on traffic levels on both sides of the connection, we recommend that you use the Idle parameter in preference to it.

Parameter Location: Answer Profile, Answer/Session options
Connection Profile, Connections/Session options

See Also: Dial, Dual Ports, Profile Reqd

Idle Logout

Description: This parameter specifies the number of minutes the Control Monitor or session can remain inactive before the Pipeline 25-Fx logs out and hangs up.

The Control Monitor is a menu-based user interface for configuring, managing, and monitoring the Pipeline 25-Fx. It consists of nine windows—eight status windows and a single edit window.

Usage: Press Enter to open a text field. Then, type a number between 0 and 60. The default setting is 0; this setting disables automatic logout. Press Enter again to close the text field.

Parameter Location: System Profile, Sys Config

Idle Pct

Description: This parameter specifies a percentage of bandwidth utilization below which the Pipeline 25-Fx clears a single-channel MP+ call. Bandwidth utilization must fall below this percentage on *both sides* of the connection before the Pipeline 25-Fx clears the call.

Usage: Press Enter to open a text field. Then, type a number between 0 and 99. The default value is 0; this setting causes the Pipeline 25-Fx to ignore bandwidth utilization when determining whether to clear a call. Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- MP+ must be the selected encapsulation method (Encaps=MPP) in a Connection Profile.
- If the device at the remote end of the link enters an Idle Pct setting lower than the value you specify, the Pipeline 25-Fx does not clear the call until bandwidth utilization falls below the lower percentage.
- If either end of a connection sets the Idle Pct parameter to 0 (zero), the Pipeline 25-Fx ignores bandwidth utilization when determining when to clear a call.
- If the time set by the Idle parameter expires, the call disconnects whether or not bandwidth utilization falls below the Idle Pct setting.
- When bandwidth utilization falls below the Idle Pct setting, the call disconnects regardless of whether the time specified by the Idle parameter has expired.
- Because the Idle Pct parameter is dependent on traffic levels on both sides of the connection, we recommend that you use the Idle parameter in preference to it.
- Idle Pct in the Answer Profile applies to incoming calls for which no Connection Profile exists; if a Connection Profile exists, the setting of its Idle Pct parameter takes precedence.
- If Profile Reqd=Yes in the Answer Profile, Idle Pct does not apply (Idle=N/A) in the Answer Profile.

Parameter Location: Answer Profile, Answer/PPP options
Connection Profile, Connections/Encaps options

See Also: Call Filter, Encaps, Idle

IF Adrs

Description: This parameter specifies the IP address of the interface at the near end of a link.

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

An IP address consists of four numbers between 0 and 255, separated by periods. If a netmask is in use on the network, you must specify it. Separate the netmask from the IP address with a slash. The default is 0.0.0.0/0.

Press Enter again to close the text field.

Example: `200.207.23.7/24`

Dependencies: The IF Adrs parameter does not apply if the Pipeline does not support IP (Route IP=No).

Parameter Location: Connection Profile: Ethernet > Connections > IP options

See Also: WAN Alias, Route IP

Ignore Def Rt (IP only)

Description: This parameter specifies whether the Pipeline 25-Fx ignores RIP (Routing Information Protocol) updates to the default route (0.0.0.0/0) in its IP routing table.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that the Pipeline 25-Fx ignores updates to the default route.
- No specifies the Pipeline 25-Fx allows updates to the default route. No is the default.

Parameter Location: Ethernet Profile, Mod Config/Ether options

IP Adrs (IP only)

Description: This parameter specifies the IP address of the Pipeline 25-Fx on the local Ethernet network, and its subnet.

Usage: Press Enter to open a text field. Then, type the IP address of the Pipeline 25-Fx on the local Ethernet network.

The address consists of four numbers between 0 and 255, separated by periods. Separate the optional netmask from the address with a slash. The IP address must be a valid IP address on the local Ethernet network.

The default value is 0.0.0.0/0.

Press Enter to close the text field.

Example: `10.2.1.1/24`

In this example, 10.2.1.1 is the Pipeline 25-Fx's IP address. The number 24 represents the number of bits in the Pipeline 25-Fx's netmask. Masking 24 bits in the Pipeline 25-Fx's address provides a subnet of 10.2.1.0.

Dependencies: Keep this additional information in mind:

- The value of the IP Adrs parameter on the local Pipeline 25-Fx must match the LAN Adrs parameter of the unit at the remote end of the link.
- The IP Adrs parameter does not apply (IP Adrs=N/A) if the Pipeline 25-Fx does not support IP (Route IP=No).
- If you do not know the right IP address to enter, you must obtain it from the network administrator.

  Do not attempt to configure an IP address by guesswork!
- The IP Adrs parameter is the same as the My Addr parameter in the Configure Profile.

Parameter Location: Ethernet Profile, Mod Config/Ether options

See Also: Encaps, Route IP

IP Gateway (IP only)

Description: IP packets whose destination is not on the local or remote LANs connected by the Pipeline are routed to the IP address specified by this parameter. This parameter defines the *default route*, the route used for IP packets for which no other routes are defined. If you are using your Pipeline to connect a single PC to a remote site, enter the IP address of the remote device as the IP Gateway.

Note: To let users on the local LAN use security cards to gain access to the remote LAN, the IP Gateway parameter must specify the APP server (the server that processes security-card passwords) on the remote LAN. For more information about security cards, see Chapter 7, "Pipeline System Security.".

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

Example: If you set the IP Gateway parameter to this address:

198.5.250.1/24

The Pipeline adds this route to its internal routing table:

Destination: 0.0.0.0
Gateway: 198.5.250.1

Dependencies: This parameter is available only on a Pipeline with the IP routing option.

Parameter Location: Configure Profile, IP

See Also: APP Host, APP Port, APP Server, Rem Addr

IPX Alias (IPX only)

Description: This parameter specifies the network number assigned to a point-to-point link.

Generally, you need to enter a value in this parameter only if the Pipeline 25-Fx operates with a non-Ascend router that uses a numbered interface. It does not

apply if you are routing from one Pipeline 25-Fx to another, or to a router that does not use a numbered interface.

Usage: Press Enter to open a text field. Then, enter an appropriate network number. The default value is 00000000. FFFFFFFF is invalid. Press Enter again to close the text field.

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

Parameter Location: Connection Profile, Connections/IPX options

See Also: Route IPX

IPX Enet# (IPX only)

Description: This parameter specifies a unique IPX network number for the Ethernet interface.

The Pipeline 25-Fx assigns an address to a workstation when it connects to the Pipeline 25-Fx; it derives the address from the network number.

Usage: Press Enter to open a text field. Then, type an IPX network number using an 8-digit (4-byte) hexadecimal value. The default is 00000000. The number you specify must be unique within your wide-area IPX network, and must match the configuration of other routers on the local Ethernet network.

When you accept the default setting of 00000000, the Pipeline 25-Fx learns its IPX network number from other routers on the Ethernet network. If you enter a value other than zero, the Pipeline 25-Fx becomes the "seeding" router and sets its IPX network number for the other routers on the Ethernet network

Example: `DE040600`

Dependencies: The IPX Enet# parameter does not apply (IPX Enet#=N/A) if the Pipeline 25-Fx is not set up for IPX routing (Route IPX=No).

Parameter Location: Ethernet Profile, Mod Config/Ether options
Configure Profile

IPX Frame

Description: This parameter specifies the Ethernet frame type to use for IPX on the Ethernet interface. If you do not specify an Ethernet frame type, the Pipeline 25-Fx cannot route IPX or perform watchdog spoofing for its IPX clients.

IPX packets can appear in more than one Ethernet frame type on an Ethernet segment. If your Pipeline 25-Fx routes IPX, it can recognize only a single IPX frame type. The Pipeline 25-Fx does not route other IPX frame types, and may attempt to bridge them. In addition, the Pipeline 25-Fx can only route and perform watchdog spoofing for the IPX frame type specified by IPX Frame.

Usage: Press Enter to cycle through the choices.

- 802.3 specifies the 802.3 frame type.

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

  For NetWare 3.11 or earlier, select 802.3.

- 802.2 specifies the 802.2 frame type.

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

  For NetWare 3.12 or later, select 802.2.

  802.2 is the default.

- SNAP specifies the SNAP frame type.

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

- Enet II specifies the Ethernet II frame type.

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

- None disables IPX routing and other IPX-specific features.

If you choose this setting, the Pipeline 25-Fx can bridge IPX, but without watchdog spoofing or the automatic RIP (Routing Information Protocol) and SAP (Service Advertising Protocol) data filters.

Dependencies: To determine the IPX frame type in use, enter the Config command on a NetWare server, or look at the NET.CFG file on an IPX client. Choose a setting based on this information:

- Select 802.3 if Frame=Ethernet_802.3.
- Select 802.2 if Frame=Ethernet_802.2.
- Select SNAP if Frame=Ethernet_SNAP.
- Select Enet II if Frame=Ethernet_II.

Parameter Location: Ethernet Profile, Mod Config/Ether options

---

IPX Net# (IPX only)

Description: This parameter lets you create a static route to another Ethernet network through the Connection Profile.

The value of IPX Net# specifies the network number of the router at the remote end of the connection.

Usage: Press Enter to open a text field. Then, type an Ethernet network number using an 8-digit (4-byte) hexadecimal value. The default is 00000000.

Specify the network number of the router at the remote end of the connection only if the router requires that the Pipeline 25-Fx know its network number before connecting. You almost never need to set this parameter in a Connection Profile.

If you accept the default of 00000000, the Connection Profile is still valid, but the Pipeline 25-Fx does not advertise the route until it makes a connection to the Ethernet network.

Example: `DE040600`

Dependencies: The IPX Net# parameter does not apply (IPX Net#=N/A) if the Pipeline 25-Fx is not set up for IPX routing (Route IPX=No).

Parameter Location: Connection Profile, Connections/IPX options

See Also: Route IPX

IPX Pool# (IPX only)

Description: This parameter specifies a unique IPX network number for all NetWare clients that are running PPP encapsulation and dialing in directly. The Pipeline 25-Fx assigns network addresses to dial-in NetWare clients when they connect to the Pipeline 25-Fx; these addresses are derived from this network number.

When you enter a value for IPX Pool#, the Pipeline 25-Fx advertises a route to this network.

Usage: Press Enter to open a text field. Then, type an Ethernet network number using an 8-digit (4-byte) hexadecimal value. The default is 00000000.

The number you specify must be unique within your wide area IPX network, and must match the configuration of other routers on the local Ethernet network.

Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- The dial-in Netware client must accept the network number set by IPX Pool#, although it can provide its own node number or accept a node number provided by the Pipeline 25-Fx.
- If IPX Frame=None or IPX Routing=No, IPX Pool#=N/A.

Example: `FF0000037`

Parameter Location: Ethernet Profile, Mod Config/Ether options

IPX RIP

Description: This parameter controls how IPX RIP will be handled on this WAN link.

When a Pipeline is used to connect NetWare clients to a very large IPX network, the IPX routing table created by the Pipeline may become very large and unmanageable, and can cause the Pipeline to run out of memory. As an alternative to maintaining these large routing tables locally, the Pipeline may have a static IPX route to the corporate network and disable IPX RIP. Either end of the WAN link may disable or fine-tune IPX RIP behavior.

Usage: Press Enter to cycle through the choices.

- Both indicates that the device will both send and receive RIP updates on this WAN link.

  Both is the default.
- Send means the device will send RIP updates but will not receive them.
- Recv means the device will receive RIP updates but will not send them.
- Off means the device will neither send nor receive IPX RIP updates on this WAN link.

Parameter Location: Connection Profile: Ethernet→Connection→any profile→ IPX options...

Dependencies: This parameter is N/A if Peer=Dialin. If this parameter is set to Off, a static IPX route is required to the remote network. A static route is defined in an IPX Routes Profile.

See Also: IPX SAP, Peer

IPX SAP

Description: This parameter controls how IPX SAP will be handled on this WAN link.

When a Pipeline is used to connect NetWare clients to a very large IPX network, the IPX service table created by the Pipeline may become very large and unmanageable, and can cause the Pipeline to run out of memory. As an

alternative to maintaining these large service tables locally, the Pipeline may create static service table entries and turn off IPX SAP. Either end of the WAN link may disable or fine-tune IPX SAP behavior.

Usage: Press Enter to cycle through the choices.

- Both indicates that the device will both send and receive SAP updates on this WAN link.

  Both is the default.
- Send means the device will send SAP updates but will not receive them.
- Recv means the device will receive SAP updates but will not send them.
- Off means the device will neither send nor receive IPX SAP updates on this WAN link.

Parameter Location: Connection Profile: Ethernet→Connection→any profile→ IPX options...

Dependencies: This parameter is N/A if Peer=Dialin. If this parameter is set to Off, a static IPX service table entry is required to the remote network. A static service entry is configured in an IPX Routes Profile.

See Also: IPX RIP, Peer

IPX SAP Filter (IPX only)

Description: This parameter specifies the number of an IPX SAP Filter Profile to be applied to a WAN session or to the Ethernet interface. Depending on how the IPX SAP Filter Profile has been defined, this parameter has one or both of the following effects:

- IPX SAP Input filters apply to all SAP packets that the Ascend unit receives.

  Input filters screen advertised services and exclude them from its service table as specified in the filters.
- IPX SAP Output filters apply to SAP response packets that the Ascend unit transmits.

  If the Ascend unit receives a SAP request packet, it applies Output filters before transmitting the SAP response, and excludes services from the response packet as specified in the filters.

Usage: Press Enter to open a text field. Then type a number between 1 and 8. The number corresponds to an IPX SAP Filter Profile in the IPX SAP Filters menu.

When you set IPX SAP Filter to 0 (zero), all SAP data is included in the service table. Zero is the default.

Press Enter again to close the text field.

Parameter Location: Ethernet Profile, Mod Config/Ether options
Answer Profile, Answer/Session options
Connection Profile, Connections/Session Options

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

---

IPX SAP Proxy

Description: This parameter enables or disables IPX SAP proxy mode in the Pipeline. When a Pipeline is used to connect NetWare clients to a very large IPX network, the SAP table created by the Pipeline can become very large and unmanageable. As an alternative, the Pipeline operating in proxy mode discards all SAP broadcasts seen on the network and resolves SAP queries from NetWare clients as it receives them, by forwarding the queries over the WAN link.

SAP proxy mode is recommended when only NetWare clients (not servers) are on the Ethernet side of Pipeline.

Note: If the Pipeline running in SAP proxy mode has NetWare servers on its Ethernet, it stores the relevant SAP entries for those servers and advertises them across the WAN interface as a normal SAP broadcast.

Usage: Press Enter to toggle between Yes and No.

- Yes enables proxy mode.
- No disables proxy mode.
  No is the default.

Parameter Location: Configure Profile
Ethernet Profile: Ethernet→Mod Config→Ether options...

Dependencies: For the Pipeline to run in proxy mode, you must supply the remote IPX network number and configure a static IPX route to that network.

See Also: IPX SAP Proxy Net #

IPX SAP Proxy Net#

Description: This parameter specifies the IPX network number of the device on the other end of the WAN link. The IPX network number must also be specified in an IPX Route Profile.

Usage: Press Enter to open a text field. Then type an 8-digit hexadecimal IPX network number. Press Enter again to close the text field.

Parameter Location: Configure
Ethernet Profile: Ethernet→Mod Config→Ether options...

Dependencies: This parameter is N/A if IPX SAP Proxy =Off, or if IPX Frame=None.

See Also: IPX SAP Proxy

LAN Adrs (IP only)

Description: This parameter specifies the IP address of a station or router at the remote end of the link specified by the Connection Profile.

Usage: Press Enter to open a text field. Then, type the IP address of a remote station or router; you can also specify a netmask.

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

The default setting is 0.0.0.0/0; an answering Connection Profile with this setting matches all incoming IP addresses.

If you do not enter a netmask, the Pipeline 25-Fx assumes the default for your network class:

- Class A: 1.0.0.0 to 127.255.255.255 /8

- Class B: 128.0.0.0 to 191.255.255.255 /16
- Class C: 192.0.0.0 to 223.255.255.255 /24

The netmask should not mask any network bits. For example, 130.15.3.44/12 is not valid because it is a Class B address whose netmask cannot be smaller than 16.

If you enter a 32-bit mask, you are specifying a connection to a specific host, rather than to a group of hosts on a subnet.

After you make your specifications, press Enter to close the text field.

Example: `200.207.23.101/24`

Dependencies: Keep this additional information in mind:

- The LAN Adrs parameter in the first Connection Profile is the same as the Rem Addr parameter in the Configure Profile.
- The value of the LAN Adrs parameter on the local Pipeline 25-Fx must match the IP Adrs parameter of the Ascend unit at the remote end of the link.
- No two calling Connection Profiles should have the same LAN Adrs.
- Setting LAN Adrs to 0.0.0.0/0 and clearing the Station parameter resets all parameters in the Connection Profile to their defaults.
- The LAN Adrs parameter does not apply (LAN Adrs=N/A) if the Pipeline 25-Fx does not support IP (Route IP=No).
- If you do not know the right IP address to enter, you must obtain it from the network administrator.

  Do not attempt to configure an IP address by guesswork!

Parameter Location: Connection Profile, Connections

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

Length

Description: This parameter indicates the number of bytes in a packet that the Pipeline 25-Fx compares to the setting of the Value parameter.

The Offset parameter specifies the starting position; the Pipeline 25-Fx ignores the portion of the packet that exceeds the Length specification. In other words, the Offset parameter hides the left-most bytes of data, while the Length parameter hides the right-most bytes of data.

The Pipeline 25-Fx applies the value of the Mask parameter before comparing the bytes to the setting of the Value parameter. The Mask value consists of the same number of bytes as the Length parameter. A mask hides the part of a number that appears behind the binary zeroes in the mask; for example, if Mask=ffff0000 in hexadecimal format, the Pipeline 25-Fx uses only the first 16 binary digits in the comparison, since f=1111 in binary format.

Usage: Press Enter to open a text field. Then, type the number of bytes to use for comparison. You can enter a number between 0 and 8.

The default value is 0. When you accept the default, Pipeline 25-Fx uses no bytes for comparison; all packets match the filter.

Press Enter again to close the text field.

Example: Suppose you have a filter that drops packets and has these specifications:

```
Forward=No
Offset=4
Length=3
Mask=ffffff
Value=123
More=No
```

When the 10-byte packet xycd123456 passes through the filter, the Pipeline 25-Fx removes the leading four bytes, because Offset=4. The data 123456 remains. Next, the Pipeline 25-Fx removes the trailing three bytes, because Length=3; only the value 123 remains. The Mask is ffffff, which contains all ones (1s) when converted to binary numbers; therefore, the Mask value does not hide any binary digits and passes 123 through. When the Pipeline 25-Fx compares 123 to the

setting of the Value parameter, a match occurs and the Pipeline 25-Fx does not forward the packet.

Dependencies: In a Filter Profile, Length does not apply (Length=N/A) for an IP filter (Type=IP).

Parameter Location: Filter Profile, Filter/Generic

See Also: Offset, Mask, Value

Link Comp

Description: This parameter turns data compression on or off for a PPP link.

Usage: Press Enter to cycle through the choices.

- Stac turns on data compression.
  The Pipeline 25-Fx applies the STACKER LZS compression/decompression algorithm. STAC is the default.
- MS-Stac turns on Microsoft LZS Coherency Compression for Windows 95.

Caution: Stacker LZS Compression (as defined in the Internet Draft of November 1995) and Microsoft LZS Coherency Compression for Windows 95 both use the same PPP option to indicate that their compression scheme is in use. That makes it difficult for routers to differentiate exactly which compression method a caller is requesting. Ascend units handle this ambiguity in the call by always using the compression scheme specified in the Connection Profile (or if there is no Connection Profile, in the Answer Profile). If the caller requests MS-Stac and the profile does not specify MS-Stac compression, the connection seems to come up correctly but no data is routed. If the profile is configured with MS-Stac and the caller does not acknowledge that compression scheme, the Pipeline 25-Fx attempts to use standard Stac compression, and if that doesn't work, it uses no compression.

- None turns off data compression.

Dependencies: Keep this additional information in mind:

- Both sides of the link must set Link Comp=Stac to turn on data compression.
- The Link Comp parameter applies only if the link uses PPP encapsulation (Encaps=PPP or Encaps=MPP).

When you choose Encaps=MPP, both the dialing side and the answering side of the link must support MP+. If only one side supports MP+, the connection uses MP or standard single-channel PPP. When you choose Encaps=PPP, the connection uses only PPP.

- Link Comp in the Answer Profile applies to incoming calls for which no Connection Profile exists; if a Connection Profile exists, the setting of its Link Comp parameter takes precedence.
- If Profile Reqd=Yes in the Answer Profile, Link Comp does not apply (Link Comp=N/A) in the Answer Profile.

Parameter Location: Answer Profile, Answer/PPP options
Connection Profile, Connections/Encaps options

See Also: VJ Comp

LQM

Description: This parameter specifies whether the Pipeline 25-Fx requests Link Quality Monitoring (LQM) when answering a PPP call.

LQM is a feature that enables the Pipeline 25-Fx to monitor the quality of a link. LQM counts the number of packets sent across the link and periodically asks the remote end how many packets it has received. Discrepancies are evidence of packet loss and indicate link quality problems.

LQM causes the generation of periodic link quality reports. Both ends of the link exchange these reports.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that the Pipeline 25-Fx requests LQM.
- No specifies that the Pipeline 25-Fx does not request LQM.
  No is the default.

Dependencies: Keep this additional information in mind:

- Both sides of the link negotiate the interval between periodic link quality reports; however, the interval must fall between the minimum interval (as set by LQM Min) and the maximum interval (as set by LQM Max).
- If LQM is turned off (LQM=No), LQM Max=N/A and LQM Min=N/A.

- LQM applies only if Encaps=PPP.
- LQM in the Answer Profile applies to incoming calls for which no Connection Profile exists; if a Connection Profile exists, the setting of its LQM parameter takes precedence.
- If Profile Reqd=Yes in the Answer Profile, LQM does not apply (LQM=N/A) in the Answer Profile.

Parameter Location: Answer Profile, Answer/PPP options
Connection Profile, Connections/Encaps options

See Also: Encaps, LQM Max, LQM Min

LQM Max

Description: This parameter specifies the maximum duration between link quality reports, measured in tenths of a second.

Usage: Press Enter to open a text field. Then, type a number between 0 and 600. The default is 600. Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- If LQM=No, the LQM Max parameter does not apply (LQM Max=N/A).
- LQM Max in the Answer Profile applies to incoming calls for which no Connection Profile exists; if a Connection Profile exists, the setting of its LQM Max parameter takes precedence.
- If Profile Reqd=Yes in the Answer Profile, LQM Max does not apply (LQM Max=N/A) in the Answer Profile.

Parameter Location: Answer Profile, Answer/PPP options
Connection Profile, Connections/Encaps options

See Also: LQM, LQM Min

LQM Min

Description: This parameter specifies the minimum duration between link quality reports, measured in tenths of a second.

Usage: Press Enter to open a text field. Then, type a number between 0 and 600. The default is 600. Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- If LQM=No, the LQM Min parameter does not apply (LQM Min=N/A).
- LQM Min in the Answer Profile applies to incoming calls for which no Connection Profile exists; if a Connection Profile exists, the setting of its LQM Min parameter takes precedence.
- If Profile Reqd=Yes in the Answer Profile, LQM Min does not apply (LQM Min=N/A) in the Answer Profile.

Parameter Location: Answer Profile, Answer/PPP options
Connection Profile, Connections/Encaps options

See Also: LQM, LQM Max

Mask

Description: In a filter of type Generic, this parameter specifies a 16-bit hexadecimal bitmask that the Pipeline 25-Fx applies to the data contained in the specified bytes in a packet. A mask hides the part of a number that appears behind the binary zeroes in the mask; for example, if Mask=ffff0000, the Pipeline 25-Fx uses only the first 16 binary digits in the comparison, since f=1111 in binary format.

The Pipeline 25-Fx applies the Mask parameter starting at the position specified by the Offset parameter. The setting you specify for Mask must contain the same number of bytes as the Length parameter. The Pipeline 25-Fx then compares the unmasked portion of the packet with the value specified by the Value parameter.

Usage: Press Enter to open a text field. Then, type a hexadecimal number. You can enter a number between 00 and ffffffffffffffff.

The default is 00. When you accept the default, the Pipeline 25-Fx uses the data in the packet as is for comparison purposes.

Press Enter to close the text field.

Example: This example specifies that the Pipeline 25-Fx masks all but the first 24 bits of the data:

```
Mask=ffffff0000000000
```

Dependencies: Mask does not apply (Mask=N/A) for an IP filter (Type=IP).

Parameter Location: Filter Profile, Filter/Generic

See Also: Length, Offset, Type, Value

Max Ch Count

Description: This specifies the maximum number of channels allowed on an MP+ call.

Usage: Press Enter to open a text field. Then, type a number between 1 and the maximum number of channels your system supports. The default setting is 1. Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- The Max Ch Count parameter applies only to dynamic MP+ calls (Encaps=MPP).
- Max Ch Count in the Answer Profile applies to incoming calls for which no Connection Profile exists; if a Connection Profile exists, the setting of its Max Ch Count parameter takes precedence.
- If Profile Reqd=Yes in the Answer Profile, Max Ch Count does not apply (Max Ch Count=N/A) in the Answer Profile.

Parameter Location: Answer Profile, Answer/PPP options
Connection Profile, Connections/Encaps options

See Also: Add Pers, Base Ch Count, Call Mgm, Encaps

Metric

Description: This parameter appears in a Connection Profile and a Static Rtes Profile. Its functionality differs depending on the profile:

- In a Connection Profile, the Metric parameter determines the virtual hop count of the link.
- In a Static Rtes Profile, the Metric parameter determines the virtual hop count of the route.

This parameter ensures that the Pipeline 25-Fx uses any available online channel before using a switched channel if there are two routes available to a single destination network. Although the actual hop count of the link or route is 1, you can enter any value between 1 and 15. This value is the virtual hop count. The higher the value entered, the less likely that the Pipeline 25-Fx will bring the link or route online. Once the connection or route is online, its metric defaults to 1.

Usage: Press Enter to open a text field, Then, type a number between 1 and 15. The default setting is 7. Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- The hop count includes the metric of each switched link in the route.

Parameter Location: Connection Profile, Connections
Static Rtes

See Also: Private

Min Ch Count

Description: This parameter specifies the minimum number of channels an MP+ call maintains.

Usage: Press Enter to open a text field. Then, type a number between 1 and 32. The default setting is 1. Press Enter again to close the text field.

Dependencies: The Min Ch Count parameter applies only to MP+ calls (Encaps=MPP).

Parameter Location: Connection Profile, Connections/Encaps options
Answer Profile, Answer/PPP options

See Also: Max Ch Count

More

Description: In a filter of type Generic, this parameter specifies whether the Pipeline 25-Fx passes the packet to the next filter specification in the profile.

Use this parameter when you need a generic filter wider than the 8-byte limit of the Length parameter. For example, suppose a packet is 16 bytes long (128 bits). You can compare only 8 bytes in a filter because the maximum value of the Length parameter is 8. To compare all 16 bytes, you specify two 8-byte filters linked by the More parameter.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that the Pipeline 25-Fx applies the next filter in the profile before deciding whether to forward the packet.

  If you set More=Yes, the filter can examine multiple noncontiguous bytes within a packet by "marrying" the current filter to the one that immediately follows it.
- No specifies that the Pipeline 25-Fx does not apply the next filter in the profile before deciding whether to forward the packet.

  No is the default.

Example: Input filter 01 and input filter 02 examine different bytes of the same packet and apply a logical AND to the results in order to determine whether the packet matches the specification:

```
In filter 01...Valid=Yes
In filter 01...Type=Generic
In filter 01...Generic...Forward=No
In filter 01...Generic...Offset=04
In filter 01...Generic...Length=8
In filter 01...Generic...Value=abc
In filter 01...Generic...More=Yes
```

```
In filter 02...Valid=Yes
In filter 02...Type=Generic
In filter 02...Generic...Forward=No
In filter 02...Generic...Offset=2
In filter 02...Generic...Length=8
In filter 02...Generic...Value=123
In filter 02...Generic...More=No
```

In this example, the Pipeline 25-Fx compares 16 bytes of each data packet. The match occurs only if *all the* noncontiguous bytes contain the specified values.

Dependencies: Keep this additional information in mind:

- The More parameter does not apply (More=N/A) if you are using an IP filter (Type=IP).
- The next filter must be a Generic filter (Type=Generic) and must be activated (Valid=Yes); otherwise, the Pipeline 25-Fx ignores the filter.

Parameter Location: Filter Profile, Filter/Generic

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

MRU

Description: This parameter specifies the maximum number of bytes the Pipeline 25-Fx can receive in a single packet on a PPP link. MRU stands for Maximum Receive Unit.

Usage: The default setting is 1524; you should accept this default unless the device at the remote end of the link cannot support it.

If the administrator of the remote network specifies that you must change this value, press Enter to open a text field. Type a number between 1 and 1524.

Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- The MRU parameter applies to any link using PPP encapsulation (Encaps=MPP or Encaps=PPP).

When you choose Encaps=MPP, both the dialing side and the answering side of the link must support MP+. If only one side supports MP+, the connection uses MP or standard single-channel PPP. When you choose Encaps=PPP, the connection uses only PPP.

- MRU in the Answer Profile applies to incoming calls for which no Connection Profile exists; if a Connection Profile exists, the setting of its MRU parameter takes precedence.
- If Profile Reqd=Yes in the Answer Profile, MRU does not apply (MRU=N/A) in the Answer Profile.

Parameter Location: Answer Profile, Answer/PPP options
Connection Profile, Connections/Encaps options

See Also: Encaps

My Addr (IP only)

See "IP Adrs (IP only)" on page 11-45.

My Name

See "Name" on page 11-67.

My Num A

Description: This parameter specifies the phone number assigned to the line. If two phone numbers are assigned to the line, specify one here and one in My Num B.

When the Pipeline 25-Fx receives a multichannel MP+ call, it reports the primary phone number (My Num A) and the secondary phone number (My Num B) to the calling party. The calling Pipeline 25-Fx can then add more channels. If you do not specify a phone number and the calling Pipeline 25-Fx needs to add more channels, it redials the phone number it used to make the first connection.

Usage: Press Enter to open a text field and then type a telephone number. The character set is limited to the following characters:

1234567890()[]!z-*#”

You can include a hyphen in the phone number but no spaces.

Example: 5105551972

Parameter Location: Configure...

Dependencies: You must get this number from the telephone company providing your service.

See Also: My Num B

My Num B

Description: This parameter specifies the phone number assigned to the line. If two phone numbers are assigned to the line, specify one here and one in My Num A.

When the Pipeline 25-Fx receives a multichannel MP+ call, it reports the primary phone number (My Num A) and the secondary phone number (My Num B) to the calling party. The calling Pipeline 25-Fx can then add more channels. If you do not specify a phone number and the calling Pipeline 25-Fx needs to add more channels, it redials the phone number it used to make the first connection.

Usage: Press Enter to open a text field and then type a telephone number. The character set is limited to the following characters:

1234567890()[]!z-*#”

You can include a hyphen in the phone number but no spaces.

Example: 5105551972

Parameter Location: Configure...

Dependencies: You must get this number from the telephone company providing your service.

See Also: My Num A

Name

Description: This parameter appears in each of these profiles:

- Security Profile
- Filter Profile
- System Profile
- IPX SAP Filters Profile
- Static Rtes Profile

The functionality of the Name parameter differs depending on the profile:

- In a Security Profile, Filter Profile, System Profile, or IPX SAP Filters Profile, the Name parameter specifies the name of the profile.

  The Pipeline 25-Fx sends the System Profile name to the remote device whenever it establishes a PPP link. The System Profile name appears in the top line of the Edit display of the Control Monitor. Always enter a system name to identify the Pipeline 25-Fx.

  When the Pipeline 25-Fx receives a PPP or MP+ call from an Ascend unit, it tries to match the caller's Name to the value of the Station parameter in some Connection Profile. If the Pipeline 25-Fx finds a match and authentication is turned on, the Pipeline 25-Fx then tries to match the caller's Send PW value to the Recv PW value in that same Connection Profile.

  The Control Monitor is the menu-based user interface for configuring, managing, and monitoring the Pipeline 25-Fx. It consists of nine windows—eight status windows and a single edit window.

  Note: The Name parameter in the System Profile is the same as the My Name parameter in the Configure Profile.

- In a Static Rtes Profile, the Name parameter specifies the name of the route's destination.

  Note that you cannot change the name of the first route; its value is always Default.

Usage: Press Enter to open a text field. Then, type a name. You can enter up to 72 characters for the Name parameter in all profiles except the Static Rtes Profile. In this profiles, you can enter up to 31 characters for the Name parameter.

Because the Pipeline 25-Fx uses the Name parameter in the System Profile for authentication, you must type it exactly as the remote network expects it. In this case, Name is case sensitive.

Press Enter again to close the text field.

Parameter Location: Security Profile, Security
Filter Profile, Filters
Dial Plan Profile, Dial Plan
System Profile, Sys Config
IPX SAP Filter Profile, IPX SAP Filters
Static Rtes Profile, Static Rtes

Net Adrs

Description: In a Bridging Profile, this parameter specifies the IP address of a device at the remote end of the link.

The Pipeline 25-Fx uses the Bridging Profile to build a bridge table of matching MAC and IP addresses. The Net Adrs parameter corresponds to the IP address of each remote device; the Enet Adrs parameter corresponds to the MAC address of each remote device.

These parameters enable the Pipeline 25-Fx to perform proxy ARP (Address Resolution Protocol). Whenever the Pipeline 25-Fx receives an ARP request from a specified IP address, it checks to see whether the IP address matches one in its bridge table. If it does, the Pipeline 25-Fx returns its own MAC address.

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

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

The default value is 0.0.0.0/0.

Press Enter to close the text field.

Example: `200.207.23.101/24`

Parameter Location: Bridging Profile, Bridge Adrs

See Also: Enet Adrs

NetWare t/o (IPX only)

Description: This parameter specifies the length of time, in minutes, that the Pipeline 25-Fx performs watchdog spoofing for NetWare connections. Here is an explanation of watchdog spoofing:

Ordinarily, when a NetWare server does not receive a reply to the watchdog session keepalive packets it sends to a client, it closes the connection. When you select Server mode for the Handle IPX parameter, however, the Pipeline 25-Fx replies to NCP watchdog requests on behalf of clients on the other side of the bridge; in other words, the Pipeline 25-Fx tricks the server watchdog process into believing that the link is still active.

Ordinarily, when a NetWare server does not receive a reply to the watchdog session keepalive packets it sends to a client, it closes the connection. When you select Server mode for the Handle IPX parameter, however, the Pipeline 25-Fx replies to NCP watchdog requests on behalf of clients on the other side of the bridge; in other words, the Pipeline 25-Fx tricks the server watchdog process into believing that the link is still active.

The time period for watchdog spoofing specified by the NetWare t/o parameter begins when the WAN session goes offline. If the WAN session reconnects, the Pipeline 25-Fx cancels the timeout.

NetWare t/o applies when the Pipeline 25-Fx is on a LAN containing a NetWare server.

Usage: Press Enter to open a text field. Then, type the timeout value in minutes. You can enter any value from 0 to 65535. The default value is 0 (zero); when you accept the default, the Pipeline 25-Fx responds to server watchdog requests indefinitely. Press Enter again to close the text field.

Dependencies: The NetWare t/o parameter does not apply (NetWare t/o=N/A) if IPX Frame=None or if Route IPX=No.

Parameter Location: Connection Profile, Connections/IPX options

See Also: IPX Frame

Network (IPX only)

Description: This parameter specifies the unique internal network number assigned to the NetWare server.

Usage: Press Enter to open a text field. Then, type the unique 4-byte hexadecimal number provided by your network administrator. The values 00000000 and ffffffff are not valid. Press Enter again to close the text field.

Example: `A00100001`

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

Parameter Location: IPX Route Profile, IPX Routes

See Also: Route IPX

Node IPX only)

Description: This parameter specifies the node number of the NetWare server.

Usage: Press Enter to open a text field. Then, type the node number of the server. Typically, a server running NetWare 3.11 or later has a node number of 0000000000001. Press Enter again to close the text field.

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

Parameter Location: IPX Route Profile, IPX Routes

See Also: Route IPX

Offset

Description: In a filter of type Generic, this parameter specifies the number of bytes masked from the start of the packet. The byte position specified by the Offset parameter is called the byte-offset.

Starting at the position specified by the Offset parameter, the Pipeline 25-Fx applies the value of the Mask parameter. A mask hides the part of a number that appears behind the binary zeroes in the mask; for example, if Mask=ffff0000 in hexadecimal format, the Pipeline 25-Fx uses only the first 16 binary digits in the comparison, since f=1111 in binary format. The Pipeline 25-Fx then compares the unmasked portion of the packet specified by the Length parameter with the value specified by the Value parameter.

Usage: Press Enter to open a text field. Then, type the number of starting bytes in a packet that the Pipeline 25-Fx ignores for comparison and masking purposes.

The default is 0. When you accept the default, the Pipeline 25-Fx starts comparing and masking data at byte 1.

Press Enter again to close the text field.

Example: Suppose you have a filter that drops packets and has these specifications:

```
Forward=No
Offset=4
Length=3
Mask=ffffff
Value=123
More=No
```

When the 10-byte packet xycd123456 passes through the filter, the Pipeline 25-Fx removes the leading four bytes, because Offset=4. The data 123456 remains. Next, the Pipeline 25-Fx removes the trailing three bytes, because Length=3; only the value 123 remains. The Mask is ffffff, which contains all ones (1s) when converted to binary numbers; therefore, the Mask value does not hide any binary digits and passes 123 through. When the Pipeline 25-Fx compares 123 to the setting of the Value parameter, a match occurs and the Pipeline 25-Fx does not forward the packet.

Dependencies: Keep this additional information in mind:

- The Offset parameter does not apply (Offset=N/A) for an IP filter (Type=IP).
- If a previous filter set More=Yes, Offset starts at the endpoint of the previous segment.

Parameter Location: Filter Profile, Filter

See Also: Length, Mask, More

Operations

Description: This parameter enables or disables read-only security.

Usage: Press Enter to toggle between Yes and No.

- Yes enables users to view Pipeline 25-Fx profiles and change the value of any parameter.

  Yes is the default.
- No permits users to view Pipeline 25-Fx profiles, but not to change the value of any parameter.

  If you specify No, users cannot access most DO commands. Only DO Esc and DO password are available.

Parameter Location: Security Profile, Security

Passwd

Description: This parameter the password that activates a Security Profile. The first Security Profile, Default, has no password.

Usage: Press Enter to open a text field. Then, type up to 20 characters. Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- Passwd is case sensitive.

  The user must enter the password exactly as you specify it here.
- If the value of the Passwd parameter in the Security Profile is *SECURE*, you cannot edit Security Profiles.

If you want to edit Security Profiles, you must log into a Security Profile whose Edit Security parameter is set to Yes.

Parameter Location: Security Profile, Security

See Also: Edit Security

Peer (IPX only)

Description: This parameter lets you select between two classes of peers to connect via the Pipeline 25-Fx—IPX routers and standalone workstations. It is best to allow two classes of peers to connect through an Ascend unit; other IPX routers, and standalone workstations. Typically, standalone workstations are mobile stations that connect via modem. By specifying a peer class for each Connection Profile, you can improve network security.

Usage: Press Enter to cycle through the choices.

- Router specifies that the caller is an IPX router.
  Router is the default.
- Dialin specifies that the caller is a dial-in NetWare client that incorporates PPP software and dial-out hardware, but does not have an Ethernet interface.
  This setting causes the Pipeline 25-Fx to assign the caller an IPX address derived from the value of IPX Pool#.

Dependencies: If IPX Frame=None or Route IPX=No, Peer=N/A.

Parameter Location: Connection Profile, Connections/IPX options

See Also: IPX Pool#

Phone 1 Usage

Description: This parameter specifies the Service Profile Identifier (SPID) for a telephone or other analog device connected to the Phone 1 port of the Pipeline. For all types of ISDN service that use SPIDs, incoming voice calls to the direc-

tory number (telephone number) corresponding to this SPID are routed to the Phone 1 port.

SPIDs identify devices connected to the ISDN line. All types of ISDN service except AT&T Custom Point-to-Point use SPIDs to specify the device that receives an incoming call. When you order ISDN service for a Pipeline, you normally get two SPIDs, one for each directory number (telephone number).

Each SPID for a Pipeline can identify more than one device. It identifies the Pipeline when the corresponding directory number is used for an incoming data call. It identifies a telephone or other analog device when the device uses the corresponding directory number for an incoming voice call. This sharing of SPIDs is possible because a single directory number can handle data or voice, but not both at the same time. The description of the Data Usage parameter explains how to use the same SPIDs for data.

Usage: Press Enter to cycle through the choices.

- Choose A to route incoming voice calls for the directory number corresponding to the SPID A parameter to the Phone 1 jack. This is normally the directory number specified by the My Num A parameter.
- Choose B to route incoming voice calls for the directory number corresponding to the SPID B parameter to the Phone 1 jack. This is normally the directory number specified by the My Num B parameter.
- Choose None to prevent analog calls from being routed to the Phone 1 jack.

Dependencies: AT&T Custom Point-to-Point service does not use SPIDs. Because of this, the Phone 1 Usage parameter is N/A for Custom Point-to-Point service. With Custom Point-to-Point service, the Pipeline can handle only one voice call at a time. An incoming voice call is always routed to the Phone 1 jack.

Parameter Location: Configure Profile, BRI

Parameter Location: Configure Profile

See Also: Phone 2 Usage, Data Usage

Phone 2 Usage

Description: This parameter specifies the Service Profile Identifier (SPID) for a telephone or other analog device connected to the Phone 2 port of the Pipeline. All incoming voice calls to the directory number (telephone number) corresponding to this SPID are routed to the Phone 2 port.

SPIDs identify devices connected to the ISDN line. All types of ISDN service except AT&T Custom Point-to-Point use SPIDs to specify the device that receives an incoming call. When you order ISDN service for a Pipeline, you normally get two SPIDs, one for each directory number (telephone number).

Each SPID for a Pipeline can identify more than one device. It identifies the Pipeline when the corresponding directory number is used for an incoming data call. It identifies a telephone or other analog device when the device uses the corresponding directory number for an incoming voice call. This sharing of SPIDs is possible because a single directory number can handle data or voice, but not both at the same time. The Description of the Data Usage parameter explains how to use the same SPIDs for data.

Usage: Press Enter to cycle through the choices.

- Choose A to route incoming voice calls for the directory number corresponding to the SPID A parameter to the Phone 2 jack. This is normally the directory number specified by the My Num A parameter.
- Choose B to route incoming voice calls for the directory number corresponding to the SPID B parameter to the Phone 2 jack. This is normally the directory number specified by the My Num B parameter.
- Choose None to prevent analog calls from being routed to the Phone 2 jack.

Dependencies: AT&T Custom Point-to-Point service does not use SPIDs. Because of this, the Phone 2 Usage parameter is N/A for Custom Point-to-Point service. With Custom Point-to-Point service, the Pipeline can handle only one voice call at a time. Incoming voice calls are always routed to the Phone 1 jack.

Parameter Location: Configure Profile, BRI

Parameter Location: Configure Profile

See Also: Phone 1 Usage, Data Usage

Phone Num Binding

Description: This parameter forces an outgoing call to use the directory number for the port to which the device is connected. It is N/A unless the value of the Switch Type parameter is NTI (Northern Telecom Custom) or NI-1 (National ISDN-1).

When ISDN service is provided by a Northern Telecom DMS-100 switch, each B channel is associated with a particular directory number (telephone number). Because of this, when a B channel is in use, its directory number is not available. If Phone Number Binding is set to No, an outgoing call that would normally be made on a particular directory number can be made on the other directory number if the B channel for the first directory number is already in use and the B channel for the second directory number is free.

If outgoing calls must come from a particular telephone number to be identified by Caller ID, setting Phone Number Binding to Yes ensures that the call is made using the directory number for the port to which the device is connected. If the B channel for this directory number is already in use, the call cannot be made.

When Phone Number Binding is N/A, any call originated at the Pipeline 25-Fx is associated with the phone number set in the Data/Phone Usage parameters. If the outgoing call is a data call and Data Usage is set to A+B, the data call will be placed from the first available phone number.

Usage: Press Enter to toggle between Yes and No.

- Yes means that an outgoing call is always made on the directory number for the port to which the device is connected. If the B channel for this directory number is already in use, the call cannot be made. Set this parameter to Yes only if calls *must* be made on a particular directory number to be identified by Caller ID.
- No means an outgoing call that would normally be made on a particular directory number can be made on the other directory number if the B channel for the first directory number is already in use and the B channel for the second directory number is free.

Dependencies: This parameter is N/A unless your ISDN switch type is NTI or NI-1.

Parameter Location: Configure Profile, BRI

Parameter Location: Configure Profile

See Also: Data Usage

Preempt

Description: This parameter specifies the number of idle seconds the Pipeline 25-Fx waits before using one of the channels of an idle link for a new call.

Usage: Press Enter to open a text field. Then, type a number between 0 and 65535. The Pipeline 25-Fx sets no time limit if you enter 0 (zero). The default setting is 60. Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- Preempt in the Answer Profile applies to incoming calls for which no Connection Profile exists; if a Connection Profile exists, the setting of its Preempt parameter takes precedence.
- If Profile Reqd=Yes in the Answer Profile, Preempt does not apply (Preempt=N/A) in the Answer Profile.

Parameter Location: Answer Profile, Answer/Session options
Connection Profile, Connections/Session options

See Also: Idle

Preference

Description: This parameter specifies the preference value for a statically configured IP route, which may be defined in an IP Route Profile or Connection 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, then the router compares the Metric field, using the route with the lower Metric.

Usage: Enter a Preference value.

The default value for static routes (configured in the IP Route Profile or Connection Profile) is 100. The default value for connected routes (such as the Ethernet) is 0. The following values are assigned to dynamic routes:

- OSPF routes=10
- ICMP redirects=30
- RIP routes=100
- ATMP routes=100

This set of preference values gives static routes and RIP routes an equal value, with ICMP Redirects taking precedence over both. Note that OSPF routes take precedence over the other types.

Parameter Location: Connection Profile: Connections/any profile/IP Options
IP Route Profile: Static Rtes/any profile/

Private

Description: This parameter appears in a Connection Profile and a Static Rtes Profile. Its functionality differs depending on the profile:

- In a Connection Profile, the Private parameter specifies whether the Pipeline 25-Fx discloses the IP address indicated by LAN Adrs when queried by RIP (Routing Information Protocol) or another routing protocol.
- In a Static Rtes Profile, the Private parameter specifies whether the Pipeline 25-Fx discloses the existence of the IP address indicated in the route when queried by RIP or another routing protocol.

Usage: Press Enter to toggle between Yes and No.

- Yes disables advertising.

  The Pipeline 25-Fx does not advertise the IP address in RIP updates that it sends.
- No enables advertising.

  The Pipeline 25-Fx advertises the IP address in RIP updates that it sends.

  No is the default.

Dependencies: Keep this additional information in mind:

- The Private parameter does not apply (Private=N/A) if the Pipeline 25-Fx does not support IP (Route IP=No).

Parameter Location: Connection Profile, Connections/IP options
Static Rtes Profile, Static Rtes

See Also: LAN Adrs, Metric, Route IP

Profile Reqd

Description: This parameter specifies whether the Pipeline 25-Fx rejects incoming calls for which it could find no Connection Profile and no entry on a remote authentication server.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that the Pipeline 25-Fx rejects incoming calls for which it can find no Connection Profile and no entry on a remote authentication server.
- No specifies that the Pipeline 25-Fx does not require a Connection Profile or a remote authentication entry.

  No is the default.

You can satisfy the Profile Reqd parameter in one of these ways:

- The source IP address of the caller matches the LAN Adrs parameter in a local Connection Profile.

  In this case, Encaps=MPP or Encaps=PPP.
- The source name of the caller matches the Station parameter in a local Connection Profile.

  In this case, Encaps=PPP or Encaps=MPP, and Recv Auth=PAP or Recv Auth=CHAP.
- The source MAC address of the caller matches the Station parameter in a local Connection Profile.

Dependencies: If you get incoming PPP bridging calls (Route IP=No) and Profile Reqd=Yes, you must also specify that the Pipeline 25-Fx authenticate incoming calls using PAP or CHAP (Recv Auth=PAP or Recv Auth=CHAP). A Connection Profile cannot match a PPP bridging call except through the name of the caller that PAP or CHAP authentication provides.

Parameter Location: Answer Profile, Answer

See Also: Encaps, Recv Auth, Route IP

Protocol

Description: In a filter of type IP, this parameter specifies the protocol number to which the Pipeline 25-Fx compares a packet's protocol number.

Usage: Press Enter to open a text field. Then, type the number of the protocol. You can enter a number between 0 and 255. The default setting is 0 (zero). When you accept the default, the Pipeline 25-Fx disregards the Protocol parameter when applying the filter.

Protocols and their associated numbers appear in Table 11-2.

Table 11-2. Protocols

Number	Name
1	ICMP (Internet Control Message Protocol)
2	IGMP (Internet Group Management Protocol)
3	GGP (Gateway-to-Gateway Protocol)
4	IP (Internet Protocol)
5	ST (Stream)
6	TCP (Transmission Control Protocol)
7	UCL
8	EGP (Exterior Gateway Protocol)
9	Any private interior gateway protocol
10	BBN-RCC-MON (BBN RCC Monitoring)
11	NVP-II (Network Voice Protocol II)
12	PUP
13	ARGUS

Table 11-2. Protocols

Number	Name
14	EMCOM
15	XNET (Cross-Net Debugger)
16	CHAOS
17	UDP (User Datagram Protocol)
18	MUX (Multiplexing)
19	DCN-MEAS (DCN Measurement Subsystems)
20	HMP (Host Monitoring Protocol)
21	PRM (Packet Radio Measurement)
22	XNS IDP (Xerox Networking System Internetwork Datagram Protocol)
23	TRUNK-1
24	TRUNK-2
25	LEAF-1
26	LEAF-2
27	RDP (Reliable Data Protocol)
28	IRTP (Internet Reliable Transport Protocol)
29	ISO-TP4 (International Standards Organization Transport Protocol Class 4)
30	NETBLT (Bulk Data Transfer Protocol)
31	MFE-NSP (MFE Network Services Protocol)
32	MERIT-INP (MERIT Internodal Protocol)

Table 11-2. Protocols

Number	Name
33	SEP (Sequential Exchange Protocol)
34	3PC (Third Party Connect Protocol)
35	IDPR (Inter-Domain Policy Routing Protocol)
36	XTP
37	DDP (Datagram Delivery Protocol)
38	IDPR-CMTP (IDPR Control Message Transport Protocol)
39	TP++ (TP++ Transport Protocol)
40	IL (IL Transport Protocol)
41	SIP (Simple Internet Protocol)
42	SDRP (Source Demand Routing Protocol)
43	SIP-SR (SIP Source Route)
44	SIP-FRAG (SIP Fragment)
45	IDRP (Inter-Domain Routing Protocol)
46	RSVP (Reservation Protocol)
47	GRE (General Routing Encapsulation)
48	MHRP (Mobile Host Routing Protocol)
49	BNA
50	SIPP-ESP (SIPP Encap Security Payload)
51	SIPP-AH (SIPP Authentication Header)

Table 11-2. Protocols

Number	Name
52	I-NLSP (Integrated Net Layer Security Protocol)
53	SWIPE (IP with Encryption)
54	NHRP (Next Hop Resolution Protocol)
55-60	Unassigned
61	Any Host Internet Protocol
62	CFTP
63	Any local network
64	SAT-EXPAK (SATNET and Backroom EXPAK)
65	KRYPTOLAN
66	RVD (MIT Remote Virtual Disk Protocol)
67	IPPC (Internet Pluribus Packet Core)
68	Any distributed file system
69	SAT-MON (SATNET Monitoring)
70	VISA (VISA Protocol)
71	IPCU (Internet Packet Core Utility)
72	CPNX (Computer Protocol Network Executive)
73	CPHB (Computer Protocol Heart Beat)
74	WSN (Wang Span Network)
75	PVP (Packet Video Protocol)

Table 11-2. Protocols

Number	Name
76	BR-SAT-MON (Backroom SATNET Monitoring)
77	SUN-ND PROTOCOL-Temporary
78	WB-MON (WIDEBAND Monitoring)
79	WB-EXPAK (WIDEBAND EXPAK)
80	ISO-IP (International Standards Organization Internet Protocol)
81	VMTP
82	SECURE-VMTP
83	VINES
84	TTP
85	NSFNET-IGP (National Science Foundation Network Interior Gateway Protocol)
86	DGP (Dissimilar Gateway Protocol)
87	TCF
88	IGRP
89	OSPF (Open Shortest Path First)
90	Sprite-RPC
91	LARP (Locus Address Resolution Protocol)
92	MTP (Multicast Transport Protocol)
93	AX.25 (AX.25 Frames)
94	IPIP (IP-within-IP Encapsulation Protocol)

Table 11-2. Protocols

Number	Name
95	MICP (Mobile Internetworking Control Protocol)
96	SCC-IP (Semaphore Communications Security Protocol)
97	ETHERIP (Ethernet-within-IP Encapsulation)
98	ENCAP (Encapsulation Header)
99	Any private encryption scheme
100	GMTP
101-254	Unassigned
255	Reserved

Dependencies: The Protocol parameter applies only if the filter is of type IP (Type=IP) and is activated (Valid=Yes).

Parameter Location: Filter Profile, Filter/IP

See Also: Type, Valid

Proxy Mode

Description: This parameter specifies under what conditions the Pipeline 25-Fx performs a proxy ARP (Address Resolution Protocol). The Pipeline 25-Fx performs a proxy ARP when it recognizes the IP address of a remote device in an ARP request, and then responds to the ARP request by sending its own MAC address.

Usage: Press Enter to cycle through the choices.

- Always specifies that the Pipeline 25-Fx responds to an ARP request regardless of whether a connection to the remote site is up.

- Inactive specifies that the Pipeline 25-Fx 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 25-Fx responds to an ARP request only if a connection to the remote site is up, regardless of whether a Connection Profile exists for the link.
- Off disables proxy mode.

  Off is the default.

Dependencies: Keep this additional information in mind:

- The Proxy Mode parameter does not apply (Proxy Mode=N/A) if the Pipeline 25-Fx does not support IP (Route IP=No).
- Enabling Proxy Mode may prevent the Pipeline 25-Fx from placing calls simply for address lookups.

Parameter Location: Ethernet Profile, Mod Config/Ether options

See Also: Net Adrs, Route IP

Recv Auth

Description: This parameter specifies the authentication protocol that the Pipeline 25-Fx uses when receiving and verifying a password for an incoming PPP call.

Usage: Press Enter to cycle through the choices.

- None specifies that the Pipeline 25-Fx does not use an authentication protocol to validate incoming calls.

  None is the default.
- PAP (Password Authentication Protocol) is a PPP authentication protocol.

  PAP provides a simple method for a host to establish its identity in a two-way handshake. Authentication takes place only upon initial link establishment, and does not use encryption.

  If you choose PAP, the Pipeline 25-Fx uses this protocol for authentication. The remote device must support PAP.
- CHAP (Challenge Handshake Authentication Protocol) is a PPP authentication protocol.

CHAP is more secure than PAP. CHAP provides a way to periodically verify the identity of a host using a three-way handshake and encryption. Authentication takes place upon initial link establishment; the Pipeline 25-Fx can repeat the authentication process any time after the connection is made.

If you choose CHAP, the Pipeline 25-Fx uses this protocol for authentication. The remote device must support CHAP.

- Either specifies that the Pipeline 25-Fx can use either PAP or CHAP.

  When you select Either, the Pipeline 25-Fx first requests authentication using CHAP, the more secure protocol. If the dial-in call rejects the request (or doesn't acknowledge it), the Pipeline 25-Fx then requests PAP authentication. If the dial-in call rejects the PAP request, the Pipeline 25-Fx terminates the link and drops the call.

Dependencies: Keep this additional information in mind:

- The link must use PPP encapsulation (Encaps=PPP).
- If you choose PAP or CHAP, you must also specify a password using Recv PW in a Connection Profile, or Auth Host on an authentication server.
- When you set Recv Auth=PAP, CHAP, or Either, the Pipeline 25-Fx can determine the IP address of a caller, even if the caller does not specify an address; the Pipeline 25-Fx derives the IP address from the Connection Profile.

Parameter Location: Answer Profile, Answer/PPP options

See Also: Recv PW, Send Auth, Send PW

Recv PW

Description: This parameter specifies the password that the remote end of the link must send. If the password specified by Recv PW does not match the remote end's value for Send PW, the Pipeline 25-Fx disconnects the link.

Usage: Press Enter to open a text field. Then, type the password that the Pipeline 25-Fx requires from the remote device on an incoming call. You can enter up to 20 characters; the password is case sensitive. Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- If Recv Auth=None, the Recv PW parameter does not apply (Recv PW=N/A).
- You must specify a value for Recv PW when the link uses PPP encapsulation (Encaps=PPP or Encaps=MPP) and the Pipeline 25-Fx uses either PAP or CHAP authentication (Recv Auth=PAP or Recv Auth=CHAP).

  When you choose Encaps=MPP, both the dialing side and the answering side of the link must support MP+. If only one side supports MP+, the connection uses MP or standard single-channel PPP. When you choose Encaps=PPP, the connection uses only PPP.
- You can store additional passwords on an authentication host.

Parameter Location: Connection Profile, Connections/Encaps options

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

Rem Addr (IP only)

See "LAN Adrs (IP only)" on page 11-54.

Rem Name

See "Station" on page 11-107.

Remote Mgmt

Description: This parameter specifies whether the device at the remote end of an MPP call can operate the Pipeline 25-Fx remotely using the DO Beg/End Rem Mgm command. In remote management, the Pipeline 25-Fx uses bandwidth between sites over the management subchannel established by the MPP protocol.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that the remote device can remotely operate the Pipeline 25-Fx. Yes is the default.
- No specifies that the remote device cannot remotely operate the Pipeline 25-Fx.

If the remote device tries to do so, the error message Remote Management Denied appears.

Dependencies: The Encaps parameter must be set to MPP.

Parameter Location: System Profile, Sys Config

See Also: DO Beg/End Rem Mgm in the "DO Command Reference" on page 11-121.

Renewal Time (IP only)

Description: This parameter specifies the lease time, in seconds, for the address defined in the Spoof Adr parameter. The default is 10 seconds. This value represents the amount of time the address will be assigned to the requesting client. After the specified number of seconds, the client must attempt to secure the IP address again. If an authenticated dial-up session is active, the Pipeline 25-Fx refuses the request, forcing the client to obtain its real IP address from the DHCP server on the remote network.

Usage: Press Enter to open a text field, and then type a number between 3 and 65535 (default 10). Press Enter again to close the text field.

Example: 60

Parameter Location: Ethernet Profile, Mod Config/DHCP Spoofing...

Dependencies: The DHCP Spoofing and Spoof Adr parameters must be configured for this feature to work.

See Also: DHCP Spoofing, Spoof Adr

Restore Cfg

Description: This command restores profiles saved using the Save Cfg parameter, or transfers the profiles to another Pipeline 25-Fx. Because the Save Cfg command does not save passwords, the Restore Cfg command does not restore them.

Usage: Follow these instructions to restore your configuration from backup:

1. Enable the Upload parameter in the Security Profile (Upload=Yes).
2. Verify that your terminal emulation program has a disk capture feature; this feature enables your emulator to capture to disk the ASCII characters it receives at its serial host port.
3. Verify that your terminal emulation program has an autotype feature; this feature enables your emulator to transmit over its serial host port the contents of a file it has built through disk capture.
4. Connect the backup device to the Pipeline 25-Fx's Control port.
5. Set the data rate of your terminal emulation program to 9600 baud or lower.
6. Set the Term Rate parameter in the System Profile to 9600.
7. Make certain that you have the Edit Security privilege; if you restore without having the Edit Security privilege, you can be locked out of some or all operations.
8. Select Restore Cfg from the Sys Diag menu.
9. When the `Waiting for upload data` prompt appears, turn on the autotype function on your emulator and supply the filename of the saved Pipeline 25-Fx data.
10. Verify that the configuration data is going to your terminal emulation screen and is being restored to the target Pipeline 25-Fx.

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

Parameter Location: Sys Diag

See Also: Save Cfg

Route

Description: This parameter specifies what type of routing (if any) applies to the first Connection Profile as well as to the Answer Profile.

Usage: Press Enter to cycle through the choices.

- None sets your Pipeline 25-Fx as a bridge (default).
- IP sets your Pipeline 25-Fx as an IP router.
- IPX sets your Pipeline 25-Fx as an IPX router.

Dependencies: Keep this additional information in mind:

- The Route setting in the Configure Profile determines the value of the Route IP and Route IPX parameters in the first Connection Profile and in the Answer Profile.
- If IP routing is enabled, you must set appropriate options in the IP Options submenu. Both sides of the connection must have IP routing enabled, so each side can be managed as a separate IP network or subnetwork.
- If IPX routing is enabled, you must set the IPX Frame type as well as appropriate options in the IPX Options submenu. Both sides of the connection must have IPX routing enabled, so each side can be managed as a separate IPX network.
- If routing is disabled, bridging must be enabled.

Parameter Location: Configure Profile

See Also: Route IP, Route IPX

Route IP (IP only)

Description: This parameter enables or disables the routing of IP data packets over the link specified in the profile.

Usage: Press Enter to toggle between Yes and No.

- Yes enables IP routing

  Yes is the default.
- No disables IP routing.

Dependencies: The effect of the Route IP parameter depends upon how you set the Bridge parameter:

- If Bridge=Yes and Route IP=Yes, the Pipeline 25-Fx routes IP packets, and bridges all other packets.
- If Bridge=Yes and Route IP=No, the Pipeline 25-Fx bridges all packets.
- If Bridge=No and Route IP=Yes, the Pipeline 25-Fx routes only IP packets.
- If Bridge=No and Route IP=No, an error occurs and you cannot save the profile.

  You must enable bridging or routing, or both.

These additional dependencies apply:

- The Route parameter in the Configure Profile affects the Route IP value in the first Connection Profile. For example, if you set Route=IPX in the Configure Profile (that is, route *only* IPX), Route IP=No in the first Connection Profile.
- IP routing must be enabled on both the dialing and answering sides of the link.

  The Connection Profile on the dialing side and the Answer Profile on the answering side must both set the Route IP parameter to Yes. Otherwise, the Pipeline 25-Fx does not route IP packets.
- Route IP in the Answer Profile applies to incoming calls for which no Connection Profile exists; if a Connection Profile exists, the setting of its Route IP parameter takes precedence.
- If Profile Reqd=Yes in the Answer Profile, Route IP does not apply (Route IP=N/A) in the Answer Profile.

Parameter Location: Answer Profile, Answer/PPP options
Connection Profile, Connections

See Also: Bridge, Encaps, Profile Reqd, Route, Route IPX

Route IPX (IPX only)

Description: This parameter specifies whether or not the Pipeline 25-Fx requests IPX routing for the connection.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that the Pipeline 25-Fx requests IPX routing.
- No specifies that the Pipeline 25-Fx does not route IPX.

  No is the default.

Dependencies: If the link supports PPP or MP+ (Encaps=PPP or Encaps=MPP), both sides of the connection must set Route IPX=Yes for IPX routing to take place.

In addition, the effect of the Route IPX parameter depends upon how you set the Bridge parameter:

- If Bridge=Yes and Route IPX=Yes, the Pipeline 25-Fx routes IPX packets, and bridges all other packets.
- If Bridge=Yes and Route IPX=No, the Pipeline 25-Fx bridges all packets.
- If Bridge=No and Route IPX=Yes, the Pipeline 25-Fx routes only IPX packets.
- If Bridge=No and Route IPX=No, an error occurs and you cannot save the profile.

  You must enable bridging or routing, or both.

This additional dependency applies:

- The Route parameter in the Configure Profile affects the Route IPX value in the first Connection Profile. For example, if you set Route=IP in the Configure Profile (that is, route *only* IP), Route IPX=No in the first Connection Profile.

Parameter Location: Answer Profile, Answer/PPP options
Connection Profile, Connections

See Also: Bridge, Route, Route IP

Save Cfg

Description: This command enables you to save all Pipeline 25-Fx profiles (except Security Profiles) to disk.

The process does not save passwords; that is, the Save Cfg command does not save the Send PW and Recv PW parameters in a Connection Profile, or the Passwd parameter in a Security Profile or an Ethernet Profile.

Usage: Follow these instructions to save your configuration:

1 Enable the Download parameter in the Security Profile (Download=Yes).

2 Verify that your terminal emulation program has a disk capture feature; this feature enables your emulator to capture to disk the ASCII characters it receives at its serial host port.

3 Verify that your terminal emulation program has an autotype feature; this feature enables your emulator to transmit over its serial host port the contents of a file it has built through disk capture.

4. Connect the backup device to the Pipeline 25-Fx's Control port.
5. Set the data rate of your terminal emulation program to 9600 baud or lower.
6. Set the Term Rate parameter in the System Profile to 9600.
7. Select Save Cfg from the Sys Diag menu.
8. Turn on the autotype function on your emulator, and start the save process by typing any key on the emulator.
9. Verify that configuration data is being echoed to the terminal emulation screen and that the captured data is being written to a file on your disk.

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

Parameter Location: Sys Diag

See Also: Restore Cfg

Sec History

Description: This parameter specifies the number of seconds the Pipeline 25-Fx uses as a sample for calculating average line utilization (ALU) of transmitted data; the Pipeline 25-Fx arrives at this average using the algorithm specified by the Dyn Alg parameter.

When ALU exceeds the Target Util threshold for a period of time greater than the value of the Add Pers parameter, the Pipeline 25-Fx attempts to add a channel.When ALU falls below the Target Util threshold for a period of time greater than the value of the Sub Pers parameter, the Pipeline 25-Fx attempts to remove a channel.

The number of seconds you choose for the Sec History parameter depends on your device's traffic patterns. For example, if you want to average spikes with normal traffic flow, you may want the Pipeline 25-Fx to establish a longer historical time period. If, on the other hand, traffic patterns consist of many spikes that are short in duration, you may want to specify a shorter period of time; doing so assigns less weight to the short spikes.

Usage: Press Enter to open a text field. Then, type a number between 1 and 300. The default value for MP+ calls is 15 seconds; the default value for dynamic AIM calls is 30 seconds. Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- The Sec History parameter applies only to dynamic MP+ calls (Encaps=MPP).
- If you specify a small value for the Sec History parameter, and increase the values of the Add Pers parameter and the Sub Pers parameter relative to the value of Sec History, the system becomes less responsive to quick spikes.
- The easiest way to determine the proper values for Sec History, Add Pers, and Sub Pers is to observe usage patterns; if the system is not responsive enough, the value of Sec History is too high.

Parameter Location: Answer Profile, Answer/PPP options
Connection Profile, Connections/Encaps options

See Also: Add Pers, Dyn Alg, Encaps, Sub Pers, Target Util

Secondary

Description: This parameter specifies a secondary Connection Profile to be dialed in the event that a session using the primary Connection Profile cannot be established.

Usage: Press Enter to open a text field. Then, type the name of the secondary Connection Profile. The name you specify must match the value of the Name parameter in a local Connection Profile

Dependencies: Keep this additional information in mind:

- Secondary Profiles can be chained. That is, secondary Connection Profiles can also have Secondary Connection profiles.

Do not confuse the Secondary parameter with the Backup parameter. A BackUp Connection Profile is used to re-establish an existing connection that has terminated; a Secondary Connection Profile is used to establish a new connection if the primary Connection Profile cannot.

- Parameters that you define in the primary Connection Profile do not automatically apply to the secondary Connection Profile.

  For example, if you set the primary Connection Profile to filter Telnet packets, you must set the secondary profile to filter Telnet packets as well.

Parameter Location: Ethernet Profile, Connections\Session options...

See Also: Backup

Send Auth

Description: This parameter specifies the authentication protocol that the Pipeline 25-Fx requests when initiating a connection using PPP or MP+ encapsulation. The answering side of the connection determines which authentication protocol, if any, the connection uses.

Usage: Press Enter to cycle through the choices.

- None specifies that the Pipeline 25-Fx does not request an authentication protocol for outgoing calls.

  None is the default.

- PAP (Password Authentication Protocol) is a PPP authentication protocol.

  PAP provides a simple method for the Pipeline 25-Fx to establish its identity in a two-way handshake. Authentication takes place only upon initial link establishment, and does not use encryption.

  If you choose PAP, the Pipeline 25-Fx requests this protocol for authentication. The remote device must support PAP.

- CHAP (Challenge Handshake Authentication Protocol) is a PPP authentication protocol.

  CHAP is more secure than PAP. CHAP provides a way for the remote device to periodically verify the identity of the Pipeline 25-Fx using a three-way handshake and encryption. Authentication takes place upon initial link establishment; a device can repeat the authentication process any time after the connection is made.

  If you choose CHAP, the Pipeline 25-Fx requests this protocol for authentication. The remote device must support CHAP.

- PAP-TOKEN is an extension of PAP authentication. This requires that the Network Access Server (NAS) be running the Ascend RADIUS daemon.

In PAP-TOKEN, the user making outgoing calls from the Pipeline 25-Fx authenticates his or her identity by entering a password derived from a hardware device, such as a hand-held security card. The Pipeline 25-Fx prompts the user for this password, possibly along with a challenge key. The NAS obtains the challenge key from a security server that it accesses through RADIUS.

RADIUS (Remote Authentication Dial In User Service) is a protocol by which users can have access to secure networks through a centrally managed server. You can store virtually all Connection Profile information on the RADIUS server in a flat ASCII database.

- PAP-TOKEN-CHAP is nearly identical to PAP-TOKEN. This requires that the NAS be running the Ascend RADIUS daemon.

  In all authentication protocols, including PAP-TOKEN and PAP-TOKEN-CHAP, the Pipeline 25-Fx individually authenticates all channels of an MP+ call. If the answering unit requires security card authentication, PAP-TOKEN and PAP-TOKEN-CHAP begin identically when authenticating the first channel of an MP+ call. However, when the Pipeline 25-Fx adds additional channels to the MP+ call, PAP-TOKEN requires security-card authentication for each new channel, while PAP-TOKEN-CHAP uses CHAP authentication for all new channels. CHAP authentication works automatically, without the use of a hand-held security card.

- CACHE-TOKEN begins authentication using a hand-held security card, and fills a token cache set up for you on the RADIUS server at the remote site. This requires that the NAS be running the Ascend RADIUS daemon.

  CHAP authenticates your subsequent calls without using your hand-held security card. After a period of time configured in your entry in the RADIUS users file, the token cache expires and the next call you place must again be authenticated using your hand-held security card.

Dependencies: Keep this additional information in mind:

- The link must use PPP or MP+ encapsulation (Encaps=PPP or Encaps=MPP).
- If you request PAP or CHAP, you must also specify a password using Send PW in a Connection Profile.
- If you request 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 25-Fx cannot extend the MP+ call beyond a single channel.

- 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.
- 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.
- For information on prompting the user for his or her password at the Pipeline 25-Fx's terminal server, see the description of the `set password` command in the *Pipeline 25-Fx User's Guide.*
- For information on prompting for a password at a host, see the APP Server, APP Host, and APP Port parameters.
- Dial Brdcast must be enabled when a PC on the same Ethernet as the Pipeline 25-Fx runs APPSRVR1 or APPSRVR2 to open a connection protected by security-card authentication.

Parameter Location: Connection Profile, Connection/Encaps options

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

Send PW

Description: This parameter specifies the password that the Pipeline 25-Fx sends to the remote end of a connection on outgoing calls. If the password specified by Send PW does not match the remote end's value for Recv PW, the remote end disconnects the link.

Usage: Press Enter to open a text field. Then, type the password that the remote end requires the Pipeline 25-Fx to send.

You can enter up to 20 characters; the password is case sensitive. Leave the field blank if the remote end does not require a password.

Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- You must specify a value for Send PW when the link uses PPP encapsulation (Encaps=PPP or Encaps=MPP) and the Pipeline 25-Fx uses PAP, CHAP, or CACHE-TOKEN authentication (Send Auth=PAP, Send Auth=CHAP, or Send Auth=CACHE-TOKEN).

  When you choose Encaps=MPP, both the dialing side and the answering side of the link must support MP+. If only one side supports MP+, the connection uses MP or standard single-channel PPP. When you choose Encaps=PPP, the connection uses only PPP.

Parameter Location: Connection Profile, Connection/Encaps options

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

Server

Description: This parameter specifies a Bootstrap Protocol (BOOTP) server for handling BOOTP requests. If a server is on the same local-area network as the Pipeline, BOOTP requests from other networks are relayed to the server. If a server is on another network, BOOTP requests from clients on the same local-area network as the Pipeline are relayed to the remote server.

Note: This parameter appears twice. Each copy can be used to specify a different BOOTP server.

Usage: Press Enter to open a text field and then type the IP address of the BOOTP server. When you're done, press Enter to close the text field.

Dependencies: If you specify two BOOTP servers, the Pipeline that relays the BOOTP request determines when each server is used. The order of the BOOTP servers in the BOOTP Relay menu does not necessarily determine which server is tried first.

Parameter Location: Mod Config, BOOTP Relay

See Also: BOOTP Relay Enable

Server Name (IPX only)

Description: This parameter appears in an IPX Routes Profile and an IPX SAP Filter Profile. Its functionality differs depending on the profile.

- In an IPX Routes Profile, the Server Name parameter specifies the name of an IPX server.
- In an IPX SAP Filters Profile, the Server Name parameter specifies the name of a NetWare server to be excluded from or included in the Ascend unit's service table.

Usage: You usage differs depending on the profile.

IPX Routes Profile

Press Enter to open a text field. Then, type the name of an IPX server. You can enter up to 48 characters, and you must limit your specification to uppercase letters, numbers, and the underscore symbol. Press Enter again to close the text field.

IPX SAP Filter Profile

Press Enter to open a text field. Then, type the server's name. You can specify letters, digits, and the underscore, up to a maximum of 20 characters. The wildcard characters * and ? may be used for partial name matches. Press Enter again to close the text field.

Dependencies: For the Server Name parameter to apply in an IPX Route Profile, you must enable IPX routing in the Connection Profile by setting Route IPX=Yes.

Parameter Location: IPX Routes Profile, IPX Routes
IPX SAP Filter Profile, IPX SAP Filters

See Also: Route IPX, Server Type

Server Type (IPX only)

Description: This parameter appears in an IPX Route Profile and an IPX SAP Filter Profile. Its functionality differs depending on the profile:

- In an IPX Route Profile, the Server Type parameter specifies the SAP (Service Advertising Protocol) service type for the server.
- In an IPX SAP Filters Profile, the Server Type parameter specifies the SAP Service Type that will be excluded from or included in the service table.

Usage: Your usage differs depending on the profile.

IPX Route Profile

Press Enter to open a text field. Then, type a valid SAP service type for the server. The SAP service type for a NetWare server is type 4. Press Enter again to close the text field.

For information on SAP service types, refer to your Novell NetWare documentation.

IPX SAP Filter Profile

Press Enter to open a text field. Then type a hexadecimal number. You can enter a number from 1 to FFFE. The default value is 0. Press Enter again to close the text field.

Parameter Location: IPX Route Profile, IPX Routes
IPX SAP Filter Profile, IPX SAP Filters

See Also: Server Name, Type, Valid

Socket (IPX only)

Description: This parameter specifies the socket number of the NetWare server.

Usage: Press Enter to open a text field. Then, type the socket number for the server. You should advertise only those NetWare servers that have well-known socket numbers. Press Enter again to close the text field.

Example: `DE040600`

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

Parameter Location: IPX Routes Profile, IPX Routes

See Also: Route IPX

SPID A

Description: This parameter specifies the ISDN BRI Service Profile Identifier (SPID) associated with My Num A. An SPID is a number assigned to a domestic ISDN BRI line for service identification at the ISDN service provider's central office. It is typically formed by adding a code to the phone number assigned to the line. Your carrier provides you with one or more SPIDs.

All U.S. domestic switch types, except AT&T Point-To-Point, can have two phone numbers. The primary phone number (My Num A) requires a matching primary SPID (SPID A). The secondary phone number (My Num B) requires a matching secondary SPID (SPID B).

When you use AT&T Point-to-Point service, only one phone number is assigned to the ISDN BRI line, and no SPIDs are used.

Usage: Press Enter to open a text field. Then, type up to 16 characters; you must limit those characters to numbers, hyphens, and parentheses. The default value is 0 (zero). Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- You must enter a value for SPID A unless you are using AT&T Point-To-Point (Link Type=P-T-P) or you are operating outside of the U.S.
- If the Pipeline 25-Fx uses only one channel of a multipoint ISDN BRI line and another device uses the other channel, you can choose to operate in single-terminal mode.
- The Pipeline 25-Fx appends the value of SPID A with a TID if you are connected to a Northern Telecom switch running NI-1 (Switch Type=NI-1).

Parameter Location: Configure Profile

See Also: My Num A, My Num B, Sec Num, SPID B, Switch Type

SPID B

Description: This parameter specifies the ISDN BRI Service Profile Identifier (SPID) associated with My Num B. An SPID is a number assigned to a domestic ISDN BRI line for service identification at the central office (CO). It is typically formed by adding a code to the phone number assigned to the line. Your carrier provides you with one or more SPIDs.

All U.S. domestic switch types, except AT&T Point-To-Point, can have two phone numbers. The primary phone number (My Num A) requires a matching primary SPID (SPID A). The secondary phone number (My Num B) requires a matching secondary SPID (SPID B).

When you use AT&T Point-to-Point service, only one phone number is assigned to the ISDN BRI line, and no SPIDs are in use.

Usage: Press Enter to open a text field. Then, type up to 16 characters; you must limit those characters to numbers, hyphens, and parentheses. The default value is 0 (zero). Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- You must enter a value for SPID A unless you are using AT&T Point-To-Point (Link Type=P-T-P) or you are operating outside of the U.S.
- If the Pipeline 25-Fx uses only one channel of a multipoint ISDN BRI line and another device uses the other channel, you can choose to operate in single-terminal mode.
- The Pipeline 25-Fx appends the value of SPID A with a TID if you are connected to a Northern Telecom switch running NI-1 (Switch Type=NI-1).

Parameter Location: Configure Profile

See Also: My Num A, My Num B, Sec Num, SPID B, Switch Type

Spoof Adr (IP only)

Description: This parameter specifies an IP address and netmask that will be assigned to the DHCP client when spoofing takes place. It must be a valid IP address on the local network.

Usage: Press Enter to open a text field, and then type a valid IP address and netmask. Press Enter again to close the text field.

Example: 188.0.5.8/24

Parameter Location: Ethernet Profile, Mod Config/DHCP Spoofing...

Dependencies: The DHCP Spoofing and Renewal Time parameters must be configured for this feature to work.

See Also: DHCP Spoofing, Renewal Time

Src Adrs

Description: In a filter of type IP, this parameter specifies the source address to which the Pipeline 25-Fx compares a packet's source address.

Usage: Press Enter to open a text field. Then, type the source address the Pipeline 25-Fx should use for comparison when filtering a packet. The address consists of four numbers between 0 and 255, separated by periods.

The null address 0.0.0.0 is the default; this setting matches all packets.

Press Enter to close the text field.

Example: `200.62.201.56`

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

Parameter Location: Filter Profile, Filters/IP

See Also: Src Mask

Src Mask

Description: In a filter of type IP, this parameter specifies the bits that the Pipeline 25-Fx should mask when comparing a packet's source address to the value of the Src Adrs parameter. The masked part of an address is hidden; the Pipeline 25-Fx does not use it for comparisons with Src Adrs. A mask hides the part of a number that appears behind each binary 0 (zero) in the mask; the Pipeline 25-Fx uses only the part of a number that appears behind each binary 1 for comparison.

The Pipeline 25-Fx applies the mask to the address using a logical AND after the mask and address are both translated into binary format.

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

The null address 0.0.0.0 is the default; this setting indicates that the Pipeline 25-Fx 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 25-Fx uses for comparison.

Press Enter to close the text field.

Example: Suppose a packet has the source address 10.2.1.1. If Src Adrs=10.2.1.3 and Dst Mask=255.255.255.0, the Pipeline 25-Fx masks the last digit and uses only 10.2.1, which matches the packet.

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

Parameter Location: Filter Profile, Filters/IP

See Also: Src Adrs

Src Port #

Description: In a filter of type IP, this parameter specifies the source port number to which the Pipeline 25-Fx compares the packet's source port number.

The Src Port Cmp criterion determines how the Pipeline 25-Fx carries out the comparison.

Usage: Press Enter to open a text field. Then, type the number of the source port the Pipeline 25-Fx should use for comparison when filtering packets. You can enter a number between 0 and 65535.

The default setting is 0 (zero); this setting means that the Pipeline 25-Fx forwards all packets.

Press Enter to close the text field.

Example: `25`

Port 25 is reserved for SMTP, so that socket is dedicated to receiving mail messages. Port 20 is reserved for FTP data messages, Port 21 for FTP control sessions, and Port 23 for Telnet sessions.

Parameter Location: Filter Profile, Filters/IP

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

Src Port Cmp

Description: In a filter of type IP, this parameter specifies the type of comparison the Pipeline 25-Fx makes when filtering for source port numbers using the Src Port # parameter.

Usage: Press Enter to cycle through the choices.

- None specifies that the Pipeline 25-Fx does not compare the packet's source port number to the value specified by Src Port #.

  None is the default.
- Less specifies that port numbers with a value less than the value specified by Src Port # match the filter.

- Eql specifies that port numbers equal to the value specified by Src Port # match the filter.
- Gtr specifies that port numbers with a value greater than the value specified by Src Port # match the filter.
- Neq specifies that port numbers not equal to the value specified by Src Port # match the filter.

Dependencies: Keep this additional information in mind:

- This parameter works only for TCP and UDP packets.

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

Parameter Location: Filter Profile, Filters/IP

See Also: Src Port #

Station

Description: This parameter specifies the name of the remote device to which the Pipeline 25-Fx makes a connection.

Usage: Press Enter to open a text field. Then, type the name or MAC address of the remote device.

You can enter up to 31 characters.

The value you specify is case sensitive, and must exactly match the name of the remote device. If you are not sure about the exact name, contact the administrator of the remote network.

Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- The Station parameter for the first Connection Profile is the same as Rem Name parameter in the Configure Profile.

- The Station parameter setting appears in the list of Connection Profiles in the Connection menu; however, if you leave the parameter blank, the LAN Adrs setting appears instead.
- The remote device that the Station parameter specifies is the device actually placing or answering the call; it is not necessarily the same as the source or destination of packets using the link.
- The Pipeline 25-Fx does not currently use the Domain Name System (DNS) to determine the IP address of the device specified by the Station parameter.
- When the Pipeline 25-Fx receives a PPP or MP+ call from an Ascend unit, it tries to match the caller's Name to the value of the Station parameter in some Connection Profile.

  If the Pipeline 25-Fx finds a match and authentication is turned on, the Pipeline 25-Fx then tries to match the caller's Send PW value to the Recv PW value in that same Connection Profile.

Parameter Location: Connection Profile, Connections

Sub-Adr

Description: This parameter determines how the Pipeline 25-Fx treats incoming calls based on whether they convey an ISDN subaddress.

Usage: Press Enter to cycle through the options.

- Termsel specifies that the Pipeline 25-Fx must use an ISDN subaddress to determine whether a call is answered.

  The called-party number must have a subaddres. Otherwise, the Pipeline 25-Fx ignores the call. If the Pipeline 25-Fx accepts the call, the subaddress becomes part of the incoming phone number.
- None specifies that the Pipeline 25-Fx does not use subaddressing.

Dependencies: Keep this additional information in mind:

- Sub-Adr applies only to ISDN lines.
- Sub-Adr=TermSel is intended for a scenario in which equipment is connected to a multidrop ISDN BRI line.

Parameter Location: System Profile, Sys Config

See Also: Pri Num, Sec Number, Dial #

Sub Pers

Description: This parameter specifies the number of seconds average line utilization (ALU) of transmitted data must fall below the threshold indicated by the Target Util parameter before the Pipeline 25-Fx begins removing bandwidth from a session. The Pipeline 25-Fx determines the ALU for a session using the algorithm specified by the Dyn Alg parameter.

When utilization falls below the threshold for a period of time greater than the value of the Sub Pers parameter, the Pipeline 25-Fx attempts to remove a channel. Using the Add Pers and Sub Pers parameters prevents the system from continually adding and subtracting bandwidth, and can slow down the process of allocating or removing bandwidth.

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

When the Pipeline 25-Fx is using MP+ (Encaps=MPP), the default value is 10.

Dependencies: Keep this additional information in mind:

- One channel must be up at all times.
- Removing bandwidth cannot (a) cause the ALU to exceed the threshold specified by the Target Util parameter or (b) cause the number of channels to fall below the amount specified by the Min Ch Count parameter.
- Sub Pers in the Answer Profile applies to incoming calls for which no Connection Profile exists; if a Connection Profile exists, the setting of its Sub Pers parameter takes precedence.
- If Profile Reqd=Yes in the Answer Profile, Sub Pers does not apply (Sub Pers=N/A) in the Answer Profile.
- Add Pers and Sub Pers have little or no effect on a system with a high Sec History value.

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

Parameter Location: Connection Profile, Connections/Encaps option
Answer Profile, Answer/PPP options

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

Switch Type

Description: This parameter specifies the network switch that provides the BRI line to the Pipeline 25-Fx and connects the line to the WAN.

A switch is the device that connects the calling party to the answering party. The connection is a switched circuit consisting of one or more channels.

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

You can select one of the switch types listed in Table 11-3.

Table 11-3. Configure Profile switch types

Switch type	Explanation
AT&T/P-T-P	AT&T Point-to-Point is the default.
AT&T/Multi-P	ATT&T Mulitpoint.
NT1	Northern Telecommunications, Inc.
NI-1	National ISDN 1.
NI-2	National ISDN-2
U.K.	United Kingdom: ISDN-2 Hong Kong: HKT Switchline BRI Singapore: ST BRI Euro ISDN countries: Austria, Belgium, Denmark, Germany, Finland, Italy, Netherlands, Portugal, Spain, Sweden This is identical to NET 3.

Table 11-3. Configure Profile switch types

Switch type	Explanation
SWISS	Switzerland: Swiss Net 2
NET 3	This is identical to U.K.
GERMAN	Germany 1TR6 version: DBP Telecom
MP GERMAN	Germany: 1TR6 multipoint
FRANC	France: FT Numeris
DUTCH	Netherlands 1TR6 version: PTT Netherlands BRI
BELGIUM	Belgium: Pre-Euro ISDN Belgacom Aline
JAPAN	Japan: NTT INS-64
AUSTRALIA	Australia and New Zealand

Dependencies: Keep this additional information in mind:

- The Switch Type parameter does not apply to a link using inband signaling

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

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

Parameter Location: Configure Profile

System Reset

Description: This command restarts the Pipeline 25-Fx and clears all calls without disconnecting the device from its power source. The Pipeline 25-Fx logs off all users, and returns user security to its default state. In addition, the Pipeline 25-

Fx performs power-on self tests (POSTs) when it restarts. These POSTs are diagnostic tests.

Usage: To perform a system reset, follow these steps:

1. Select System Reset and press Enter.
   The Pipeline 25-Fx prompts you to confirm that you want to perform the reset.
2. Confirm the reset.
   The Pipeline 25-Fx displays the message `System reset in progress`. In addition to clearing calls, the Pipeline 25-Fx performs a series of POSTs. The POST display appears.
   If you do not see the POST display, press Ctrl-L.
   While the yellow CON LED on the front panel remains solidly lit, the Pipeline 25-Fx checks system memory, configuration, and line connections. If the Pipeline 25-Fx fails any of these tests, the CON LED remains lit or blinks.
   When the tests are complete, this message appears:
   `Power-On Self Test PASSED`
3. Press any key to display the Main Edit menu.

Parameter Location: Sys Diag

Target Util

Description: The Target Util parameter specifies the percent bandwidth utilization at which the Pipeline 25-Fx adds or subtracts bandwidth dynamically.

This parameter specifies the target percentage of bandwidth utilization for an MP+ call (Encaps=MPP).

The Pipeline 25-Fx uses the historical time period specified by the Sec History parameter as the basis for calculating average line utilization (ALU) of transmitted data. It then compares ALU to the amount specified in the Target Util parameter.

When ALU exceeds the threshold defined by Target Util for a period of time greater than the value of the Add Pers parameter, the Pipeline 25-Fx attempts to add a channel. When ALU falls below the threshold defined by Target Util for a

period of time greater than the value of the Sub Pers parameter, the Pipeline 25-Fx attempts to remove a channel.

Usage: Press Enter to open a text field. Then, type a number between 0 and 100. Press Enter again to close the text field.

The default is 70. When the value is 70%, the device adds bandwidth when it exceeds a 70 percent utilization rate, and subtracts bandwidth when it falls below that number.

Dependencies: When selecting a target utilization value, keep these guidelines in mind:

- Monitor how the application behaves when using different bandwidths.
  For example, an application might be able to use 88% of a 64-kbps link, but only 70% of a 256-kbps link.
- Monitor the application at different loads.

Parameter Location: Answer Profile, Answer/PPP options
Connection Profile, Connections/Encaps options

See Also: Add Pers, Dyn Alg, Sec History, Sub Pers

TCP Estab

Description: In a filter of type IP, this parameter specifies whether the filter should match only established TCP connections.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that you want the filter to match only those TCP connections that are established.
- No specifies that you want the filter to match both initial and established TCP connections.
  No is the default.

Dependencies: The TCP Estab parameter does not apply (TCP Estab=N/A) if the Protocol field is set to any value other than 6 (TCP).

Parameter Location: Filter Profile, Filter/IP

Term Rate

Description: This parameter specifies the data rate for the Control Monitor port in bits per second.

The Control Monitor is a menu-based user interface for configuring, managing, and monitoring the Pipeline 25-Fx. It consists of nine windows—eight status windows and a single edit window.

Usage: Press Enter to cycle through the choices.

- 57600
- 38400
- 19200
- 9600
  9600 is the default.
- 4800
- 2400
- 1200
- 300

Dependencies: Whenever you modify the Term Rate parameter, you must set the data rate of your terminal accordingly.

- When you operate the Pipeline 25-Fx from a local terminal, the most common data rate is 9600 bps.
- When you operate the Pipeline 25-Fx remotely, the most common data rate is 2400 bps.

Parameter Location: System Profile, Sys Config

Tick Count (IPX only)

Description: This parameter identifies the distance to the destination network in IBM PC clock ticks (18 Hz). This value is for round-trip timer calculation and for determining the nearest server of a given type.

Usage: In most cases, the default value (12) is appropriate. If you need to change this value, press Enter to open a text field. Then, type an appropriate value. Press Enter again to close the text field.

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

Parameter Location: IPX Routes Profile, IPX Routes

See Also: Route IPX

Type

Description: This parameter appears in a Filter Profile or an IPX SAP Filter Profile. Its functionality differs depending on the profile:

- In a Filter Profile, the Type parameter specifies how the Pipeline 25-Fx applies a filter to a packet.
- In an IPX SAP Profile, the Type parameter specifies whether the filter excludes the service from the service table.

Usage: Your usage differs depending on the profile.

Filter Profile

Press Enter to cycle through the choices.

- Generic specifies that the filter examines byte and offset values within a packet, regardless of which protocol is in use.
- Ip specifies that the filter examines the protocol ID number, address, and port specifications in an IP packet.

IPX SAP Filter Profile

Press Enter to cycle through the choices.

- Exclude specifies that the filter excludes the service from the service table. Exclude is the default.
- Include specifies that the filter includes the service in the service table.

Dependencies: Keep this additional information in mind:

- In a Filter Profile for a filter of type Generic, the Pipeline 25-Fx uses these parameters to specify how the filter operates:
  - Length
  - Mask
  - More
  - Offset
  - Value
- In a Filter Profile for a filter of type IP, the Pipeline 25-Fx uses these parameters to specify how the filter operates:
  - Dst Adrs
  - Dst Mask
  - Dst Port #
  - Dst Port Cmp
  - Protocol
  - Src Adrs
  - Src Mask
  - Src Port #
  - Src Port Cmp
  - TCP Estab

Parameter Location: Filter Profile, Filters
IPX SAP Filter Profile, IPX SAP Filters

See Also: Server Name, Server Type, Station, UDP Port, Valid

UDP Cksum

Description: This parameter specifies that the Ascend unit generates a UDP checksum whenever it sends out a UDP packet.

Currently the Pipeline uses UDP when generating queries and responses for the following protocols:

- ATMP
- SYSLOG
- DNS
- ECHOSERV
- RADIUS
- TACACS
- RIP
- SNTP
- TFTP

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that the Ascend unit generates a UDP checksum when transmitting a UDP packet.

  Specify this setting if data integrity is of the highest concern for your environment, and having redundant checks is important; this setting is also appropriate if your UDP-based servers are located on the remote side of a WAN link that is prone to errors.

- No specifies that the Ascend unit does not generate a UDP checksum when transmitting a UDP packet.

  No is the default. Accept this setting if you plan to use the data integrity guarantee of the Ethernet or PPP checksum only.

Parameter Location: Ethernet Profile: Ethernet→Mod Config

Valid

Description: This parameter activates or deactivates a filter. Its functionality differs depending on the profile:

- In a Filter Profile, the Valid parameter activates or deactivates a call filter or a data filter.
- In an IPX SAP Filter Profile, the Valid parameter activates or deactivates the Input filter or the Output filter.

Usage: Press Enter to toggle between Yes and No.

- Yes activates the filter.
- No deactivates the filter.
  No is the default.

Dependencies: Keep this additional information in mind:

- When Valid=No, N/A appears in all fields of the filter specification; therefore, you cannot define a filter specification unless Valid=Yes.
- If you are using more than one filter, set Valid=Yes and Forward=Yes in at least one filter; otherwise, the Pipeline 25-Fx drops all packets.
- To forward all packets, set all filters to Valid=No.

Parameter Location: Filter Profile, Filters
IPX SAP Filter Profile, IPX SAP Filters

See Also: Server Name, Server Type, Type

Value

Description: In a filter of type Generic, this parameter specifies a 16-bit hexadecimal value to compare against the data contained within the specified bytes in a packet. You specify the bytes using the Length, Offset, and Mask parameters.

Usage: Press Enter to open a text field. Then, type a hexadecimal number. You can enter a number from 00 to ffffffffffffffff.

The default is 00. When you accept the default, the bytes must contain nothing to match the filter.

Press Enter again to close the text field.

Example: `e0e0030000000000`

Dependencies: Keep this additional information in mind:

- The Pipeline 25-Fx 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.

Parameter Location: Filter Profile, Filter/Generic

See Also: Length, Mask, Offset

VJ Comp

Description: This parameter turns TCP/IP header compression on or off. VJ Comp stands for Van Jacobson Compression.

Usage: Press Enter to toggle between Yes and No.

- Yes turns on TCP/IP header compression for both ends of the link.
  Yes is the default. The Ascend unit must include the optional compression module.
- No turns off TCP/IP header compression.

Dependencies: Keep this additional information in mind:

- VJ Comp applies only to packets in TCP applications, such as Telnet.
  Telnet is a protocol used to link two computers in order to provide a terminal with a connection to the remote machine. The remote machine is known as the Telnet host. When you start a Telnet session, you connect to the Telnet host and log in. The connection enables you to work with the remote machine as though you were at a terminal connected to it.
- Turning on header compression is most effective in reducing overhead when the data portion of the packet is small.

Parameter Location: Answer Profile, Answer/PPP options
Connection Profile, Connections/Encaps options

WAN Alias (IP only)

Description: This parameter specifies the IP address of the link's remote interface to the WAN.

The WAN Alias parameter applies only if the remote end of a link uses an implementation of PPP that requires that both ends of a WAN connection be on the same subnet.

If a router requires an IP number for each interface over which it sends or receives packets, that router is said to use numbered interfaces. The WAN Alias parameter assigns a single IP number to all WAN lines connected to the Pipeline 25-Fx. Furthermore, the Pipeline 25-Fx assumes that all devices using numbered interfaces have agreed on the network number of the WAN; that is, if 10.0.2.1 is the Pipeline 25-Fx's interface to the WAN, then the WAN has a network number 10.0.2.0 and all other devices using numbered interfaces agree to have a 10.0.2.*x* address.

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

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

The default is 0.0.0.0/0.

Press Enter again to close the text field.

Example: `200.207.23.7/24`

Dependencies: The WAN Alias parameter does not apply if the Pipeline 25-Fx does not support IP (Route IP=No).

Parameter Location: Connection Profile, Connections

See Also: Route IP, Route

DO Command Reference

This section lists the DO commands in alphabetical order. Each listing provides information in this format:

Command Name

Description: The Description text explains the command.

Dependencies: The Dependencies text tells you what other information you need to use the command.

See Also: The See Also text points you to related information.

DO command overview

The DO command menu is a context-sensitive list of commands that appears when you press Ctrl-D.

To type a DO command, press and release the Control Monitor's Control-D combination, and then press and release the next key in the sequence. The PF1 function key on a VT-100 monitor is equivalent to the DO command.

Table 11-4 lists the available DO commands.

Table 11-4. DO commands

Command	Description
DO Beg/End Rem Mgm (DO 8)	Begin/End remote management.
DO Contract BW (DO 5)	Decrease bandwidth.
DO Dial (DO 1)	Dial the selected or current profile.
DO ESC (DO 0)	Abort and exit the DO menu.
DO Hang Up (DO 2)	Hang up from a call in progress.

Table 11-4. DO commands

Command	Description
DO Save (DO S)	Save parameter values into the specified profile.
DO Password (DO P) 9	Log into or out of the Pipeline.

Alphabetical DO command listing

DO Beg/ End Rem Mgm (DO 8)

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

```
REMOTE MANAGEMENT VIA port
```

In this message, *port* specifies the serial host port through which you are conducting remote management.

To end a remote management session, enter DO 8 or Ctrl-D 8. You cannot exit remote management from a port other than the port from which you began remote management. When the message at the top of the Control Monitor screen disappears, you are viewing the screens associated with the local Pipeline.

Dependencies: Keep this additional information in mind:

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

See Also: Call Type, Operations, Remote Mgmt

DO Contract BW (DO 5)

Description: The DO Contract BW command decreases the bandwidth of the current Connection Profile by the maximum number of channels possible without clearing the call.

Dependencies: Keep this additional information in mind:

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

See Also: Max Ch Count, Min Ch Count, Base Ch Count, Operations

DO Dial (DO 1)

Description: The DO Dial command dials a selected Connection Profile.

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

Dependencies: Keep this additional information in mind:

- DO Dial is not available when the link is busy.
- You cannot place a call from the secondary port of a dual-port pair.
- The DO Dial command does not appear if you are not logged in with operational privileges.

  See Operations in Chapter 11, “Reference,” for more information.
- You cannot dial if you have not selected the correct profile, if Dial # does not appear in the profile, or if no IP address is set for the profile when IP routing is enabled.

DO ESC (DO 0)

Description: The DO ESC command exits the DO menu.

DO Hang Up (DO 2)

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

Dependencies: Keep this additional information in mind:

- You must be in a menu specific to an online serial host port or session to use this command.
- The DO Hangup command does not appear if you are not logged in with operational privileges.

See Also: Call Type, Operations

DO Save (DO S)

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

Dependencies: Keep this additional information in mind:

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

DO Password (DO P)

Description: 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.

Login procedure

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

Logout Procedure

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 VT-100 control port.

Dependencies: 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.

See Also: Auto Logout, Idle Logout

Parameter Tables

This section contains tables showing the location, possible values, and default value of each parameter that appears in the Pipeline interface. The parameters are listed as they appear in each profile; the profiles appear in alphabetical order.

For complete information on the parameters listed here, refer to “Parameter reference” on page 11-2.

Answer Profile parameters

Table 11-5. Answer Profile parameters

Location	Parameter	Possible values	Default value
Ethernet→Answer→ Answer Profile	Force 56	Yes No	No
	Profile Reqd	Yes No	Yes
Ethernet→Answer→ PPP options	Route IP *(IP only)*	Yes No	Yes
	Route IPX *(IPX only)*	Yes No	Yes
	Bridge	Yes No	No
	Recv Auth	PAP CHAP Either None (Recv Auth in Configure Profile)	None
	MRU	Integer between 128 and 1524	1524
	LQM	Yes No	No
	LQM Min	Integer between 0 and 65535	600
	LQM Max	Integer between 0 and 65535	600
	Link Comp	Stac MS-Stac None	Stac

Table 11-5. Answer Profile parameters (continued)

Location	Parameter	Possible values	Default value
	VJ Comp	Yes No	Yes
	Dyn Alg	Constant Linear Quadratic	Quadratic
	Sec History	Integer between 1 and 300	When Encaps = MPP, the default value is 15.
	Add Pers	Integer between 1 and 300	When Encaps = MPP, the default value is 5.
	Sub Pers	Integer between 1 and 300	When Encaps = MPP, the default value is 10.
	Min Ch Count	Integer between 1 and 32	1
	Max Ch Count	Integer between 1 and the maximum number of channels your system supports	1
	Target Util	Integer between 1 and 100	70
	Idle Pct	Integer between 0 and 99	0
Ethernet→Answer→ Session options	Data Filter	Integer between 0 and 3	0
	Call Filter	Integer between 0 and 3	0
	Idle	Integer between 0 and 65535	120
	Preempt	Integer between 0 and 65535	60

Table 11-5. Answer Profile parameters (continued)

Location	Parameter	Possible values	Default value
	IPX SAP Filter *(IPX only)*	Integer between 0 and 2	0

Bridging Profile parameters

Table 11-6. Bridging Profile parameters

Location	Parameter	Possible values	Default value
Ethernet→ Bridge Adrs→ Any Bridging Profile	Enet Adrs	12-digit hexadecimal string	000000000000
	Net Adrs	IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255	0.0.0.0
	Connection #	Integer between 1 and 4	0

Configure Profile parameters

Table 11-7. Configure Profile parameters

Location	Parameter	Possible values	Default value
Configure	Ethernet	UTP AUI	UTP
	Bridge	No Transparent IPX Client	No
	Route	IP *(IP only)* IPX *(IPX only)* No	No
	IPX Frame	None 802.3 802.2 SNAP Enet_II	None
Configure→ BRI	Switch Type	AT&T/Multi-P NTI NI-1 AT&T/P-T-P International Models: U.K. NET 3 SWISS MP GERMAN GERMAN FRANCE BELGIUM JAPAN AUSTRALIA	AT&T/Multi-P (for a U.S. version of the Pipeline) For non-U.S. versions, the default value is dependent upon installed options.
	My Num A	Text string containing up to 16 characters	[ ]

Table 11-7. Configure Profile parameters (continued)

Location	Parameter	Possible values	Default value
	My Num B	Text string containing up to 16 characters	[ ]
	SPID A (U.S. models only)	Text string containing up to 16 characters	[ ]
	SPID B (U.S. models only)	Text string containing up to 16 characters	[ ]
	Data Usage	A B A+B	A+B
	Phone 1 Usage	A B None	A
	Phone 2 Usage	A B None	B
	Phone Num Binding	Yes No	No
Configure→ PPP	My Name	Text string containing up to 16 characters (Name in System Profile)	[ ]
	Rem Name	Text string containing 31 alphanumeric characters (Station in 1st Conn. Profile)	[ ]
	Dial #	Text string containing up to 37 characters (Dial # in 1st Conn. Profile)	[ ]

Table 11-7. Configure Profile parameters (continued)

Location	Parameter	Possible values	Default value
	Send Auth	PAP CHAP PAP-TOKEN PAP-TOKEN-CHAP CACHE-TOKEN None (Send Auth in 1st Conn. Profile)	None
	Send PW	Text string containing up to 20 characters (Send PW in 1st Conn. Profile)	[ ]
	Recv Auth	PAP CHAP Either None (Recv Auth in Answer Profile)	None
	Recv PW	Text string containing up to 20 characters (Recv PW in 1st Conn. Profile)	[ ]
	Call Filter	None IP Call NetWare Call AppleTalk	None
Configure→ IP	My Addr	IP address in dotted decimal notation *n.n.n.n/nn*, where *n* is an integer between 0 and 255, and *nn* is a subnet mask between 8 and 32 (IP Adrs in Ethernet Profile)	0.0.0.0/0

Table 11-7. Configure Profile parameters (continued)

Location	Parameter	Possible values	Default value
	IP Gateway	IP address in dotted decimal notation *n.n.n.n/nn*, where *n* is an integer between 0 and 255, and *nn* is a subnet mask between 8 and 32 (Gateway in Default Static Rtes Profile)	0.0.0.0/0
	Rem Addr	IP address in dotted decimal notation *n.n.n.n*/*nn*, where *n* is an integer between 0 and 255, and *nn* is a subnet mask between 8 and 32 (LAN Adrs in 1st Conn. Profile)	0.0.0.0/0

Connection Profile parameters

Table 11-8. Connection Profile parameters

Location	Parameter	Possible values	Default value
Ethernet→ Connections→ Any Connection Profile	Station	Text string containing 31 alphanumeric characters (Rem Name in Configure Profile)	[ ]
	Active	Yes No	Yes
	Encaps	MPP MP PPP	MPP
	Dial #	Text string containing up to 37 characters (Dial # in Configure Profile)	[ ]

Table 11-8. Connection Profile parameters

Location	Parameter	Possible values	Default value
	Route IP *(IP only)*	Yes No (Route in Configure Profile)	No
	Route IPX *(IPX only)*	Yes No (Route in Configure Profile)	No
	Bridge	No Transparent IPX Client (Bridge in Configure Profile)	No
	Dial Brdcast	Yes No	No
Ethernet→ Connections→ Any Connection Profile→ Encaps options (when Encaps=MPP)	Send Auth	PAP CHAP PAP-TOKEN PAP-TOKEN-CHAP CACHE-TOKEN None (Send Auth in Configure Profile)	None
	Send PW	Text string containing up to 20 characters (Send PW in Configure Profile)	[ ]
	Aux Send PW	Text string containing up to 20 characters	[ ]
	Recv PW	Text string containing up to 20 characters (Recv PW in Configure Profile)	[ ]

Table 11-8. Connection Profile parameters

Location	Parameter	Possible values	Default value
	DBA Monitor	Transmit Transmit-Recv None	Transmit-Recv
	Base Ch Count	Integer between 1 and the number of channels available	1
	Min Ch Cnt	Integer between 1 and 32	1
	Max Ch Count	Integer between 1 and the maximum number of channels your system supports	1
	MRU	Integer between 128 and 1524	1524
	LQM	Yes No	No
	LQM Min	Integer between 0 and 65535	600
	LQM Max	Integer between 0 and 65535	600
	Link Comp	Stac MS-Stac None	Stac
	VJ Comp	Yes No	Yes
	Dyn Alg	Constant Linear Quadratic	Quadratic
	Sec History	Integer between 1 and 300	15
	Add Pers	Integer between 1 and 300	5

Table 11-8. Connection Profile parameters

Location	Parameter	Possible values	Default value
	Sub Pers	Integer between 1 and 300	10
	Target Util	Integer between 1 and 100	70
	Idle Pct	Integer between 0 and 99	0
Ethernet→ Connections→ Any Connection Profile→ Encaps options (when Encaps=PPP)	Send Auth	PAP PAP-TOKEN CHAP None	None
	Send PW	Text string containing up to 20 characters	[ ]
	Recv PW	Text string containing up to 20 characters	[ ]
	MRU	Integer between 128 and 1524	1524
	LQM	Yes No	No
	LQM Min	Integer between 0 and 65535	600
	LQM Max	Integer between 0 and 65535	600
	Link Comp	Stac MS-Stac None	Stac
	VJ Comp	Yes No	Yes

Table 11-8. Connection Profile parameters

Location	Parameter	Possible values	Default value
Ethernet→ Connections→ Any Connection Profile→ IP options *(IP only)*	LAN Adrs	IP address in dotted decimal notation *n.n.n.n*/*nn*, where *n* is an integer between 0 and 255, and *nn* is a subnet mask between 8 and 32 (Rem Addr in 1st Conn. Profile)	0.0.0.0/0
	WAN Alias	IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255	0.0.0.0
	Metric	Integer between 1 and 15	7
	Preference	Integer between 0 and 100	100 (static routes)
	Private	Yes No	No
Ethernet→ Connections→ Any Connection Profile→ IPX options *(IPX only)*	Peer	Router Dialin	Router
	Dial Query	Yes No	No
	IPX Net#	Hexadecimal number (4 bytes)	00000000
	IPX Alias	Hexadecimal number (4 bytes)	00000000
	IPX RIP	Both Send Recv Off	Both

Table 11-8. Connection Profile parameters

Location	Parameter	Possible values	Default value
	IPX SAP	Both Send Recv Off	Both
	NetWare t/o	Integer between 0 and to 65535 (minutes)	30
Ethernet→ Connections→ Any Connection Profile→ Session options	Data Filter	Integer between 0 and 3	0
	Call Filter	Integer between 0 and 3	0
	Idle	Integer between 0 and 65535 (seconds)	120
	Preempt	Integer between 0 and 65535 (seconds)	60
	IPX SAP Filter *(IPX only)*	Integer between 0 and 2	0
	Secondary	Text string containing up to 31 alphanumeric characters	[ ]
Ethernet→ Connections→ Any Connection Profile→ Telco options	AnsOrig	Both Ans Only Call Only	Both
	Callback	Yes No	No

Table 11-8. Connection Profile parameters

Location	Parameter	Possible values	Default value
	Data Svc	56K 56KR 64K Voice	56K
	Force 56	Yes No	No
	Bill #	Text string containing up to 10 characters	[ ]

Ethernet Profile parameters

Table 11-9. Ethernet Profile parameters

Location	Parameter	Possible values	Default value
Ethernet→ Mod Config	Bridging	Yes No	No
	IPX Routing *(IPX only)*	Yes No	Yes
	ICMP Redirects *(IP only)*	Accept Ignore	Accept
	UDP Cksum	Yes No	No
Ethernet→ Mod Config→ BOOTP Relay	BOOTP Relay Enable	Yes No	No
	Server	IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255,	0.0.0.0
Ethernet→ Mod Config→ Ether options *(IP only)*	Ethernet IF	UTP AUI	UTP
	IP Adrs	IP address in dotted decimal notation *n.n.n.n/nn*, where *n* is an integer between 0 and 255, and *nn* is a subnet mask between 8 and 32 (My Addr in Configure Profile)	0.0.0.0/0
	Ignore Def Rt	Yes No	No

Table 11-9. Ethernet Profile parameters (continued)

Location	Parameter	Possible values	Default value
	Proxy Mode	Off Inactive Active Always	Off
	Filter	Integer between 0 and 3	0
	IPX Frame	None 802.3 802.2 SNAP Enet_II	None
Ethernet→ Mod Config→ Ether options *(IPX only)*	Ethernet IF	UTP AUI	UTP
	Filter	Integer between 0 and 2	0
	IPX Frame	None 802.3 802.2 SNAP Enet_II	None
	IPX Enet#	Hexadecimal number (4 bytes)	00000000
	IPX Pool#	Hexadecimal number (4 bytes)	00000000
	IPX SAP Filter	Integer between 0 and 2	0
	IPX SAP Proxy	Yes No	No

Table 11-9. Ethernet Profile parameters (continued)

Location	Parameter	Possible values	Default value
	IPX SAP Proxy Net#	Hexadecimal number (4 bytes)	00000000
	Handle IPX Type20	Yes No	No
Ethernet→ Mod Config→ DHCP Spoofing *(IP only)*	DHCP Spoofing	Yes No	No
	Spoof Adr	IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255	0.0.0.0
	Renewal Time	Integer between 3 and 65535 (seconds)	10
Ethernet→ Mod Config→ Auth *(IP only)*	APP Server	Yes No	No
	APP Host	IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255	0.0.0.0
	APP Port	Integer	0

Filter Profile parameters

Table 11-10.Filter Profile parameters

Location	Parameter	Possible values	Default value
Ethernet→ Filters→ Any Filter Profile	Name	Text string containing up to 16 characters	[ ]
Ethernet→ Filters→ Any Filter Profile → Input filters→ Any Input filter Filters→ Any Filter Profile → Output filters→ Any Output filter	Valid	Yes No	No
	Type	Generic Ip	Generic
Ethernet→ Filters→ Any Filter Profile → Input filters→ Any Input filter→ Generic Ethernet→ Filters→ Any Filter Profile → Output filters→ Any Output filter → Generic	Forward	Yes No	No
	Offset	Decimal integer between 0 and 1510	0
	Length	Decimal integer between 0 and 8	0
	Mask	Hexadecimal string between 00 and ffffffffffffffff	00
	Value	Hexadecimal string between 00 and ffffffffffffffff	00

Table 11-10.Filter Profile parameters (continued)

Location	Parameter	Possible values	Default value
	Compare	Equals NotEquals	Equals
	More	Yes No	No
Ethernet→ Filters→ Any Filter Profile →Input filters→ Any Input filter→ Ip Ethernet→ Filters→ Any Filter Profile → Output filters→ Any Output filter → Ip	Forward	Yes No	No
	Src Mask	IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255	0.0.0.0
	Src Adrs	IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255	0.0.0.0
	Dst Mask	IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255	0.0.0.0
	Dst Adrs	IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255	0.0.0.0

Table 11-10.Filter Profile parameters (continued)

Location	Parameter	Possible values	Default value
	Protocol	Any value between 0 and 255, but only the following are implemented: 0 (None) 1 (ICMP) 6 (TCP) 17 (UDP) 89 (OSPF)	0
	Src Port Cmp	None Less Eql Gtr Neq	None
	Src Port #	Integer between 0 and 35565	0
	Dst Port Cmp	None Less Eql Gtr Neq	None
	Dst Port #	Integer between 0 and 35565	0
	TCP Estab	Yes No	No

IPX Routes Profile parameters (IPX only)

Table 11-11.IPX Routes Profile parameters

Location	Parameter	Possible values	Default value
Ethernet→ IPX Routes→ Any IPX Route Profile	Server Name	Text string containing up to 48 characters	[ ]
	Active	Yes No	Yes
	Network	Hexadecimal number (4 bytes)	00000000
	Node	Node number of a NetWare server	000000000001
	Socket	Number between 0000 and 9999	0000
	Server Type	Number between 0000 and 9999	0000
	Hop Count	Integer between 1 and 15	1
	Tick count	Integer between 1 and 65535	12
	Connection #	Integer between 1 and 4	0

IPX SAP Profile parameters

Table 11-12.IPX SAP Filter Profile parameters

Location	Parameter	Possible values	Default value
Ethernet→ IPX SAP Filters→ Any IPX SAP Filter	Name	Text string containing up to 16 characters	[ ]
Ethernet→ IPX SAP Filters→ Any IPX SAP Filter→ Input SAP Filters→ Any Input SAP filter Ethernet→ IPX SAP Filters→ Any IPX SAP Filter→ Output SAP Filters→ Any Output SAP filter	Valid	Yes No	No
	Type	Include Exclude	Exclude
	Server Type	Hexadecimal number between 0 and FFFF	0
	Server Name	Text string containing up to 20 characters, including the wildcard characters * and ?	[ ]

Static Rtes Profile parameters

Table 11-13.Static Rtes Profile parameters

Location	Parameter	Possible values	Default value
Ethernet→ Static Rtes→ Any Static Rtes Profile	Name	Text string containing up to 31 characters	[ ], except for the first profile, whose name is Default
	Active	Yes No	No
	Dest	IP address in dotted decimal notation *n.n.n.n/nn*, where *n* is an integer between 0 and 255, and *nn* is a subnet mask between 8 and 32. The default route is fixed at 0.0.0.0/0.	0.0.0.0/0
	Gateway	IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255	0.0.0.0
	Metric	Integer between 0 and 15	7
	Private	Yes No	No

Security Profile parameters

Table 11-14.Security Profile parameters

Location	Parameter	Possible values	Default value
System→ Security→ Any Security Profile	Name	Text string containing up to 16 characters	[ ], except for the first profile, whose password is Default
	Passwd	Text string containing up to 20 characters	[ ], except for the first profile, which has no password
	Operations	Yes No	Yes
	Edit Security	Yes No	Yes
	Edit System	Yes No	Yes
	Field Service	Yes No	Yes

System Profile parameters

Table 11-15.System Profile parameters

Location	Parameter	Possible values	Default value
System→ Sys Config → System Profile	Name	Text string containing up to 16 characters (My Name in Configure Profile)	[ ]
	Term Rate	300 1200 2400 4800 9600 19200 38400 57600	9600
	Console	Standard	Standard
	Remote Mgmt	Yes No	Yes
	Sub-Adr	TermSel None	None
	Auto Logout	Yes No	No
	Idle Logout	Integer between 0 and 60 (minutes)	0

Status Menu Reference

12

This chapter lists the Pipeline's status menus in alphabetic order. Each listing provides information in this format:

Menu Name

Description: The Description text explains the menu.

Usage: The Usage text explains how to interpret the menu display.

Dependencies: The Dependencies text tells you what other information you need to interpret status menu information.

See Also: The See Also text points you to related information.

Status menu listing

Dyn Stat

Description: The Dyn Stat menu shows the name, quality, bandwidth, and bandwidth utilization of each online connection.

Usage: This screen shows an example Dyn Stat display:

```
20-500 Dyn Stat
Qual Good 00:02:03
56K     1 channels
CLU  12%  ALU  23%
```

You can press the Down Arrow key to see other connections; more than one connection can be online at once.

Each line of the menu is described in the following paragraphs.

Line 1

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

Line 2

The second line lists the quality of the link and the amount of time the link has been active. When a link is online more than 96 hours, the Pipeline reports the duration in number of days. The link quality can have one of the values listed in Table 12-1.

Table 12-1. Link quality values

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

Line 3

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

Line 4

The last line displays these values:

- CLU
  CLU specifies the current line utilization—the percentage of bandwidth currently being used by the call, divided by the total amount of bandwidth available.
- ALU
  ALU specifies the average line utilization—the average amount of available bandwidth used by the call during the current history period as specified by the Sec History and Dyn Alg parameters.

Dependencies: The Dyn Stat menu applies only to links whose Encaps parameter in the Connection Profile has the value MPP.

See Also: Dyn Alg, Encaps, and Sec History in Chapter 11, “Reference.”

Ether Stat

Description: The Ether Stat menu displays the number of Ethernet frames received and transmitted and the number of collisions at the Ethernet interface.

Usage: This screen shows an example Ether Stat display:

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

This screen contains the fields described in Table 12-2.

Table 12-2. Ether Stat fields

Field	Description
Rx Pkt	Displays the number of Ethernet frames received from the Ethernet interface.
Col	Indicates the number of collisions detected at the Ethernet interface.
Tx Pkt	Specifies the number of Ethernet frames transmitted over the Ethernet interface.

Dependencies: Keep this additional information in mind:

- The counts return to zero when the Pipeline is switched off or reset; otherwise, the counts continuously increase up to the maximum allowed by the display.

HW Config

Description: The HW Config menu displays the hardware installed on the Pipeline.

Usage: This screen shows an example HW Config display:

```
00-400 HW Config
>BRI Interface
 Adrs: 00c07b547960
 Enet I/F: AUI
```

This screen contains the fields described in Table 12-2.

Table 12-3. Ether Stat fields

Field	Description
BRI Interface	Type of interface used
Adr	MAC Address of the Pipeline.
Enet I/F	The Ethernet interface you are using on the Pipeline (either UTP or AUI).

Line Status

Description: The Line Status menu shows the dynamic status of each WAN line, the condition of its electrical link to the carrier, and the status of each line's individual channels. The Link Status menu appears only if an ISDN line is installed.

Usage: This screen shows an example Line Status menu:

```
10-100 1   NT1/CSU 0
Link   P   CARRIER
B1     ***.....
B2     ***.....
```

Each line of the menu is described in the following paragraphs.

Line 1

The first line of the Line Status menu contains the menu number of lines connected.

Line 2

The second line of the Line Status menu uses one-character abbreviations to characterize the overall state of the line. Table 12-4 lists the abbreviations.

Table 12-4. Line status abbreviations

Abbreviation	Description
P	The line is in a point-to-point active state and is physically connected.
D	The line is in a multipoint active state, initialized in dual-terminal mode, and is physically connected.
M	The line is in a multipoint active state, initialized in single-terminal mode, and is physically connected.
.	The line is not active at this time, but it is physically connected.

Table 12-4. Line status abbreviations

Abbreviation	Description
X	The line is not physically connected and cannot pass data. In some countries outside the U.S., the character X might appear even though the line is physically connected.
-	The line is disabled. The Chan Usage parameter in the Configure Profile is set to disable one of the B channels.

Line 3 and Line 4

The third and fourth lines describe the state of the B1 and B2 channels, respectively. The state is represented by a single character. Table 12-5 lists each line status character.

Table 12-5. Line status characters

Character	Description
.	The channel is not available because the line is disabled, has no physical link, or does not exist, or because the Chan Usage parameter in the Configure Profile is set to disable one of the B channels.
*	The channel is connected in a current call
-	The channel is currently idle (but in service).
d	The Pipeline is dialing from this channel for an outgoing call.
r	The channel is ringing for an incoming call.
n	The channel is marked Leased in the Configure Profile.

See Also: Chan Usage in Chapter 11, “Reference.”

Sessions

Description: The Sessions status menu indicates the number of active bridging/routing links. An online link, as configured in the Connection Profile, constitutes a single active session. A session can be PPP encapsulated. The Pipeline treats each multichannel MP+ or MP link as a single session.

Usage: This screen shows the Sessions display when the Ethernet module is installed in expansion slot #5:

```
20-100 Sessions
>5 Active
 0 Headquarters
```

Each line of the menu is described in the following paragraphs.

Line 1

The first line specifies the menu number and name of the menu.

Line 2

The second line indicates the number of active sessions.

Line 3 and succeeding lines

The third and all remaining lines indicate the state of each active session, and the name, address, or CLID of the remote end. Each line uses the format *y zzzzz*, where *y* is a session status character and *zzzzz* indicates the name, address, or CLID of the remote device.

Table 12-6 lists the session status characters that can appear.

Table 12-6. Session status characters

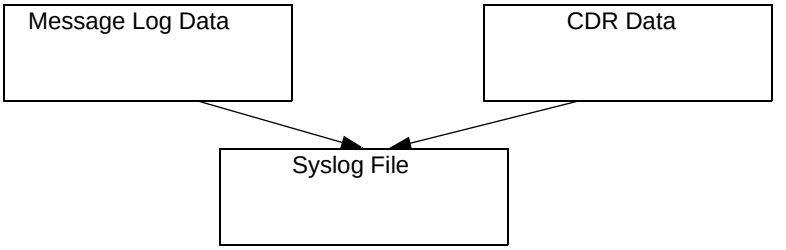
Character	Description
Blank	No calls exist and no other Pipeline operations are being performed

Table 12-6. Session status characters

Character	Description
R	R indicates Ringing; an incoming call is ringing on the line, ready to be answered.
A	A indicates Answering; the Pipeline is answering an incoming call.
C	C indicates Calling; the Pipeline is dialing an outgoing call.
O	O indicates Online; a call is up on the line.
H	H indicates Hanging up; the Pipeline is clearing the call.

Syslog

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



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

The data for level 4 (warning) and level 6 (informational) syslog messages is derived from the Message Log displays. See Table 12-9, "Message Log informational messages" on page 13 and Table 12-10, "Message Log warning messages" on page 14 for the meanings of these informational and warning messages.

Level 4 and 6 messages are presented in the format ASCEND: slot *aa* port *bb*, line *cc*, channel *dd*, *text1*, *text2*. Each element is described in Table 12-7.

Table 12-7. Syslog warning and informational message format

Element	Description
aa	The module's slot number.
bb	The serial port.
cc	The line.
dd	The channel.
text1	Line 3 of the Message Log (System) display.
text2	Line 4 of the Message Log (System) display. Note that *text2* names the remote end of a session for the "LAN session up" and "LAN session down" messages (*text1*). *text2* specifies the system name, IP address, or MAC address of the remote end.

Note: Slot *aa*, port *bb*, line *cc*, and channel *dd* are suppressed when not applicable or unknown.

Level 5 messages are presented in the format ASCEND: call *yy xx* slot *ss* port *pp zz*K *nn*. Each element is described in Table 12-8.

Table 12-8. Syslog notice message format

Element	Description
yy	The event ID in the CDR display.

Table 12-8. Syslog notice message format

Element	Description
xx	The event description in the CDR display.
ss	The module's slot number.
pp	The serial host port.
*zz*K	The data service.
nn	The phone number.

Note: Slot *ss* and port *pp* are suppressed when not applicable or unknown.

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 example syslog entries follow:

```
Oct 21 11:18:07 marcsmax ASCEND: slot 0 port 0, line 1, channel 1, \
                                                    No Connection
Oct 21 11:18:07 marcsmax ASCEND: slot 4 port 1, Call Terminated
Oct 21 11:19:07 marcsmax ASCEND: slot 4 port 1, Outgoing Call, 123
```

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

System Events

Description: The System Events Status window provides a log of up to 32 of the most recent system events the Pipeline has recorded.

This example shows a System Event record generated by an incoming call not yet assigned to a channel:

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

The message logs update dynamically. Press the Up Arrow key to display the previous entry. Press the Down Arrow key to display the next entry. To clear all messages from the Message Log while using the Palmtop Controller, enter the SHFT-> command (delete). When you are using the Control Monitor, the Delete key clears all the messages in the log.

The Message Log displays the information described in the following paragraphs.

Line 1

The first line of the menu shows the status menu number and the time the event occurred.

Line 2

The second line identifies the log entry number (M00-M31) and, if applicable, the line and channel on which the event occurred.

Lines are numbered starting with the base system ISDN lines—lines 1 and 2. A DDS 56 line is line 3.

Line 3

The third line contains the text of the message. The message can contain either basic information or a warning. Table 12-9 lists the informational messages that can appear.

Table 12-9. Message Log informational messages

Message	Explanation
Incoming Call	The Pipeline has answered an incoming call at the network interface, but has not yet routed the call.
Assigned to port	The Pipeline has determined the assignment of an incoming call to a serial host port, a digital modem, the packet-handling module, or the terminal server.
Outgoing Call	The Pipeline has dialed a call.
Added Bandwidth	The Pipeline has added bandwidth to an active call.
Removed Bandwidth	The Pipeline has removed bandwidth from an active call.
Call Terminated	An active call was disconnected normally, although not necessarily by operator command.
Incomplete Add	An attempt to add channels to an inverse-multiplexing call failed; the Pipeline added some channels, but fewer than the number requested. This situation can occur when placing a call; the first channel connects, but the requested base channel count fails.
Sys use exceeded	Call usage for the entire system has exceeded the maximum specified by the Max DS0 Mins parameter in the System Profile.
Ethernet up	The Ethernet interface has been initialized and is running.
LAN session up	This message appears after Incoming Call if a PPP, MP+ or session is established

Table 12-9. Message Log informational messages

Message	Explanation
LAN session down	This message appears before Call Terminated if a PPP or MP+ is terminated
Callback Pending	The Pipeline is waiting for callback from the remote end.
Handshake Complete	The handshake completed, but no channels were added. Either an operator entered the DO R command to resynchronize channels, or an attempt to add channels to an inverse-multiplexing call failed.
Requested Service Not Authorized	This message appears in the terminal server interface if the user requests a service not authorized by the RADIUS server.

Table 12-10 lists the warning messages.

Table 12-10.Message Log warning messages

Warning	Explanation
Busy	The phone number was busy when the call was dialed.
No Connection	The remote end did not answer when the call was dialed.
No Channel Avail	No channel was available to dial the initial call.
Not Enough Chans	A request to dial multiple channels or to increase bandwidth could not be completed because there were not enough channels available.
No Chan Other End	No channel was available on the remote end to establish the call.
Network Problem	The call setup was faulty because of problems within the WAN network or in the Line Profile configuration.
Call Disconnected	The call has ended unexpectedly.
Far End Hung Up	The remote end terminated the call normally.

Table 12-10.Message Log warning messages

Warning	Explanation
Internal Error	Call setup failed because of a lack of system resources. If this type of error occurs, notify Ascend customer support.
Incoming Glare	The Pipeline could not place a call because it saw an incoming "glare" signal from the switch. Glare occurs when you attempt to place an outgoing call and answer an incoming call simultaneously. If you receive this error message, you have probably selected incorrect Configure Profile parameters.
Wrong Sys Version	The remote-end product version was incompatible with the version of the local Pipeline. The software version appears on the Sys Options status menu.
Request Ignored	The Pipeline denied a request to manually change bandwidth during a call.
Remote Mgmt Denied	The Pipeline rejected a request to run the remote Pipeline by AIM remote management because the Remote Mgmt parameter in the System Profile at the remote end is set to No.
Call Refused	An incoming call could not be connected to the specified serial host port, digital modem, packet-handling module, or terminal server because the resource was busy or otherwise unavailable.
No Phone Number	No phone number exists in the Call Profile being dialed.
Dual Port req'd	The call could not be placed because both ports of the dual-port pair were not available.
LAN security error	This warning appears after Incoming Call but before Call Terminated if a PPP, MP+, or terminal server session has failed authentication, another session by the same name already exists, or the timeout period for RADIUS/TACACS authentication has been exceeded.

Line 4

The fourth line contains a message parameter. The message parameters listed in Table 12-11 can appear.

Table 12-11.Message Log parameters

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

Table 12-11.Message Log parameters

Message parameter	Explanation
CLID	When an incoming call is answered and the calling party number is known, line 4 specifies the CLID (calling line ID). When the CLID appears, the MBID does not.

Sys Options

Description: The Sys Options menu provides a read-only list that identifies your Pipeline and names each of the features with which it has been equipped.

Usage: This screen shows the Sys Options menu:

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

The Sys Options menu can contain the information listed in Table 12-12.

Table 12-12.Sys Options information

Option	Description
Security Prof: 1, Security Prof: 2...	Shows which of the nine Security Profiles is controlling the user interface.
Software	Defines the version and revision of the system ROM code.
S/N	Displays 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.

Table 12-12.Sys Options information

Option	Description
Access Router	
Switched Installed or Switched Not Inst	Indicates whether the Pipeline can place calls over switched circuits.
FR Rel Installed	Displays whether the frame relay option is installed
Dyn Bnd Installed or Dyn Bnd Not Inst	Displays whether Dynamic Bandwidth Allocation functionality is available.
ISDN Sig Installed	Displays whether ISDN signalling is available.

WAN Stat

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

Usage: This screen shows WAN statistics:

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

Each line of the menu is described in the following paragraphs.

Line 1

The first line displays the menu number and name of the menu. You can press the Down Arrow key to get per-link statistics. The first line of a per-link display indicates the name, IP address, or MAC address of the remote device. The per-

link count is updated every 30 seconds; the overall count is updated at the end of every active link.

Line 2

The second line specifies the number of received frames.

Line 3

The third line displays the number of transmitted frames.

Line 4

The fourth line indicates the number of errored frames. CRC checking is performed on PPP and MP+ links. An errored CRC frame contains at least one data error.

Troubleshooting

A

This appendix contains:

This appendix describes some common problems, instructions for diagnosing problems, and some suggestions on how to solve them. If the hints and instructions in this appendix don't solve your problem, you can find further troubleshooting information in Chapter 9, "Pipeline System Administration."

Cabling problems: Rule these out first

If you're unable to establish a connection with a remote network, first check that the ISDN line is plugged into the Pipeline. Telephone companies report that this is the most common cause of initial failures.

Another common problem is incorrect Ethernet cabling. The cross-over cable provided in the Pipeline package can be used only in a direct connection between the Ethernet adapter (or external transceiver) in the computer and the Pipeline. If you are connecting the Pipeline to a 10BaseT hub, you must use a regular 10BaseT cable between the hub and the Pipeline, and between the hub and the computer.

For Macintosh computers, sometimes the port you used to plug the serial cable into in the Macintosh doesn't work. You can use either the modem or printer port in the Macintosh. If one doesn't work, try the other one.

See "Check the installation" on page A-10 for related information.

Common problems and their solutions

This section lists problems you might encounter and describes ways to resolve them.

General problems

When the list of DO commands appears, most operations are not available.

You might need to select a specific Connection Profile in order to see certain DO commands. For example, to dial a Connection Profile, you must move to the Connection Profile in the Connections menu, and then type Ctrl-D 1.

Note that you cannot dial if Operations=No for the control port. If a call is already active, DO 2 (Hang Up) appears instead of DO 1 (Dial).

Profile configuration problems

The most common problems result from improperly configured profiles.

The data appears to be corrupted on one-channel or two-channel calls dialed in the U.S. to another country.

On some international calls, the data service per channel is not conveyed by the WAN to the Pipeline answering the call. You must therefore set Force 56=Yes in the Connection Profile. If you do not, the Pipeline incorrectly thinks that the call uses 64-kbps channels.

The first channel of an inverse multiplexing or MP+ call connects, but then the call clears or does not connect on the remaining channels.

The most common error in defining Connection Profiles is specifying incorrect phone numbers. The Pipeline cannot successfully build inverse multiplexing or MP+ calls if the phone numbers in the Connection Profile of the called unit are incorrect. The phone numbers that you specify in the Connection Profile are the numbers local to your unit. Do not enter the phone numbers of the Pipeline you are calling in the Connection Profile.

When the Pipeline tries to place a call, the error message No Channel Avail appears in the Message Log display.

Check the configuration of your line in the Configure profile.

Hardware configuration problems

If you cannot communicate with the Pipeline through the VT-100 control terminal, you might have a terminal configuration, control port cable, or Pipeline hardware problem.

No data is displayed on the VT-100

If the Pipeline is in this state, verify that the unit completes all of the power-on self tests successfully by following these steps:

1. Verify that the Pipeline and your terminal are set at the same speed.
2. Locate the LED labeled CON.
3. Switch on the Pipeline.

   The CON LED should remain off except during the power-on self tests. If you are using the Control Monitor, type Ctrl-L to refresh the screen.

   If the CON LED remains on longer than a minute, there is a Pipeline hardware failure. A blinking CON LED also indicates a hardware failure. Should these situations arise, contact Ascend Customer Support.

The CON LED is off, but no data is displayed on the Control Monitor's VT-100 terminal.

If the unit passed its power-on self tests and you still cannot communicate with the Control Monitor, type Ctrl-L to refresh the screen. If you still do not see any data, check the cabling between the Pipeline and your terminal by following these steps:

1. Check the pin-out carefully on the 9-pin cable.

   The control terminal plugs into the HHT-VT-100 cable or 9-pin connector labeled Terminal on the back of the Pipeline. If you are connecting to an IBM PC-like 9-pin serial connector, a straight-through cable is appropriate. Otherwise, you might need a 9-to-25 pin conversion cable.
2. Check the flow control settings on your VT-100 terminal.

   If you are not communicating at all with the Pipeline, see whether you can establish communications after you have turned off all transmit and receive flow control at your terminal or terminal emulator.
3. Determine whether you need a null-modem cable converter.

   In general, these are not required for communications to the Pipeline. However, so many different cable and terminal configurations are available that occasionally a null-modem cable converter might be required.

Random characters appear on the Control Monitor screen.

If random or illegible characters appear on your display, there is probably a communications settings problem. You must make these settings:

- 9600 bits per second data rate
- 8 data bits
- 1 stop bit
- No flow control
- No parity

If you have changed the data rate through the Sys Config menu, make certain that your VT-100 terminal matches that rate.

The start-up display indicates a power-on self test failure.

If the start-up display indicates a failure in any of its tests, an internal hardware failure has occurred with the unit. In this case, contact Ascend Customer Support.

Problems configuring the Pipeline

There are two common problems associated with the Pipeline configuration procedure:

- The communications program does not display a profile when you press Ctrl-L
- A profile appears when you press Ctrl-L, but it isn't the Configure profile shown in this manual

If you see garbage characters on the screen, make sure that vt100 emulation is set to the right speed (9600 bps).

No profile appears in your communications program

If no profile appears when you press Ctrl-L in your communication program, one of these conditions could be causing the problem:

- Your Pipeline is not receiving power
- Your Pipeline is not connected to the serial port of your computer
- Your communications program is not configured correctly for your Pipeline, or it is not communicating on the right port.
- There is a hardware problem with the Pipeline

To diagnose and solve the problem, follow these steps:

1 Check the pwr LED on the front panel of the Pipeline.

If the pwr LED is not on, the unit is not receiving power. It may not be connected to a power source. Continue to step 2.

If the light is on, continue to step 4.

2 Connect your Pipeline to a power source.

If your Pipeline is plugged into a power strip or surge protector, make sure the power strip or surge protector is plugged in and turned on.

Once you are sure the Pipeline is connected to a power source, if the pwr LED is on, continue to step 3.

If the pwr LED is still not on, contact the Ascend Technical Assistance Center at 1-800-ASCEND-4.

3 Check the con LED.

If the con LED goes off within thirty seconds after you connect the Pipeline to a power source, continue to step 4.

If the con LED is blinking or on more than thirty seconds after you have connected the Pipeline to a power source, contact the Ascend Technical Assistance Center at 1-800-ASCEND-4.

4 Press Ctrl-L to refresh the screen.

If no profile appears, continue to step 5.

If a profile appears, but it isn't the Configure profile, go to "A profile appears but it isn't the Configure profile" on page A-7."

5 Check to see if your Pipeline is connected to your computer's serial port.

If necessary, connect the Pipeline to your computer and continue to the next step.

If your Pipeline is connected to your computer, continue to step 6.

6 Press Ctrl-L to refresh the screen.

If no profile appears, continue to step 7.

If a profile appears, but it isn't the Configure profile, go to "A profile appears but it isn't the Configure profile" on page A-7."

7 Check to see if your communications program is configured for the Pipeline.

Your communications program should be configured as follows:

- VT100
- 9600 bits per second
- 8 data bits
- No parity
- 1 stop bit
- No flow control
- Direct connect

If necessary, configure your communications program, then continue to the next step.

8 Press Ctrl-L to refresh the screen.

If no profile appears, contact your network administrator.

If a profile appears but it isn't the Configure profile, continue to the next section.

A profile appears but it isn't the Configure profile

If a profile appears, but it isn't the Configure profile, your Pipeline may already have been configured.

Solving this problem is easy: press Escape until you reach the Main Edit Menu, and then select Configure.

ISDN BRI interface problems

Provisioning or switch type problems

If voice calls are not being received correctly, it's possible that your ISDN line was provisioned incorrectly at the central office switch. Especially if your ISDN

line was installed before you were aware of the provisioning information recommended for the Pipeline, this is a likely cause.

If you are unable to receive a voice call while a data call is in progress, it's possible that your line was configured with the Point-to-Point switch type. In cases where both B channels are in use for a multi-channel data call, the Point-to-Point switch is not able to pass on a voice call for the Pipeline to service.

If you suspect a provisioning or switch type problem, call the telephone company and work through the provisioning information described at the beginning of this guide.

SPID format problems

If the SPIDs entered in the Pipeline configuration are incorrect, the Pipeline will be unable to access the ISDN line.

The most common problem with SPIDs is that they were entered incorrectly, either by mistake or because the telephone company provided the wrong information. If wrong or incomplete information was provided about the SPID numbers assigned to your ISDN line, try adding 00 to the end of the SPID number. Or, if the suffix ends in a double digit, such as 01 or 02, try replacing those two digits with a single digit, such as 1 or 2. If neither of these suggestions works, call the telephone company and request that they verify the SPIDs you have.

Dialing and answering do not operate reliably.

To resolve this problem, follow these steps:

1 Check your cabling.

The first and most critical aspect of ISDN BRI interfaces is the cable or cables connecting the Pipeline to the WAN line or WAN-terminating equipment. Typically, WAN interface cabling problems appear immediately after installation. If you are unsure about the cabling required for your application, contact Ascend Customer Support. The installation instructions in the *Pipeline 25-Fx User's Guide* describe the general ISDN BRI interface requirements, and Appendix E, "Pipeline 25-Fx Specifications," lists cabling pin-outs.

The status of an ISDN BRI line in the WAN Status windows is No Logical Link.

In some countries outside the U.S., it is common for no logical link to exist before the Pipeline places a call.

In the U.S., when you first plug a line into the Pipeline or switch power on, the central office switch can take as long as 15 minutes to recognize that the line is now available. You might have to wait that long for the line state to change to Active (A). The physical link can exist without a logical link up on the line.

If you wait longer than 15 minutes and the line is still not available, follow these steps:

1. Check whether all the ISDN telephone cables are wired straight through.

   If you are running multipoint (passive bus) on your switch, all of the ISDN telephone cables must be wired straight through. If any of the cables are wired to cross over, you will not be able to place calls.
2. Check that 100% termination is provided on each ISDN line.
3. Check whether you have correctly specified the SPIDs (Service Profile Identifiers) in the Configure Profile for each line.

   If the SPIDs are not correctly specified, the line status might indicate No Logical Link. Check with your system manager or carrier representative to obtain the SPID or SPIDs for your line. You specify your SPIDs in the Configure Profile.

Bridge/router problems

The quality of the link is questionable.

When running FTP (File Transfer Protocol), the data transfer rate appears in bytes per second. Multiply this rate times 8 to get the bits per second. For example, suppose that you are connected to Detroit on a 56-kbps B channel and that FTP indicates a 5.8 kbyte/s data rate; in this case, the link is running at 5.8x8=46.8 kbps, or approximately 83% efficiency. Many factors can affect efficiency, including the load on the FTP server, the round-trip delay, the overall traffic between endpoints, and the link quality.

You can check link quality in the WAN Stat status menu, or by running a ping between the same endpoints. Dropped packets hurt the link's efficiency, as does round-trip delay. Random round-trip delay indicates heavy traffic, a condition that also drops the efficiency of the link.

The Pipeline hangs up after answering an IP call.

To resolve this problem, follow these steps:

1 If you are running PPP, check that you have entered the proper passwords.

2 Check that Auth is set to PAP or CHAP.

3 If you are routing IP over PPP, check that the calling device gives its IP address

Some calling devices supply their names, but not their IP addresses. However, you can derive an IP address if the calling device is listed in a local Connection Profile. Try enabling PAP or CHAP for the Recv Auth parameter so that the Pipeline matches the caller's name to the Station parameter in a Connection Profile and gets the corresponding LAN Adrs.

Problems accessing the remote network

If, when you press Ctrl-D in the Configure profile, the status window in the upper right corner displays a message other than LAN Session Up, you should first disconnect the Pipeline from the phone line connection, reconnect it, then try accessing the remote network again. If you still cannot access the remote network, one or a combination of the following may be a problem:

- Your Pipeline may not be installed correctly
- Your Pipeline may not be configured correctly
- Your phone line may not have been activated, or there may be a problem with the telephone network

Check the installation

1 Make sure your Pipeline is connected to your phone line.

2 Check the WAN LED on the front panel of your Pipeline.

If the WAN LED is not blinking, continue to the next section, “Configuration problems” on page A-11.

If the WAN LED is blinking, one of the following may be the case:

- Your Pipeline may not be connected to the phone line.
- If you do not have an integrated NT1 interface, your Pipeline may not be connected to an NT1.
- Your phone line may not be activated.
- Your ISDN channel may be temporarily unavailable.
- You may have entered an incorrect switch type. Check the setting in the Configure profile.
- You may have entered the wrong SPID. Check the setting in the Configure profile, and confirm the values with your service provider.

3 Check to make sure you have connected your Pipeline to your ISDN line.

If necessary, connect your Pipeline to your ISDN line. If your Pipeline does not have an integrated NT-1 interface, make sure it is connected to an NT-1, and that the NT-1 is connected to the ISDN line as shown in your NT-1 manual.

Once you are connected, if the WAN LED is still blinking, continue to step 4.

4 Contact your ISDN service provider to see if your lines have been activated. If they have been activated, check to see if your service provider is experiencing problems with their telephone network.

If your lines are not activated, wait until they are, then try the call again.

If your service provider is having problems with the lines, wait for a while, then try the call again.

If the lines are activated and your service provider is experiencing no problems, but the wan LED is still blinking, you may have a configuration problem. Continue to the next section.

Configuration problems

If you are sure your Pipeline is properly installed, your lines are activated, and your service provider is not experiencing any problems, but the wan LED is still blinking, you may have a configuration problem.

1 Start your communications program and press Ctrl-L to refresh the screen.

The Configure profile appears in the Edit window:

2 Check to see if you saved your Configure profile.

If an asterisk (*) appears next to Save, you have made changes to the Configure profile but did not save them. Continue to step 3.

If an asterisk does not appear next to Save, continue to step 4.

3 Press Ctrl-N until the cursor moves to Save, then press Enter.

Your Configure profile is saved to the Pipeline. Try accessing the network again.

If you still have problems, continue to the next step.

4 At the Configure profile, press Ctrl-D to have the Pipeline manually dial the remote site, then look at the 10-100 and 20-100 status windows to see the status of your ISDN or SW56 line:

See Appendix B, “System Event Messages,” for more information about the messages you can see in these windows.

- If an X appears in the Link field of the 10-100 status window instead of a P, M, or D, your ISDN line is not activated or you have entered an incorrect switch type.
- If an asterisk (*) appears in the B1 or B2 field of the 10-100 status window and the remote site’s name appears in the 20-100 Sessions status window, your Pipeline is connected to the remote site. Skip to step 6.
- If an asterisk (*) appears in either the B1 or B2 fields of the 10-100 status window but then disappear, any of the following configuration settings may be incorrect:
  - Rem Name: You may have entered the wrong name for the remote host.
  - Rem Addr: You may have entered the wrong IP address for the remote host.
  - Send Auth: You may have selected the wrong authentication protocol.
  - Send PW: You may have entered the password incorrectly.
  - My Name: The name you assigned to your Pipeline does not match the name expected by the remote host.
  - My Addr: The IP address you entered for your Pipeline is incorrect.
  - Check the parameters you specified in the Configure profile against those you recorded in the Configuration tables. If they match, you may need to verify the parameters with the network administrator.

  Continue to step 5.

- If a D appears in either the B1 or B2 fields of the 10-100 status window, you may have entered the wrong phone number for the remote site or the wrong SPID for your ISDN line configuration. Continue to step 5.

5 Check the Configure profile to make sure the configuration information is entered accurately.

If you entered the information incorrectly, enter the correct information in the appropriate field of the Configure profile. Be sure to save the Configure profile.

If the information is entered correctly, make sure the information you specified is accurate:

- Contact your network administrator to confirm addresses, names, and the remote phone number.
- Contact the service provider who installed your ISDN line to confirm your SPID or SPIDs.

Once you have confirmed that all the information is entered correctly and you have saved the Configure profile, try accessing the network again. If you still have trouble, continue to step 6.

6 If you are routing, check to make sure you have configured your computer's IP address accurately.

Refer to your computer's manual for instructions on configuring your computer's IP address.

If you still cannot access the remote network, contact the network administrator or the Internet Service Provider you are trying to access. If this also fails, contact the Ascend customer service department at the sites listed at the front of this guide.

System Event Messages

B

This appendix contains:

List of system event messages

This section lists system event messages and their meanings.

Table B-1. System Events

Event Message	Meaning
Added Bandwidth	Bandwidth has been added to an active call.
Assigned To Port	The assignment of an incoming call to a serial host port or the Ethernet module has been determined.
Busy	Number at other end is busy.
Call Disconnected	The call ended unexpectedly.
Call Refused	An incoming call could not be connected to the specified serial host port because it was busy or otherwise unavailable.
Call Terminated	An active call was disconnected normally, although not necessarily by operator command.
Ethernet Up	Appears after the Ethernet interface has been initialized and is running.
Far End Hung Up	The far end terminated the call normally.
Incoming Call	An incoming call has been answered at the network interface, but has not yet been assigned to a serial host port or to the IP router.
Incoming Glare	The Pipeline 25-Fx received an incoming glare signal from the switch. Your telephone lines may be configured incorrectly.

Table B-1. System Events (continued)

Event Message	Meaning
Incomplete Add	An attempt to add channels to an inverse-multiplexing call failed; some channels were added, but less than the number requested. This can also occur when placing a call and the first channel connects, but the requested base channel count fails.
Internal Error	Call setup failed because of a lack of system resources, such as insufficient memory. If this type of error occurs, notify the Ascend Technical Assistance Center.
LAN Security Error	An MPP, PPP, or terminal server session is terminated because of a security violation; for example, you entered an incorrect password.
LAN Session Down	Appears before call terminated if a PPP or an MPP session is terminated.
LAN Session Up	Appears after incoming call if a PPP or an MPP session is established.
Missing Wink-Start	The switch did not reply with the wink-start signal, either because the line was out of service or because the switch was busy. In either case, the Pipeline 25-Fx could not even start to dial a call over that line.
Network Problem	Call could not be completed because of a network problem.
No Chan Other End	No channel was available on the far end to establish the call.
No Channel Avail	No channel was available for the call.

Table B-1. System Events (continued)

Event Message	Meaning
No Connection	The far end did not answer when the call was dialed.
No Phone Number	There is no phone number entered in the Connection profile from which you tried to place a call.
No Trunk Available	All lines are out of service.
Not Enough Chans	A request to dial multiple channels or to increase bandwidth could not be completed because there were not enough channels available at that time.
Outgoing Call	The Pipeline 25-Fx has dialed a call.
Remote Mgmt Denied	A request to run the remote Pipeline 25-Fx by remote management was rejected.
Removed Bandwidth	Bandwidth has been subtracted from an active call.
Request Ignored	The request to manually change bandwidth during a call was denied.
Trunk Down	One or more lines are out of service.
Trunk Up	One or more lines were out of service, but have now returned to service.
Wrong Sys Version	The software at the far end is incompatible with the Pipeline 25-Fx system software.

ISDN Cause Codes

C

This appendix contains:

Checking the status windows

ISDN cause codes can help you diagnose problems with calls. They appear in the 00-200 System Events status window.

List of cause codes

The cause codes listed on this table are not valid for German 1TR6 networks (WANs).

Table C-1. ISDN Cause Codes

Code	Cause
0	Valid cause code not yet received
1	Unallocated (unassigned) number
2	No route to specified transit network (WAN)
3	No route to destination
4	Send special information tone
5	Misdialed trunk prefix
6	Channel unacceptable
7	Call awarded and being delivered in an established channel
8	Prefix 0 dialed but not allowed
9	Prefix 1 dialed but not allowed
10	Prefix 1 dialed but not required
11	More digits received than allowed, call is proceeding
16	Normal clearing

Table C-1. ISDN Cause Codes (continued)

Code	Cause
17	User busy
18	No user responding
19	No answer from user (user alerted)
21	Call rejected
22	Number changed
23	Reverse charging rejected
24	Call suspended
25	Call resumed
26	Non-selected user clearing
27	Destination out of order
28	Invalid number format (incomplete number)
29	Facility rejected
30	Response to STATUS ENQUIRY
31	Normal, unspecified
33	Circuit out of order
34	No circuit/channel available
35	Destination unattainable
37	Degraded service
38	Network (WAN) out of order

Table C-1. ISDN Cause Codes (continued)

Code	Cause
39	Transit delay range cannot be achieved
40	Throughput range cannot be achieved
41	Temporary failure
42	Switching equipment congested
43	Access information discarded
44	Requested circuit channel not available
45	Pre-emptied
46	Precedence call blocked
47	Resource unavailable, unspecified
49	Quality of service unavailable
50	Requested facility not subscribed
51	Reverse charging not allowed
52	Outgoing calls barred
53	Outgoing calls barred within CUG
54	Incoming calls barred
55	Incoming calls barred within CUG
56	Call waiting not subscribed
57	Bearer capability not authorized
58	Bearer capability not presently available

Table C-1. ISDN Cause Codes (continued)

Code	Cause
63	Service or option not available, unspecified
65	Bearer service not implemented
66	Channel type not implemented
67	Transit network selection not implemented
68	Message not implemented
69	Requested facility not implemented
70	Only restricted digital information bearer capability is available
79	Service or option not implemented, unspecified
81	Invalid call reference value
82	Identified channel does not exist
83	A suspended call exists, but this call identity does not
84	Call identity in use
85	No call suspended
86	Call having the requested call identity has been cleared
87	Called user not member of CUG
88	Incompatible destination
89	Non-existent abbreviated address entry
90	Destination address missing, and direct call not subscribed
91	Invalid transit network selection (national use)

Table C-1. ISDN Cause Codes (continued)

Code	Cause
92	Invalid facility parameter
93	Mandatory information element is missing
95	Invalid message, unspecified
96	Mandatory information element is missing
97	Message type non-existent or not implemented
98	Message not compatible with call state or message type non-existent or not implemented
99	Information element non-existent or not implemented
100	Invalid information element contents
101	Message not compatible with call state
102	Recovery on timer expired
103	Parameter non-existent or not implemented, passed on
111	Protocol error, unspecified
127	Internetworking, unspecified

Upgrading Pipeline Software

D

This appendix contains:

What you need to upgrade system software

Ascend system software is continually being enhanced to support new features and improve performance. The Pipeline is designed so that you can upgrade the system software and take advantage of these new features without returning the unit to the factory.

To upgrade the system software you need the following:

- The new system software. Contact the Ascend Technical Assistance Center for upgraded software, as described at the front of this guide.
- A serial connection between a PC and the Pipeline so you can access the configuration software by using your communications program

Note: Windows versions of communications programs do *not* work with this procedure. If you are using a Macintosh communications program, Macbinary must be turned off.

The upgrade procedure

Upgrading system software is a three- or four-part process, depending on the Security profile that is currently activated. The steps required include the following:

1 If necessary, activate a Security profile that allows for field upgrade.

2 Backing up your configured profiles to your computer's hard disk.

3 Download the system software to the Pipeline.

4 Restore your Pipeline configuration

Instructions for completing these tasks are described in this appendix. Before you go any further, check to see which version of the system software is currently installed on your Pipeline and which Security profile is activated.

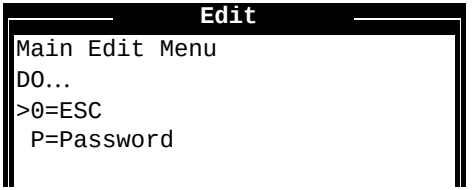
To see which software version is currently running on the Pipeline, look in the Sys Option status window. See Appendix B, "System Event Messages," for details.

Activating a Security Profile

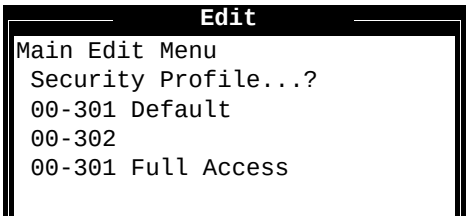
If the Security Profile that is currently activated has Field Service disabled, you need to activate a security profile that has Field Service enabled in order to upgrade your system software.

To activate the security profile that has Field Service enabled:

1 Press Ctrl-D to open the DO menu, and then press P (or select P=Password).

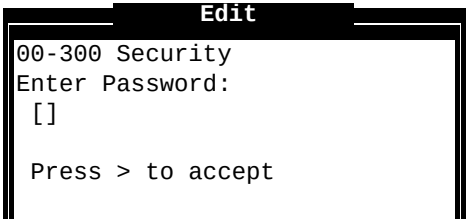


2 In the list of Security Profiles that opens, select the Security Profile you want to enable. By default Field Service is enabled in the Full Access Profile.



The Pipeline then prompts for that profile's password.

3 Type the password you assigned to the profile and press Enter to accept it.



If you enter the right password, a message states that the password was accepted and the Pipeline is using the new security level.

```
Message #119
Password accepted.
Using new security level.
```

If the password you enter is incorrect, you are prompted again to enter the password.

Backing up the Pipeline configuration

Before you overwrite the software in the Pipeline, make sure that you save your existing configuration to disk.

Note: When you backup the Pipeline configuration, the configuration data is written to a text file on the disk of the accessing host (the computer connected to the Pipeline Control port). *Passwords are not saved.* Send and Recv passwords, Security Profile passwords, and passwords specified in the Ethernet Profile (Mod Config menu), are all set to the null password when you restore a configuration from a saved file. We strongly recommend that you record these passwords off-line if you need to restore them.

Before you start the backup, verify that your terminal emulation program has a disk capture feature. Disk capture allows your emulator to capture to disk the ASCII characters it receives at its serial port. You should also verify that the data rate of your terminal emulation program is set to 9600 baud or lower and that the Term Rate parameter in the System Profile (Sys Config menu) is also set to 9600. Higher speeds might cause capture errors.

You can cancel the backup process at any time by typing Ctrl-C.

To save the Pipeline configuration (except passwords) to disk:

1 In the Sys Diag menu, select Save Config and press Enter.
The following message appears:

```
Ready to download - type any key to start...
```

2 Turn on the Capture feature of your communications program and supply a filename for the saved profiles.

   Consult the documentation for your communications program if you have any questions about how to turn on the Capture feature.

3 Press any key to start saving your configured profiles.

   Rows of configuration information are displayed on the screen as the file is downloaded to your hard disk. When the file has been downloaded to your hard disk, your communications program displays a message indicating the download is complete.

4 Turn off the Capture feature of your communications program.

5 Print a copy of your configured profiles for later reference.

Note: If you examine the saved Pipeline data file, notice that some of the lines begin with *START*= and other lines begin with *END*=. These START/STOP lines and the block of data contained between them constitute a profile. If a parameter in a profile is set to its default value, it does not appear. In fact, you can have profiles with all parameters at their defaults and the corresponding START/STOP blocks would be empty.

Upgrading the system software

Note: Uploading system software overwrites all existing profiles. Save your current profiles to your hard disk before you begin upgrading system software or you will have to reconfigure all your profiles.

To place the Pipeline in boot mode:

1 From any menu in the Pipeline software, type the following four-key sequence in rapid succession (press each key in the sequence shown, one after the other, as quickly as possible):

   Esc [Esc -

   Esc is the escape key, [is the left bracket key, and - is the minus key. Press these keys in the sequence shown, one after the other in rapid succession. If you don't see the following string of Xmodem control characters:

   CKCKCKCK

   the most likely cause is that you didn't press the four-key sequence quickly enough. Try again—most people use both hands and keep one finger on the escape key.

2 As soon as the Xmodem strings are displayed

CKCKCKCK

use the Xmodem file transfer protocol to send the system binary to the Pipeline. Your communications program begins sending the binary file to your Pipeline. This normally takes anywhere from 5 to 15 minutes.

Note: The time displayed on the screen does not represent real time. Don't worry if your communication program displays several "bad batch" messages. This is normal.

When the upload process is complete, the Pipeline resets itself. When the self-test is complete, the Configure profile appears in the Edit window with all parameters set to default values.

You are ready to restore your configured profiles to your Pipeline. Continue to the next section.

Restoring the Pipeline configuration

Once you have upgraded your system software, you can restore your saved configured profiles.

Note: When you perform the Restore Cfg, extra information is occasionally placed at the end of the saved configuration file. The configuration file must start with the word START and end with the words END DOWNLOAD. Before restoring your configuration, you should verify that your text file is in this format.

Note: If the upgraded system software probably includes new parameters, you may have to reconfigure some parameters, as well as configure the new parameters.

Before you start the restore procedure, verify that your terminal emulation program has an autotype (or ASCII file upload) feature. Autotype allows your emulator to transmit a text file over its serial port. You should also verify that the data rate of your terminal emulation program is set to 9600 baud or lower and that the Term Rate parameter in the System Profile (Sys Config menu) is also set to 9600. Higher speeds might cause transmission errors.

You can use the Restore Cfg command to restore a full configuration that you saved by using the Save Cfg command, or to upload more specific configuration

information obtained from Ascend, for example, a single filter stored in a special configuration file. To load configuration information from disk, first connect the backup device to the Pipeline Control port. Then:

1 In the Sys Diag menu, select Restore Cfg and press Enter.

The following message appears:

```
Waiting for upload data...
```

2 Use the Send ASCII File feature of the communications software to send the Pipeline the configuration file.

If you have any questions about how to send an ASCII file, consult the documentation for your communications program. When the restore has been completed, the following message appears:

```
Restore complete - type any key to return to menu
```

3 Press any key to return to the configuration menus.

If you restored a complete configuration, the passwords used in your Security profiles have been wiped out. To reset them:

1 Press Ctrl-D to invoke the DO menu, select Password, and choose the Full Access profile.

2 When you are prompted to enter the password, press Enter (the null password).

After you have restored your privileges by entering the null password, we recommend that you immediately open the Connection Profiles, Security Profiles, and Ethernet Profile (Mod Config menu) and reset the passwords to their previous values.

After you have you want to set security on the upgraded Pipeline, re-activate the appropriate Security profile. Use the procedure explained in “Activating a Security Profile” on page D-3 and select the appropriate Security Profile.

Pipeline 25-Fx Specifications

E

This appendix contains these sections:

Hardware specifications

Dimensions

8.2 in x 6 in x 1.2 in [20.8 cm x 15.24 cm x 3.05 cm]

Weight

2.25 lbs [1.02 kg]

LAN interface

10 MB/S Ethernet (10Base-T)

The Pipeline 25-Fx supports the physical specifications of IEEE l802.3 with Ethernet 2 (Ethernet/DIX) framing. It provides a single Ethernet interface that supports 10Base-T (Unshielded Twisted Pair) Twisted pair Ethernet and IEEE 802.3 (10Base-T) with an RJ-45 connector.

To connect a single computer with a 10Base-T Ethernet interface, use the 10Base-T Ethernet crossover cable included with the Pipeline 25-Fx.

ISDN interface

BRI S/T Interface (model: P25-1S-PX)

BRI U Interface (model: P25-1U-PX)

Software upgrade

Via built-in flash RAM

Power requirements

The Pipeline 25-Fx's source power requirements are listed in Table E-1.

Table E-1. Pipeline 25-Fx power requirements

Element	Value
Voltage	90-130 VAC, 0.4A 47-63 Hz. 20-240 VAC, 0.2A 47-63 Hz.
Phase	Single
Frequency	47-63 Hz
Power	11W (nominal) to 13.5W (maximum)

The configuration settings for the Pipeline 25-Fx are stored in battery-protected memory. When the Pipeline 25-Fx is turned off, the profiles are not lost.

Note: Use a protected AC power source, or add surge protection between the power source and the Pipeline 25-Fx.

Environmental requirements

For best results, you should house the Pipeline 25-Fx in a room with constant temperature and humidity. In general, cooler environments are better, and an operating temperature of 32° to 104° Fahrenheit (0° to 40° Celsius) is recommended. Storage temperatures of -40° to 176° Fahrenheit (-71.4° to 80° Celsius) are acceptable.

Humidity should be high enough to prevent accumulation of static electricity, but low enough to prevent condensation. An operating relative humidity of up to 90% is acceptable.

You can operate the Pipeline 25-Fx at altitudes of 0 to 14800 ft. (0-4500 m).

Safety certifications

FCC Class B, CSA, UL

EMI/RF

FCC Part 68, FCC part 15

ISDN port specifications

The Pipeline 25-Fx BRI interface is a 'Western Electric' type RJ-45 port. Connection between this port and the WAN is via a (non-integral) interconnecting cable/connector set. The pin-outs for the Pipeline 25-Fx S interface BRI port are shown in Table E-2.

Table E-2. ISDN S interface pinouts

BRI Logical Interface	RJ-45 TE (Terminal Equipment)
Transmit (output) + Transmit (output) -	Pin 3 Pin 6
Receive (input) + Receive (input) -	Pin 4 Pin 5
The S interface cable can be up to 1000m in length.	

The pin-outs for the Pipeline 25-Fx U interface BRI port are shown in Table E-3.

Table E-3. ISDN U interface pinouts

BRI Logical Interface	RJ-45 TE (Terminal Equipment)
Transmit (output) + Transmit (output) -	Pin 3 Pin 6
Transmit/Receive (output) + Transmit/Receive (output) -	Pin 4 Pin 5
The U interface cables can be up to 18000 ft (5486m) in length.	

Control port specifications

The Control port uses a standard DE-9 female connector that conforms to the EIA RS-232 standard for serial interfaces.

The Pipeline 25-Fx uses the RS-232 pinouts listed in Table E-4.

Table E-4. Terminal port and cabling pinouts

DE-9 pin number	RS-232 signal name	Function	I/O
1	DCD	Data Carrier Detect	O
2	RD	Serial Receive Data	O
3	SD	Serial Transmit Data	I
4	DTR	Data Terminal Ready	I
5	GND	Signal Ground	
6	DSR	Data Set Ready	O
7	RTS	Request to Send	I
8	CTS	Clear to Send	O
*9	*RI	*Ring Indicator	*O

*Pin 9 is not active (Ring Indication signal not supplied).

Phone jack specifications

Maximum ringer equivalence (REN) of analog devices connected to the Pipeline 25-Fx: 3.0 A

Ringer voltage: 90 Vrms (AC) with a -15 VDC offset

Ringer frequency: 20 Hz for products sold in the United States. For other countries, this can be set at the factory to 25 Hz or 30 Hz.

Software specifications

Protocols supported

TCP/IP routing

WAN Protocols Supported: PPP, Multilink PPP (MP), Multilink Protocol Plus (MP+)

Bandwidth Management: Multilink PPP (MP), Multilink Protocol Plus (MP+), TCP header compression, STAC data compression (optional)

Security

PAP, CHAP

Management

Directly via the Control port

Remotely from another Ascend product via the Ascend Management Protocol (AMP)

Ascend Internetworking Glossary

F

This glossary contains definitions of terms that apply to the entire Ascend product family, including both Pipeline and MAX units.

3.1 Khz audio bearer service—A bearer service provided by some telephone companies to send data calls over voice trunks. To prevent corruption of the data, switches must be set to turn off echo cancellers on the trunks. The service is sometimes referred to as "data over voice."

Note: Currently, Ascend parameter settings for voice transmission make no distinction between Digital/data bearer and 3.1Khz audio bearer services. Voice settings apply only to true voice service, which does not include 3.1Khz audio bearer service.

10BaseT—An IEEE standard (802.3) for operating 10 Mbps Ethernet networks with twisted-pair cabling and a wiring hub.

analog data—Data that can have any value in a range and that can change continuously; the time of day represented by clock hands, or the temperature represented by a liquid thermometer are examples of analog data.

analog signal—A type of signal that encodes data transmitted over wire or through the air, and is commonly represented as an oscillating wave. An analog signal can take any value in a range, and changes smoothly between values.

An analog signal can transmit analog or digital data. For example, a radio station sends analog music data using analog signals, while a modem transmits digital data using analog signals.

ARP—Address Resolution Protocol. This portion of the TCP/IP protocol maps an IP address to the physical address (Ethernet Address) of the PC that it is on, helping to identify PCs on an Ethernet LAN. See also Ethernet and TCP/IP.

asynchronous transmission—A mode in which the sending and receiving serial hosts know where a character begins and ends because each byte is framed with additional bits, called a *start bit* and a *stop bit*. A start bit indicates the beginning of a new character; it is always 0 (zero). A stop bit marks the end of the character. It appears after the parity bit, if one is in use.

AUI—Autonomous Unit Interface or Attachment Unit Interface. This refers to the 15-pin D connector and cables that connect single and multiple channel equipment in an Ethernet transceiver.

B channel—A 64-kbps channel that carries user data.

Backbone—The part of the communications network designed to carry the bulk of traffic. Provides connectivity between subnetworks in an enterprise-wide network.

Backbone Router —Routers designed to be used to construct backbone networks using leased lines. Typically do not have any built-in digital dial-up WAN interfaces. Typical manufacturers include Cisco, Wellfleet, 3Com, CrossCom, and so on.

Bit—Contraction of the term “BInary digiT.” The smallest unit of information a computer can process, representing one of two states (usually indicated by “1” and “0”).

Bridge—A device or setup that connects and passes data, voice, or video between two network segments, based on the destination field in the packet header. Ascend units are learning bridges, because they pass all packets to the next network segment (the ISDN line), and builds a table to identify the destination addresses that are local and remote. After learning the addresses on both sides of a network, the bridge passes only packets for the remote network. (Contrast with router).

call—A single session in which a calling device and an answering device connect over the WAN.

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

You can manipulate the information in order to create a wide range of different reports, including reports based on individual call costs, inverse multiplexed WAN session costs, costs on an application-by-application basis, bandwidth usage patterns over specified time periods, and so on. You can use this information to better understand your bandwidth usage patterns and, if necessary, make adjustments to the ratio of switched to dedicated bandwidth between network sites.

channels—A portion of a line's bandwidth. A line contains a fixed number of channels. Each line can contain switched channels only, nailed-up channels only, or a combination of switched and nailed-up channels.

A line can have these types of channels:

- DS0

  A DS0 is a 64-kbps channel on a line using inband signaling. For information on inband signaling, see the entry for Inband signaling.

- B channel

  A B channel is a 56-kbps or 64-kbps channel that carries user data on a line using ISDN D-channel signaling. For information on ISDN D-channel signaling, see the entry for ISDN D-channel signaling.

- D channel

  A D channel carries WAN synchronization information on a line using ISDN D-channel signaling. For information on ISDN D-channel signaling, see the entry for ISDN D-channel signalling.

CHAP—Challenge Handshake Authentication Protocol. This security protocol allows access between data communications systems prior to and during data transmission. CHAP uses challenges to verify that a user has access to a system.

circuit—A connection between endpoints over a physical medium.

circuit-level inverse multiplexing—A method of inverse multiplexing in which the inverse mux slices the data stream into equal portions, and transmits each portion over an available circuit. The receiving end adjusts for network-induced delay and reassembles the data packets into their proper order. The AIM and BONDING protocols define how circuit-level inverse multiplexing works. Applications that require transparent digital circuits, such as videoconferencing, nailed-up backup and overflow, and bulk file transfer applications, use circuit-level multiplexing.

codec (COder/DECoder)—A device that encodes analog data into a digital signal for transmission over a digital medium.

CPE (Customer Premises Equipment)—Terminal equipment located on the customer premises which connects to the telephone network.

Crossover cable—A cable with wires that "cross over," so the terminating ends of the cable have opposite wire assignments. (Contrast with straight-through cable).

CSU (Channel Service Unit)—A device used to connect a digital phone line coming in from the phone company to network access equipment located on the customer premises. A CSU may also be built into the network interface of the network access equipment.

D4-framed T1 line—A T1 line that uses the D4 format, also known as the Superframe format, to frame data at the physical layer. The D4 format consists of 12 consecutive frames, each one separated by framing bits.

D channel—A channel that carries WAN synchronization and signalling information.

data service—A service provided over a WAN line and characterized by the unit measure of its bandwidth. A data service can transmit either data or digitized voice.

data over voice—The sending of digital data over telephone trunks conditioned for voice. "Data over voice" can refer to sending data either with voice bearer service or with 3.1KHz audio bearer service.

DCE (Data Communications Equipment)—As defined in the RS-232 specification, equipment to which DTE (Data Terminal Equipment) is connected, often to enable access to network facilities. A DCE converts the format of the data coming from the DTE into a signal suitable to the communications channel. DCE often refers to equipment such as network access equipment, and DTE refers to application equipment, such as a videoconference terminal.

digital data—Data that can have only a limited number of separate values. The time of day represented by a digital clock, or the temperature represented by a digital thermometer are examples of digital data; the digital values do not change continuously, but remain at one discrete value and then change to another, discrete value.

digital modem—An internal device in the MAX that enables it to communicate over a digital line (such as a T1 PRI line) with a station using a modem connected to an analog line. Incoming modem calls and incoming digital calls come over the same digital line.

The MAX can accept an incoming call from the network either as a pure digital stream, or as a PCM (Pulse Coded Modulation) encoded digital stream. A PCM-encoded digital stream contains a digitized version of the analog waveform sent by a caller attached to a modem. The MAX can also convert outgoing data into analog waveforms, convert these waveforms to a PCM-encoded digital stream, and send them to the network over a digital line. The network presents the data to the receiving modem in analog form over an analog line. The data looks exactly as it would appear if it had been sent by an analog-based modem.

digital signal—A type of signal that encodes data transmitted over a wire using a limited number of discrete values. The value of the data encoded in a digital signal depends upon the state of the signal during a particular time period. Therefore, the sender and the receiver must synchronize their clocks. Each clock runs at a baud rate, the number of times per second the state of the signal is read or set. Several clocking schemes are available, and digital signals often include clock timing cues.

A digital signal can transmit analog or digital data. For example, a CD encodes music data into digital signals, while the wires between computers transmit digital data in digital signals.

DLCI (Data Link Connection Identifier)— In a Frame Relay network, DLCIs uniquely identify each virtual circuit. In most circumstances, DLCIs have strictly local significance at each Frame Relay interface.

DOSBS—Data Over Subscriber Bearer Service. Equivalent to 3.1KHz audio bearer service.

domain identifier—The portion of a domain name that appears last and specifies the type of organization to which the host belongs. The Internet's Network Information Center (NIC) provides these domain identifiers:

Domain Identifier	Explanation
.arpa	ARPANET

Domain Identifier	Explanation
.com	Commercial enterprise
.edu	Educational institution
.gov	Governmental organization
.mil	Military organization
.org	An organization not covered by the other categories.

domain name—The portion of a symbolic name that corresponds to the network number in the IP address. In the symbolic name steve@crocker.com, the domain name is crocker.com.

Domain Name System (DNS)—A TCP/IP service that enables you to specify a symbolic name instead of an IP address. A symbolic name consists of a username and a domain name in the format *username@domain name*. The username corresponds to the host number in the IP address. The domain name corresponds to the network number in the IP address. A symbolic name might be steve@crocker.com or joanne@cal.edu. The domain identifier is the last part of the domain name, and identifies the type of organization to which the host belongs.

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

Drop-and-Insert—A feature that enables a single T1 access line to carry both data and voice traffic.

The MAX uses a pre-allocated portion of the T1 access line to use both nailed-up and switched circuits for LAN internetworking. The remaining portion of the line can go to a PBX with a T1 interface; the PBX can access both nailed-up and switched circuits for voice purposes. You can also use Drop-and-Insert to share access line bandwidth between the MAX and equipment other than a PBX, such as a channel bank or T1 multiplexer.

DS0—A 64 kbit/s unit of transmission bandwidth. A worldwide standard speed for digitizing one voice conversation, and more recently, for data transmission. Twenty-four DS0's (24x64 kbit/s) equal one DS1.

DTE (Data Terminal Equipment)—As defined in the RS-232 specification, equipment to which DCE (Data Communications Equipment) is connected, such as personal computers or data terminals. DTE often refers to application equipment, such as a videoconference terminal or LAN bridge or router, while DCE refers to equipment such as network access equipment.

dual-port call—A call in which the serial host (such as a video codec) performs inverse multiplexing on two channels so that the call can achieve twice the bandwidth of a single channel. The serial host provides two ports, one for each channel. Two serial host ports on the MAX connect a dual-port call to the serial host; these ports are the *primary port* and the *secondary port*. Because the MAX places the two calls in tandem and clears the calls in tandem, it considers them a single call.

Dynamic Bandwidth Allocation (DBA)—Adding or subtracting bandwidth from a switched connection in real time without terminating the link. MPP and AIM support Dynamic Bandwidth Allocation based upon a set of parameters you specify.

Ascend units use the historical time period specified by the Sec History parameter as the basis for calculating average line usage (ALU). It then compares ALU to the amount specified in the Target Util parameter. When ALU exceeds the threshold defined by Target Util for a period of time greater than the value of the Add Pers parameter, the Ascend unit attempts to add the number of channels specified by the Inc Ch Count parameter. When ALU falls below the threshold defined by Target Util for a period of time greater than the value of the Sub Pers parameter, the Ascend unit attempts to remove the number of channels specified by the Dec Ch Count parameter.

If you use a circuit between two locations to capacity 24 hours per day, using a nailed-up line is more cost effective than using a switched line. However, if you need the circuit only sporadically, or if the circuit is sometimes underutilized, it often makes more sense to lease a smaller amount of nailed-up bandwidth and then supplement it with additional switched bandwidth as traffic requirements dictate.

For example, you might establish some connections only when you need to transfer data, and a single circuit can accommodate low traffic levels. However, if traffic levels grow beyond the capacity of the circuit (such as during a large file transfer), DBA automatically adds additional switched channels. When traffic levels subside, DBA automatically removes the channels from the connection. The bandwidth and connection costs are thereby reduced. You pay only for bandwidth when you need it.

E1 DPNSS line *Please define.*

E1 DASS 2 line *Please define.*

E1 PRI line—An ISDN line that consists of 32 64 kbps channels. This type of line uses 30 B channels for user data, 1 64 kbps D channel for ISDN D-channel signalling, and one framing channel. The B channels can be all switched, all nailed up, or a combination of switched and nailed up. This type of PRI line is a standard in Europe and Asia called CEPT G.703.

Ethernet—A local area network that connects devices like computers, printers, and terminals. Ethernet operates over twisted-pair or coaxial cable at speeds at 10 or 100 Mbps.

Ethernet transceiver—An Ethernet device that connects workstations to standard thick or thin Ethernet-style cable. This device sends and receives information and often offers data packet collision detection.

Filter—A set of rules that define what packets may pass through a network. Filters can use destinations, sources or protocols to determine what to do with packets. One of the packet's headers must contain information that matches the information in the rules or the packet filter will discard it. See also Firewall, Secure Access Firewall, Secure Access Manager.

Firewall—A hardware/software tool that allows a network administrator to determine what type of users can access the resources on the network. The firewall provides a mechanism to monitor and funnel data from authorized users (only) through the firewall to and from the network. A firewall may be a software program that runs on a UNIX or other platforms or it may be a part of a proprietary operating system. A firewall by itself does not perform the routing function. See also Filter, Secure Access Firewall, Secure Access Manager.

fractional T1 line—A T1 line that contains both switched and nailed-up channels. T1 PRI and ISDN BRI lines can also be fractional T1 lines.

Frame Relay—A form of packet switching, but using smaller packets and less error checking than traditional forms of packet switching (such as X.25). Now a new international standard for efficiently handling high-speed, bursty data over wide area networks.

GloBanD—A European Switched Nx64 data service consisting of a single circuit whose bandwidth is a multiple of 64 kbps. This circuit consists of one or more B channels. For example, if a caller requests 512 kbps service, the line uses 8 B channels to supply the requested bandwidth. This service is available over T1 PRI lines only, and follows the CCITT Q.931 recommendation. It differs from MultiRate in being an overlay network, rather than an integral part of the worldwide switched digital infrastructure.

H0 channel—In Switched-384 data service, a circuit consisting of 6 B channels, or 384 kbps.

H11 channel—In Switched-1536 data service, a circuit consisting of 24 B channels, or 1536 kbps.

HDLC (High-level Data Link Control)—A synchronous, bit-oriented Link Layer protocol for data transmission. Frame Relay is an example of an HDLC-based packet protocol.

host—A computer on a network.

IEEE—Institute of Electrical and Electronics Engineers. An organization that maintains the standards for 10BaseT and other communications standards.

inband signalling—A type of signalling in which a line uses 8 kbps of each 64 kbps channel for WAN synchronization and signalling. The remaining 56 kbps handle the transmission of user data. Another term for inband signalling is *robbed-bit signalling*. Robbed-bit refers to the 8 kbps of each channel used for signalling. T1 access lines containing one or more switched channels, and Switched-56 lines use inband signalling.

inverse multiplexer—Equipment that performs inverse multiplexing at each end of a connection. An inverse multiplexer is also known as an *inverse mux*.

inverse mux—An inverse multiplexer.

inverse multiplexing—A method of combining individually dialed channels into a single, higher-speed data stream. Each end of the connection uses an *inverse multiplexer*, or *inverse mux*.

For example, suppose one site has three ISDN BRI lines connected to an inverse mux and another site has a T1 access line connected to an inverse mux. The user at the first site can place a 336 kbps call to the second site using inverse multiplexing. Because each BRI line has two 64 kbps channels (with 56 kbps reserved for data on each channel), the inverse mux places six individual calls over Switched-56 services to the answering T1-based inverse mux. The two inverse muxes combine the six calls into a single data stream at 336 kbps (6X56 kbps).

There are two types of inverse multiplexing: *packet-level inverse multiplexing* and *circuit-level inverse multiplexing*.

In packet-level inverse multiplexing, the inverse mux performs its function at the packet level using the MP or MPP protocol. One data packet goes over the first circuit, the next goes over the second circuit, and so on, until all the data packets are distributed over all the available circuits. The receiving end adjusts for network-induced delay and reassembles the data packets into their proper order. This inverse multiplexing technique is also referred to as *load balancing*. Telecommuting applications use packet-level inverse multiplexing.

In circuit-level inverse multiplexing, the inverse mux slices the data stream into equal portions, and transmits each portion over an available circuit. The receiving end adjusts for network-induced delay and reassembles the data packets into their proper order. The AIM and BONDING protocols define how circuit-level inverse multiplexing works. Applications that require transparent digital circuits, such as videoconferencing, nailed-up backup and overflow, and bulk file transfer applications, use circuit-level multiplexing.

IP address—An address that uniquely identifies each host on a network or internet.

An IP address has a length of 32 bits, and is divided into four 8-bit parts, each separated by a period, as in 149.122.3.30. This kind of notation is called *dotted decimal notation*. Each part can consist of a number between 1 and 255.

An IP address consists of a *network number* and a *host number*. IP addresses come in three types: Class A, Class B, and Class C. The class of an IP address determines which portion of the address belongs to the network number and which portion belongs to the host number. The first bits of the IP address identify the class.The Internet’s Network Information Center (NIC) determines the type of class assigned a network.

A Class A address starts with 0 as the class identifier, followed by 7 bits for the network number and 24 bits for the host number.Therefore, the first number in dotted decimal form is the network number; the next three numbers make up the host number. For example, in the IP address 127.120.3.8, the network number is 127 and the host number is 120.3.8. This type of address is used by the largest organizations, because this scheme allows for over 16 million different host numbers. However, it also limits network numbers to a total of 128.

A Class B address starts with binary 10 as the class identifier, followed by 14 bits for the network number and 16 bits for the host number. Therefore, the first two dotted decimal numbers comprise the network number, and the second two dotted decimal numbers comprise the host number. For example, in the IP address147.14.86.24, the network number is 147.14 and the host number is 86.24. More network numbers are available, but fewer hosts (approximately 65,000).

A Class C address starts with binary 110 as the class identifier, followed by 21 bits for the network number and 9 bits for the host number. Therefore, the first three dotted decimal numbers comprise the network number, and the last dotted decimal number comprises the host number. For example, in the IP address 225.135.38.42, the network number is 225.135.38 and the host number is 42. Many network numbers are available, but only 254 hosts per network number. The numbers 0 and 255 are reserved.

You can tell the type of class an IP address falls into by looking at the first 8-bit portion of the dotted decimal form of the address. Class A addresses begin with a number between 0 and 127. Class B addresses begin with a number between 128 and 223. Class C addresses begin with a number between 192 and 233.

In addition to an IP address, you can use a symbolic name provided by Domain Name Services (DNS) to designate an Internet address.

IP subnet—Internet Protocol Subnet. An IP subnet or subnet mask is a way to subdivide a network into smaller networks, so you can have a greater number of computers on a network with a single IP address. The IP subnet is a number that you append to the IP address. For example, 195.112.56.75/14, 195.112.56.75/15, and 195.112.56.75/16 are all IP addresses with subnets of 14, 15, and 16.

ISDN—Integrated Services Digital Network. A system that provides simultaneous voice and high-speed data transmission through a single channel to

the user's premises. ISDN is an international standard for end-to-end digital transmission of voice, data, and signaling.

ISDN BRI line—A line that uses two B channels for user data, and one 16-kbps D channel for ISDN D-channel signalling. Both B channels can be switched, both channels can be nailed up, or one channel can be switched and the other nailed up. BRI stands for *Basic Rate Interface*. A line of this type can connect to standard voice service, Switched-56 data service, or Switched-64 data service.

ISDN D-channel signalling—A type of signalling in which a D channel handles WAN synchronization and signalling, and the B channels carry the user data. Another term for ISDN D-channel signalling is *out-of-band signalling*. T1 PRI, E1 PRI, and ISDN BRI lines use ISDN D-channel signalling.

LAN—See Local Area Network.

Leased Lines—A circuit rented for exclusive use twenty-four hours a day, seven days a week from a telephone company. The connection exists between two predetermined points and cannot be switched to other locations.

line—A physical interface to the WAN.

Local Area Network— A network that interconnects devices over a geographically small area, typically in one building or a part of a building. The most popular LAN type is Ethernet, a 10 Mbps standard that works with 10BaseT, 10Base2, or 10Base5 cables. When you interconnect a single computer to the Pipeline with the crossover cable in your package, you are creating a two-node Ethernet network.

loopback—A test that enables the Ascend unit to place a call to itself over the WAN, and to send a user-specified number of packets over the connection. The loopback tests the Ascend unit's ability to initiate and receive calls, and diagnoses whether the connection over the digital access line and the WAN is sound.

Define difference between a local loopback and a remote loopback.

LQM (Line Quality Monitoring)—A feature that enables the Ascend unit to monitor the quality of a link.

LQM counts the number of packets sent across the link and periodically asks the remote end how many packets it has received. Discrepancies are evidence of packet loss and indicate link quality problems. The Ascend unit can tear down and reestablish a call if the problems on the link exceed a specified threshold.

modem (MOdulator/DEModulator)—A DCE (Data Circuit-Terminating Equipment) installed between a DTE (Data Terminal Equipment) and an analog transmission channel, such as a telephone line. A DTE refers to a device that an operator uses, such as a computer or a terminal. The DCE connects the DTE to a communications channel, such as a telephone line. A modem takes digital data from a DTE, translates (or modulates) the 1s and 0s into analog form, and sends the data over the channel. The receiving modem demodulates the analog signal into digital data and sends it to the DTE to which it is attached.

MP (Multilink PPP)—A proposed standard for inverse multiplexing, a method of combining individually dialed channels into a single, higher-speed data stream. MP is an extension of PPP that supports the ordering of data packets across multiple channels.

MPP (Multichannel Point-to-Point Protocol)—A protocol that extends the capabilities of MP to support inverse multiplexing, session management, and bandwidth management. MPP allows you to combine up to 30 individual channels into a single high-speed connection.

MPP consists of two components: a low-level channel identification, error monitoring, and error recovery mechanism, and a session management level for supporting bandwidth modifications and diagnostics. MPP enables the Ascend unit to add or remove channels from a connection as bandwidth needs change without disconnecting the link. This capability is called Dynamic Bandwidth Allocation, or DBA.

Both the dialing side and the answering side of the link must support MPP. If only one side supports MPP, the connection uses MP or standard single-channel PPP.

MPP calls cannot combine an ISDN BRI channel with a channel on a T1 access line or a T1 PRI line.

MultiRate—A data service consisting of a single circuit whose bandwidth is a multiple of 64 kbps. This circuit consists of one or more B channels. For example, a user can dial a first call at 384 kbps (using 6 B channels), and then dial at second call at 512 kbps (using 8 B channels). This service is available over T1 PRI lines only. MultiRate is also known as Switched Nx64 data service.

nailed line—A permanent connection between endpoints over which two parties exchange data. A nailed line is also known as a *private line* or a *leased line*.

NFAS (Non-Facility Associated Signalling)—A special case of ISDN signalling in which two or more T1 PRI lines use the same D channel, and you can add a backup D channel. NFAS is required for Switched-1536 data service; because all 24 channels of the T1 PRI line carry user data, the D channel must be on another line.

NT1—An ISDN BRI line terminating device at the subscriber's location that provides line maintenance access, timing, and echo cancellation. NT1s may be built into other pieces of equipment or stand alone.

Octet—Eight data bits.

packet-level inverse multiplexing—A method of inverse multiplexing in which the inverse mux performs its function at the packet level using the MP or MPP protocol. One data packet goes over the first circuit, the next goes over the second circuit, and so on, until all the data packets are distributed over all the available circuits. The receiving end adjusts for network-induced delay and reassembles the data packets into their proper order. This inverse multiplexing technique is also referred to as *load balancing*. Telecommuting applications use packet-level inverse multiplexing.

PAP—Password Authentication Protocol. A security protocol that uses password protection to allow access to a network or host.

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

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

The receiving device checks whether the sum of 1s in a character is even or odd. If the device is using even parity, the sum of 1s in a character should be even; if the device is using odd parity, the sums of bits in a character should be odd. If the

sum of the bits does not equal the parity setting, the receiving device knows that an error has occurred during the transmission of the data.

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

PBX (Private Branch Exchange)—An internal telephone network, such as those used in large offices, in which one incoming number directs calls to various extensions and from one office to another.

POST (Power-On Self Test)—A diagnostic test the Ascend unit performs when it first starts up or after a system reset. While the yellow FAULT LED on the front panel remains solidly lit, the Ascend unit checks system memory, configuration, installed modules, and the T1 connections. If the Ascend unit fails any of these tests, the AFAULT (or CON) LED remains lit or blinks.

PPP (Point-to-Point Protocol)—Provides a standard means of encapsulating data packets sent over a single-channel WAN link. It is the standard WAN encapsulation protocol for the interoperability of bridges and routers. PPP is also supported in workstations, allowing direct dial-up access from a personal computer to a corporate LAN or ISP. Using PPP ensures basic compatibility with non-Ascend devices. Both the dialing side and the answering side of the link must support PPP.

promiscuous mode—A Bridging parameter mode that determines that the Ethernet controller in the Ascend unit accepts all packets and passes them up the protocol stack for a higher-level decision on whether to route, bridge, or reject them. This mode is appropriate if you are using the Ascend unit as a bridge.

protocol—A set of rules governing message exchange over a network or internetwork. Examples of commonly used protocols are TCP/IP (Transmission Control Protocol/Internet Protocol), PPP (Point-to-Point Protocol), and IPX (Internet Packet Exchange).

RADIUS (Remote Access DIalup User Service)—A protocol by which users can have access to secure networks through a centrally managed server. RADIUS provides authentication for a variety of services, such as login, dialback, SLIP, and PPP.

In a RADIUS query, the MAX provides a user ID and password to the server. The server sends back a complete profile, which specifies routing, packet filtering, destination-specific static routes, and usage restrictions specific to the user. In

addition, the MAX can use the data in the RADIUS database to create and advertise static routes and to place outbound calls.

The communications channel between a RADIUS client and server is provided by UDP/IP, with messages acknowledged. The primary advantage in using RADIUS to authenticate incoming calls is that you can maintain all user information offline on a separate UNIX-based server. You store virtually all Connection Profile information on the RADIUS server in a flat ASCII database. This server can accept authentication requests from many machines, which makes swapping out one dial-in network server for another much easier.

Remote LAN Access—The process of allowing branch offices, telecommuters, and traveling computer users to access the corporate LAN backbone over dedicated or dialed, digital or analog lines.

remote management—A management feature that uses bandwidth between sites over the management subchannel established by the AIM (Ascend Inverse Multiplexing) protocol. Any Ascend unit can control, configure, and obtain statistical and diagnostic information about any other Ascend unit; multi-level security assures that unauthorized personnel do not have access to remote management functions.

RFC (Request For Comments)—The document series, begun in 1969, which describes the Internet suite of protocols and related experiments. Not all (in fact very few) RFCs describe Internet standards, but all Internet standards are written up as RFCs. The RFC series of documents is unusual in that the proposed protocols are forwarded by the Internet research and development community, acting on their own behalf, as opposed to the formally reviewed and standardized protocols that are promoted by organizations such as CCITT and ANSI. A complete list of RFCs can be found at http://www.internic.net/rfc/.

RS-232—A set of EIA standards specifying various electrical and mechanical characteristics for interfaces between DTE and DCE data communications devices. The standard applies to both synchronous and asynchronous binary data transmission at rates below 64 kbit/s.

Router—An interconnection device that can connect individual LANs. Unlike bridges, which logically connect at OSI layer 2, routers provide logical paths at OSI layer 3. Like bridges, remote sites can be connected using routers over dedicated or switched lines to create WANs.

Routing—A device or setup that finds the best route between any two networks, even if there are several networks to traverse. (Contrast with bridge).

S interface—*n. See* S/T interface.

S-interface—*adj. See* S/T-interface.

S/T interface—*n.* The electrical interface between a network terminator (NT1) device and one or more ISDN communications devices that do not contain their own NT1s.

S/T-interface—*adj.* Specifies an ISDN communications device that connects to an external network terminator (NT1).

Secure Access Firewalls—Secure Access Firewall is a software option for Ascend units that offers a fully integrated firewall security for remote networking. It uses state-of-the-art dynamic firewall technology to deliver a comprehensive security solution for the corporate LAN, remote office LAN and telecommuter's LAN that stops intruders from breaking and entering into networks. Securing the perimeter of the local network where it meets the Internet sets the stage for using the Internet for Intranet applications.

Secure Access Manager (SAM)—Secure Access Manager gives network administrators granular control over the security functions of the entire network directly from the central site. Through this Windows-based application, network administrators can configure the Secure Access Firewall(s) off-line and download the configuration to remote locations. The menu-driven program enables network administrators to easily configure the firewall on the network.

serial host port—The V.35, RS-499, or X.21 port on the MAX.

serial host—A device, such as a videoconferencing codec, that is connected to a serial host port communicating over a point-to-point link. *Define point-to-point link.* To a serial host, the MAX appears to be a cable or DCE (Data Communications Equipment).

serial host port module—A module on the MAX that connects to a serial host through its serial host port.

session—The state a connection reaches when both parties can communicate with each other.

signaling types—The sending device and the receiving device must send signals in order to synchronize their clocks and determine where one block of data ends and the next begins.To maintain synchronization and transfer data effectively, a line uses one of the these signaling types:

- inband signaling

- ISDN D-channel signaling

See also, inband signalling, ISDN D-channel signalling

SLIP (Serial Line IP)—A protocol that enables your computer to send and receive IP packets over a serial link.

SMDS—Switched Multimegabit Data Service. A packet-based network service allowing the creation of high-speed data networks (up to 45 Mbit/s). Now in the testing and initial implementation phases.

SNMP (Simple Network Management Protocol)—A standard way for computers to share networking information.

In SNMP, two types of communicating devices exist: *agents* and *managers*. An agent provides networking information to a manager application running on another computer. The agents and managers share a database of information, called the *Management Information Base* (*MIB*). An agent can use a message called a *traps-PDU* to send unsolicited information to the manager.

The MAX supports SNMP MIB II, T1 MIB, and Ascend Enterprise MIBs. You can therefore manage the MAX from a central SNMP manager, such as SunNet Manager™ or HP Open View™. Because the WAN interface is integrated into the MAX, you can manage it using the SNMP T1 MIB and Ascend Enterprise MIB. Most other kinds of WAN interfaces, such as channel banks, T1 muxes, and CSU/DSUs, cannot be incorporated into SNMP. The MAX can send alarms, call detail reporting, and other management information to an SNMP manager without being polled.

SNMP security is implemented using the *community name* sent with each request. Ascend supports two community names, one with read-only access, and the other with read/write access, to the MIB.

SPID—Service Profile Identifier. Your ISDN service provider (telephone company) uses this number at the Central Office switch to identify services on your ISDN line. This number is derived from a telephone number.

Straight-through cable—A cable with wires that have terminating ends with the same wire assignments.

Switched-56—A data service consisting of a single 56 kbps channel. This service is available over any type of line. It is the only service available to T1 access lines and Switched-56 lines.

Because Switched-56 was the first available data service, both the service itself and the lines that accessed it were called Switched-56. However, any type of line can now access Switched-56 data service, and there are other new services in addition to Switched-56.

Switched-56 line—A line that provides a single 56 kbps data channel with inband signalling.

Switched-64—A data service consisting of a single 64 kbps channel. This service is available over T1 PRI and ISDN BRI lines only.

Switched-384—A data service consisting of a single 384 kbps circuit, called an *H0 channel*. The H0 channel is comprised of 6 B channels. This service is available over T1 PRI lines only. Switched-384 is also known as *H0* data service.

Switched-1536—A data service consisting of a single 1536 kbps circuit, called an *H11 channel*. The H11 channel is comprised of all 24 channels on the line. You must use two T1 PRI lines to access Switched-1536. One line carries the user data, and the other line contains the D-channel. NFAS is required for this data service because the D channel must be on a separate line. This service is available over T1 PRI lines only. Switched-1536 is also known as *H11* data service.

switched circuit—A temporary connection between endpoints, established for the duration of a call, over which two parties exchange data. The circuit is disconnected when the call ends.

symbolic name—A name used in place of an IP address. A symbolic name consists of a username and a domain name in the format *username@domain name*. The username corresponds to the host number in the IP address. The domain name corresponds to the network number in the IP address. A symbolic name might be steve@crocker.com or joanne@cal.edu.

synchronization—In serial data transmission, a method of ensuring that the receiving end can recognize characters in the order in which the transmitting end sent them, and can know where one character ends and the next begins. Without synchronization, the receiving end would perceive data simply as a series of binary digits with no relation to one another.

synchronous transmission—A transmission mode in which the data moves in large blocks, called messages or frames. Both the sending device and the receiving device must maintain synchronization in order to determine where one block of data ends and the next begins. Synchronization can take one of these forms:

- Each side can transmit a separate synchronizing signal, called a clock.
- Each frame or message can contain synchronization information.

In the latter method, each block of data starts with one or more control characters, usually eight bytes long, called a SYNC. The receiver interprets the SYNC as a signal that it can start accepting data. Synchronous transmission can be up to 20 percent faster than asynchronous transmission.

T1 line—A line that consists of 24 64 kbps channels. Two types of T1 lines are available: *T1 access lines* and *T1 PRI lines*.

T1 access line—A 1.544 mbps T1 line that provides 24 56 kbps data channels and uses inband signalling. This type of line can contain all switched channels, all nailed-up channels, or a combination of switched and nailed-up channels. You can connect this type of line to standard voice or Switched-56 data services. Using a feature called *Drop-and-Insert*, the MAX can use a portion of a T1 access line for data purposes and pass the remaining portion of the line's bandwidth to a PBX for voice purposes.

T1 PRI line—A T1 line that uses 23 B channels for user data, and one 64 kbps D channel for ISDN D-channel signalling. The B channels can be all switched, all nailed up, or a combination of switched and nailed up. This type of PRI line is a standard in North America, Japan, and Korea. PRI stands for *Primary Rate Interface*. You can connect this type of line to standard voice, or Switched-56, Switched-64, Switched-384, Switched-1536, and MultiRate data services. Using a feature called *PRI-to-TI conversion*, the MAX can share the bandwidth of a T1 PRI line with a PBX.

T3 —A digital transmission link with a capacity of 45 Mbit/s, or 28 T1 lines.

TACACS (Terminal Access Concentrator Access Control Server)—A very simple query/response protocol that enables the MAX to check a user's password, and enable or prevent access. A TACACS server supports only the basic password exchanges that PAP uses; it does not support CHAP.

Tariff—Documents filed by a regulated telephone company with a state public utility commission or the Federal Communications Commission. Document details services, equipment, and pricing publicly offered by the telephone company.

TCP/IP (Transmission Control Protocol/Internet Protocol)—A family of protocols that defines the format of data packets sent across a network, and is the

communications standard for data transmission between different platforms. The TCP/IP family consists of these protocols and services:

- Transport protocols—these protocols control data transmission between computers:
  - TCP (Transmission Control Protocol)
  - UDP (User Datagram Protocol)
- Routing protocols—these protocols control addressing and packet assembly, and determine the best route for a packet to take to arrive at its destination:
  - IP (Internet Protocol)
  - ICMP (Internet Control Message Protocol)
  - RIP (Routing Information Protocol)
  - OSPF (Open Shortest Path First)
- Gateway protocols—these protocols enable networks to share routing and status information:
  - EGP (Exterior Gateway Protocol)
  - GGP (Gateway-to-Gateway Protocol)
  - IGP (Interior Gateway Protocol)
- Network address services and protocols—these services and protocols handle the way that each computer on a network is identified:
  - DNS (Domain Name System)
  - ARP (Address Resolution Protocol)
  - RARP (Reverse Address Resolution Protocol)
- User services—these services provide applications a computer can use:
  - BOOTP (Boot Protocol)
  - FTP (File Transfer Protocol)
  - Telnet
- Miscellaneous services
  - NFS (Network File System)
  - NIS (Network Information Service)
  - RPC (Remote Procedure Call)
  - SMTP (Simple Mail Transfer Protocol)
  - SNMP (Simple Network Management Protocol)

Telecommuter—A work-at-home computer user who connects to the corporate LAN backbone using remote access technologies (for example, using a modem over analog lines, ISDN Terminal Adapter (TA) or ISDN router over ISDN lines, or CSU/DSU over Switched 56 lines).

Telnet—A protocol used to link two computers in order to provide a terminal connection to the remote machine.

Instead of dialing into the computer, you connect to it over the Internet using Telnet. When you issue a Telnet session, you connect to the Telnet host and log in. The connection enables you to work with the remote machine as though you were a terminal connected to it.

If your MAX has an Ethernet card installed, you can remotely manage it by establishing a Telnet session to the remote unit from any Telnet workstation on the network and viewing the MAX interface on a Telnet VT-100 window. All Pipeline units except for the Pipeline 25 also support Telnet.

An IP host can use Telnet to emulate a terminal. When you use the MAX to initiate a terminal server session over Telnet or through the local Control/Console port, the session has a subset of the features available to a terminal server session over an asynchronous WAN link.

terminal—A computer that does not have its own processor and that must connect to a terminal server in asynchronous mode in order to use its CPU. VT100, ANSI, and TTY are all types of terminals.

terminal emulator—A program that makes your computer look like a terminal so that you can connect to a terminal server. Your computer acts like a terminal during the connection; all processing is taking place remotely. A terminal emulator is also called a *terminal emulation program*.

terminal server—A terminal server is a computing device to which a terminal can connect over a LAN or WAN link. A terminal communicates with the terminal server over an asynchronous serial port (typically an RS-232 port) through a modem. A terminal converts the data it receives from the terminal server into a display and does no further processing of the data. A terminal also converts the operator's keystrokes into data for transmission to the terminal server.

terminal server session—An end-to-end connection between a terminal and a terminal server. Usually, the terminal server session begins when the call goes on line and ends when the call disconnects.

- A terminal server session can be either local or remote:

  A *local terminal server session* takes place when a terminal (or a computer emulating a terminal) is connected to the Ascend unit's Control port, or when you open a Telnet connection to the Ascend unit from an IP host.

  In either case, you select the TermServ command from the Sys Diag menu and press Enter to begin the terminal server session. A local terminal server session has access to only a subset of the commands available to a remote terminal server session.
- A *remote terminal server session* takes place through a digital modem or through a V.110 or V.120 connection to the MAX.

  A *digital modem* is a device that can communicate over a digital line (such as a T1 PRI line) with a station using a modem connected to an analog line. When you access a terminal server through a digital modem, V.110, or V.120 connection, the remote terminal server session begins immediately; you need not enter the TermServ command.

Using an integrated digital modem, the MAX allows a user to set up a remote terminal server session at raw data rates of up to 28,8 kbps, not including data compression. The MAX supports all the common capabilities of standard terminal servers, including Telnet, Domain Name Services (DNS), login and password control, call detail reporting, and authentication services.

Thick Ethernet—A term that describes a type of Ethernet cable. Thick Ethernet, or Thicknet, is .4" diameter coaxial cable for Ethernet networks.

Thin Ethernet— A term that describes a type of Ethernet cable. Thin Ethernet, or Thinnet, is .2" diameter coaxial cable for Ethernet networks.

U interface—*n.* The electrical interface between an ISDN telephone line and a network terminator (NT1) device.

U-interface—*adj.* Specifies an ISDN communications device that connects directly to an ISDN telephone line. A U-interface device contains its own network terminator (NT1).

UTP cable—Unshielded Twisted Pair cable. Two paired wires with wire twisted two or more times per inch to help cancel out noise.

Videoconferencing—The use of digital video transmission systems to communicate between sites using video and voice. Digital video transmission systems typically consist of camera, codec (coder-decoder), network access equipment, network, and audio system.

VT-100—An ASCII character data terminal, consisting of screen and keyboard. Manufactured by Digital Equipment Corporation (DEC), the VT-100 has become an industry standard data terminal. VT-100 emulation software allows a standard PC to act as a VT-100 terminal.

WAN—See Wide Area Network.

WAN synchronization

Watchdog Spoofing—Ordinarily, when a NetWare server does not receive a reply to its watchdog session keepalive packets it sends to a client, it closes the connection. Watchdog spoofing allows Ascend units to reply to these NetWare Core Protocol (NCP) watchdog packets on behalf of clients on the other side of the bridge. In other words, the Ascend unit tricks the server watchdog process into believing that the link is still active.

Wide Area Network—A data network typically extending a LAN outside a building or beyond a campus, over IXC or LEC lines to link to other LANs at remote sites. Typically created by using *bridges* or *routers* to connect geographically separated LANs.

WINS (Windows Internet Name Service)—

Index

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

X

Y