Pipeline 7.0.0 Addendum

Ascend Communications, Inc.
Part Number: 7820-0377-002
For software version 7.0.0
November 23, 1998

Caution: You must use the software loading procedure explained in “Upgrading system software” to load this version of software onto your system. Read the instructions carefully before upgrading your system.

How to obtain technical assistance

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

Enabling Ascend to assist you

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

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

Calling Ascend from within the United States

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

Priority Technical Assistance

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

Ascend Advantage Pak

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

Other telephone numbers

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

Contacting Ascend from outside the United States

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

Telephone outside the United States	(+01) (510) 769-8027 (800) 272-3634
Australia	(+61) 3 9656 7000
Austria/Germany/Switzerland	(+33) 492 96 5672
Benelux	(+33) 492 96 5674
France	(+33) 492 96 5673
Italy	(+33) 492 96 5676
Japan	(+81) 3 5325 7397
Middle East/Africa	(+33) 492 96 5679
Scandinavia	(+33) 492 96 5677
Spain/Portugal	(+33) 492 96 5675
UK	(+33) 492 96 5671

Note: For a list of support options in the Asia Pacific Region, refer to http://apac.ascend.com

Obtaining assistance through correspondence

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

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

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

Finding information and software on the Internet

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

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

Contents

Introduction

This addendum contains new features and applies only to the Pipelines unless otherwise noted in the text.

What is in this addendum

The documentation that came with your Pipeline unit describes how to install the hardware and configure the system. However, since the documentation was published, new system software has been released that contains features that are not yet included in the product documentation. This addendum describes those new features.

Related publications

Additional information is available in the Pipeline documentation set. The Pipeline documentation set consists of the following manuals:

- *Pipeline Start Here 50/75/85* and the *Pipeline 130 Start Here*. These documents explain how to install the Pipeline and describe how to set up a basic configuration.
- *Pipeline User's Guide 50/75/85* and the *Pipeline 130 User's Guide.* These documents explain how to configure the Pipeline as a router or bridge, and how to manage the inbound and outbound traffic over the unit.
- *Pipeline Reference Guide 50/75/85* and the *Pipeline 130 Reference Guide.* These documents contain an alphabetical listing of all the parameters, fields in the status menus, and how to use the DO commands.
- *Pipeline 220 User's Guide*. This guide explains how to install, configure, and administer the unit. It also explains how to navigate the Java-based Ascend Configurator, which runs on any Windows 95 or Windows NT 4.0 computer.
- *Pipeline 220 VT100 Interface Configuration Guide*. This guide describes how to configure the Pipeline 220 using the VT100 interface.
- *Pipeline 220 VT100 Reference Guide.* This guide describes the parameters and commands for the Pipeline 220 VT100 interface.

Known Issues

When upgrading from 6.0.*x* or 6.1.*x* to 7.0.0, the current values associated with the X.25 protocol may return to their default values. Check the X.25 fields under *Ethernet > Connections > Interface Options > X.25 Prof* after performing an upgrade. Update the fields to the values you want. This can also occur if you downgrade from 7.0.0 to a 6.0.*x* or 6.1.*x* release.

The *Ans Voice Call* parameter must be set to *no* on the Pipeline 50 and 130 for Japan.

The following warning applies to Pipeline 220 users in Australia:

Warning: THIS EQUIPMENT MUST ONLY BE INSTALLED AND MAINTAINED BY SERVICE PERSONNEL.

Note: At press time, additional changes for configuring and using the AO/DI feature may be forthcoming. Please see "Finding information and software on the Internet" on page vi of this document for any updates.

Always On/Dynamic ISDN (AO/DI)

Ascend units affected: Pipeline 50, 75, and Pipeline 85 v2 only

With this release, the above Pipelines support Always On/Dynamic ISDN (AO/DI) which is described in the Internet Engineering Task Force (IETF) draft titled *Always On/Dynamic ISDN*, dated October, 1997. AO/DI enables you to send and receive data through a nailed X.25 connection over a D-channel and use circuit switched ISDN B-channels only when required on the basis of increased bandwidth utilization.

Introduction

AO/DI is a networking service that enables you to send and receive data by means of an X.25 connection over an ISDN line as well as by means of switched B-channels. Through its use of X.25 and Bandwidth Allocation Control Protocol (BACP), the Pipeline avoids dialup charges and usage of switched B-channels whenever it sends or receives data.

In a traditional ISDN environment, data moves across B-channels, and signaling information moves across the D-channel. Because signaling information uses a small percentage of available D-channel bandwidth, AO/DI was developed to maximize bandwidth usage while reducing the necessity that all data travel over B-channels. Implementation of AO/DI enables you to configure a nailed X.25 connection over a BRI line's D-channel.

Among the functions that can take advantage of AO/DI are the following:

- Transfer of email
- Reception of news broadcasts and other pushed information
- Automated collection of data

AO/DI enables you to use X.25 bandwidth up to 9600 bps. If data transfers require more bandwidth, B-channels are dialed and combined using BACP. Pipeline units support X.25 over the D-channel only. Contact your carrier for more details.

How it works

When you configure AO/DI for a connection, data flows over the X.25 connection as long as bandwidth usage is less than the value specified in the Ethernet > Connections > *any Connection profile* > Encaps options > Target Util parameter. The Pipeline dials a B-channel if the Average Line Utilization (ALU) for the connection stays above the value in Target Util for the amount of seconds specified in the Ethernet > Connections > *Any* Connection profile > Encaps Options > Add Pers parameter.

When the Pipeline uses a B-channel to transport data, it stops sending data over the X.25 D-channel connection. Because the 9600 bps bandwidth available over the X.25 D-channel connection is so small when compared to that available through the B-channel, it is not efficient to continue to transfer data over the X.25 D-channel connection simultaneously. This strategy improves through put and reduces connections costs.

When ALU for the connection drops below the value specified in the Target Util parameter for the amount of seconds specified in the Sub Pers parameter, the Pipeline disconnects the switched channel and data traffic flows over the X.25 D-channel connection.

Configuring An AO/DI connection

Configuring an AO/DI connection consists of the following steps:

- Create an X.25 profile that defines the X.25 connection.
- Configure the Answer profile to enable BACP and MP support.
- Create a Connection profile for each AO/DI connection.

Configuring the X.25 profile

To configure the Pipeline to support the X.25 connection:

1 Open Ethernet > X25 > *any X25 profile*.

2 Set Name to a descriptive name for the X.25 link.

3 Set Active to Yes.

4 Set TEI to the value specified by your X.25 carrier.
You can set TEI to any value from 0 to 63. The default value is 23. If you set TEI to 0, the Ascend unit requests a TEI assignment from the network.

5 Set Call Type to D-Channel.

6 Set Nailed Grp that AO/DI-related Connection profiles reference when using the X.25 connection.
The value specified for Nailed Grp must match the value specified in the Ethernet > Connections > *any Connection profile* > Telco options > Group parameter of any AO/DI-related profile that uses the X.25 connection.

7 Set X.25 highest SVC as directed by your carrier.

8 Set X.25 lowest SVC as directed by your carrier.

9 Set X.121 src addr. This address is calling address that the Pipeline sends when establishing the X.25 SVC connection. Contact your carrier for the correct value.

10 Set any remaining X.25 parameters as your carrier specifies.

11 Exit and save the settings.

Configuring the Answer profile

To configure the Answer profile to allow support of AO/DI:

1 From the main Edit menu, select Ethernet > Answer profile.

2 Open the PPP options submenu.

3 Set BACP = Yes.

4 Exit and save the Answer profile.

Configuring a Connection profile to support AO/DI

Before you configure a Connection profile to support AO/DI, you must understand each of the X.25 parameters related to the Connection profile.

Understanding the X.25 connection parameters

The following table provides background information about the X.25 connection parameters.

Parameter	Description
X.25 profile name	This 15-character text field specifies the name of an X.25 profile that the Pipeline uses for this logical connection. If the matching X.25 profile cannot be found, the Pipeline does not start a session for this Connection profile. To guard against this misconfiguration, an active Connection profile specifying X.25 encapsulation cannot be saved unless you define the named X.25 profile and make it active.
Rev Charge Accept	Specifies whether the X.25 facility field indicates *reverse charge request* when the X.25 user calls a host. The default is No.
RPOA	Specifies the set of Recognized Private Operating Agency (RPOA) user facilities to use in the next call request. The RPOA facilities provide the data network identification code for the requested initial RPOA transit network. You can specify up to 4 digits. The default is null.
CUG Index	Specifies the Closed User Group (CUG) index/selection facility to use in the next call request. The closed user group selection/ index facility specifies to the called switch the closed user group selected for a virtual call. You can specify up to two digits. The default is null.
NUI	Specifies the set of Network User Identification (NUI) related facilities to use in next call request. NUI provides information to the network for billing, security, network management purposes, and for activating subscribed facilities. You can specify the NUI to use in the next call request. You can specify up to six digits. The default is null.

Parameter	Description
Call mode	Specifies whether the Pipeline can initiate, receive a call request on the connection. • Incoming—Specifies that the Pipeline does not issue a call request when data arrives for forwarding. If there is no virtual circuit established, the Pipeline drops the IP packet. If a host receives an incoming call from a host whose called address matches the value specified in Answer X.121 addr or if Answer X.121 addr is blank, the Pipeline accepts the call. • Outgoing—Specifies that the Pipeline automatically issues a call request to the number specified in the Remote X.121 addr parameter when data needs to be forwarded across the link. If the Pipeline receives an incoming call request, the Pipeline rejects the call. • Both—Specifies that the Pipeline accepts both incoming and outgoing call requests. For incoming calls, if a host receives an incoming call from a host whose called address matches the value specified in Answer X.121 addr or if Answer X.121 addr is blank, the Pipeline accepts the call. For outgoing calls, the Pipeline does not establish a virtual circuit until data needs to be forwarded across the link.
Answer X.121 Addr	Matches the value specified in the X.121 src addr parameter of the X.25 profile on the Pipeline. You should not leave Answer X.121 address blank if Call Mode specifies either Both or Incoming. You can substitute the beginning portion of the address with the wildcard * which indicates that the Pipeline should accept any value, requiring a match only on the trailing digits that you specify after the wildcard character.
Remote X.121 Addr	Specifies the value specified in the X.121 source address of the remote X.25 host to which the profile connects. You should not leave Remote X.121 addr blank if you set Call Mode to Both or Outgoing. If you configure a value for Remote X.121 address, the Pipeline attempts to match the incoming call to Remote X.121 address as well as Answer X.121 address. You can substitute the beginning portion of the address with the wildcard * which indicates that the Pipeline should accept any value, requiring a match only on the trailing digits that you specify after the wildcard character. For outgoing calls, the Pipeline dials only the trailing digits specified, ignoring the beginning wildcard character.

Configuring a Connection profile

To configure a Connection profile to support AO/DI:

1 From the main Edit menu select Ethernet > Connections > *any Connection profile*.

2 Set Active to Yes.

3 Set Encaps to MP.

4 Set Dial # to the phone number that the Pipeline dials when additional bandwidth from a B-channel is needed.

5 Open the Telco options submenu

6 Set Call Type to AO/DI.

7 Set Group to the group number that you specified in the Ethernet > X25 > X25 profile > Nailed Grp parameter.

8 From the Connection profile menu, open the Encaps options submenu.

9 Set BACP to Yes.

10 Set Interface Type to X.25.

11 From the Connection profile main menu, open the Interface options submenu.

12 Specify the Recv PW used to authenticate the caller.

13 Set X.25 Prof to the name of the X.25 profile that the Pipeline uses for the connection.

14 Specify the parameters used for the X.25 connection.

The Pipeline attempts to bring up the link only if you set the Call Mode parameter to Outgoing, or Both (when there is data to be forwarded).

If you set Call Mode to Incoming or Both, proceed as follows:

1 From the Connection profile menu, open the Interface options submenu.

2 Set Answer X.121 addr to the value specified in the X.121 src addr parameter of the X.25 profile on the Pipeline.

If you set Call Mode to Outgoing or Both, proceed as follows:

1 From the Connection profile menu, open the Interface options submenu.

2 Set Remote X.121 addr to the value specified in the X.121 source address of the remote X.25 host to which the profile connects. You should not leave Remote X.121 addr blank if you set Call Mode to Both or Outgoing. Also, for incoming calls, the Pipeline attempts to match the calling number of the incoming call to Remote X.121 address (if specified) and the called number of the incoming call to Answer X.121 address (if specified).

Exit and save the Connection profile.

When you enable the Connection profile, the Pipeline attempts to bring up an X.25 virtual call connection over the D-channel. When the session and profile are active, the Connection profile displays an asterisk to the left of the profile name on the Ethernet > Connections submenu which indicates that a call is up or is available for a call.

Note: When you modify *any* AO/DI-related X.25 profile or Connection profile, you must disable all AO/DI-related profiles and re-enable them.

Displaying AO/DI operation

To make sure AO/DI is installed and configured properly, you can display one status window to indicate whether or not the Pipeline supports AO/DI, and another to observe active AO/DI calls.

Displaying whether or not the Pipeline supports AO/DI

The Sys Option window provides a read-only list that identifies the Pipeline and names each of the features (including AO/DI) with which it has been equipped. Press the tab key to highlight any status window, then use the left and right arrow keys to display the Sys Option window.

When the Pipeline displays the Sys Option window, press the down arrow key until the AO/DI feature appears. For example, the following screen indicates that the Pipeline supports AO/DI:

```
00 - 100 Sys Option ??
Dyn Bnd Not Inst
ISDN Sig Installed
AO/DI Installed
```

If you ordered AO/DI but the Pipeline displays `AO/DI Not Inst`, contact your authorized Ascend reseller.

Displaying active AO/DI calls

The Dyn Stat window displays the name, quality, bandwidth, and bandwidth utilization of each online connection. For example, when the Pipeline establishes an AO/DI connection for MBRUNCAT, the following text appears:

```
MBRUNCAT
Qual Good 05:07:00
9k      1 channels
CLU   0%  ALU   0%
```

When the Pipeline adds a B-channel on the basis of bandwidth utilization, the following text appears:

```
MBRUNCAT
Qual Good 05:07:00
56k     2 channels
CLU  50%  ALU  34%
```

Although the connection contains two active channels, data passes only over the B-channel as described in “How it works” on page 2 of this document.

When the Pipeline adds a second B-channel on the basis of bandwidth utilization, the following text appears:

```
MBRUNCAT
Qual Good 05:07:00
112k    3 channels
CLU  88%  ALU  64%
```

The 112k indicates that data flows through the two B-channels only.

New Field Options and Parameters

Following is a breakdown of new field options and parameters relating to AO/DI and their path location:

- Ethernet > Connections > Telco Options ***AO/DI***
- Ethernet > Connections ><profile name> > Encaps Options > Interface Type ***X.25***
  The above option must be selected in order to display the *Interface Options* parameters (see next item) will not display.

Ethernet > Connections > Interface Options - see “Understanding the X.25 connection parameters” on page 4 for parameter descripitions.

Enhanced ringer frequency support

Ascend units affected: newer Pipeline 75 and 85 units only (v2P75)

The Pipeline now supports a greater range of ringer frequencies. Ringer frequency controls the timing and interval of rings sent to an analog devices attached to the Pipeline phone ports.

Ringer frequency specifications

Ringer frequency is set internally, on the basis of the destination country. This internal configuration is performed during manufacturing and cannot be changed by the consumer. The following table lists the ringer frequency supported for each country.

Country	Ringer frequency
Australia	35 Hz
Austria	35 Hz
Belgium	25 Hz
France	25 Hz
Germany	35 Hz
Italy	35 Hz
Japan	20 Hz
Singapore	25 Hz
Switzerland	35 Hz
U.K.	25 Hz
US	20 Hz

Reverse Tunnel Network Address Translation

Ascend units affected: Pipeline 50, Pipeline 75, Pipeline 130, Pipeline 220

Reverse Tunnel Network Address Translation (RT NAT)

RT NAT is a feature that enables proxy Network Address Translation (NAT) functionality for the remote end of a tunnel in that it performes NAT on the far side address of traffic flowing through the tunnel. This feature allows the remote user to essentially be treated as a part of the local network. As part of the local network, the remote user has the same basic access privileges as any other member of the local network.

Configuring Reverse Tunnel NAT

Configuring Reverse Tunnel NAT consists of using the SecureConnect Manager to configure a reverse tunnel for the firewall and install it on the Pipeline. See the *SecureConnect Manager User's Guide* for more information. The user guide is a PDF file on CD-ROM or diskette, whichever was shipped with your unit and can be read by Adobe Acrobat.

SecureConnect

Ascend units affected: Pipelines 50, 75, 85, 130, and 220

SecureConnect features are now integrated into the Pipeline family of products. The SecureConnect features for the Pipelines include SecureConnect firewall and IPSec encryption. IPSec is the standard protocol for creating encrypted Virtual Private Network tunnels.

The interface for creating Pipeline SecureConnect firewalls and VPN tunnels is SecureConnect Manager. The SecureConnect Firewall feature and the SecureConnect Manager interface replace Secure Access Firewall and Secure Access Manager, respectively. The SecureAccess feature and inteface did not support encrypted Virtual Private Network tunnels.

Note: PCs running the IntragyAccess SecureConnect Client application also support SecureConnect Firewall and IPSec encryption.

SecureConnect specifications

SecureConnect Firewall is a security feature of the True Access™ Operating System (TAOS) on most Ascend Pipeline routers. It provides dynamic security that monitors and controls incoming and outgoing Internet Protocol (IP) traffic. SecureConnect firewalls can include Virtual Private Network (VPN) tunnel configurations, which permit users to securely transmit and receive authenticated and encrypted data. Encryption and authentication provided by SecureConnect VPN tunnels are based on the Internet Protocol Security (IPSec) protocol.

Ascend Pipeline routers that support the SecureConnect Firewall feature include the Pipeline 50, 75, 85, 130 and 220 models. The SCF feature is enabled on these Pipeline routers when they are shipped. You do not have to enter a feature code to enable the feature before you install firewalls on Pipeline routers.

Pipline 50, 75, 85, 130 and 220 models shipped to countries that are not subject to United States Commerce Department restrictions support DES encryption with 40-bit keys. To create firewalls that use DES encryption with 56-bit keys, or 3DES encryption, you must obtain the SecureConnect Firewall software upgrade. United States and Canadian customers, banks, and subsidiaries of United States companies located in countries outside the United States and Canada can order the SecureConnect software upgrade. No encryption software can be exported to Cuba, Iran, Iraq, Libya, or North Korea.

Caution: If your Pipeline supports SecureConnect Firewall and IPSec, do not execute your unit's fclear command unless you make note of your IPSec feature code. Your router's SecureConnect Firewall and IPSec encryption features are turned on when you receive the unit. The fclear command erases the code that activates the SCF and IPSec features. If you want to copy the code that activates the features, it is in your router's System > Feature Codes > IPSec menu.

IPSec

Ascend's implementation of tunneling in SecureConnect Firewalls is based on IPSec, a protocol developed by the Internet Engineering Task Force (IETF). IPSec is the creation of an IETF work group, whose goal is to develop a network-layer protocol that uses cryptography to provide four basic security elements for IP packets transmitted and received over the Internet. In addition, IPSec can also provide replay protection and non repudiation.

Note: Ascend's implementation of IPSec for SecureConnect firewalls complies with the best practices of the IETF IPSec Working Group's IPSec protocol. Because some of the underlying elements of the protocol's architecture, such as the Encapsulating Security Payload, are in review, Ascend's implementation of IPSec might change.

The goal of the IPSec protocol is to provide the following types of security for traffic transmitted over a public network such as the Internet:

- Authentication, which proves that the received data is the same as the transmitted data and that the avowed sender is the actual sender.
- Confidentiality, which prevents someone other than the intended receiver from deciphering the transmitted data.
- Integrity, which proves that the received data has not been altered during transmission.
- Non repudiation, which proves that the sender did transmit the data even if he or she denies doing so.

SecureConnect Manager

You can install SecureConnect Manager (SCM) software on a PC running the Windows 95 or Windows NT operating system. SCM's shell enables you to call up screens with which you can create the components that you can include in a SecureConnect firewall: the Main firewall, a firewall section, a tunnel configuration, and a tunnel ruleset.

The *SecureConnect Manager User's Guide* is a PDF file which can be read by Adobe Acrobat. For more information about SecureConnect Firewall and IPSec encryption for Virtual Private Network tunnels, consult the *SecureConnect Manager User's Guide*. The user guide is on CD-ROM or diskettes, whichever was shipped with your unit.

IntragyAccess SecureConnect Client

SecureConnect Client (SCC) is a feature of IntragyAccess that enables you to install SecureConnect firewalls on a PC. Firewalls installed with SCC control the traffic that enters and leaves all of the PC's remote access interfaces.

IntragyAccess is cross-platform desktop client software that provides integrated support for flexible desktop communications.

Upgrading system software

This section explains how to upgrade your system software. It contains the following sections:

- Guidelines for upgrading system software
- Upgrading system software with a standard load
- Upgrading system software with an fat load
- Recovering from a failed fat load upgrade

Which binary to use

For any new Pipeline 50, 75, or 85 (no switch on back panel), use b2a.p75. For older models, see the README information on the Ascend FTP server where the binaries are stored. For most older Pipeline 75 models, use b.p75. Similarly, for older Pipeline 50 models, use b.p50, however, note that there are several models.

To see the name of the last binary loaded , look in the Sys Options status window. From the VT100 window tab to the Sys Options window and use the down arrow to see the software load. For example:

```
00-100 Sys Option
>Access Router          ^
 Load: b2.p75
 Switched Installed     v
```

Guidelines for upgrading system software

The following table lists the different formats for Ascend system software. How you upgrade your unit depends on the version of software you are upgrading to.

Format of load	Size
Standard (thin)	Less than 448 Kb.
Fat	Compressed size larger than 448 Kb
Extended	Compressed size larger than 448 Kb

These restrictions apply when upgrading:

- You must use TFTP to upload a fat or extended load.

  Note: To use Trivial File Transfer Protocol (TFTP) you need a TFTP server on your computer (host) or accessible over the Ethernet. You can obtain a TFTP server from software download sites on the Internet. Additionally, you need a Pipeline model 50 or higher. The Pipeline 25 models do not support TFTP.

- **If you use TFTP, you must execute the `fsave` command immediately after executing the `tload` command. Failure to do so might cause your Pipeline to lose its configuration.**

- Before you can upgrade to a fat or extended load, you must first upgrade to a version of software that understands the new format, then upgrade to the fat or extended load. You can upgrade directly to a thin load (which is fat-load aware) or an extended-aware load from any version of software.

Before you begin

Caution: Uploading system software via the serial console overwrites all existing profiles. Save your current Pipeline configuration before you begin. After upgrading the system software, restore the configuration. Since the saved configuration is readable text, you can manually reenter the settings, if necessary. For more information, see how to save a configuration in your Pipeline documentation. Using TFTP will preserve your configuration.

Before upgrading your system software:

1 Obtain the appropriate load file, either by downloading it from the FTP server or by contacting Ascend technical support.

Caution: Be sure your unit can handle the binary, for example, an older Pipeline (with a switch on the back) cannot use a binary for a version 2 Pipeline (such as b2.p75). If you "upgrade" to a version of software not supported by your unit, the unit will no longer function and you will need to return it to Ascend for repair.

To see the name of the last binary loaded , look in the Sys Options status window. From the VT100 window tab to the Sys Options window and use the down arrow to see the software load. For example:

```
00-100 Sys Option
>Access Router          ^
 Load: b2.p75
 Switched Installed     v
```

2 Save the current configuration.

Note: For security reasons, passwords are not included in the saved configuration text file. When you restore the configuration, the default (factory-set) passwords are reinstated. See the section on Security Profiles in your documentation for more information.

3 If necessary, activate a Security Profile that allows for field upgrade.

If you are not sure how, see the section on Security Profiles in your documentation.

4 If you are using TFTP, load the correct binaries into the /home directory on the TFTP server (/tftpboot on most Unix systems).

Upgrading system software with a standard load

You can upgrade system software with a standard load using either the serial console or using TFTP over the Ethernet.

Upgrading using the serial console

1. From the VT100 interface, access the diagnostics monitor by typing these characters in rapid succession:

   Press Ctrl-D to invoke the DO menu and select D=Diagnostics.

2. Enter `fsave` to save your current configuration to flash memory.
3. Enter `quit` to exit the Diagnostic interface.
4. 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 -

   (Press the escape key, the left bracket key, the escape key, and the minus key, in that order, in rapid succession.) The following string of Xmodem control characters appear:

   CKCKCKCK

   If you do not see these characters, you probably did not press the four-key sequence quickly enough. Try again—most people use both hands and keep one finger on the escape key.

5. Use the Xmodem file transfer protocol to send the system file to the Pipeline.
6. Your communications program begins sending the file to your Ascend unit. This normally takes anywhere from 5 to 15 minutes. The time displayed on the screen does not represent real time. Do not worry if your communication program displays several “bad batch” messages. This is normal.
7. When the upgrade process completes, the Pipeline resets. When the self-test completes, the unit’s initial menu appears in the Edit window with all parameters set to default values.
8. From the VT100 interface, access the diagnostics monitor by typing these characters in rapid succession:

   Press Ctrl-D to invoke the DO menu and select D=Diagnostics.

9. Type `nvramclear` to clear any differences in NVRAM memory before and after the upgrade. After the Ascend unit clears NVRAM memory, it automatically resets.
10. The unit resets a second time to load the configuration from flash memory.

This completes the upgrade.

Note: You can also restore your configuration from the text file saved on your hard disk. If you are not sure how to restore a configuration, see the section on restoring a configuration in the documentation.

Upgrading standard load using TFTP

1. Obtain the correct binary from ftp.ascend.com/pub/Software-Releases/Pipeline. Place the binary in a TFTP boot directory accessible via the Ethernet. Be sure the TFTP server is running. Be sure you know the IP address or host name of the server.
2. From the Pipeline VT100 interface, press Ctrl-D to invoke the DO menu and select D=Diagnostics.
3. At the > prompt, type:

   `tload` *hostname filename*

   where *hostname* is the name or IP address of your TFTP server (which is your computer or a server on your LAN that has a TFTP server program running), and *filename* is the name of the binary that you placed in your TFTP server’s boot directory.

For example:

```
tload hummer b.p75
or
tload 198.168.100.169 b.p75
```

loads b.p75 into the Pipeline from a host named *hummer*, or loads b.p75 into the Pipeline from a host with an IP address of 198.168.100.169.

4. Enter the following command to save your configuration to flash memory:

```
fsave
```

5. Enter the following command to clear any differences in NVRAM memory before and after the upgrade.

```
nvramclear
```

After executing this command, the Pipeline will be inaccessible while it clears NVRAM and resets. Please wait for the unit to reset before attempting to use it.

This completes the upgrade.

Upgrading system software to a fat or extended load

1. If you want to upgrade your system to a fat or extended load, and your unit currently is using a standard (thin) load, you must first upgrade your system to a standard (thin) load version that understands the new format. Start with the upgraded thin load and then upgrade an extend load.
2. Obtain the correct binary from ftp.ascend.com/pub/Software-Releases/Pipeline. Place the binary in a TFTP boot directory accessible via the Ethernet. Be sure the TFTP server is running. Be sure you know the IP address or host name of the server.
3. From the Pipeline VT100 interface, press Ctrl-D to invoke the DO menu and select D=Diagnostics.
4. At the > prompt, type:

```
tload  hostname filename
```

where *hostname* is the name or IP address of your TFTP server (which is your computer or a server on your LAN that has a TFTP server program running), and *filename* is the name of the binary that you placed in your TFTP server's boot directory.

For example:

```
tload hummer b.p75
or
tload 198.168.100.169 b.p75
```

loads b.p75 into the Pipeline from a host named *hummer*, or loads b.p75 into the Pipeline from a host with an IP address of 198.168.100.169.

5. Enter the following command to save your configuration to flash memory:

```
fsave
```

6. Enter the following command to clear any differences in NVRAM memory before and after the upgrade.

```
nvramclear
```

After executing this command, the Pipeline will be inaccessible while it clears NVRAM and resets. Please wait for the unit to reset before attempting to use it.

7. Repeat the procedure, this time uploading the fat or extended load. Be sure your system is backed up before you begin so you can revert to a saved configuration, if necessary.

After a successful upgrade, one of the following messages appears.

- If the load is thin:

```
UART initialized
thin load: inflate
.....................................................
starting system...
```

- If the load is fat:

```
UART initialized
fat load: inflate
.....................................................
starting system...
```

- If the load is extended:

```
UART initialized
extended load: inflate
.....................................................
starting system...
```

This completes the update load if you have no errors. If the upgrade is not successful, refer to "Recovering from a failed upgrade" next.

Recovering from a failed upgrade

If a load has an "incompatible format" message, you must first download a thin or extended-aware load that can understand the new format.

If a load has a CRC error, the following message appears:

```
UART initialized
fat load: bad CRC!!
forcing serial download at 57600 bps
please download a "thin" system...
```

Immediately after this message appears, the serial console speed is switched to 57600 bps, and the Pipeline initiates an Xmodem serial download. To recover from this error and load the new system, you must load a thin system that is fat load aware, or a extended-aware system:

1 Invoke your Xmodem software to load the thin load through the console port.

2 After you have finished loading the prerequisite load, reboot the unit.

3 Download the new load using the tloadcode command.

When you download an extended load, messages similar to the following appear on the diagnostics monitor screen:

```
> tload 192.168.1.82 b.p50
saving config to flash
.....................................
loading code from 192.168.1.82:69
file b.p50..
fat load part 1:
.............................................................
fat load part 2:
.............................................
```

Note the "fat load part *x*:" messages. They notify you when the first and second halves of the load are being loaded