DSLPipe User’s Guide

Ascend Communications

Ascend is a registered trademark, and DSLPipe, MAX, MAX TNT, MultiDSL, and Secure Access Firewall are trademarks of Ascend Communications, Inc. Other trademarks and trade names in this publication belong to their respective owners.

Copyright © 1997 Ascend Communications, Inc. All Rights Reserved.

This document contains information that is the property of Ascend Communications, Inc. This document may not be copied, reproduced, reduced to any electronic medium or machine readable form, or otherwise duplicated, and the information herein may not be used, disseminated or otherwise disclosed, except with the prior written consent of Ascend Communications, Inc.

Part Number 7820-0518-001 June 3, 1997

Contents

Introducing the DSLPipe

1

Overview of DSL

Digital Subscriber Line (DSL) is dedicated, digital service between your DSLPipe and DSL equipment at the phone company. When your DSLPipe connects to the DSL signal, the line stays up continuously and is not shared by any other subscriber.

You can utilize an existing phone line to connect your DSLPipe to the central office of the phone company. (In telephone company parlance this is referred to as the local loop.) One end of a single, unshielded twisted-copper pair is connected to DSL equipment at the phone company (referred to as Central Office Equipment, or COE), and the other end is connected to your DSLPipe (referred to as Customer Premises equipment, or CPE).

Depending on the type of DSL service you subscribe to, SDSL or ADSL (described below), you can achieve data transmission rates between 128 Kbps and 7 Mbps. (In this first release, the maximum rate is 2.56 Mbps.)

How is that possible on ordinary phone lines? DSL signals use a higher frequency to transmit data—voice transmissions use between 300 and 3,400 Hz, and DSL uses up to 1.2 MHz. (Hz stands for Hertz, which is one cycle per second. MHz refers to millions of cycles per second.)

Your DSLPipe and the DSL equipment at the phone company are designed to handle these frequencies—ordinary phone equipment is not, and that is why the equipment at both ends of the service must work together. In fact, when you subscribe to DSL, your data is not carried on the public telephone network until after it leaves the central office and enters the packet-switched telephone network. It does not consume the resources of the local phone network. The

connection between your DSLPipe and the DSL equipment (such as an Ascend MAX TNT) at the CO are independent of the phone company's normal phone service.

The distance between your premises and the phone company's central office is an important factor when planning for DSL service. The maximum distance a DSL line can function is 17,000 feet. The speed of the data transmission decreases as the length of the line increases. Optimum rates are achieved when the length of the line is 10,000 feet or less, which is generally available in metropolitan areas.

Types of DSL service supported

There are two general types of DSL service supported by the DSLPipe family of products:

- Symmetric Digital Subscriber Line (SDSL)
- Asymmetric Digital Subscriber Line (ADSL). ADSL comes with Rate Adaption and Carrier-less Amplitude and Phase Modulation, and is referred to as RADSL-CAP.

The terms symmetric and asymmetric correspond to the rate of incoming and outgoing data. In SDSL both incoming and outgoing data rates are the same (symmetric). In RADSL-CAP, downstream data (data to the DSLPipe) is faster than upstream data (data from the DSLPipe), so it is called an asymmetric digital subscriber line. The data rates achievable by the different types of DSL service are shown in the table below:

Table 1-1. DSL services and statistics

DSL service	Upstream	Downstream	Voice	Maximum length
SDSL	768 Kbps	768 Kbps	No	12,000 feet
RADSL-CAP	1.0 Mbps 544 Kbps	7 Mbps 640 Kbps	To be supported with splitter	10,000 feet 17,000 feet

DSL facilities are built into the hardware

There are three DSLPipe models, each one supporting a different type of DSL service. You cannot change the type of service by downloading different software, as the capabilities are built into the hardware. The type of model is listed on the bottom of the unit. The models and service types supported are:

- DSLPipe-S supports SDSL.
- DSLPipe-C supports RADSL-CAP.
- DSLPipe-D supports RADSL-DMT.

RADSL uses either Carrierless Amplitude Phase (CAP) modulation or Discrete Multi-Tone (DMT) modulation. CAP and DMT are two different line encoding techniques. The difference is in how data transmission rates are optimized. Currently only CAP is available on the DSLPipe-C. (DMT is expected to be supported in a future release.)

How rate adaption works with RADSL-CAP

Rate adaption is available only with RADSL-CAP (not with SDSL). Very simply, rate adaption lets the DSL signal continue to transmit data even if noise is blocking some frequencies. The DSL bandwidth is periodically monitored with test packets. Frequencies influenced by noise show errors in return packets (or don't get any return packets). Frequencies with high error counts or those that cannot return packets are bypassed until test results show they are clear.

Single, unshielded twisted-copper cable is subject to noise from external sources and nearby cables. Without rate adaption, DSL equipment cannot adjust to noise on the line and is forced to drop the signal entirely. With rate adaption, impaired frequencies are bypassed, and the transmission continues, and recovers as soon as the line is clear.

Voice integration

By using a device to split the line, you can integrate analog voice and data over the same wire with RADSL service. (This is not an option with SDSL.) The splitter must be used at both ends of the line—the end at your premises and the end at the central office. Splitters only work in pairs. At your end the splitter

divides the line and provides an analog jack; at the central office, the splitter divides the line and connects to the public-switched telephone network (PSTN), enabling phone service.

Transport protocols supported

DSL technology is based on the physical layer (that is, layer 1 of the OSI model). It can use any of the available transport protocols, including Point-to-Point Protocol (PPP) and Frame Relay (FR).

Applications

You can use your DSLPipe for Internet access, telecommuting, remote office connectivity, multimedia, and video conferencing. All of these applications can be efficiently served with the data transmission rates supplied by DSL.

Additionally, you can add Secure Access Firewall to a DSLPipe unit by obtaining a hash code to enable the software. (Contact the Technical Assistance Center for more information.)

How to get started

After reading the important safety information below, install your DSLPipe and configure the on-board software according to the instructions in the chapters on installation and configuration. Sample configurations are included to guide you through the setup.

Remember that the DSLPipe at the customer side is only half the required equipment in a digital subscriber loop—the equipment at the central office must be installed, configured, and linked to the same line you are using in order for your unit to connect to a signal.

Other options

The chapter on wide area networking describes how to connect using PPP and Frame Relay and the associated options. The DSLPipe can bridge and route networking traffic. The chapters on bridging and routing describe a number of options, including how to set up IP and IPX routing, and how to bridge AppleTalk packets.

At any time you can design filters to limit the flow of data in and out of your network. You can secure the settings in the DSLPipe, administer the unit locally or by remote access, and upgrade the on-board software. These topics are each described in a subsequent chapter.

You can find hardware specifications for your DSLPipe, information about how the equipment at the central office is set up, and product warranty information in the appendixes.

Important safety instructions

The following safety instructions apply to the DSLPipe:

1 Read and follow all warning notices and instructions.

2 The maximum recommended ambient temperature for DSLPipe models is 104˚ Fahrenheit (40˚ Celsius). Care should be given to allow sufficient air circulation or space between units when the DSLPipe is installed in a closed

or multi-unit rack assembly, because the operating ambient temperature of the rack environment might be greater than room temperature.

3 Installation in a rack without sufficient air flow can be unsafe.

4 Racks should safely support the combined weight of all equipment.

5 The connections and equipment that supply power to the DSLPipe should be capable of operating safely with the maximum power requirements of the DSLPipe. In the event of a power overload, the supply circuits and supply wiring should not become hazardous. The input rating of the DSLPipe is printed on its nameplate.

6 Models with AC power inputs are intended to be used with a three-wire grounding type plug—a plug which has a grounding pin. This is a safety feature. Equipment grounding is vital to ensure safe operation. Do not defeat the purpose of the grounding type plug by modifying the plug or using an adapter.

7 Before installation, use an outlet tester or a voltmeter to check the AC receptacle for the presence of earth ground. If the receptacle is not properly grounded, the installation must not continue until a qualified electrician has corrected the problem. Similarly, in the case of DC input power, check the DC ground(s).

8 If a three-wire grounding type power source is not available, consult a qualified electrician to determine another method of grounding the equipment.

9 Models with DC power inputs must be connected to an earth ground through the terminal block Earth/Chassis Ground connectors. This is a safety feature. Equipment grounding is vital to ensure safe operation.

- Before installing wires to the DC power terminal block, verify that the wires are not connected to any power source. Installing live wires (that is, wires connected to a power source) is hazardous.
- Connect the equipment to an 18 VDC supply source that is electrically isolated from the AC source. The 18 VDC source should be reliably connected to earth ground.

10 Installation in restricted access areas must comply with Articles 110-16, 110-17, and 110-18 of the National Electrical Code, ANSI/NFPA 70.

11 Do not allow anything to rest on the power cord, and do not locate the product where anyone will walk on the power cord.

12 Do not attempt to service the product yourself. Opening or removing covers can expose you to dangerous high voltage points or other risks. Refer all servicing to qualified service personnel.

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

14 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 the appropriate regulatory agencies and inspection authorities to ensure compliance.

15 A rare phenomenon can create a voltage potential between the earth grounds of two or more buildings. If products installed in separate buildings are **interconnected**, the voltage potential can cause a hazardous condition. Consult a qualified electrical consultant to determine whether or not this phenomenon exists and, if necessary, implement corrective action before interconnecting the products.

If the equipment is to be used with telecommunications circuits, take the following precautions:

- 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.

Contacting the Technical Assistance Center

Table 1-2. How to get help

Ways to get support	Telephone number or address
Telephone in the United States	800-ASCEND-4 (800-272-3634)
Telephone outside the United States	510-814-2333
E-mail	support@ascend.com
Facsimile (fax)	510-814-2312

Be sure you have the following information when calling for assistance:

- Product name and model
- Software version
- Whether you are routing or bridging
- Type of computer you are using
- Description of the problem

Obtaining new features and product updates

You can find out about new features and product improvements, and obtain the latest software releases on the Ascend product line at our web site at http://www.ascend.com. For software upgrades, release notes, and addenda to this manual, log onto the Ascend FTP site at ftp.ascend.com.

Documentation conventions

Table 1-3. Documentation conventions

Convention	Meaning
Monospace text	Represents text that appears on your computer's screen, or that could appear on your computer's screen.
`Boldface mono-space text`	Represents characters that you enter exactly as shown (unless the characters are also in ***`italics`***—see *Italics*, below). If you could enter the characters, but are not specifically instructed to, they do not appear in boldface.
Italics	Represent variable information. Do not enter the words themselves in the command. Enter the information they represent. In ordinary text, italics are used for titles of publications, for some terms that would otherwise be in quotation marks, and to show emphasis.
[ ]	Square brackets indicate an optional argument you might add to a command. To include such an argument, type only the information inside the brackets. Do not type the brackets unless they appear in bold type.
>	Points to the next level in the path to a parameter. The parameter that follows the angle bracket is one of the options that appears when you select the parameter that precedes the angle bracket.
Press Enter	Means press the Enter, or Return, key or its equivalent on your computer.
Note:	Introduces important additional information.
 **Caution:**	Warns that a failure to follow the recommended procedure could result in loss of data or damage to equipment.
 **Warning:**	Warns that a failure to take appropriate safety precautions could result in physical injury.

Installing the DSLPipe

2

Box Contents

Be sure you have each of the items listed below. If you are missing any item, please contact the Technical Assistance Center.

- DSLPipe unit. Each unit supports only one type of service, as listed below:
  - DSLPipe-S supports SDSL. This type of unit is set up as Customer Premises Equipment (CPE) at the factory. To convert it to Central Office Equipment (COE), see "How to convert a DSLPipe-S to a COE unit" on page B-1.
  - DSLPipe-C supports Rate Adaptive ADSL with Carrier-less Amplitude and Phase Modulation (RADSL-CAP). DSLPipe-C units are manufactured as either CPE or COE units. They cannot be converted.
- A 10Base-T Ethernet crossover cable.

  The ends of this cable are yellow. If you are using the DSLPipe with only one computer and the computer has a 10Base-T Ethernet interface, you can use this cable to connect the computer directly to the 10Base-T Ethernet jack on the DSLPipe.
- A DB-9–to–DB-25 serial cable. Use this cable to connect the Terminal port on the DSLPipe to a serial port on a computer.
- A power supply.
- Two manuals: this one and the *Reference Guide*.
- A registration card.

Installation steps

Installation consists of these general steps:

- Attach the cables to the DSLPipe
- Launch VT-100 terminal-emulation software so you can access the configuration screens
- Power-on the DSLPipe
- Configure the DSLPipe

Figure 2-1. DSLPipe-C backpanel.

The backpanel contains the following ports:

- PWR. Connect the power cable here.
- Terminal. Connect a serial cable from this port to the serial port of a PC to access the configuration interface.
- 10 BT. Connect the 10Base-T Ethernet cable from here to your computer's Ethernet adapter.
- Splitter (DSLPipe-C only). Currently not supported.
- WAN. This connects your DSLPipe to the wide area network. Connect your DSL telephone line here.

Starting the DSLPipe

Warning: You **must** perform the following steps **in the order listed.** Plugging the power supply into the wall socket before plugging the power cable into the DSLPipe can create sparks, cause an electrical fire, or destroy the DSLPipe.

1 Plug the power cord into the Power jack on the back of the DSLPipe.

2 Insert the Power supply plug into an electrical outlet.

Because the DSLPipe has no power switch, plugging in the power supply turns the unit on. After you plug in the DSLPipe, it takes about a minute before it is ready to use.

Description of the front-panel lights

The green lights on the front panel of the DSLPipe have the following meanings:

Table 0-1. LED meanings

LED label	Description
PWR	When lit, the power to the unit is on.
ACT	When lit or flashing, Ethernet activity is being detected.
LNK	When lit, the link to the Ethernet is connected.
WAN	When flashing, the physical connection to the wide area network is not established. When off, the physical connection is not active. When lit, the physical connection has an active session.
CON	When lit, there is a fatal condition, or the power-on self-test is in progress.

Using the On-Board Software

3

How to use the configuration software

To perform the initial configuration of the DSLPipe, connect a serial cable to the DSLPipe control port and set the terminal emulation package in your communications software as follows:

- VT100 emulation
- 9600 bits per second
- 8 data bits
- No parity
- 1 stop bit
- No flow control
- Direct connect

After communication has been established, press Control-L to see the main screen of the configuration software.

The DSLPipe menus and status displays

The program interface consists of a menu panel on one side and eight status displays on the other. The Main Edit menu allows you to configure the DSLPipe; the status windows allow you to monitor the DSLPipe status.

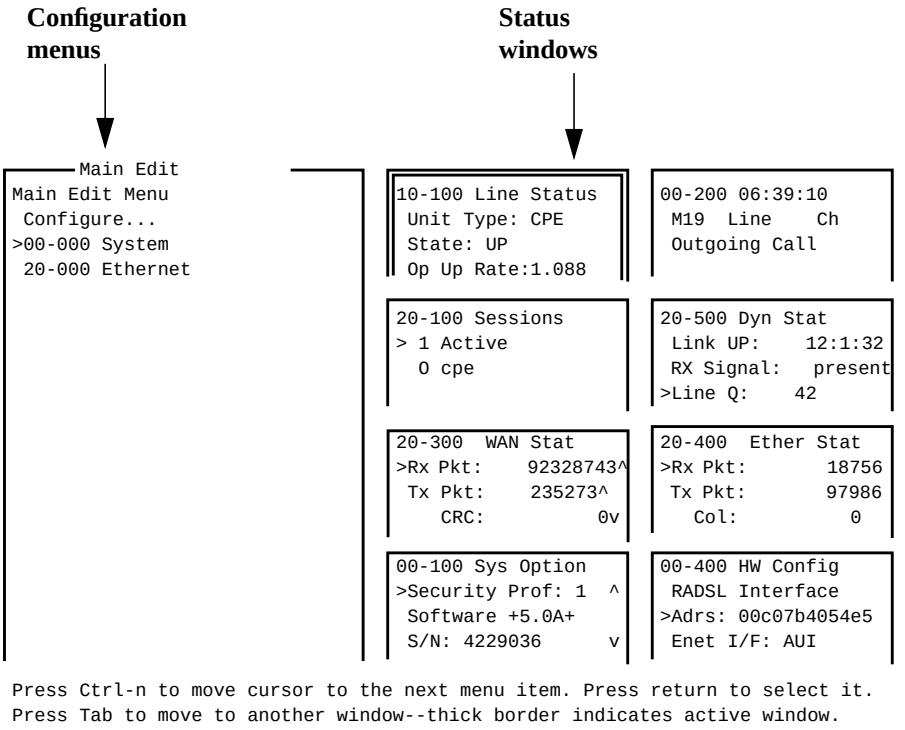


Figure 3-1. DSLPipe configuration interface

Quick reference for navigating the interface

This table is a quick reference to using the DSLPipe configuration program.

If you want to...	Do this
Make a menu or status window active.	Press the Tab key until the window has a thick double line around it. Back-Tab or Ctrl-O moves you in the opposite direction.
Select a menu or a text field.	Press Down-Arrow (or Control-N) or Up-Arrow (or Control-P).

If you want to...	Do this
Open a menu or a text field.	Press Enter or Right-Arrow.
Exit a menu or a text field.	Press Left-Arrow or Escape.
Refresh the screen display.	Press Ctrl-L.
Access the Do menu to change your security level or access the diagnostic interfaces.	Press Control-D.

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 DSLPipe displays the submenu when you select the menu option.

Table 3-1 lists the special-purpose keys and key combinations you can use in the Control Monitor display. (Note that not all keys or key combinations are valid for all systems.)

Table 3-1. Special purpose keys for Control Monitor display

Key combination	Operation
Right Arrow, 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.
Enter	Enumerated parameter: Select the next value. String value: Enter the current input. Menu: Open the current selection.

Table 3-1. Special purpose keys for Control Monitor display (Continued)

Key combination	Operation
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.

Opening menus and profiles

The Main Edit Menu contains a list of menus, each of which can contain profiles and submenus. A profile is a group of parameters to which you can assign values.

In the menu that is currently open, the cursor character (>) points to one item in the menu. To move the cursor down, press Ctrl-N (next) or the Down-Arrow key.

To move it up, press Ctrl-P (previous) or the Up-Arrow key. (Note that some VT100 emulators do not support the use of arrow keys.)

```
Main Edit Menu
>Configure...
 00-000 System
 20-000 Ethernet
 30-000 Nailed T1
```

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.

```
20-000 Ethernet
>20-100 Connections
 20-200 Bridge Adrs
 20-300 Static Rtes
  ....
```

The Ethernet menu contains profiles related to network functionality, such as bridging, routing, and WAN connections. The Mod Config profile in this menu is used to configure the Ethernet interface.

```
20-A00 Mod Config
>Ether options...
 SNMP options...
 Bridging=Yes
 IPX Routing=No
 Shared Prof=No
 Telnet PW=*SECURE*
 RIP Policy=Split Horzn
    ...
```

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 indicates that a parameter does not apply, based on the value of parameter it is subordinate to. Some parameters provide edit fields, others are enumerated.

Name fields accept up to 72 characters. Dial-out numbers accept up to 24 digits.

How to edit fields

To edit a text-based parameter (such as a password), move the cursor to the parameter and press Enter. An edit field opens, delimited by brackets, as shown for the Telnet PW parameter in the illustration that follows. (Before editing a password, “About DSLPipe passwords” on page 3-7.)

```
20-A00 Mod Config
 Ether options...
 Telnet PW=*SECURE*
 [ ]
```

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, then delete or overtype the characters.

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

How to choose one of the predefined values

When a parameter contains a set of predefined values, you select one by simply placing the cursor beside the parameter and pressing Enter until the correct value appears. When the parameter is set to the value you want, move to the next parameter with the up or down arrow keys.

Saving your changes

When you are finished editing a profile, press the Esc key. If you have entered or changed any parameters, the Exit menu appears:

```
 EXIT
>0=ESC (Don’t exit)
 1=Exit and discard
 2=Exit and save
```

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

About DSLPipe passwords

The DSLPipe provides multiple security levels, each of which you define in a Security profile. When the unit is shipped from the factory, there are no defined restrictions. To see the list of Security Profiles, open the System menu in the Main Edit Menu, select Security, and press Enter.

```
00-300 Security
>00-301 Default
 00-302
 00-303 Full Access
```

When the DSLPipe is powered on, it activates the Security profile named Default, which has no password. Before you put the unit on line, you should restrict the privileges assigned in the Default profile.

The Full Access profile should not be restricted, but you should change the password that grants access to this profile. You can create additional profiles with intermediate restrictions.

DSLPipe-C status windows

This section explains the information in the DSLPipe-C Status windows.

DSLPipe-C line status

The Line Status window displays the status of the RADSL link.

Unit type

Description: Type of DSLPipe equipment.

Values: Values can be any of the following.

- COE (Central Office Equipment)
- CPE (Customer Premise Equipment)

State

Description: The state of the RADSL connection. Values can be any of the following.

- Hndshake

  Indicates the units are trying to establish a connection. This node is waiting for the remote nodes connection request. If this condition persists, it could indicate the connection between the units is faulty.

- Training

  Indicates the units are negotiating a connection.

- Up

  Indicates the RADSL connection is operating normally and data can be transferred between nodes.

- Down

  Indicates the RADSL port is down. Data can not be transmitted between nodes. The link goes down if one of the nodes loses power or when the line quality degrades.

  – The COE unit determines the line quality from the Line Q db reading. If the difference between the Line Q reading and the Connect SQ db reading is greater than 6db for 8 seconds, the COE unit disconnects the line. This could occur when a line becomes open or the remote unit loses power.

  – The CPE unit determines the line quality using the RS Errs reading. If the CPE unit detects a very high rate of RS Errors (255 every 50ms) for 8 consecutive seconds, it disconnects the line.

- Download

  Indicates the unit is downloading firmware code into the unit.

- Idle

  Indicates the unit has been reset and has not been downloaded yet.

Op Up Rate

Description: The operational upstream data rate. Possible values are:

- 1.088 Mbps

- 952 Kbps
- 816 Kbps
- 680 Kbps
- 544 Kbps
- 408 Kbps
- 272 Kbps

RADSL ensures maximum throughput for the given line conditions; the better the line quality the higher the data rate.

Note: Currently the DSLPipe units support a maximum transmission rate of 2.56Mbps downstream and 1.0Mbps upstream for up to12,000 feet (3.7 km).

Op Dwn Rate

Description: The operational downstream data rate. Possible values are:

- 2.560 Mbps
- 2.240 Mbps
- 1.920 Mbps
- 1.600 Mbps
- 1.280 Mbps
- 960 Kbps
- 640 Kbps

RADSL ensures maximum throughput for the given line conditions; the better the line quality the higher the data rate.

Note: Currently the DSLPipe units support a maximum transmission rate of 2.56Mbps downstream and 1.0Mbps upstream for up to12,000 feet (3.7 km).

Firmware Rel

Description: Indicates the firmware version of the DSLPipe.

Hardware Ver

Description: Indicates the hardware version of the DSLPipe.

Op Up Const

Description: Indicates the operational upstream constellation.This correlates to rate. Constellation is the number of points within the digital spectrum. Possible values are:

- 256U(ncoded)
- 256
- 128
- 64
- 32
- 16
- 8

Op Dwn Const

Description: Indicates the operational downstream constellation.This correlates to rate. Constellation is the number of points within the digital spectrum. Possible values are:

- 256U(ncoded)
- 256
- 128
- 64
- 32

- 16
- 8

DSLPipe-C dynamic statistics

The Dyn Stat window displays the dynamic statistics for the RADSL link.

Port Up

Description: Indicates how long the link has been up in the format dd:hh:mm, where dd indicates the days, hh indicates the hours, and mm indicates the minutes.

RX signal

Description: Indicates this node is receiving a signal from the remote node.

Line Q

Description: Indicates the line quality of the link in decibels.

Port Up Down

Description: Indicates the number of times the link has transitioned from an Up state to a Down state since the DSLPipe was last reset.

Self Test

Dependencies: Indicates whether the unit has passed Power On Self Test (POST). Possible values are:

- Passed
- Failed

RS Errs

Description: Indicates the Reed Solomon errors that have not been corrected. This value is only used by the CPE unit. If the CPE unit detects a very high rate of RS Errors (255 every 50ms) for 8 consecutive seconds, it disconnects the line.

RS Corr

Description: Indicates the number of Reed Solomon corrected errors.

TX Power

Description: Indicates the transmission power level in db.

Attn Level

Description: Indicates the attenuation level.

Connect SQ

Description: Indicates the signal quality (SQ) reading. Connect SQ is related to Line Q when the line is active. If the difference between the Line Q reading and the Connect SQ db reading is greater than 6db for 8 seconds, the COE unit disconnects the line. This occurs when a line becomes open or the remote unit loses power.

CRC Errors

Description: When connected, the COE determines whether or not to disconnect on the basis of the number of HDLC CRC errors received in an eight-seconds period.

How to confirm what hardware options are installed

This first line in the HW Config status window indicates what hardware options are installed. For example, if Rate Adaptive Digital Subscriber Line (RADSL) is installed, it is listed here.

DSLPipe-S status windows

This section explains the SDSL-specific information in the DSLPipe-S Status windows.

DSLPipe-S line status

The Line Status window displays the status of the SDSL link.

Unit type

Description: Type of DSLPipe equipment.

Values: Values can be any of the following.

- COE (Central Office Equipment)
- CPE (Customer Premise Equipment)

State

Description: The state of the SDSL connection. Values can be any of the following.

- Config
  DSP configuration (internal functions).
- Pend Down
  Monitoring line to determine if conditions warrant disconnect for about 8 seconds (noise of -5dB or lower).
- Up
  The line is connected.

- DetectLost
  Loss of signal (LOS).
- DOWN
  The line is down.
- Activate
  Starting to train with the remote node.
- Pend up
  Waiting for the remote node to transition from training to Port Up state.
- Start up
  Another cycle of the training process.

Up Rate

Description: The operational upstream data rate.

- 784000 bps

Down Rate

Description: The operational downstream data rate.

- 784000 bps

Firmware Version

Description: Indicates the firmware version of the DSLPipe.

Hardware Version

Description: Indicates the hardware version of the DSLPipe.

Dynamic statistics for DSLPipe-S

The Dyn Stat window displays the dynamic statistics for the SDSL link.

Port timer up

Description: Indicates how long the link has been up in the format dd:hh:mm, where dd indicates the days, hh indicates the hours, and mm indicates the minutes.

RX signal

Description: Indicates this node is present and receiving a signal from the remote node or not present.

Line Q

Description: Indicates the noise margin of the link in decibels. A value of -5dB or greater indicates good quality.

Port Up Down

Description: Indicates the number of times the link has transitioned from an Up state to a Down state since the DSLPipe was last reset.

Self Test

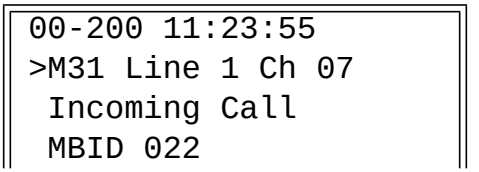
Dependencies: Indicates whether the unit has passed Power On Self Test (POST).

Attn Level **Description:** Indicates the attenuation level.

General status windows

System Events

The System Events Status window provides a log of up to 32 of the most recent system events the DSLPipe has recorded.



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 **Description:** The first line of the menu shows the status menu number and the time the event occurred.

Line 2 **Description:** 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.

Lines are numbered starting with the base system ISDN lines—lines 1 and 2. A T1 or DDS 56 line is line 3.

Line 3 **Description:** The third line contains the text of the message. The message can contain either basic information or a warning.

Line 4 **Description:** The fourth line contains a message parameter.

Sessions

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.

```
20-100 Sessions
>5 Active
 0 Headquarters
```

Each line of the menu is described in the following paragraphs.

Line 1 **Description:** The first line specifies the menu number and name of the menu.

Line 2 **Description:** The second line indicates the number of active sessions.

Line 3+

Description: The third and all remaining lines indicate the state of each active session, and the name, address, or CLID of the remote end. Each line uses the format *y zzzzz*, where *y* is a session status character and *zzzzz* indicates the name, address, or CLID of the remote device. Table 3-2 lists the session status characters that can appear.

Table 3-2. Session status characters

Character	Description
Blank	No calls exist and no other DSLPipe operations are being performed
R	R indicates Ringing; an incoming call is ringing on the line, ready to be answered.
A	A indicates Answering; the DSLPipe is answering an incoming call.
C	C indicates Calling; the DSLPipe is dialing an outgoing call.
O	O indicates Online; a call is up on the line.
H	H indicates Hanging up; the DSLPipe is clearing the call.

WAN Stat

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.

```
20-300 WAN Stat
>Rx Pkt:  387112
 Tx Pkt:   22092
    CRC:  0
```

Each line of the menu is described in the following paragraphs.

Line 1

Description: 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

Description: The second line specifies the number of received frames.

Line 3

Description: The third line displays the number of transmitted frames.

Line 4

Description: The fourth line indicates the number of frames with errors. CRC checking is performed on PPP links.

Ether Stat

The Ether Stat menu displays the number of Ethernet frames received and transmitted and the number of collisions at the Ethernet interface.

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

This screen contains the fields described in Table 3-3.

Table 3-3. 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.

Sys Options

The Sys Options menu provides a read-only list that identifies your DSLPipe and names each of the features with which it has been equipped.

```
00-100 Sys Options
>Security Prof:1   ^
 Software +1.0+
 S/N:42901
```

The Sys Options menu can contain the information listed in Table 3-4.

Table 3-4. Sys Options information

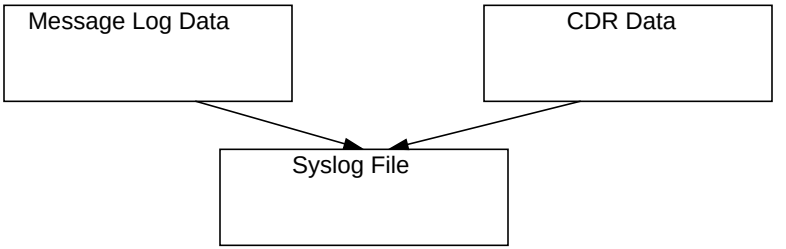
Option	Description
Security Prof: 1, Security Prof: 2...	Shows which of the nine Security Profiles is controlling the user interface.
Software	Defines the version and revision of the system ROM code.

Table 3-4. Sys Options information

Option	Description
S/N	Displays the serial number of the DSLPipe. The serial number of your DSLPipe can also be found on the model number/serial number label on the DSLPipe's bottom panel.
FR Rel Installed	Displays whether the frame relay option is installed

Syslog

Syslog is not a DSLPipe 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.

Configuring the DSLPipe

4

Information you need to know

Before you begin, gather the following information from your service provider or corporate administrator:

- IP address for your DSLPipe, and the subnet mask; the IP address of the remote host (the computer you plan to call), and its subnet mask.
- The name of your local unit and the remote unit (as supplied by the service provider or administrator). Each name is associated with the IP address of the unit.
- The encapsulation method. The choices are Point-to-Point Protocol (PPP) and Frame Relay (FR). For Frame Relay, you also need to know the Data Link Connection Indicator (DLCI).

Additionally you need to determine whether you will bridge or route. You should route if possible, as routing is more efficient and makes call management easier. Bridging is necessary when you cannot subnet your IP network, and when you need to use non-routable protocols such as NetBIOS, or DECnet. Bridge when you are connecting networks of the same type (such as all IP, or all IPX). Route when you are connecting different types of networks (such as connecting an IP network to an IPX network).

The following two parameters must be set as follows:

- Channel Usage = Leased/Unused.
- Call Type = Nailed (meaning always connected).

Example configurations

Configuring a single-user RADSL-CAP pair of units

This example configuration shows how to connect two DSLPipe units over an ADSL connection. The settings shown below use sample information.

To configure the Customer Premises Equipment (CPE):

1. From the Main Edit menu, select Configure.
2. Specify the following values:
   - Chan Usage=**Leased/Unused**
   - My Name=**DSLPipe-CPE**
   - My Addr=**192.1.2.1/24**
   - Rem Name=**DSLPipe-COE**
   - Rem Addr=**192.1.1.1/24**
   - Route=**IP**
   - Bridge=**No**
3. From the Main Edit menu, select Ethernet>Connections>DSLPipe-COE Connection profile.
4. Specify the following values:
   - Active=**Yes**
   - Encaps=**FR**
   - Bridge=**No**
   - Route IP=**Yes**
5. Open the Encaps Options submenu.
6. Specify the following values:
   - FR Prof=**Frame Relay**
   - DLCI=**16**
7. Exit the Connection profile and save your changes.
   Next, set up the Frame Relay profile.
8. Open the Ethernet>Frame Relay>Frame Relay profile.

9 Specify the following values:

- Name=**Frame Relay**
- Active=**Yes**
- Call Type=**Nailed**
- LinkUp=**Yes**

10 Exit the Frame Relay profile and save your changes.

Configuring the COE DSLPipe

To configure the Central Office Equipment (COE):

1 From the Main Edit menu, select Configure.

2 Specify the following values:

- Chan Usage=**Leased/Unused**
- My Name=**DSLPipe-COE**
- My Addr=**192.1.1.1/24**
- Rem Name=**DSLPipe-CPE**
- Rem Addr=**192.1.2.1/24**
- Route=**IP**
- Bridge=**No**

3 From the Main Edit menu, select Ethernet>Connections>DSLPipe-CPE Connection profile.

4 Specify the following values:

- Active=**Yes**
- Encaps=**FR**
- Bridge=**No**
- Route IP=**Yes**

5 Open the Encaps Options submenu.

6 Specify the following values:

- FR Prof=**Frame Relay**
- DLCI=**16**

7 Exit the Connection profile and save your changes. Next, set up the Frame Relay profile.

8 Open the Ethernet > Frame Relay > Frame Relay profile.

9 Specify the following values:

- Name=**Frame Relay**
- Active=**Yes**
- Call Type=**Nailed**
- LinkUp=**Yes**

10 Exit the Frame Relay profile and save your changes.

Configuring a customer-side SDSL unit

Before you configure the DSLPipe, make sure:

- The PC connected to the DSLPipe has an IP address on the same subnet as the DSLPipe.
- The IP address of the DSLPipe is configured as the default gateway for the PC.

To configure the DSLPipe:

1 From the Main Edit menu, select Configure.

2 Specify the following values:

- Chan Usage=**Leased/Unused**
- My Name=**cpe**
- My Addr=**192.168.216.141/24**
- Rem Name=**coe-11-1**
- Rem Addr=**192.168.215.135/24**
- Route=**IP**

3 Exit and save the Configure profile.

4 From the Main Edit menu, select Ethernet>Connections>coe-11-1.

5 Specify the following values:

- Active=**Yes**
- Encaps=**FR**

– `Route IP=`**`Yes`**

6 Open the Encaps Options submenu.

7 Specify the DLCI used for this profile:

– `FR Prof=`**`16`**

8 Exit and save the Connection profile.

Configuring your computer

If you are connecting to either an IP or AppleTalk network, configure the computer that connects to the remote network through the DSLPipe as follows:

- Specify the IP address of the DSLPipe as the default gateway.
- Assign an IP address to your computer that is on the same IP subnet as the Pipeline. (Your system administrator will provide the subnet address for you. Note that this address is a valid IP address only on the local network, not across the Internet.)
- Specify the Domain Name Server (DNS) used by the remote network on your computer. (Your system administrator will give you the DNS to use.)

The settings let the DSLPipe recognize the computer(s) connected to it, and let the computer(s) recognize the DSLPipe as the gateway to the remote network.

If you are connecting to an IPX network, your network administrator will supply you with settings used by a remote NetWare client.

Wide Area Networking 5

Introduction to WAN connections

The basic elements of WAN connections include link encapsulation, nailed groups, and call initiation. Call-initiation profiles are specified in the Connection profile. A profile is a saved group of settings that defines a particular connection. You can save up to eight connection profiles.

Link encapsulations

In addition to basic Telco options and authentication, one of the main agreements between the caller and the answering device must be the type of link encapsulation used. The caller must encapsulate all outbound packets before sending them across the WAN, and the answering device must unencapsulate them before forwarding the packets. Following are the types of link encapsulation supported by the DSLPipe:

- Point-to-Point Protocol (PPP), a single-channel connection that connects to any other device running PPP.

  PPP connections support password authentication using Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP), and can support IP routing, IPX routing, or protocol-independent bridged connections. They can be dial-in or dial-out switched connections.

- Frame Relay RFC 1490

  The Frame Relay RFC 1490 standard does no support authentication.

  A Frame Relay gateway connection supports routing and bridging to and from the switch across a nailed connection.

  Some Ascend units provide Frame Relay operations as a software option.

Nailed groups

A nailed connection is a permanent link that is always up as long as the physical connection persists. If the unit or central switch resets or if the link is terminated, the DSLPipe attempts to restore the link at 10-second intervals. If the DSLPipe or the far-end unit is powered off, the link is restored when power is restored.

To make channels available for a nailed connection, you have to designate them for nailed usage and assign them to a group number.

Note: Make sure the group numbers are unique across all WAN interfaces.

Recommended group numbers

Use profiles to assign group numbers to channels as follows:

- For PPP encapsulated connections to other routers/bridges, use the Group parameter in the Telco options submenu of the Connection profile to set the group number.
- For Frame Relay encapsulated connections, use the Nailed Grp parameter in the Frame Relay profile to set the group number.

Connection profiles

Connection profiles contain parameters that define individual connections.

Table 5-1. Connection profile parameters

Location	Parameters
Ethernet > Connection > *any profile* (an individual connection profile)	Station=[] Active=No Encaps=*encapsulation method* Dial #=[] Calling #=[] Route IP=No Route IPX=No Bridge=Yes Dial brdcast=No
Ethernet > Connection > *any profile* > Encaps options...	*Depends on encapsulation method selected.* See: • "Configuring a PPP connection" on page 5-4. • "Configuring Frame Relay connections" on page 5-6.
Ethernet > Connection > *any profile* > IP options...	See Chapter 7, "Setting up IP Routing."
Ethernet > Connection > *any profile* > Telco options...	AnsOrig=Ans Only Callback=No Call Type=Switched Group=N/A FT1 Caller=N/A Data Svc=56KR Force 56=N/A Bill #=[]

For details on each parameter, see the *Reference Guide*.

Configuring a PPP connection

To configure a PPP connection, you must perform the following tasks:

- Determine the appropriate routing, authentication, and compression settings.
- Configure the PPP connection in a Connection profile.
- Configure the routing or bridging setup of the DSLPipe and for the WAN connection.

These are the parameters related to PPP configurations:

Table 5-2. PPP parameters

Location	**Parameters**
Ethernet > Connections > *any profile* (an individual connection profile)	Encaps=PPP
Ethernet > Connections > *any profile* > Encaps options...	Send Auth=CHAP Send PW=*SECURE* Recv PW=*SECURE* MRU=1524 LQM=No LQM Min=600 LQM Max=600 Link Comp=Stac VJ Comp=Yes

Unless the Send Auth parameter is set to None, the DSLPipe must be assigned a name in the System profile:

1 Open the System profile.

2 Specify a name for the DSLPipe unit in the Name parameter.
For example:

```
Name=MYPIPE1
```

3 Close the System Profile.

To configure a PPP connection:

1. Open the Connection profile.
2. Specify the name of the remote device in the Station parameter.

   For example:

   ```
   Station=remotepipe
   ```

   Make sure you enter the name exactly, including case changes and spaces or underscores.
3. Activate the profile.

   ```
   Active=Yes
   ```
4. Select PPP encapsulation.

   ```
   Encaps=PPP
   ```
5. Open the Encaps Options submenu.
6. Set the Send Auth parameter to CHAP or PAP.

   For example:

   ```
   Send Auth=CHAP
   ```

   Both sides of the connection must support the selected protocol.
7. Enter the password sent from the DSLPipe to the remote device in the Send PW parameter's edit field. For example:

   ```
   Send PW=*SECURE*
   ```
8. Enter the password the remote device sends to the DSLPipe in the Recv PW parameter's edit field. For example:

   ```
   Recv PW=*SECURE*
   ```
9. If appropriate, turn on data compression.

   For example:

   ```
   Link Comp=Stac
   VJ Comp=Yes
   ```
10. Press Esc to close the Connection profile.
11. Choose 2=Exit and Accept to save the profile.

Configuring Frame Relay connections

Before you begin

Connection profiles define logical links to an end-point on the Frame Relay network. Each Connection profile must specify a Data Link Connection Identifier (DLCI) for that link. A DLCI is a number between 16 and 991, which is assigned by the Frame Relay administrator. A DLCI is not an address, but a local label that identifies a logical link between a device and a Frame Relay switch. (That is, the DLCIs enable the Frame Relay switch to identify the logical link associated with each Connection profile.) The switch uses the DLCI to route frames through the network, and the DLCI may change as frames are passed through multiple switches.

Note: You need at least one Frame Relay profile and Connection profile to define a logical link to the Frame Relay network.

To configure a Frame Relay connection, you must perform the following tasks:

- Obtain the DLCIs you need from the Frame Relay administrator.
  Each connection requires its own DLCI.
- Obtain the routing/bridging information for the remote network.
- Configure the Frame Relay connection in a Connection profile.
- Configure the routing or bridging setup in the DSLPipe and across the WAN connection.

Options for configuring logical links

A Connection profile defines a logical link to an end-point reached through a Frame Relay switch. The DSLPipe supports Frame Relay “Gateway” mode. A Frame Relay gateway connection is a bridging or routing link between the DSLPipe and a remote network via a Frame Relay switch. When the DSLPipe receives IP packets destined for that network, it encapsulates the packets in Frame Relay (as specified in RFC 1490) and forwards the data stream with the specified DLCI to the Frame Relay switch. The Frame Relay switch uses the DLCI to route the frames to the right destination.

Figure 5-1 shows a DSLPipe with three gateway connections to customer premise equipment (CPE) at remote sites across the Frame Relay network. Gateway connections can support bridging and routing, so the DSLPipe can forward any type of protocol traffic from the local network onto the Frame Relay network.

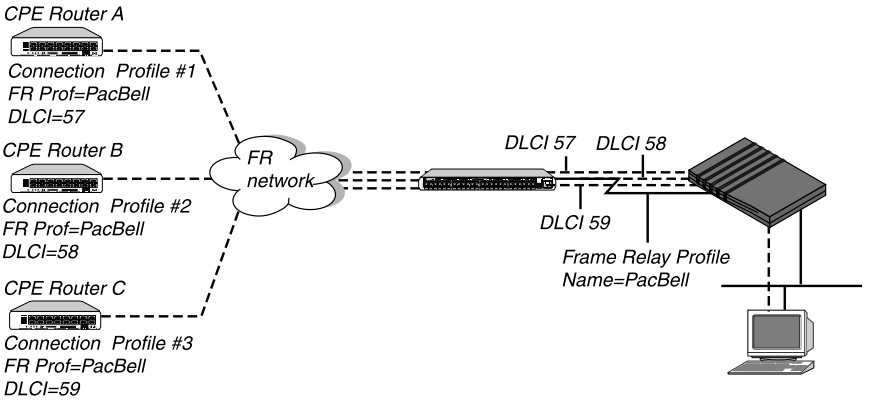


Figure 5-1. Gateway connections to the Frame Relay network

Connection profiles #1, #2, and #3 use Frame Relay encapsulation (RFC 1490) and include both a DLCI number for the logical link and the name of the Frame Relay profile for the nailed connection. Frame Relay profile #1 defines a nailed connection between the DSLPipe and a Frame Relay switch. The Connection profiles and the Frame Relay profile in this example are defined below:

Connection profiles (gateway)

```
20-101
Station=CPEA
Active=Yes
Encaps=FR
Encaps options...
   FR Prof=PacBell
   DLCI=57
```

Frame Relay profile

```
20-501 PacBell
Name=PacBell
Active=Yes
Call Type=Nailed
Nailed Grp=1
Data Svc=64K
Link Mgmt=T1.617D
...
```

Connection profiles (gateway) **Frame Relay profile**

```
20-102
Station=CPEB
Active=Yes
Encaps=FR
Encaps options...
   FR Prof=PacBell
   DLCI=58

20-103
Station=CPEC
Active=Yes
Encaps=FR
Encaps options...
   FR Prof=PacBell
   DLCI=59
```

Configuring a Frame Relay profile

Table 5-3 shows configuration parameters needed to create a nailed connection to the Frame Relay switch with sample values.

Table 5-3. Frame Relay profile parameters

Location	Parameters with example values
Ethernet > Frame Relay > Frame Relay profile	Name=PacBell7 Active=Yes Call Type=Nailed Nailed Grp=1 Data Svc=64k Dial #=N/A Link Mgmt=T1.617D N391=6 N392=3 N393=4 T391=10 T392=15 MRU=1532

The parameters are described in detail in the *Reference Guide*.

To define the Frame Relay profile:

1 Open a Frame Relay profile and assign it a name.

For example:

```
Name=PacBell
```

The name can contain up to 15 alphanumeric characters. You have to use this name in Connection profiles that use this connection to the switch.

2 Activate the profile.

For example:

```
Active=Yes
```

3 Specify that this is a nailed connection and enter the group number of the nailed channels to be used.

For example:

```
Call Type=Nailed
Nailed Grp=1
```

Nailed is the default for Frame Relay connections. When the call type is nailed, dial numbers and other telephone company parameters are N/A.

4 Specify the link management protocol used between the DSLPipe and the Frame Relay switch.

For example:

```
Link Mgmt=T1.617D
```

If you specify Link Mgmt=T1.617D, set the following additional parameters:

```
N391
N392
N393
T391
T392
```

N391 specifies how many polling cycles the DSLPipe waits before requesting a full status report. N392 is the maximum number of error events that can occur in the sliding window defined by N393. N393 specifies the width of the sliding window used by the N392 parameter.

T391 specifies the number of seconds between Status Enquiry messages. T392 specifies the number of seconds that the DSLPipe waits for a Status Enquiry message before recording an error.

See the *Reference Guide* for more details.

5 Close the Frame Relay profile.

Configuring a gateway connection

Table 5-4 shows the Connection profile parameters for Frame Relay gateway connections with sample values.

Table 5-4. Frame relay gateway connection parameters

Location	Parameters
Ethernet > Connections > *any profile* (Connection profile)	Encaps=FR
Ethernet > Connections > *any profile* > Encaps options...	FR Prof=Pac Bell DLCI=17

The parameters are described in detail in the *Reference Guide*.

Note: This section shows how to configure the Frame Relay setup. Routing and bridging parameters must also be configured to have a working connection.

To configure a Frame Relay gateway connection to Customer Premises Equipment (CPE) on the Frame Relay network:

1 Open a Connection profile and specify the name of the CPE.

For example:

```
Station=CPEA
```

2 Activate the profile.
For example:

```
Active=Yes
```

3 Select Frame Relay encapsulation.
For example:

```
Encaps=FR
```

The DSLPipe uses this encapsulation method to encapsulate packets before routing them out to the CPE, and removes the Frame Relay encapsulation from packets coming in from the CPE.

4 Open the Encaps Options submenu.

5 Set the DLCI parameter to the number assigned by the Frame Relay administrator.

For example:

```
DLCI=500
```

The Frame Relay administrator must assign the DLCI number. It determines how packets will be routed at the Frame Relay switch.

6 Specify the name of the Frame Relay profile that defines the nailed connection to the Frame Relay switch.

For example:

```
FR Prof=PacBell
```

The name must match the Name parameter in the Frame Relay profile exactly, including case changes.

7 Close and save the Connection profile.

Setting up Bridging

6

Introduction to Ascend bridging

This section describes when you should use bridging, provides an overview of packet bridging, and explains how the DSLPipe brings up a bridged connection.

When should you use bridging or routing?

In the DSLPipe, bridges are used primarily to provide connectivity for protocols other than IP and IPX (AppleTalk, for example). They can also be used to join segments of an IP or IPX network. 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.

Bridging is very easy to configure and is commonly used to:

- Provide non-routed protocol connectivity with another site
- Link two sites so that their nodes appear to be on the same LAN
- Support protocols that depend on broadcasts to function, such as BOOTP

Be aware that bridges examine *all* packets on the LAN (called “promiscuous mode”), so they incur greater processor and memory overhead than routers. On heavily loaded networks, this increased overhead can result in slower performance.

Routing is much faster than bridging, and has these advantages:

- Routers examine packets at the network layer (instead of the link layer, used by bridges), so you can filter on logical addresses, providing enhanced security and control.

- Routers support multiple transmission paths to a given destination, enhancing the reliability and performance of packet delivery.

From a practical point of view, you should always route if possible, as routing is more efficient and makes call management easier. Bridging is necessary when you cannot subnet your IP network, and when you need to use non-routable protocols such as AppleTalk, NetBIOS, or DECnet.

How a bridged WAN connection is initiated

When the DSLPipe is configured for bridging, it accepts all packets on the Ethernet and forwards only those that have one of the following:

- A physical address that is not on the local Ethernet segment (the segment to which the DSLPipe 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 DSLPipe receives a packet whose destination MAC address is not on the local network, it first checks its internal bridge table. If it finds the packet's destination MAC address in its bridge table, the DSLPipe dials the connection and bridges the packet. If the address is *not* specified in its bridge table, the DSLPipe checks for active sessions that have bridging enabled. If there are one or more active bridging links, the DSLPipe forwards the packet across *all* active sessions that have bridging enabled.

Note: The DSLPipe 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 find-

ing the proper Connection Profile. For more detailed information, see “Managing the bridge table” on page 6-6.

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 receive all packets with that destination address. As a router, the DSLPipe discards broadcast packets. As a bridge, it forwards packets with the broadcast destination address 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: ARP broadcast packets that contain an IP address in the bridge table are a special case. For details, see “Static bridge-table entries” on page 6-8.

How bridged connections are established

The DSLPipe uses station names and passwords to sync up a bridging connection, as shown in Figure 6-1.

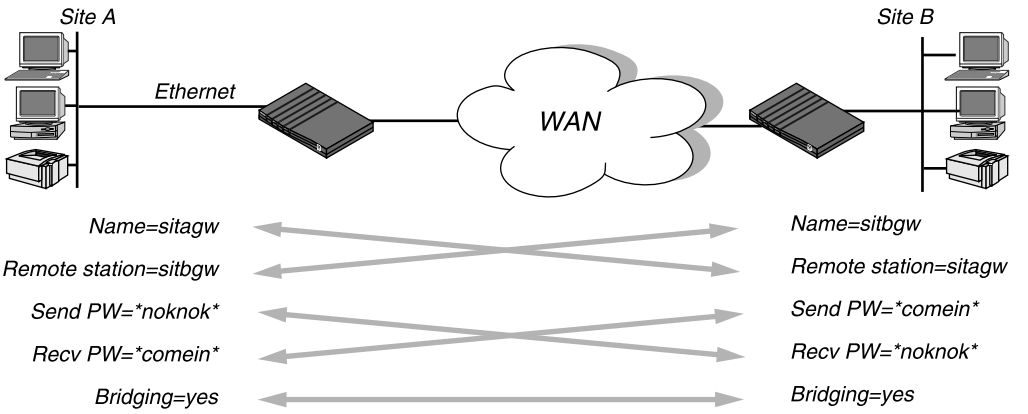


Figure 6-1. Negotiating a bridge connection (PPP encapsulation)

The system name assigned to the DSLPipe in the Name parameter of the System Profile must be *exactly* the same device name specified in the Connection profile on the remote bridge (the match is case sensitive). Similarly, the name assigned to the remote bridge must be exactly the same name specified in the Station parameter of that Connection Profile.

Note: The most common cause of trouble when initially setting up a PPP bridging connection is that the names are not specified exactly. Check for case, dashes, spaces, underscores, and so forth.

About IPX bridging

IPX bridging has special requirements for facilitating NetWare client/server logins across the WAN and preventing IPX RIP and SAP broadcasts from keeping a bridged connection up indefinitely. These requirements are handled by the parameters shown in Table 6-1.

Table 6-1. IPX bridging parameters

Location	Parameters with example values
Ethernet > Connections > *any profile* > IPX options	Handle IPX=Client (for client bridging)
Ethernet > Connections > *any profile* > IPX options	NetWare t/o=30 Handle IPX=Server (for server bridging)

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. Also, if Route IPX is set to Yes in the Connection profile, the Handle IPX parameter is set to N/A, but acts as if it is set to Server.

When there is no server support on the local network

If the local Ethernet supports NetWare clients only and no NetWare servers, the bridging connection should enable a local client to bring up the WAN connection by querying (broadcasting) for a NetWare server on a remote network. However,

the connection should not stay up indefinitely because of RIP or SAP broadcasts. To accomplish this, set Handle IPX=Client.

When there is no server support on the remote network

If the local network supports NetWare servers (or a combination of clients and servers) and the remote network supports NetWare clients only, the bridging connection should enable the DSLPipe to respond to NCP watchdog requests for remote clients, but to bring down inactive connections whenever possible. To accomplish this, specify a timeout value (for example, set NetWare t/o=30), and set the Handle IPX parameter to Server.

When there is server support on both networks

If NetWare servers are supported on both sides of the WAN connection, it is strongly recommended that you use an IPX routing configuration instead of bridging IPX. If you bridge IPX in that type of environment, client/server logins are lost when the DSLPipe brings down an inactive WAN connection.

IPX routing and bridging on the same connection

When IPX routing is enabled for a connection, the DSLPipe routes only one packet frame type across that connection. For example, if the IPX frame type is set to 802.3, only 802.3 packets are routed. If some NetWare servers on the local network use a different frame type, such as 802.2, those packets are bridged if bridging is enabled, or discarded if bridging is *not* enabled.

Examples

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 all other packets are bridged, including IPX packets in other frame types, AppleTalk packets, NetBios packets, DECnet and so forth.

If the DSLPipe 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.

Enabling bridging

The DSLPipe has a global bridging parameter that must be enabled for any bridging connection to work. The Bridging parameter causes the DSLPipe unit's Ethernet controller to run in promiscuous mode. In promiscuous mode, the Ethernet driver accepts all packets, regardless of address or packet type, and passes them up the protocol stack for a higher-layer decision on whether to route, bridge, or reject the packets.

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

Table 6-2. Bridging in the Ethernet Profile

Location	Parameter with example value
Ethernet > Mod Config (Ethernet profile)	Bridging=Yes

To enable bridging on Ethernet:

1. Open the Ethernet profile.
2. Turn on the global bridging parameter.

   ```
   Bridging=Yes
   ```
3. Close the Ethernet profile.

Managing the bridge table

To forward bridged packets to the right network destination, the DSLPipe uses a bridge table that associates end nodes with particular connections. It builds this table dynamically, as described in "Transparent bridging" on page 6-7. It also incorporates the entries found in its Bridge profiles. Bridge profiles are analogous to static routes in a routing environment. You can define up to eight destination nodes and their connection information in Bridge profiles.

Parameters that affect the bridge table

Table 6-3 shows configuration parameters directly related to the bridge table.

Table 6-3. Bridge table parameters

Location	Parameters with example values
Ethernet > Mod Config (Ethernet profile)	Bridging=Yes
Ethernet > Connections > *any profile* (Connection profile)	Bridge=Yes Dial Brdcast=No
Ethernet > Bridge Adrs > *any profile* (Bridge profile)	Enet Adrs=CFD012367 Net Adrs=10.1.1.12 Connection #=7

For details on each parameter, see the *Reference Guide*.

Transparent bridging

As a transparent (or learning) bridge, the DSLPipe keeps track of where addresses are located as it forwards packets. It records each packet's source address in a bridging table. A Connection profile is associated with an address when it is used to dial the link or when it matches an incoming call.

Figure 6-2 shows the physical addresses of some nodes on the local Ethernet and one at a remote site. The DSLPipe at site A, configured as a bridge, gradually learns addresses on both networks by looking at each packet's source address.

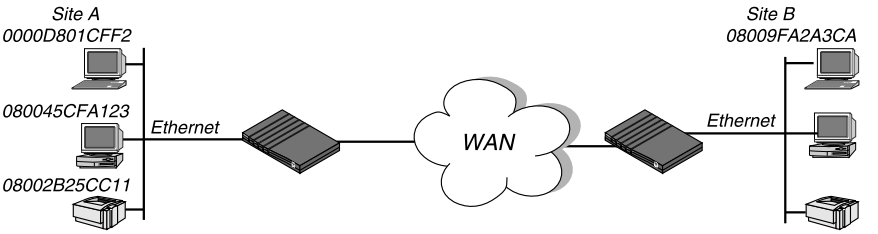


Figure 6-2. How the DSLPipe creates a bridging table

The resulting bridging table looks like this:

0000D801CFF2	SITEA
080045CFA123	SITEA
08002B25CC11	SITEA
08009FA2A3CA	SITEB (Connection Profile #5)

Entries in the DSLPipe unit's bridge table must be relearned within a fixed aging time limit, or they are removed from the table.

Static bridge-table entries

The administrator can specify up to eight static bridge-table entries in Bridge profiles. Each connection that has a static bridge table entry can have the Dial Brdcast parameter set to No.

Dial Brdcast is a very convenient way of bridging packets if the DSLPipe has only a few bridging connections, but it can be expensive in an environment where many profiles support bridging. (For more information, see "Broadcast addresses and Dial Brdcast" on page 6-3.) If Dial Brdcast is turned off in a Connection profile, the DSLPipe does not initiate dialing for that connection on the basis of broadcast requests. Instead, it relies on its bridging table to recognize which Connection profile to use.

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

To define a static bridge-table entry:

1. Open a Bridge profile.
2. Specify the physical address of the remote host.
   For example:
   ```
   Enet Adrs=0080AD12CF9B
   ```
   Get this address from the administrator of the far-end device. For more information, see “Physical addresses and the bridge table” on page 6-2.
3. If the far-end is a segment of the local IP network, specify an address on that segment. For example:
   ```
   Net Adrs=10.2.3.133
   ```
   For more details, see “An example IP bridged connection” on page 6-15.
4. Specify the number of the Connection profile for this connection.
   For example:
   ```
   Connection #=2
   ```
   You don’t have to specify the whole number, just the unique portion of it.
5. Close the Bridge Profile.

Configuring bridged connections

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

Connection profiles must enable bridging, and if the remote network is not recorded as a static bridge-table entry, Dial Brdcast must also be enabled.

Table 6-4 shows Connection profile parameters related to protocol-independent bridging.

Table 6-4. Bridging parameters in Connection profiles

Location	Parameters with example values
Ethernet > Connections > *any profile* (Connection profile)	Station=SITEBGW Bridge=Yes Dial Brdcast=No
Ethernet > Connections > *any profile* > Encaps options...	Send Auth=None Recv PW=N/A Send PW=N/A
Ethernet > Connections > *any profile* > IPX options...	Handle IPX=Client

For details on each parameter, see the *Reference Guide.*

An example AppleTalk bridged connection

An AppleTalk connection at the link level requires a bridge at either end of the connection. Be careful when specifying names. Names are case sensitive, and dashes, spaces, underscores and other details must be retained. The most common cause of trouble when initially setting up a bridging connection is that the wrong name is specified for the DSLPipe or the remote device. Make sure you type the name exactly as it appears in the remote device.

The following example assumes that Bridging has been enabled on the Ethernet interface (as discussed in “Enabling bridging” on page 6-6).

In the example, Dial Brdcast is turned off in the Connection profiles and a Bridge profile is specified. This is not required. You can turn on Dial Brdcast and omit the Bridge profile if you prefer.

To configure the local DSLPipe for a bridged connection:

1. Open the System profile.
2. If the DSLPipe does not already have a system name, assign one.
   For example:
   ```
   Name=SITEAGW
   ```

Bridged connections use system names for part of the authentication process.

3. Close the System profile.
4. Open Connection profile #5.
5. Set these parameters:

```
Station=SITEBGW
Active=Yes
Encaps=PPP
Bridge=Yes
Dial Brdcast=No
```

```
Encaps options...
    Send Auth=CHAP
   Recv PW=*SECURE*
   Send PW=*SECURE*
```

6. Close Connection profile #5.
7. Open a Bridge profile.
8. Set these parameters:

```
Enet Adrs=0080AD12CF9B
Net Adrs=0.0.0.0
Connection #=5
```

9. Close the Bridge profile.

To configure the remote Pipeline unit for a bridged connection:

1. Open the System profile (on the remote Pipeline).
2. If the DSLPipe does not already have a system name, assign one.

   For example:

```
Name=SITEBGW
```

3. Close the System profile.
4. Open Connection profile #2 on the Pipeline.
5. Set these parameters:

```
Station=SITEAGW
Active=Yes
Encaps=PPP
```

```
Bridge=Yes
Dial Brdcast=No

Encaps option...
    Send Auth=CHAP
    Recv PW=*SECURE*
    Send PW=*SECURE*
```

6 Close Connection profile #2.

7 Open a Bridge profile.

8 Set these parameters:

```
Enet Adrs=0CFF1238FFFF
Net Adrs=0.0.0.0
Connection #=2
```

9 Close the Bridge profile.

An example IPX client bridge (local clients)

In the following example, the local Ethernet supports NetWare clients, and the remote network supports NetWare servers and clients.

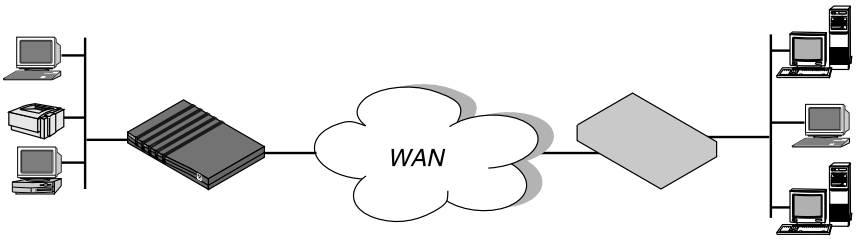


Figure 6-3. An example IPX client bridging connection

To configure the DSLPipe in this example:

1 Open the System profile.

2 If the DSLPipe does not already have a system name, assign one.

For example:

```
Name=SITEAGW
```

3 Close the System profile.

4. Open the Ethernet profile.
5. Open the Ether Options submenu.
6. Set the IPX Frame type.

```
IPX Frame=802.3
```

7. Close the Ethernet profile.
8. Open a Connection profile.
9. Set these parameters:

```
Station=SITEBGW
Active=Yes
Encaps=PPP
Route IPX=No
Bridge=Yes
Dial Brdcast=Yes

Encaps options...
    Send Auth=CHAP
    Recv PW=*SECURE*
    Send PW=*SECURE*

IPX options...
    Handle IPX=Client
```

10. Close the Connection Profile.

Dial Brdcast is enabled to allow service queries to bring up the connection.

When Handle IPX=Client, the DSLPipe applies a data filter that discards RIP and SAP periodic broadcasts at its WAN interface, but forwards RIP and SAP queries. That way, local clients can locate a NetWare server across the WAN, but routine broadcasts do not keep the connection up unnecessarily.

An example IPX server bridge (local servers)

In the following example, the local network supports a combination of NetWare clients and servers, and the remote network only supports clients.

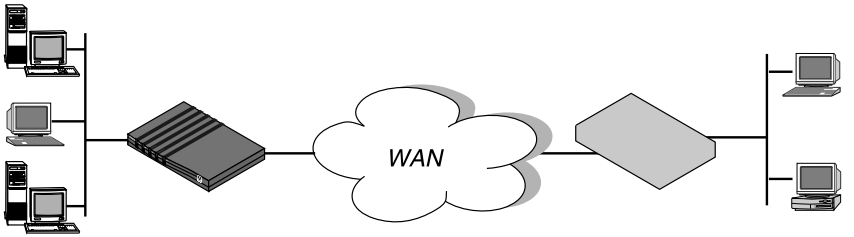


Figure 6-4. An example IPX server bridging connection

To configure the DSLPipe in this example:

1. Open the System profile.
2. If the DSLPipe does not already have a system name, assign one.
   For example:

   ```
   Name=SITEAGW
   ```
3. Close the System profile.
4. Open the Ethernet profile.
5. Open the Ether Options submenu.
6. Set the IPX Frame type.
   For example:

   ```
   IPX Frame=802.3
   ```
7. Close the Ethernet profile.
8. Open a Connection profile.
9. Set these parameters:

   ```
   Station=SITEBGW
   Active=Yes
   Encaps=PPP
   Route IPX=No
   Bridge=Yes
   Dial Brdcast=Yes

   Encaps options...
       Send Auth=CHAP
       Recv PW=*SECURE*
       Send PW=*SECURE*
   ```

```
IPX options...
    NetWare t/o=30
    Handle IPX=Server
```

10 Close the Connection profile.

When Handle IPX=Server, the DSLPipe applies a data filter that discards RIP and SAP broadcasts at its WAN interface, but forwards RIP and SAP queries. It also 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 DSLPipe performs watchdog spoofing 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 more information, see Chapter 8, "Setting up IPX Routing.")

An example IP bridged connection

If you are bridging between two segments of the same IP network, you can use the Net Adrs parameter in a Bridge profile to enable the DSLPipe to respond to ARP requests while bringing up the bridged connection.

If an ARP packet contains an IP address that matches the Net Adrs parameter of a Bridge profile, the DSLPipe responds to the ARP request with the Ethernet (physical) address specified in the Bridge profile, and brings up the specified connection. In effect, the DSLPipe acts as a proxy for the node that actually has that address.

In this example, two segments of an IP network are connected across the WAN.

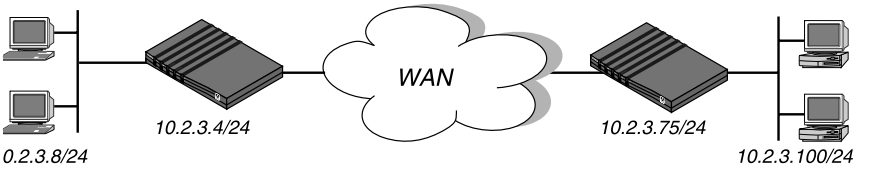


Figure 6-5. An example IP bridging connection

To configure the first DSLPipe shown in Figure 6-5:

1. Open the System profile.
2. If the DSLPipe does not already have a system name, assign one.

   For example:

   ```
   Name=SITEAGW
   ```
3. Close the System profile.
4. Open Connection profile #7 (for example).
5. Set these parameters:

   ```
   Station=SITEBGW
   Active=Yes
   Encaps=PPP
   Route IP=No
   Bridge=Yes
   Dial Brdcast=No
   ```

   ```
   Encaps options...
       Send Auth=CHAP
       Recv PW=*SECURE*
       Send PW=*SECURE*
   ```
6. Close Connection profile #7.
7. Open a Bridge profile.
8. Set these parameters:

   ```
   Enet Adrs=0CFF1238FFFF
   Net Adrs=10.2.3.100/24
   Connection #=7
   ```
9. Close the Bridge profile.

Setting up IP Routing

7

Introduction to IP routing on the DSLPipe

This section describes how the DSLPipe establishes IP routing connections, gives an overview of RIP-v2, and explains the syntax of netmask notation.

The most common uses for IP routing connections in the DSLPipe are to:

- Enable IP connections to the Internet (through Internet Service Providers)
- Connect distributed IP subnets to a corporate backbone (telecommuting and remote office hubs)

The DSLPipe supports IP routing over PPP, MP, MP+, and frame relay connections. The DSLPipe is fully interoperable with non-Ascend products that conform to the TCP/IP protocol suite and associated RFCs.

IP routing connections have a level of built-in authentication, because the DSLPipe matches the IP address of a Connection profile to the source IP address of a caller. For most sites, however, this level of security is not enough and a form of password authentication is used as well. (For more information, see Chapter 9, “Setting up Security,”)

Note: IP routing can be configured along with protocol-independent bridging and IPX routing in any combination. However, you cannot bridge *and* route IP packets across the same connection. When you configure the DSLPipe 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. (For more information about bridging, see Chapter 6, “Setting up Bridging,”)

Netmask notation

In the DSLPipe, IP addresses are specified in decimal format (not hexadecimal). For example:

```
198.5.248.40
```

If no netmask is specified, the DSLPipe assumes a default netmask based on the "class" of the address:

Table 7-1. IP address classes and default netmasks

Class	Address range	Network 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

For example, a class C address such as 198.5.248.40 has 24 network bits, as shown in Figure 7-1. That leaves 8 bits for the host portion of the address, so up to 255 hosts can be supported on the class C network.

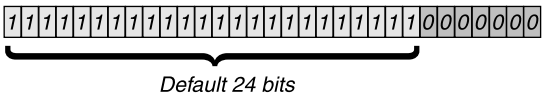


Figure 7-1. A class C address

To specify a netmask, the DSLPipe does not use dotted decimal format, as in:

```
IP Address=198.5.248.40
Netmask=255.255.255.248
```

Instead, it includes a netmask modifier that specifies the total number of network bits in the address. For example:

198.5.248.40/29

In the example address shown above, the /29 specification indicates that an additional 5 bits of the address will be interpreted as a subnet number.

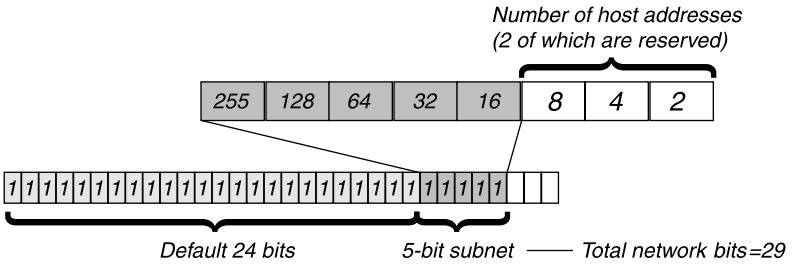


Figure 7-2. A 29-bit netmask and number of supported hosts

Eight bit-combinations are possible in 3 bits. Of those eight possible host addresses, two are reserved:

000 — Reserved for the network base (the cable)
001
010
100
110
101
011
111 — Reserved for the broadcast address of the subnet

Table 7-2 shows how standard subnet address format relates to Ascend notation for a class C network number.

Table 7-2. Standard netmasks and Ascend netmask notation

Netmask	Ascend notation	Number of host addresses
255.255.255.0	/24	254 hosts + 1 broadcast, 1 network base
255.255.255.128	/25	126 hosts + 1 broadcast, 1 network base
255.255.255.192	/26	62 hosts + 1 broadcast, 1 network base

Table 7-2. Standard netmasks and Ascend netmask notation (Continued)

Netmask	Ascend notation	Number of host addresses
255.255.255.224	/27	30 hosts + 1 broadcast, 1 network base
255.255.255.240	/28	14 hosts + 1 broadcast, 1 network base
255.255.255.248	/29	6 hosts + 1 broadcast, 1 network base
255.255.255.252	/30	2 hosts + 1 broadcast, 1 network base
255.255.255.254	/31	invalid netmask (no hosts)
255.255.255.255	/32	1 host — a host route

Note: A host route is a special case IP address with a subnet mask of /32; for example, 198.5.248.40/32. Host routes are required for a dial-in host.

The broadcast address of any subnet is always all ones. The network base address represents the network cable itself, which is always address 0. For example, if the DSLPipe configuration assigns the following address to a remote DSLPipe router:

```
198.5.248.120/29
```

The Ethernet attached to that router has the following address range:

```
198.5.248.120 – 198.5.248.127
```

The "0" address (198.5.248.120) is reserved for the cable itself. The broadcast address is 198.5.248.127, and the router itself uses one of the host addresses. That leaves five remaining host addresses on that remote subnet, which can be assigned in any order to five hosts on that subnet.

As another example, if the DSLPipe configuration assigns the following address to a remote router:

```
192.168.8.64/26
```

The Ethernet attached to that router has the following address range:

```
192.168.8.64 – 192.168.8.127
```

The “0” address for this subnet is 192.168.8.64.The broadcast address must be the network base address plus six ones (six ones in base 2 equals 63 decimal, and 64+63=127) 192.168.8.127.

Connection profiles and IP routes

The DSLPipe creates a routing table when it powers up. It adds all routes it knows about to the table, including connected routes (such as Ethernet) and routes configured in its resident Connection profiles and Static Rtes profiles. If RIP is enabled on Ethernet, it supplies information about routes learned from other routers to the routing table. If RIP is enabled on an active connection, it supplies information about the routes received from the far-end of that connection to the routing table.

There are some static routes that the DSLPipe cannot read at power-up. They do not become part of the routing table until they are up and usable. Such routes include those added via the IPROUTE ADD terminal server command.

How the DSLPipe uses its routing table

When the DSLPipe receives an IP packet whose destination address is not on the local network, it checks its routing table for the destination network and:

- If it finds a route to that network, it forwards the packet to the gateway indicated by that route. If the gateway is not local, the DSLPipe opens a WAN connection to forward the packet.
- If it does not find a route to that network, it forwards the packet to the default router.
- If it does not find a route to that network and no default route has been configured, it drops the packet.

When the DSLPipe receives an incoming IP routing call, it examines the source IP address and looks for a matching profile. If the source matches a resident Connection profile, the DSLPipe updates its routing table, if necessary, with the route to the source network.

If the Answer profile is configured without authentication requirements (an unlikely scenario) and Profile Reqd is set to No, the DSLPipe accepts *any* IP routing connection that comes in. In that case, it does not have a route for the

incoming source IP address, and builds a temporary route using an assumed Class A (8), B (16), or C (24) netmask for the source IP address. If this type of connection is with a router or a host that does not recognize the initial temporary route (that is, one from another manufacturer), you might have to turn on RIP or configure a static route to build a route to that network.

RIP-v2 and RIP-v1 routing

The DSLPipe includes a Routing Information Protocol (RIP) version 2 implementation (RIP-v2), which includes a set of improvements to RIP-v1. You can configure the DSLPipe to send, receive, or send and receive, RIP-v1 or RIP-v2 on Ethernet or any WAN interface.

Note: RIP-v2 is a compatible upgrade to RIP-v1, but do not run RIP-v2 and RIP-v1 on the same network in such a way that the routers receive each other's advertisements. RIP-v1 "guesses" subnet masks, while RIP-v2 handles them explicitly. Running the two versions on the same network can result in RIP-v1 "guesses" overriding accurate subnet information obtained via RIP-v2.

RIP-v2 includes the following improvements to RIP-v1:

- Subnet routing

  The biggest difference between RIP-v1 and RIP-v2 is the inclusion of subnet mask information in RIP-v2 routes.

  RIP-v1 recognized subnet information only within the subnet and purposely did not advertise netmasks to other routers. There was no way to distinguish between a subnet and a host entry except to routers directly connected to the subnet. When a RIP-v1 router receives an IP address, it assumes the default subnet mask.

  RIP-v2 passes the netmask in parallel with the address. This enables support not only of reliable subnet routing, but also of variable length masks within the same network as well as Classless Inter-domain Routing (CIDR).

  If a RIP-v1 router receives a RIP-v2 update that includes netmasks, it ignores the subnet information.

- Authentication

  RIP-v1 provided no way of authenticating its routing advertisements. Any program that transmitted packets on UDP port 520 was considered a router with valid distance vectors.

RIP-v2 packets include an authentication field that can contain a simple password. If a RIP-v1 router receives a RIP-v2 packet that contains a password, it ignores the field.

- Routing domains

  To enable multiple networks to share a common backbone, RIP-v2 uses a routing domain number that enables routers to recognize packets bound for a particular domain number in the router's networks.

- Multicasting

  RIP-v1 uses a broadcast address for sending updates, so its tables are received not only by routers but by all hosts on the cable as well.

  RIP-v2 uses an IP multicast address for periodic multicasts to RIP-v2 routers only. This is one area of possible incompatibility with RIP-v1, because RIP-v1 nodes will probably not receive the multicasts. The DSLPipe can be configured to interact specifically with RIP-v1, although this is not recommended.

Connecting to a local IP network

To connect the DSLPipe to your local IP network, you need to assign the DSLPipe Ethernet interface an IP address. In addition, you might want to perform one or more of the following tasks:

- Enable proxy ARP to let the DSLPipe respond to ARP requests for remote nodes.
- Configure DNS or WINS information to enable users to Telnet in using hostnames.
- Configure the DSLPipe to generate UDP checksums.
- Update other IP routers on the backbone.

Table 7-3 shows the relevant configuration parameters. (For details on each parameter, see the *Reference Guide*, and for information about using RIP on Ethernet, see "Enabling the DSLPipe to use dynamic routing" on page 7-20.)

Table 7-3. IP routing parameters in the Ethernet profile

Location	Parameters with example values
Ethernet > Mod Config> Ether options… (Ethernet profile)	IP Adrs=10.2.3.1/24 2nd Adrs=10.128.8.55/24 Proxy Mode=Off UDP Cksum=Yes
Ethernet > Mod Config > DNS…	Domain Name=abc.com Pri DNS=10.2.3.56/24 Sec DNS=10.2.3.107/24 List Attempt=No
Ethernet > Static Rtes > *any profile* (Static Rtes profile)	Name=xyz.com Active=Yes Dest=198.2.3.0/24 Gateway=198.2.3.4 Metric=2 Preference=100 Private=No

Assigning the Ethernet interface IP address

The DSLPipe Ethernet interface must have a unique IP address that is consistent with the addresses of other hosts and routers on the same network.

To assign the DSLPipe an IP address on the Ethernet:

1. Open the Ethernet profile.
2. Open the Ether Options submenu.
3. Enter the IP address for the DSLPipe Ethernet interface in IP Adrs.
   For example:
   IP Adrs=10.2.3.1
4. Close the Ethernet profile.

After you have configured the IP address, you can Ping the DSLPipe from a host to verify that it is up and running on the network. (How to use the Ping command is described in “Using Ping to verify the address” on page 7-11.)

Creating a subnet for the DSLPipe

On a large corporate backbone, administrators often configure subnets to increase the network address space, segment a complex network, and control routing in the local environment. For example, suppose the main backbone IP network is 10.0.0.0, and supports a Cisco router at 10.0.0.17.

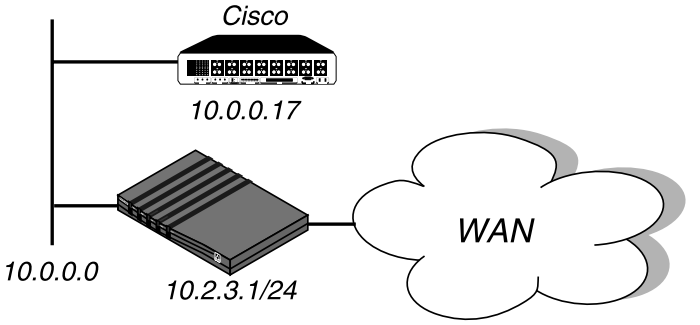


Figure 7-3. Creating a subnet for the DSLPipe

You can place the DSLPipe on a subnet of that network by entering a subnet mask in its IP address specification, for example:

1 Open the Ethernet profile.

2 Open the Ether Options submenu.

3 Enter the IP address for the DSLPipe Ethernet interface in the IP Adrs field.
For example:
IP Adrs=10.2.3.1/24

4 Close the Ethernet profile.

With this subnet address, the DSLPipe requires a static route to the backbone router on the main network. Otherwise, it can only reach the subnets to which it is directly connected.

To create the static route and make the backbone router the default route:

1 Open the Static Rtes menu.

2 Open the Default profile.

3 Specify the IP address of a backbone router in the Gateway field.
For example:

Gateway=10.0.0.17

4 Leave the other parameters at their default values.
For example:
Active=Yes
Dest=0.0.0.0/0
Metric=1
Private=Yes

5 Close the Default Static Rtes profile.

Assigning two addresses: Dual IP

The DSLPipe can assign two separate IP addresses to a single physical Ethernet port and route between them—a feature often referred to as “dual IP.” The two addresses provide logical interfaces to two networks or subnets on the same backbone.

Usually devices connected to the same physical wire belong to the same IP network. With dual IP, one wire can support two IP networks. Devices on the wire are assigned to one network or the other. The devices route information to each other through the DSLPipe.

Dual IP is also used to distribute the load of routing traffic to a large subnet by assigning IP addresses on that subnet to two or more routers on the backbone. With a direct connection to the subnet as well as to the backbone network, each of the routers routes packets to devices on the subnet and includes the route in their routing table updates.

Dual IP also allows you to make a smooth transition when changing IP addresses. That is, a second IP address can act as a placeholder while IP addresses are changed on other network equipment.

Figure 7-5 shows two routers configured with a second address on the same subnet.

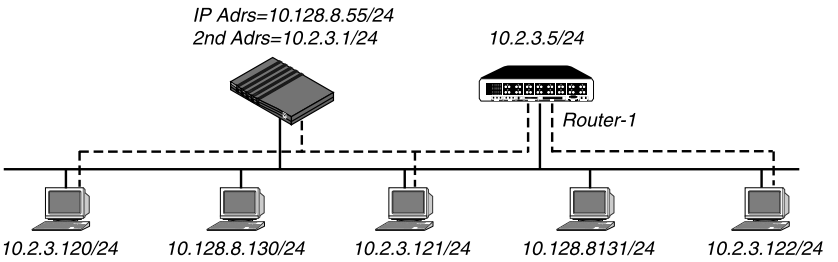


Figure 7-4. Dual IP and shared subnet routing

Note: The second IP address is also sometimes used to provide a placeholder address while the local IP network switches to a different network address.

To assign two addresses to the DSLPipe Ethernet interface:

1. Open the Ethernet profile.
2. Open the Ether Options submenu.
3. Enter the IP address for the DSLPipe Ethernet interface in the IP Adrs field.
   For example:
   IP Adrs=10.2.3.1/24
4. Type the second IP address in the 2nd Adrs field.
   For example:
   IP Adrs=10.128.8.55/24
   After you have configured the IP addresses, you can Ping the addresses from another IP host on each of the IP subnets to verify that both logical interfaces are accessible.

   Note: For other routers to recognize the DSLPipe on either of its two networks, you must either turn on RIP on the Ethernet interface or configure static routes in those routers.
5. Close the Ethernet profile.

Using Ping to verify the address

The Ping command sends an Internet Control Message Protocol (ICMP) mandatory echo request datagram, which asks the remote station “Are you

there?" If the echo request reaches the remote station, the station sends back an ICMP echo response datagram, which tells the sender "Yes, I am alive." This exchange verifies that the transmission path is open between the DSLPipe and another station.

To verify that the DSLPipe is up on the local network, invoke the terminal server interface and enter this command:

```
ping <host-name>
```

For example:

```
ping 10.1.2.3
```

You can terminate the Ping exchange at any time by pressing Ctrl-C. (For more information about verifying that a device is on the network, see Chapter 6, "Setting up Bridging.")

Enabling proxy mode in the DSLPipe

When a dial-in host has an IP address on the same network as the DSLPipe, only the DSLPipe keeps track that packets addressed to the host must be routed across the WAN. To other local routers and hosts, the address appears to be on the local network. Therefore, they might broadcast Address Resolution Protocol (ARP) requests on the local network expecting the apparently local host to respond with its physical address. Because the host is not really local, it cannot receive the requests. But if the DSLPipe is in Proxy Mode, serving as a proxy for the remote host, it responds with its own physical address.

To enable the DSLPipe to respond to ARP requests for remote devices that have local IP addresses:

1. Open the Ethernet profile.
2. Open the Ether Options submenu.
3. Turn on Proxy Mode.
   If the IP addresses were assigned dynamically, use this setting:
   Proxy Mode=Active
   If the IP addresses are assigned statically, use this setting instead:
   Proxy Mode=Always
4. Close the Ethernet profile.

Enabling DNS on the DSLPipe

If the local network supports Domain Name System (DNS) servers, you can configure the local domain name and the IP addresses of those servers in the Ethernet profile.

If the DSLPipe is configured for DNS, users can execute TCP/IP commands such as Telnet and Ping from the DSLPipe terminal server interface with host names instead of IP addresses. In addition, the List Attempt parameter helps avoid tearing down physical links by enabling the user to try one entry in the DNS list of hosts, and if that connection fails, to try the next entry, and so on.

To configure the DSLPipe for DNS:

1 Open the Ethernet profile.

2 Open the DNS submenu.

3 Enter your domain name.
For example:
Domain Name=eng.abc.com

4 Specify the IP address of the primary and secondary DNS servers.
For example:
Pri DNS=10.2.3.56
Sec DNS=10.2.3.107

5 If your site supports multiple addresses for a DNS host name, turn on List Attempt.
List Attempt=Yes

6 Close the Ethernet profile.

Generating UDP checksums

User Datagram Protocol (UDP) supports the optional use of a checksum field for checking the integrity of both the UDP header and data. The DSLPipe always checks the UDP checksum field of each UDP packet it receives, and generates Ethernet and PPP checksums for the appropriate packets. However, it does not generate UDP checksums unless you set the UDP Cksum parameter.

You should turn on UDP checksums if data integrity is of the highest concern for your environment and you need redundant checks. UDP checksums are also appropriate if your UDP-based servers are located on the remote side of a WAN link that is prone to errors.

Currently the DSLPipe uses UDP when generating queries and responses for the following protocols:

- SYSLOG
- DNS
- ECHOSERV
- RIP
- SNTP
- TFTP

To configure the DSLPipe to generate checksums for these packets:

1 Open the Ethernet profile.

2 Turn on UDP checksums.
UDP Cksum=Yes

3 Close the Ethernet profile.

Updating other routers on the backbone

If you want to update the routing tables of other local routers whenever the DSLPipe brings up a remote connection, configure the DSLPipe to send RIP updates over the Ethernet interface. The DSLPipe then broadcasts RIP packets containing information about each route change. RIP updates are sent every 30 seconds, so within a minute or so, all routers on the local network are informed about the new route. You can also configure the DSLPipe to receive RIP updates on Ethernet, or to both send and receive the updates. (For instructions, see “Configuring RIP-v2 on Ethernet” on page 7-21.)

Managing the routing table

The DSLPipe routing table is created when the DSLPipe powers up. (Which routes are included and when is discussed in “Connection profiles and IP routes” on page 7-5.) To manage the routing table, you might want to perform one or more of the following tasks:

- Configure static routes in IP Route and Connection profiles.
- Configure a default route for packets with an unknown destination.
- Turn off ICMP Redirects or understand how they can affect the routing table.
- Configure RIP-v1 or RIP-v2 on Ethernet.
- Turn off RIP on WAN connections or learn how it affects the routing table.
- Assign a preference for RIP or static routes (known as route preferences).
- Display the routing table and understand its entries.

Parameters that affect the routing table

Table 7-4 shows parameters that affect the DSLPipe IP routing table. (For details about each parameter, see the *Reference Guide*.

Table 7-4. IP routing connections and routing parameters

Location	Parameters with example values
Ethernet > Mod Config (Ethernet profile)	RIP Policy=Poison Rvrs (RIP-v1 only) RIP Summary=Yes (RIP-v1 only) ICMP Redirects=Accept Adv Dialout Routes=Trunks Up
Ethernet > Mod Config > Ether options…	IP Adrs=10.2.3.2/245 2nd Adrs=0.0.0.0/0 RIP=Both-v2 Ignore Def Rt=No
Ethernet > Connections > *any profile* > (Connection profile)	Route IP=Yes

Table 7-4. IP routing connections and routing parameters

Location	Parameters with example values
Ethernet > Connections > *any profile* > IP options…	LAN Adrs=10.9.8.10/22 WAN Alias=0.0.0.0 Metric=1 Preference=100 Private=No RIP=Off
Ethernet > Static Rtes > *any profile* (Static Rtes profile)	Name=SITEBGW Active=Yes Dest=10.2.3.0/24 Gateway=10.2.3.4 Metric=2 Preference=100 Private=No
Ethernet > Answer > PPP options…	Route IP=Yes
Ethernet > Answer > Session options…	RIP=Both-v2

Note: When more than one DSLPipe is in use in redundant configurations on the same network, you can use the Adv Dialout Routes parameter to instruct the DSLPipe to stop advertising IP routes that use dial services if for any reason its trunks are in the alarm condition. If one of the redundant DSLPipe units loses its dialout lines temporarily, and the Adv Dialout Routes parameter is set to Always, that unit continues to receive outbound packets that should be forwarded to the redundant DSLPipe. To prevent the problem, set Adv Dialout Routes to Trunks Up. For details on these parameters, see the *Reference Guide*.

Static and dynamic routes

A static route is a path from one network to another, which specifies the destination network and the router to use to get to that network. For routes that must be reliable, the administrator often configures more than one path (adds a secondary route), in which case the DSLPipe chooses the primary route on the basis of an assigned metric.

A dynamic route is a path to another network that is "learned" dynamically rather than configured in a profile. A router that uses RIP broadcast its entire routing table every 30 seconds, updating other routers about which routes are usable. Hosts that run ICMP can also send ICMP Redirects to offer a better path to a destination network.

Note: A dynamic route can overwrite or "hide" a static route to the same network if the dynamic route's metric is lower than that of the static route. However, dynamic routes age and if no updates are received, they eventually expire. In that case, the "hidden" static route reappears in the routing table.

Configuring static routes

Every Connection profile that specifies an explicit IP address is a static route. The network diagram in Figure 7-5 shows a static route to a subnet specified in the LAN Adrs parameter (10.9.8.10/22) of a Connection profile. With this LAN Adrs parameter setting, the implied static route is defined with the following addresses:

- Dest=10.9.8.10/22
- Gateway=10.9.8.10

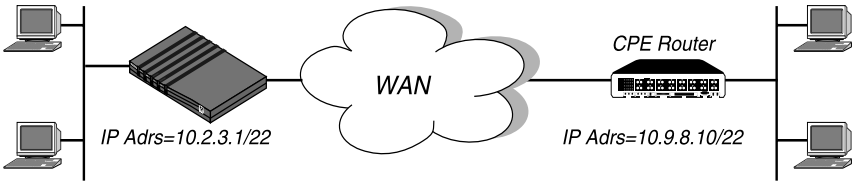


Figure 7-5. An IP routing connection serving as a static route

Note: If you do not specify the netmask in the LAN Adrs parameter, the DSLPipe inserts a default netmask which assumes the entire far-end network is accessible. Normally, if the far-end router's address includes a netmask, you should include it.

When RIP is turned off in a Connection profile, the DSLPipe does not listen to RIP updates across that connection. To route to other networks through that connection, it must rely on a Static Rtes profile. The network diagram in

Figure 7-6 shows a remote network that does not have its own Connection profile, but can be reached through an existing Connection profile.

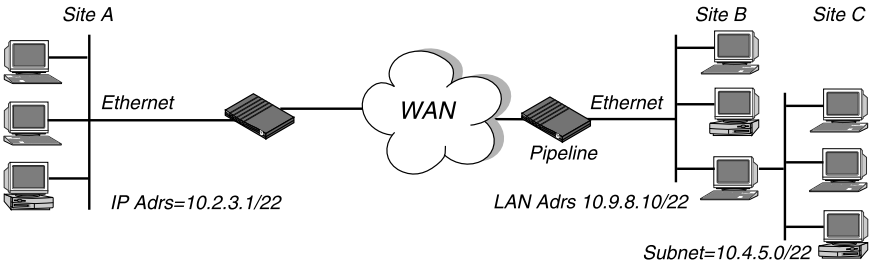


Figure 7-6. A two-hop connection that requires a static route when RIP is off

In the example network shown in Figure 7-6, if RIP is off in the Connection profile for site B, the DSLPipe must have a Static Rtes profile to site C. A sample profile is shown below:

```
Name=sitec-net
Active=Yes
Dest=10.4.5.6/22
Gateway=10.9.8.10
Metric=2
Private=Yes
```

Creating a Static Rtes profile

To configure a Static Rtes profile:

1. Open the Static Rtes menu.
2. Open an Static Rtes profile.
3. Assign the route a name.
   For example:
   Name=victor-gw
4. Specify that the route should be added to the routing table.
   Active=Yes
5. Specify the destination network.
   For example:
   Dest=10.210.1.30/12

The DSLPipe must have a Connection profile that specifies this address.

If the address includes a netmask, 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:

Dest=10.0.0.0

6 Specify the address of the router to use for that destination.

For example:

Gateway=10.9.8.10

This parameter states that the path to the destination subnet is through the IP router at 10.9.8.10.

7 Specify a metric for this route.

For example:

Metric=1

RIP uses distance vector metrics, so the metric is interpreted like a hop count. If the DSLPipe has more than one possible route to a destination network, it chooses the one with the lower metric.

8 Specify whether this route is private.

For example:

Private=No

This setting specifies that the DSLPipe will disclose the existence of the route when queried by RIP or another routing protocol.

9 Close the Static Rtes profile.

Configuring the default route

If no routes exist for the destination address of a packet, the DSLPipe forwards the packet to the default route. Most sites use the default route to specify a local IP router (such as a Cisco router or a UNIX host running the route daemon). This helps to offload routing tasks to other devices.

Note: If there is no default route, the DSLPipe drops packets for which it has no route. By default, the DSLPipe uses the value you entered for the Rem Adr parameter in the Configure Profile as the default gateway.

To configure the default route:

1 Open the Static Rtes menu.

2 Open the first Static Rtes profile.

   The name of that profile is always Default, and its destination is always 0.0.0.0 (you cannot change these values).

3 Specify that the route should be added to the routing table.

   Active=Yes

4 Specify the address of the router to use for packets with unknown destinations.

   For example:

   Gateway=10.9.8.10

5 Specify a metric for this route.

   For example:

   Metric=1

6 Specify whether this route is private.

   For example:

   Private=Yes

   This setting specifies that the DSLPipe will not disclose the existence of the route when queried by RIP or another routing protocol.

7 Close the Static Rtes profile.

Enabling the DSLPipe to use dynamic routing

In addition to RIP, the DSLPipe can use Internet Control Message Protocol (ICMP) Redirects to acquire routes dynamically. ICMP dynamically determines the best IP route to a destination network or host and uses ICMP redirect packets to transfer packets over a more efficient route. ICMP redirect packets are one of the oldest route discovery methods on the Internet and one of the least secure, due to the possibility of receiving counterfeit ICMP redirects. You can configuring the DSLPipe to ignore ICMP redirects to promote security.

To ignore ICMP redirects:

1 Open the Ethernet profile.

2 Make sure that ICMP redirects are not accepted.

   ICMP Redirects=Ignore

3 Close the Ethernet profile.

If you are using RIP-v1

The Internet Engineering Task Force (IETF) has voted to move RIP-v1 into the "historic" category so its use is no longer recommended. You can upgrade all routers and hosts to RIP-v2. If you need to maintain RIP-v1, create a separate subnet and place all RIP-v1 routers and hosts on that subnet.

Note: RIP Policy and RIP Summary are relevant only to RIP-v1 and should not be set when interacting with RIP-v2 routers.

If the DSLPipe Ethernet interface is on a RIP-v1 subnet:

1. Open the Ethernet profile.
2. Open the Ether Options submenu.
3. Turn on RIP-v1.

   For example:

   RIP=Both-v1

   This setting means that the DSLPipe transmits and receives RIP-v1 updates on the local Ethernet. If you do not want the DSLPipe to be informed about local routing changes (for example, if all local routing is handled by a default router), you can use the following setting instead:

   RIP=Send-v1

   Or, if you do not want the DSLPipe to transmit its WAN connections to the RIP-v1 routers on the local subnet:

   RIP=Recv-v1
4. Set Ignore Def Rte to Yes.

   The default route specifies a static route to another IP router, which is often a local router such as a Cisco or another DSLPipe. When the Ignore Def Rte parameter is set to Yes (recommended), RIP updates will not modify the default route in the DSLPipe routing table.
5. Close the Ethernet profile.

Configuring RIP-v2 on Ethernet

To turn on RIP-v2 on the local Ethernet:

1. Open the Ethernet profile.
2. Open the Ether Options submenu.

3 Turn on the RIP parameter.

For example:

RIP=Both-v2

This setting means that the DSLPipe transmits and receives RIP-v2 updates on the local Ethernet. If you do not want the DSLPipe to be informed about local routing changes (for example, if all local routing is handled by a default router), you can use the following setting instead:

RIP=Send-v2

4 Set Ignore Def Rte to Yes.

The default route specifies a static route to another IP router, which is often a local router such as a Cisco or another DSLPipe. When the Ignore Def Rte parameter is set to Yes (recommended), RIP updates will not modify the default route in the DSLPipe routing table.

5 Close the Ethernet profile.

Configuring RIP for incoming WAN connections

Many sites turn off RIP on the WAN interface because it tends to cause very large local routing tables. If RIP is enabled to both send and receive RIP updates over the WAN interface, the DSLPipe broadcasts its routing table to the remote network and listens for RIP updates from that network. Gradually, all routers on both networks implement consistent routing tables (all of which may become quite large).

To configure the Answer profile for RIP and IP routing:

1 Open the Answer profile.

2 Open the PPP Options submenu.

3 Turn on IP routing.

Route IP=Yes

4 Open the Session Options submenu.

5 Turn on the RIP parameter.

For example:

RIP=Recv-v2

This setting means that the DSLPipe receives RIP-v2 updates across incoming connections with other IP routers. If you do not want the DSLPipe to accept RIP updates on the WAN, use the following settings:

RIP=Off

6 Close the Answer profile.

Configuring RIP for a particular connection

You can turn off RIP for a particular connection by configuring it in the Connection profile.

Note: Because RIP updates are sent every 30 seconds, you should configure WAN connections that use RIP with the Idle value set to less than 30 or apply a Call filter for RIP updates on the WAN. Otherwise, those connections never disconnect, because RIP traffic resets the Idle timer.

To configure a Connection profile for RIP and IP routing:

1 Open the Connection profile.

2 Turn on IP routing.

Route IP=Yes

3 Open the IP Options submenu.

4 Turn on the RIP parameter.

For example:

RIP=Recv-v2

This setting means that the DSLPipe receives RIP-v2 updates from the other IP router.

If the remote router is running RIP-v1 and the local network is running RIP-v2, or if you simply do not want the DSLPipe to send or receive RIP updates on this connection, use the following setting:

RIP=None

5 Close the Connection profile.

Route preferences

If multiple routes exist for a given address and netmask pair, the route with the lower Preference is better. If two routes have the same Preference, then the lower Metric is better. When choosing which routes should be put in the routing table, the router first compares their Preference values, preferring the lower number. If the Preference values are equal, the router then compares the Metric field, and

uses the route with the lower Metric. Other routes remain latent or “hidden,” and are used in case the best route is removed.

The default route preferences are as follows:

- Connected routes, such as Ethernet, have a Preference=0.
- Routes learned from ICMP Redirects have a Preference=30.
- A static route has a Preference=100.
  You can modify the default in the Connection or Static Rtes profile.
- Routes learned from RIP have a Preference=100.
- Routes placed in the table by SNMP MIB II have a Preference=100.

Setting the route preference of a WAN connection

By default, the static route associated with a Connection or Static Rtes profile has a preference value of 100. Static routes and RIP routes therefore have equal value, with ICMP Redirects (if the unit accepts them) taking precedence over both.

To specify that the static route configured in a Connection profile takes precedence over a route to the same destination learned from RIP:

1 Open the Connection profile.

2 Open the IP Options submenu.

3 Specify a preference value lower than 100.
For example:
LAN Adrs=10.9.8.10/22
WAN Alias=0.0.0.0
Metric=5
Preference=50
Private=No
RIP=Off

4 Close the Ethernet profile.

Viewing the routing table

The IPROUTE SHOW terminal-server command includes information relevant to multiple IP routing protocols. To view the IP routing table, invoke the terminal server interface and at the prompt, enter:

```
iproute show
```

The output looks similar to the following table:

Table 7-5. Sample output from the IPROUTE SHOW command

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	-	ie0	CP	0	0	389	20887
255.255.255.255/32	-	ie0	CP	0	0	0	20887

The column headings shown here are described in “Fields in the routing table” on page 7-26. The routes in this table are:

Destination	Gateway	IF	Flg	Pref	Met	Use	Age
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 Static Rtes profile for the default route specifies a Preference of 1, so this route is preferred over dynamically learned routes.

Destination	Gateway	IF	Flg	Pref	Met	Use	Age
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.

Destination	Gateway	IF	Flg	Pref	Met	Use	Age
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.

Destination	Gateway	IF	Flg	Pref	Met	Use	Age
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.

Destination	Gateway	IF	Flg	Pref	Met	Use	Age
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.

Destination	Gateway	IF	Flg	Pref	Met	Use	Age
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.

Destination	Gateway	IF	Flg	Pref	Met	Use	Age
10.1.2.1/32	-	ie0	CP	0	0	389	20887

This is another loopback route, a host route with the local Ethernet address. It is private, so it will not be advertised.

Destination	Gateway	IF	Flg	Pref	Met	Use	Age
255.255.255.255/32	-	ie0	CP	0	0	0	20887

This is a private route to the broadcast address. It is used in cases where the router needs to broadcast a packet but is otherwise unconfigured. The route is typically used when trying to locate a server on a client machine to handle challenges for a token security card.

Fields in the routing table

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 DSLPipe 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) do not have a gateway address.

- 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.

  – wan*n* specifies one 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 (Placed in the table via SNMP MIB II.)

  – R (A RIP dynamic route.)

  – S=Static (A locally configured Static Rtes profile or Connection profile route.)

  – ?=Unknown (Indicates an error.)

  – G=Gateway (A gateway is required in order to reach this route.)

  – P=Private (This route will not be advertised via RIP.)

  – T=Temporary (This route will be destroyed when its interface goes down.)

  – *=Hidden (A hidden route means that there is a better route in the table, so this route is hidden “behind” the better route. If the better route goes down, then this route might be used.)

- 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. (For instructions, see “Route preferences” on page 7-23.)

- Metric

  The Metric column shows the RIP-style metric for the route, with a valid range of zero to 16.

- Use

  This is a count of the number of times the route has been referenced since it was created. (Many of the references are internal, so this is not a count of the number of packets sent using this route.)

  Unused routes are indicated by a 0 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 (referred to as “flapping”).

Setting up IPX Routing

8

Introduction to DSLPipe IPX routing

To support Internet Packet Exchange (IPX) routing between sites that run Novell NetWare version 3.11 or later, the DSLPipe operates as an IPX router with one interface on the local Ethernet and the other across the wide-area network (WAN). Each IPX Connection profile is an IPX WAN interface.

The most common uses for IPX routing in the DSLPipe are to:

- Integrate multiple NetWare local-area networks (LANs) to form an interconnected WAN.
- Allow dial-in NetWare clients to access local NetWare services.

The DSLPipe supports IPX routing over Point-to-Point Protocol (PPP), Multilink PPP (MP), and frame relay connections. Support for both the IPXWAN and PPP Internet Protocol Control Protocol for IPX (IPXCP) makes the DSLPipe fully interoperable with other vendors' products that conform to these protocols and associated RFCs.

Note: IPX can be transmitted using different frame types. The DSLPipe routes only one IPX frame type, and it routes and spoofs IPX packets only if they are encapsulated in that type of frame. If bridging is enabled in the same Connection profile as IPX routing, the DSLPipe will bridge any other IPX-packet frame types. (For more information see Chapter 6, "Setting up Bridging.")

Unlike an IP routing configuration, where the DSLPipe uniquely identifies the calling device by its IP address, an IPX routing configuration does not include a built-in way to uniquely identify callers. For that reason, password authentication

is required unless IP routing is configured in the same Connection profile. (For details, see Chapter 9, “Setting up Security,”)

IPX Service Advertising Protocol (SAP) tables

The DSLPipe follows standard IPX SAP behavior for routers. However, when the connection is to another DSLPipe configured for IPX routing, both ends of the connection exchange their entire SAP tables, so all remote services are immediately added to each unit’s SAP table.

NetWare servers broadcast SAP packets every 60 seconds to make sure that routers know about their services. Routers build a SAP table with an entry for each service advertised by each known server. When a router stops receiving SAP broadcasts from a server, it ages the SAP-table entry and eventually removes it from the table.

Routers use SAP tables to respond to client queries. When a NetWare client sends a SAP request to locate a service, the DSLPipe consults its SAP table and replies with its own hardware address and the internal address of the requested server (similar to proxy mode in an IP environment, described on page 7-12).

The client can then transmit packets whose destination address is the internal address of the server. When the DSLPipe receives those packets, it consults its RIP table. If it finds an entry for that destination address, it brings up the connection or forwards the packet across the active connection.

IPX Routing Information Protocol (RIP) tables

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.

The DSLPipe follows standard IPX RIP behavior for routers when connecting to other-vendor units. However, when it connects to another DSLPipe configured for IPX routing, both ends of the connection immediately exchange their entire RIP tables. In addition, the DSLPipe maintains those RIP entries as static until the unit is reset or power-cycled.

The destination of an IPX route is the internal network of a server. For example, NetWare file servers are assigned an internal IPX network number by the

network administrator and typically use the default node address of 000000000001. This is the destination network address for file read/write requests. (If you are not familiar with internal network numbers, see your NetWare documentation for more information.)

IPX routers broadcast RIP updates periodically and whenever a WAN connection is established. The DSLPipe receives RIP broadcasts from a remote device, adds 1 to the hop count of each advertised route, updates its own RIP table, and broadcasts updated RIP packets on connected networks in a split-horizon fashion.

The DSLPipe recognizes network number –2 (FFFFFFFE hex) as the IPX RIP default route, and forwards any packet with an unrecognized address to the IPX router advertising that default route.For example, if the DSLPipe receives an IPX packet destined for network 77777777 and it does not have a RIP table entry for that destination, the DSLPipe forwards the packet towards network number FFFFFFFE, if available, instead of simply dropping the packet. If more than one IPX router is advertising the default route, the DSLPipe bases its routing decision on Hop and Tick count.

Extensions to standard IPX

NetWare uses dynamic routing and service location to let clients locate a server dynamically, regardless of where it is physically located. This scheme is designed for LAN environments. For WAN functionality, the DSLPipe provides the following extensions to standard IPX:

- Dial Query
- Watchdog spoofing
- Virtual IPX network defined for dial-in clients
- IPX Route profiles
- IPX SAP filters

Table 8-1 shows the parameters related to the DSLPipe IPX extensions:

Table 8-1. DSLPipe extensions to standard IPX routing

Location	**Parameters with example values**
Ethernet > Connections > *any profile* > IPX options... (Connection profile)	Peer=Dialin (for dynamic addressing) IPX RIP=None IPX SAP=Send Dial Query=No Handle IPX=Client (IPX client bridging) Netware t/o=30 (watchdog spoofing)
Ethernet > Mod Config > Ether options... (Ethernet profile)	IPX Pool #=CFCF1234
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
Ethernet > IPX SAP filters > *any profile* (IPX SAP filter profile)	Name=optional Input SAP filters... Output SAP filters Valid=Yes Type=Exclude Server Type=0004 Server Name=SERVER-1

For information about the Handle IPX parameter and IPX bridging, see Chapter 6, “Setting up Bridging.” For details on other parameters, see the *Reference Guide* and the discussion below.

Dial Query

Dial Query is a Connection profile parameter that instructs the DSLPipe to bring up that connection when it receives a SAP query for service type 0004 (a file server) when that service type is not present in the DSLPipe SAP table. If the DSLPipe has no SAP table entry for service type 0004, it brings up every connection that has Dial Query set to Yes. For example, if five Connection profiles have Dial Query set to Yes, the DSLPipe brings up all five connections in response to the query.

Note: If the DSLPipe has a static IPX route to a remote server, it will bring up that connection instead of the more costly solution of bringing up every connection that has Dial Query set.

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 to watchdog packets for a certain amount of time, the server logs the client out.

Repeated watchdog packets can cause a WAN connection to stay active. But if the DSLPipe filters out the packets, client logins are dropped by the remote server. To prevent repeated client logouts while allowing WAN connections to be brought down in times of inactivity, the DSLPipe responds to watchdog requests as a proxy for remote IPX routed or bridged clients. Responding to NCP requests is commonly called watchdog spoofing. To the server, a spoofed connection looks like a normal, active client login session, so it does not log the client out.

When a remote client link goes down, the timer begins counting. When the value of the Netware t/o (timeout) field is reached, the DSLPipe stops responding to watchdog packets for the client, and the connection is released by the server. If there is a reconnection of the WAN session before the timeout value is reached, the timer is reset.

Note: The DSLPipe software filters IPX watchdog packets automatically on all IPX routing connections and all IPX bridging connections that have watchdog spoofing enabled. The DSLPipe applies a call filter implicitly, which prevents the idle timer from resetting when IPX watchdog packets are sent or received. This filter is applied after the standard data and call filters.

IPX Route profiles

Static IPX routes are specified in IPX Route profiles. When the DSLPipe unit's RIP and SAP tables are cleared due to a reset or power-cycle, the static routes are added when the unit initializes. Each static route contains the information needed to reach one server.

When the DSLPipe is connecting to another DSLPipe, you can choose not to configure a static route. Instead, you can use the DO menu to manually dial the initial connection to that site following a power-cycle or reset. Once connected, the DSLPipe downloads the RIP table from the remote site and maintains the routes as static until the next power-cycle or reset.

Static routes need manual updating whenever the specified server is removed or has an address change. However, static routes are a way to ensure that the DSLPipe can bring up the appropriate connection in response to clients' SAP requests and to prevent timeouts when a client takes a long time to locate a server on the WAN. (For more information, see "Configuring a static IPX route" on page 8-14.)

IPX SAP filters

You may not want the DSLPipe SAP table to include long lists of all servers available at a remote site. IPX SAP filters let you exclude services from the SAP table, or explicitly include certain services.

SAP filters can be applied to inbound or outbound SAP packets. Inbound filters control which services are added to the DSLPipe unit's SAP table from advertisements on a network link. Outbound filters control which services the DSLPipe advertises on a particular network link. (For more information, see "Managing IPX SAP filters" on page 8-17.)

WAN considerations for NetWare client software

In most cases, NetWare clients on a wide-area network do not need special configuration. But the following issues sometimes affect NetWare clients in an 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. (For more information, see your NetWare documentation.)

- Local copy of LOGIN.EXE

  Due to possible performance issues, executing programs remotely is not recommended. You should 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, they should have PBURST.NLM loaded. (For more information, see your NetWare documentation.)

- Macintosh or UNIX clients

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

  If Macintosh clients need to access NetWare servers across the WAN using AppleTalk (rather than MacIPX), the WAN link must support bridging, or else the AppleTalk packets will not make it across the connection.

  If UNIX clients need to access NetWare servers using TCP/IP (rather than UNIXWare), the DSLPipe must be configured as a bridge or IP router, or else the TCP/IP packets will not make it across the connection.

Adding the DSLPipe to the local IPX network

To connect the DSLPipe to your local IPX network, you must perform the following tasks:

- Turn on IPX routing.
- Specify the IPX frame type the DSLPipe will route and watchdog spoof.
- Specify the DSLPipe IPX network number (or allow it to learn the number from other routers).

In addition, you might want to define an IPX network number for dial-in clients. Table 8-2 shows IPX routing parameters configured in the Ethernet profile.

Table 8-2. IPX routing parameters in the Ethernet profile

Location	Parameters with example values
Ethernet > Mod Config (Ethernet profile)	IPX Routing=Yes
Ethernet > Mod Config > Ether options...	IPX Frame=802.2 IPX Enet #=00000000 IPX Pool #=cccc1234 IPX SAP Filter=1

For details on each parameter, see the *Reference Guide*.

Checking local NetWare configurations

IPX packets are supported in more than one Ethernet frame type on an Ethernet segment. However, the DSLPipe can only route and perform watchdog spoofing for the IPX frame type you specify. (It will bridge other IPX packet types if bridging is enabled.)

To check the IPX configuration of a NetWare server on the local Ethernet:

1. Go to the NetWare server's console.
2. Type LOAD INSTALL to view the AUTOEXEC.NCF file.
3. Look for lines similar to these:

```
internal network 1234
Bind ipx ipx-card net=CF0123FF
Load 3c509 name=ipx-card frame=ETHERNET_8023
```

The first line specifies the internal network number of the server. If you are not familiar with internal network numbers, see your NetWare documentation. The DSLPipe does not require internal network numbers.

The "Bind" line specifies the IPX network number in use on the Ethernet. The DSLPipe must use the same IPX network number for its Ethernet interface. You

can specify the number explicitly in the DSLPipe Ethernet profile, or leave the DSLPipe number set to zero to enable it to "learn" the number from other routers.

The "Load" 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 your NetWare documentation.

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

Configuring IPX on the DSLPipe Ethernet interface

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

To turn on IPX routing in the DSLPipe:

1. Open the Ethernet profile.
2. Turn on IPX routing:

   ```
   IPX Routing=Yes
   ```

To specify the IPX frame type:

3. Open the Ether Options submenu.
4. Select the IPX frame type.

   For example:

   ```
   IPX Frame=802.2
   ```

   Note: Make sure that the type you choose is consistent with the frame type in use by most servers on the local network.

To allow the DSLPipe to learn its IPX network number:

5. Set the IPX Enet number to zero.

   ```
   IPX Enet #=00000000
   ```

This causes the DSLPipe to listen for its network number and acquire it from another router. Or you can enter an IPX network number other than zero, for example:

```
IPX Enet #=C90AB997
```

Note: If you specify an IPX network number other than zero, the DSLPipe becomes a "seeding" router and other routers can learn their number from the DSLPipe. In that case, make sure that the number you enter is the same one used by other IPX routers on the same network. (For more information about seeding routers, see the you NetWare documentation.)

6 Close the Ethernet profile.

You can IPXPing the DSLPipe from a NetWare server or client to verify that it has acquired its IPX address and is up and running on the network.

Using IPXPing to check the configuration

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

Enter the IPXPING command in this format:

ipxping *hostname*

where *hostname* is either the IPX address of the NetWare workstation or the advertised name of a server. The IPX address consists of the IPX network and node numbers for a station, as in:

ipxping CFFF1234:000000000001

If you are using IPXPing to verify connectivity with an advertised NetWare server, you can simply enter the name of the server, as in:

ipxping server-1

You can terminate the IPXPing at any time by pressing Ctrl-C.

Defining a virtual IPX network for dial-in clients

Dial-in clients do not belong to an IPX network, so they must be assigned an IPX network number to establish a routing connection with the DSLPipe. To provide an IPX network number for dial-in clients, you must define a virtual IPX network in the Ethernet profile. The DSLPipe advertises the route to this virtual network and assigns it as the network address for dial-in clients.

Note: The most common configuration mistake on NetWare internetworks is in assigning duplicate network numbers. Make sure that the network number you specify in the IPX Pool# field is unique within the entire IPX routing domain of the DSLPipe unit.

To configure the DSLPipe with an IPX network for dial-in clients:

1. Open the Ethernet profile.
2. Open the Ether Options submenu.
3. Set the IPX Pool # parameter to a 32-bit hexadecimal IPX network number that is unique within your entire IPX routing domain.

   For example:

   ```
   IPX Pool #=cccc1234
   ```
4. Close the Ethernet profile.

Working with the RIP and SAP tables

In managing the RIP and SAP tables, you might want to perform one or more of the following tasks:

- View the RIP and SAP tables
- Configure RIP in a Connection profile
- Configure a static route
- Configure SAP in a Connection profile
- Define and apply an IPX SAP filter

Discussion about performing each of these tasks follows. Additionally, you might want to define standard call filters or data filters to control WAN traffic and

connections. Call and data filters are discussed in Chapter 10, “Setting up Filters.”

Viewing the RIP and SAP tables

To see the current RIP table, invoke the terminal server (described on page 11-13) and type:

```
show netware networks
```

The current RIP table will be displayed, and will be similar to the following:

```
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
```

The RIP table includes these fields:

- Network. Internal network number of a NetWare server.
- Next Router. Address of an IPX router used to forward packets to that server.
- Hops. Hop count to the destination network (server).
- Ticks. Tick count (18 ticks/second) to the destination network (server). Best routes are calculated on the basis of tick count, not hop count.
- Origin. Name of the Connection profile used to reach the server.

To see the current IPX SAP table, in the terminal server, type the following:

```
show netware servers
```

You'll see a SAP table similar to the following:

```
        IPX address                    type      server name
EE000001:000000000001:0040             026b      SERVER1___
EE000001:000000000001:4510             0004      NOVL1
EE000001:000000000001:4005             0278      SERVER2____
A30E0A04:000000000001:8060             0047      EPS_0E0A04
A30E1347:000000000001:8060             0047      EPS_0E1347
A30E0EB8:000000000001:8060             0047      EPS_0E0EB8
A30EB294:000000000001:8060             0047      EPS_04B294
```

Fields in the SAP table, and their contents, are:

- IPX Address. IPX address of one server.
  The IPX address uses the following format:
  network number:*node number*:*socket number*
- Service Type. Hexadecimal value representing a type of NetWare service. For example, the number for file servers is 0004.
- Server Name. Server's name (up to 35 characters).

Configuring RIP in a Connection profile

By default, the IPX RIP parameter in a Connection profile is set to Both, indicating that RIP broadcasts will be exchanged in both directions. You can disable the exchange of RIP broadcasts across a WAN connection, or specify that the DSLPipe will only send or only receive RIP broadcasts on that connection. (If the DSLPipe does not receive RIP broadcasts from a remote unit, you should configure a static route to at least one server on that network. See "Configuring a static IPX route" on page 8-14.)

To restrict RIP exchanges across a WAN connection:

1 Open a Connection profile that has IPX routing enabled.

2 Open the IPX Options submenu.

3 Set the IPX RIP parameter to a value other than the default setting of Both. For example:

```
IPX RIP=Recv
```

This setting specifies that the DSLPipe receives the RIP table from the other IPX router but will not upload its RIP table. To disable IPX RIP altogether, set:

```
IPX RIP=None
```

4 Close the Connection profile.

Configuring a static IPX route

Each static IPX route contains all of the information needed to reach one NetWare server on a remote network. When the DSLPipe receives an outbound packet for that server, it finds the referenced Connection profile and dials the connection.

Table 8-3 shows IPX Route profile parameters:

Table 8-3. IPX Route profile parameters

Location	Parameters with example values
Ethernet > IPX Routes > *any profile* (IPX Route profile)	Server Name=SERVER-1 Active=Yes Network=ccccfff1 Node=000000000001 Socket=0000 Server Type=0004 Hop Count=2 Tick Count=12 Connection #=1

For details on each parameter, see the *Reference Guide*.

Note: You don't need to create IPX routes to servers 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, you should define a static route to the remote site even if your environment requires dynamic routes. If you have one static route to a remote site, it should specify a "master" NetWare server that knows about many other services. NetWare

workstations can then learn about other remote services by connecting to that remote NetWare server.

Note: Remember that static IPX routes are manually administered, so they must be updated if there is a change to a remote server.

To define an IPX Route profile:

1. Open the IPX Routes menu.
2. Open an IPX Route profile.
3. Specify the name of the remote NetWare server.
   For example:
   ```
   Server Name=SERVER-1
   ```
4. Specify that the route should be added to the RIP table:
   ```
   Active-Yes
   ```
5. Enter the remote server's internal network number.
   For example:
   ```
   Network=ABC01FFF
   ```
6. Enter the remote server's node number.
   For example:
   ```
   Node=0000000000001
   ```
   The default 0000000000001 is typically the node number for NetWare file servers.
7. Specify the remote server's socket number.
   For example:
   ```
   Socket=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 in IPX Route profiles. To bring up a connection to a remote service that uses a dynamic socket number, specify a "master" server with a well-known socket number on that network.
8. Specify the SAP Service Type.
   For example:
   ```
   Service Type=0004
   ```

NetWare file servers are SAP Service type 0004.

9 Specify the distance in hops to the server.

For example:

```
Hop count=2
```

Usually the default of 2 is appropriate.

10 Specify the distance to the server in ticks (18 ticks/second).

For example:

```
Tick count=12
```

Usually the default of 12 is appropriate, but you might need to increase this value for very distant servers.

11 Specify the number of the Connection profile that defines the WAN connection.

A Connection profile is referenced by the unique part of the number it is assigned in the Connections menu (1, 2, 3, and so forth).

```
Connection #=2
```

12 Close the IPX Route profile.

Configuring SAP in a Connection profile

By default, the IPX SAP parameter in a Connection profile is set to Both, indicating that SAP broadcasts will be exchanged in both directions. If SAP is enabled to both send and receive broadcasts on the WAN interface, the DSLPipe broadcasts its SAP table to the remote network and listens for service updates from that network. Eventually, both networks have a table of all services on the WAN.

To control which services are advertised and where, you can disable the exchange of SAP broadcasts across a WAN connection, or specify that the DSLPipe will only send or only receive SAP broadcasts on that connection.

To restrict SAP broadcasts across a WAN connection:

1 Open a Connection profile that has IPX routing enabled.

2 Open the IPX Options submenu.

3 Set the IPX RIP parameter to a value other than the default setting of Both.

For example:

```
IPX SAP=Recv
```

This setting specifies that the DSLPipe receives SAP table updates from the remote router. If you do not want the DSLPipe to send or receive SAP broadcasts on this connection, use the following setting:

```
IPX SAP=None
```

4 Close the Connection profile.

Managing IPX SAP filters

IPX SAP filters include or exclude specific NetWare services from the DSLPipe unit's SAP table.

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

Table 8-4 shows IPX SAP filter parameters:

Table 8-4. IPX SAP filter profile parameters

Location	Parameters with example values
Ethernet > IPX SAP Filters > *any profile* (IPX SAP Filter profile)	Name=optional Input filters... Output filters... Valid=Yes Type=Exclude Server Type=0004 Server Name=SERVER-5
Ethernet > Connections > *any profile* > Sessions options… (Connection profile)	IPX SAP Filter=1
Ethernet > Mod Config > Ether options… (Ethernet profile).	IIPX SAP Filter=1

Table 8-4. IPX SAP filter profile parameters (Continued)

Location	Parameters with example values
Ethernet > Answer > Sessions options... (Answer profile)	IPX SAP Filter=1

For details on each parameter, see the *Reference Guide.*

Defining an IPX SAP filter

To define an IPX SAP filter:

1. Open the IPX SAP Filters menu, then open a profile.
2. Specify a name for the profile.
3. Open the list of Input filters.

   Input filter conditions are applied to all SAP packets received by the DSLPipe. They screen advertised services and exclude (or include) them from the DSLPipe SAP table.

   You can specify up to 12 filters to include or exclude services from particular servers. These filters are applied in the order in which they are listed in the Input filters menu.

```
50-801 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
```

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

5 Set the Valid parameter. Yes activates the filter; No deactivates the filter and is the default.

For example:

```
Valid=Yes
```

6 Set the filter type by pressing Enter to cycle through the choices of Include or Exclude.

For example:

```
Type=Exclude
```

7 Specify the service type (a hexadecimal number from 0 to FFFE).

For example:

```
Server Type=4
```

File servers are service type 4. (See your NetWare documentation for other service types.)

8 Specify the name of the NetWare server.

For example:

```
Server Name=SERVER-1
```

```
50-801 File Server
 In filter 01
 >Valid=Yes
  Type=Exclude
  Server Type=4
  Server Name=SERVER-1
```

9 Close the In filter.

10 Specify up to 12 input filters as needed.

11 Press Escape as necessary to return to the top level of the profile.

12 Open the list of Output filters.

Output filter conditions are applied to SAP response packets transmitted by the DSLPipe. If the DSLPipe receives a SAP request packet, it applies Output filters before transmitting the SAP response, and excludes (or includes) services from the response packet as specified by the filter conditions.

You can specify up to 12 filters to include or exclude types of services from particular servers. Filters are applied in the order in which they are listed in the Out filter menu.

When you have specified the Output filters you need:

13 Close the IPX SAP filter profile.

Applying an IPX SAP filter

You can apply an IPX SAP filter to the local Ethernet or to WAN interfaces, or both.

- On Ethernet, a SAP filter includes or excludes specific servers or services from the table.

  If directory services is not supported, servers or services that are not in the DSLPipe table will be inaccessible to clients across the WAN.
- In the Answer profile, a SAP filter screens service advertisements from across the WAN.
- In a Connection profile, a SAP filter screens service advertisements to and from a specific WAN connection.

To apply an IPX SAP filter profile:

1 Open the profile.

2 Open the Session Options submenu (Answer and Connection profiles) or Ether Options submenu (Ethernet profile).

3 Specify the number of the IPX SAP filter profile you defined.

You apply an IPX SAP Filter profile by specifying the unique part of the number it is assigned in the IPX SAP Filters menu. For example, to apply the filter defined as 20-801:

```
IPX SAP Filter=1
```

4 Close the profile.

A filter applied to the Ethernet interface takes effect immediately.

Configuring IPX routing connections

This section describes how to configure IPX routing connections. It describes typical host software requirements and includes the following example configurations:

- Example dial-in client connection
- Example with servers on both sides of the link
- Example with servers on only one side of the link

Table 8-5 shows connection parameters related to IPX routing.

Table 8-5. IPX routing connection parameters

Location	**Parameters with example values**
Ethernet > Connections > *any profile* (Connection profile)	Station=device-name Route IPX=Yes
Ethernet > Connections > *any profile* > Encaps options...	Recv PW=*SECURE* Send PW=*SECURE* Send Auth=CHAP
Ethernet > Connections > *any profile* > IPX options...	Peer=Router Dial Query=No IPX Net#=cfff0003 IPX Alias#=00000000 Handle IPX=None Netware t/o=30
Ethernet > Connections > *any profile* > Sessions options…	IPX SAP Filter=1

For details on each parameter, see the *Reference Guide*.

An example with NetWare servers on both sides of the link

The illustration below shows the DSLPipe connected to an IPX network that supports both servers and clients. The example shows how it will make the connection to a remote site that also supports both servers and clients.

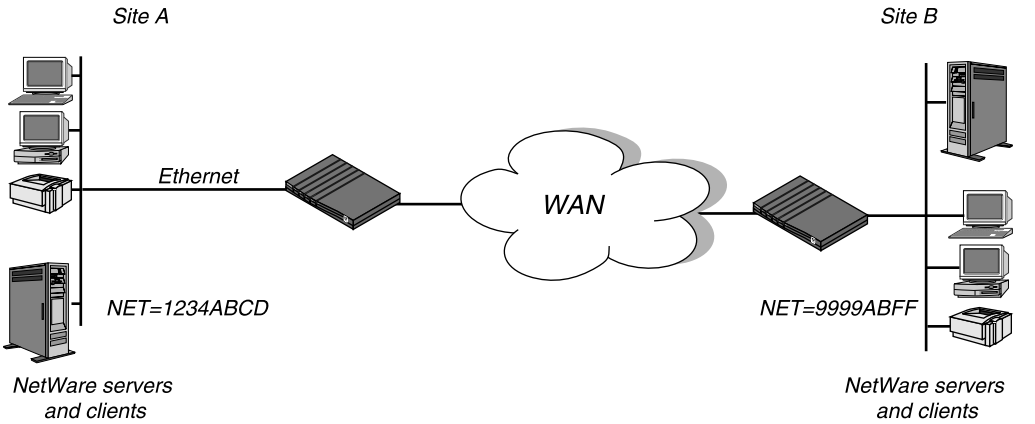


Figure 8-1. A connection with NetWare servers on both sides

In this example, site A and site B are both existing Novell LANs that implement NetWare 3.12 and NetWare 4 servers, NetWare clients, and a DSLPipe. The NetWare server at site A is configured with the following 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 is configured as follows:

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

To configure the DSLPipe at site A:

1 Assign the DSLPipe a name if it does not already have one.

To assign the DSLPipe a name, open the System profile and specify the name in the Name parameter. For example:

```
Name=SITEAGW
```

2 Open the Connection profile for site B.

For sake of example, the Connection profile for site B is profile #5. A profile's number is the unique part of the number it is assigned in the Connections menu. For example, the Connection profile defined as 20-105 is #5.

Set up the Connection profile as follows:

```
Station=SITEBGW
Active=Yes
Encaps=MPP
Dial #=555-1212
Route IP=No
Route IPX=Yes
Bridge=No
Dial brdcast=N/A

Encaps options...
    Send Auth=CHAP
    Recv PW=*SECURE*
    Send PW=*SECURE*

IPX options...
    IPX RIP=None
    IPX SAP=Both
    NetWare t/o=30
```

3 Close Connection profile #5.

4 Open the Ethernet profile and make sure that it is set up for IPX routing.

For example:

```
IPX Routing=Yes

Ether options...
    IPX Frame=802.2
    IPX Enet #=1234ABCD
```

5 Close the Ethernet profile.

Because IPX RIP is set to None in the Connection profile, configure a static route to the remote server:

6 Open an IPX Route profile.

7 Set up a route to the remote NetWare server with the following settings:

```
Server Name=SERVER-2
Active=Yes
Network=013DE888
Node=000000000001
Socket=0451
Server Type=0004
Connection #=5
```

Note: The Connection # parameter in the IPX Route profile must match the number of the Connection profile you configured for connection to that site.

8 Close the IPX Route profile.

To configure the DSLPipe at site B:

1 Assign the DSLPipe a name if it does not already have one.

To assign the DSLPipe a name, open the System profile and specify the name in the Name parameter. For example:

```
Name=SITEBGW
```

2 Open the Connection profile for site A.

For sake of example, the Connection profile for site A is profile #2. A profile's number is the unique part of the number it is assigned in the Connections menu. For example, the Connection profile defined as 20-102 is #2.

Set up the Connection profile as follows:

```
Station=SITEAGW
Active=Yes
Encaps=FR
Dial #=555-1213
Route IP=No
Route IPX=Yes
Bridge=No
Dial brdcast=N/A

Encaps options...
    Send Auth=CHAP
    Recv PW=*SECURE*
    Send PW=*SECURE*
```

```
IPX options...
    IPX RIP=None
    IPX SAP=Both
    NetWare t/o=30
```

3 Close Connection profile #2.

4 Open the Ethernet profile and make sure that it is set up for IPX routing. For example:

```
IPX Routing=Yes
```

```
Ether options...
    IPX Frame=802.2
    IPX Enet #=9999ABFF
```

5 Close the Ethernet profile.

Because IPX RIP is set to None in the Connection profile, configure a static route to the remote server:

6 Open an IPX Route profile.

7 Set up a route to the remote NetWare server using these settings:

```
Server Name=SERVER-1
Active=Yes
Network=CFC12345
Node=000000000001
Socket=0451
Server Type=0004
Connection #=2
```

Note: The Connection # parameter in the IPX Route profile must match the number of the Connection profile you configured to that site.

8 Close the IPX Route profile.

An example with local NetWare servers only

In the following example, the DSLPipe is connected to a local IPX network that has both servers and clients, and the DSLPipe will connect to a geographically remote network that supports one or more NetWare clients. Figure 8-2 shows the example setup.

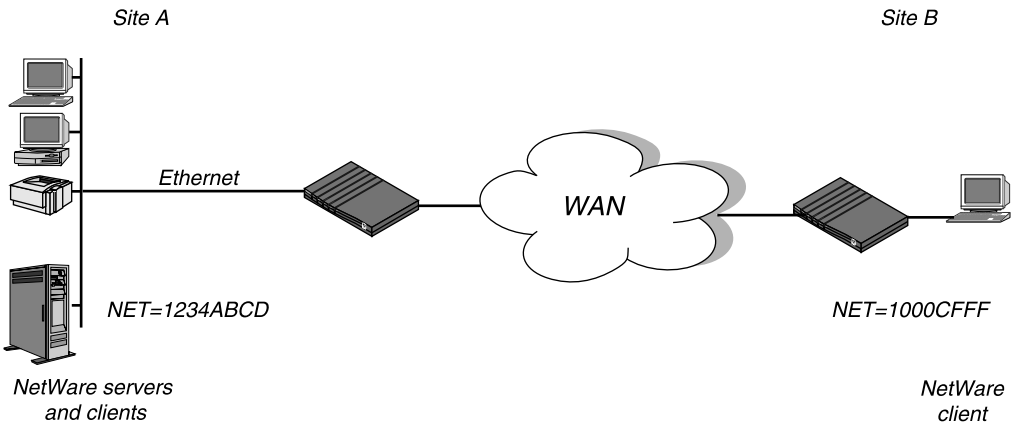


Figure 8-2. A dial-in client that belongs to its own IPX network

In this example, site A implements NetWare 3.12 servers, NetWare clients, and a DSLPipe. The NetWare server at site A is configured with the following 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 DSLPipe. It is not an existing Novell LAN, so the DSLPipe configuration creates a new IPX network (for example, 1000CFFF).

Note: The new IPX network number assigned to site B 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 example assumes that the Ethernet profile and Answer profile have already been set up to enable IPX routing. Because no static routes are used, the initial connection between the two Ascend units should be manually dialed (using the DO menu).

To configure the DSLPipe at site A:

1 Assign the DSLPipe a name if it does not already have one.

To assign the DSLPipe a name, open the System profile and specify the name in the Name parameter. For example:

```
Name=SITEAGW
```

2 Open the Connection profile for site B.

Set up the Connection profile as follows:

```
Station=SITEBGW
Active=Yes
Encaps=FR
Dial #=555-1212
Route IP=No
Route IPX=Yes
Bridge=No
Dial brdcast=N/A

Encaps options...
    Send Auth=CHAP
    Recv PW=*SECURE*
    Send PW=*SECURE*

IPX options...
    IPX RIP=Both
    IPX SAP=Both
    NetWare t/o=30
```

3 Close the Connection profile.

To configure the site B Ascend unit:

1 Assign the Ascend unit a name if it does not already have one.

To assign the Pipeline a name, open the System profile and specify the name in the Name parameter. For example:

```
Name=SITEBGW
```

2 Open the Connection profile for site A.

Set up the Connection profile like this:

```
Station=SITEAGW
Active=Yes
Encaps=MPP
```

```
Dial #=555-1213
Route IP=No
Route IPX=Yes
Bridge=No
Dial brdcast=N/A

Encaps options...
    Send Auth=CHAP
    Recv PW=*SECURE*
    Send PW=*SECURE*

IPX options...
    IPX RIP=Both
    IPX SAP=Both
    NetWare t/o=30
```

3 Close the Connection profile and save your changes.

Setting up Security

9

Recommended security measures

When the DSLPipe is shipped from the factory, its security features are all set to defaults that enable you to configure and set up the DSLPipe without any restrictions. Before you make the DSLPipe generally accessible, you should change these default security settings to protect the configured unit from unauthorized access.

You should set these important security features before putting the DSLPipe online:

- Change the Full Access security level password.

  A user who knows the password to the Full Access level will be able to perform any operation on the DSLPipe, including changing the configuration. The Full Access password is set to "Ascend" by default, and you should assign your own password. (For instructions, see "Changing the Full Access security level password" on page 9-2.)

- Activate the Full Access security level.

  After you change the password, activate the Full Access security level for your own use in performing the rest of these basic security measures. (For instructions, see "Activating the Full Access security level" on page 9-3.)

- Make the default security level very restrictive.

  The DSLPipe provides terminal services via Telnet. Any user who Telnets to the unit is assigned the default security level, which is initially without restrictions. You should turn off all privileges in the Default security profile. (For instructions, see "Making the Default security level restrictive" on page 9-4.)

- Assign a Telnet password.

Until you assign a Telnet password, any local user who has the DSLPipe unit's IP address can Telnet into it. Once you assign the password, all incoming Telnet sessions (from the local network or across the WAN) will be prompted to enter that password. (For instructions, see "Assigning a Telnet password" on page 9-5.)

- Change the SNMP community strings.

  The DSLPipe supports SNMP traps, which allows it to send alarms, report on call details, and send other management information to an SNMP management station without being polled. The DSLPipe default read and write community strings should be changed to prevent unauthorized access to the DSLPipe by an SNMP management station. (For instructions, see "Changing the SNMP read-write community string" on page 9-5.)

- Require profiles for incoming connections.

  The DSLPipe unit's Answer profile can be used to build unrestricted connections (connections for which no name or password is required). Although some sites allow this type of connection, many do not. You should restrict incoming connections to those with a configured profile. (For instructions, see "Requiring profiles for incoming connections" on page 9-6.)

- Turn off ICMP Redirects.

  To secure the DSLPipe unit's IP routes, you should configure the unit to ignore ICMP (Internet Control Message Protocol) Redirect packets. (For instructions, see "Turning off ICMP redirects" on page 9-7.)

Changing the Full Access security level password

The Full Access security profile is intended to provide unrestricted access to the DSLPipe. This is the "super-user" profile that enables you to configure, dial-up remote locations, reset the unit, upgrade system software, and so forth.

Note: Write down and save the Full Access password in a safe place. Make sure when you open the Full Access profile that you do not turn off the Edit Security privilege, or you will be unable to edit privileges when Full Access is activated.

To change the Full Access password:

1 Open the Security menu below the System menu.

Open the Full Access profile.

```
00-300 Security
>00-301 Default
 00-302
 00-303 Full Access
```

```
00-303 Full Access
 Name=Full Access
>Passwd=ascend
 Operations=Yes
 Edit Security=Yes
 Edit System=Yes
 Field Service=Yes
```

2 Open the Passwd parameter and specify a new password, then press Enter.

For example:

```
Passwd=my-password
```

Note: Passwords are case-insensitive. A user can specify the password "my-password" as "My-Password" or "MY-PASSWORD" and the DSLPipe accepts it.

3 Leave all other privileges enabled.

Note: Do not turn off the Edit Security privilege in this profile!

4 Close the Full Access profile.

Now only users who have the password you assigned will be able to activate the Full Access security level.

Activating the Full Access security level

To activate the Full Access profile, do the following:

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

```
00-300 Security
DO...
>0=ESC
 P=Password
```

2 In the list of security profiles, select Full Access. The DSLPipe prompts for the password.

```
00-300 Security
Enter Password:
 []

 Press > to accept
```

Type the password you specified in the Full Access profile and press Enter.

A message states that the password was accepted and the DSLPipe is using the new security level. If the password you enter is incorrect, you are prompted again to enter the password.

Making the Default security level restrictive

The Default security level is always assigned to all users who Telnet into the unit or access the terminal server interface in another way, and it is activated for the console whenever the unit is reset. You cannot change the name of the Default security profile or assign a password to it, but you should turn off its operations privileges.

To set the default security level to allow only read privileges:

1 Open the Security menu below the System menu.

2 Open the Default profile.

3 Restrict the Operations privilege.
For example:

```
Operations=No
```

When you restrict this privilege, all other privileges are N/A.

4 Close the Default profile.

From now on, users who access the DSLPipe terminal server will be unable to make any changes to its configuration or perform restricted operations. For all users with the default security level, passwords (including the null password) will be hidden by the string *SECURE* in the DSLPipe user interface.

Caution: If you reset or power-cycle the DSLPipe, 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. Use the default password “Ascend” to access the Full Access profile.

Assigning a Telnet password

Assign a Telnet password to prevent unauthorized Telnet sessions. The Telnet password can be up to 20 characters in length.

To assign a Telnet password:

1 Open the Ethernet profile.

2 Enter a Telnet password up to 20 characters long.

For example:

```
Telnet PW=telnet-pwd
```

3 Close the Ethernet profile.

Now any user who opens a Telnet session to the DSLPipe will be prompted to supply this password.

Changing the SNMP read-write community string

SNMP community strings are identifiers that SNMP-manager applications must specify before they can access the Management Information Base (MIB). The DSLPipe has two community strings:

- Read Comm

The read community string is set to “public” by default. It enables an SNMP manager to perform read commands (for example, Get and Get next) to request specific information.

- R/W Comm

  The read-write community string enables an SNMP manager to perform both read and write commands (for example, Get, Get next, and Set), which means the SNMP application can access management information, set alarm thresholds, and change some settings on the DSLPipe. By default, the read-write community string is set to the value “write.”

Note: There is no way to turn off SNMP write, so you must change the default read-write string to secure the DSLPipe against unauthorized SNMP access.

To change the read-write community string:

1. Open the Ethernet profile.
2. Open the SNMP Options submenu.
3. Enter up to 16 alphanumeric characters in the R/W Comm parameter.

   For example:

   ```
   R/W Comm=unique-string
   ```
4. Close the Ethernet profile.

Requiring profiles for incoming connections

There are many authentication measures you can set for incoming connections. At the most basic level, you can configure the DSLPipe to reject all incoming connections for which it has no matching profile.

To require configured profiles for all incoming connections:

1. Open the Answer profile.
2. Specify that a matching profile is required for incoming calls.

   ```
   Profile Reqd=Yes
   ```
3. Close the Answer profile.

(For more information about securing incoming connections, see “Connection security” on page 9-11.)

Turning off ICMP redirects

Internet Control Message Protocol (ICMP) was designed to dynamically find the most efficient IP route to a destination. ICMP Redirect packets are one of the oldest route discovery methods on the Internet and one of the least secure. It is possible to create counterfeit ICMP Redirects and change the way a device routes packets. If the DSLPipe is routing IP, you should turn off ICMP redirects.

To configure the DSLPipe to ignore ICMP redirect packets, do the following:

1 Open the Ethernet profile.

2 Turn off ICMP redirects.

For example:

```
ICMP Redirects=Ignore
```

3 Close the Ethernet profile.

DSLPipe Security profiles

When the DSLPipe is shipped from the factory, its security privileges are open to enable you to configure and set it up without any restrictions. (For recommended settings for the two predefined security profiles, see “Recommended security measures” on page 9-1.)

Default security level

The DSLPipe has three possible security levels, including the default. The Default security profile has no password. This security level is always activated for all users who Telnet into the unit or access the terminal server interface in another way. The Default security level is activated for the console whenever the unit is reset, so that the privileges enabled in the Default profile are generally available. As such, be sure to set Operations=No in the Default profile, to prevent unauthorized changes to other settings.

Security profile passwords

Passwords are case-insensitive in the DSLPipe. If you specify the password “my password,” the DSLPipe accepts that string in any case combination (such as “My-Password” or “MY-PASSWORD”).

Users who do not have Edit Security privileges, described next, can see the DSLPipe menus, but all passwords are displayed as *SECURE* instead of the actual password. If a user has Edit Security privileges, passwords in Security profiles can be seen and changed.

Security privileges

In addition to Default security, there are eight more security profiles you can customize to include any combination of the following privileges:

- Operations

  If Operations=Yes, users can change parameter settings and access most DO commands, which are manual commands used to change security levels or manually dial or clear calls. (To learn more about DO commands, see “Using DO commands” on page 11-8.)

- Edit Security

  If Edit Security=Yes, users can edit Security profiles. All passwords in Security profiles are visible as text. This is the most powerful privilege you can assign, because it allows users to change their own privileges at will. When Edit Security=No, all passwords are hidden by the string “*SECURE*.”

- Edit System

  If Edit System=Yes, users can edit the System profile and other system-wide settings.

- Field Service

  If Field Service=Yes, users can perform field service operations, such as uploading new system software to the DSLPipe unit. Field service operations are special diagnostic routines not available through DSLPipe menus.

For complete information on each parameter, see the *Reference Guide*.

Using the Full Access profile

The Full Access profile should be reserved for the super-user login: yourself and anyone else who will be reconfiguring the DSLPipe, testing lines, dialing remote locations, resetting the unit, and upgrading system software.

Note: Be sure you write down the new Full Access password and store it in a safe place. If you restrict all other levels and then forget the Full Access password, you will need to call Customer Support to access the unit.

The default settings for the Full Access profile are as follows:

```
Name=Full Access
Passwd=Ascend
```

Note: You should change this default password, as described in “Recommended security measures” on page 9-1

```
Operations=Yes
Edit Security=Yes
```

Note: Do not turn off the Edit Security privilege, or you will be unable to edit privileges when Full Access is activated!

```
Edit System=Yes
Field Service=Yes
```

When you log into the DSLPipe, you will only be able to view settings, because the Default profile will be active. To make any changes or perform any administrative tasks, you’ll need to activate the Full Access profile in the DO menu. (To learn more about DO commands, see “Using DO commands” on page 11-8.)

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

```
00-300 Security
DO...
>0=ESC
 P=Password
```

2 In the list of Security profiles that opens, select Full Access.

The DSLPipe prompts for the password.

3 Type the password for the Full Access profile and press Enter.

Defining new security profiles

If you do not want other users to change the DSLPipe configuration profiles or perform administrative tasks in the DSLPipe, you do not need to define any security profiles beyond Default and Full Access. However, you can define additional security profiles with various privileges, as described below.

To define a Security profile:

1 Open the Security menu below the System menu.

2 Open an unnamed profile.

3 Specify a name for the profile (up to 16 characters).

For example:

```
Name=Calabasas
```

4 Specify a new password, and then press Enter.

```
Passwd=*SECURE*
```

As soon as you press Enter, the DSLPipe hides the password string you specified by displaying the string *SECURE*.

5 Set the privileges for this profile.

For example:

```
Name=Calabasas
Passwd=*SECURE*
Operations=Yes
Edit Security=No
Edit System=No
Field Service=No
```

6 Close the new Security profile.

Connection security

Connection security has two levels: caller authentication regulating authorized access, and network security preventing unauthorized wide-area network access.

All authentication relies on the DSLPipe finding a matching profile to verify information presented by the caller.

- Authentication mechanisms

  Password authentication, such as PAP and CHAP, requires a name and password from the caller.

  Calling-line ID (CLID) authentication verifies that the call is coming from the expected phone number.

  Callback authentication instructs the DSLPipe to hang up and call back before performing password authentication. Callback provides the highest level of control, assuring that incoming calls are coming from a known user or network.

  Note: Any form of authentication requires a configured profile. See "Requiring profiles for incoming connections" on page 9-6 for details on configuring the DSLPipe to always require a matching profile, regardless of whether authentication is enforced.

- Network security

  Filters are one of the most effective methods of protecting your site from unwanted WAN access. Filters are described briefly in this chapter; see the Chapter 10, "Setting up Filters," for full details.

PAP and CHAP authentication

Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) require Point-to-Point Protocol (PPP) encapsulation. These authentication protocols apply to PPP, Multilink PPP (MP), and Multichannel PPP (MP+) connections to the DSLPipe. Both sides of the connection must support the same protocol.

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 in the clear, so it

is not a very strong authentication method. PAP provides baseline security when your system interoperates with equipment from other vendors.

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. This use of an incrementally changing identifier and a variable challenge value protects against playback attack.

Note: In addition to the PAP and CHAP authentication, there are other parameters, such as Telco and session options, that affect whether the DSLPipe is able to build the connection. For example, if the AnsOrig parameter is set to prevent incoming calls, the DSLPipe will never reach the stage of authenticating an incoming call using that profile.

Table 9-1 shows PAP and CHAP parameters in the DSLPipe.

Table 9-1. PAP and CHAP authentication parameters

Location	Parameters with example values
System > Sys Config (System profile)	Name=mygw
Ethernet > Connections > *any profile* (Connection profile)	Station=dialgw Encaps=PPP (or MPP)
Ethernet > Connections > *any profile* > Encaps options...	Recv PW=*SECURE* Send Auth=CHAP Send PW=*SECURE*
Ethernet > Names/Passwords > *any profile* (Password profile)	Name=Fred Recv PW=*SECURE*

For details on each parameter, see the *Reference Guide*.

Name and password verification

During authentication, the calling device often requires the DSLPipe unit's name and password as well. The DSLPipe name is specified in the System profile. The Send PW parameter is a password sent to the calling device.

If the Recv Auth parameter in the Answer profile is set to Either, the DSLPipe uses PAP or CHAP authentication, depending on what the caller supports. If it is set just to PAP, the DSLPipe would reject passwords presented with CHAP, and vice versa.

When the DSLPipe receives a PPP call, it tries to match the caller's name and password to a configured Connection profile. If the DSLPipe doesn't find any matching profile, it ends the call. If the DSLPipe does find a matching profile, it authenticates using PAP or CHAP, and then establishes the connection.

Added steps for IP routing connections

When an IP routing connection is being authenticated, the IP address is verified as part of the PPP negotiation before a call is established.

If the caller's PPP software presents an IP address, the DSLPipe must find a Connection profile that matches that address. Otherwise, it ends the call without completing PAP or CHAP authentication. If it finds a profile, it authenticates the connection, and then establishes the connection.

Table 9-2 shows IP parameters that can affect PPP negotiation.

Table 9-2. Additional IP parameters that affect PPP negotiation

Location	Parameters with example values
Ethernet > Connections > *any profile* > IP options...	LAN Adrs=10.5.6.7/24

For details on each parameter, see the *Reference Guide*.

(For information about IP routing connections, see Chapter 7, "Setting up IP Routing.")

Network security

Network security is related to packets coming in from any wide-area network (WAN) connection. This section describes the following network security mechanisms:

- Filters
- Restricting SNMP access

For recommendations about ICMP Redirect packets, see “Recommended security measures” on page 9-1.

Filters

This section gives you an overview of how filters work for network security purposes.

Network security filters are data filters, which may be applied to incoming or outgoing data streams, or both. Data filters can prevent certain packets from reaching the local network or going out from the local network to the WAN. For example, you can use data filters to drop packets addressed to particular hosts, or prevent certain types of packets from reaching the local network.

Filters can also be used to prevent remote users from accessing information on your local network, even if they know how to “spoof” a local source address that would enable them to get past a filter. For example, you can define a filter that drops inbound packets whose source address is on the local network or the loopback address.

Each filter consists of an ordered list of conditions (“rules”) based on either IP-specific or protocol-independent information. For an IP filter, you can filter packets based on any combination of the following elements:

- Source address
- Destination address
- Protocol number
- Source port
- Destination port

- A flag indicating if a TCP session is established

For a protocol-independent filter, you can specify data values and masks that the DSLPipe uses when determining whether to drop or forward packets.

(For information about how to organize and create Filter profiles, refer to Chapter 10, “Setting up Filters.”)

Setting up Filters

10

Introduction to filters

Filters define packet conditions. When a filter is in use, the DSLPipe examines every packet in the packet stream and takes action if the defined filter conditions are present. The action the DSLPipe takes depends both on the conditions specified within the filter and how the filter is applied.

The default action when no filter is used is to forward all packets and allow all packets to reset the idle timer, which is used to determine when to disconnect inactive sessions.

You can define conditions in filters to drop all packets except the ones you explicitly allow, or allow all packets except the ones you explicitly drop. Additionally, you can specify whether to apply the filter to inbound packets, outbound packets, or all packets, regardless of whether they are coming from the wide-area network (WAN), or leaving the local network.

Depending on how a filter is used, it is either a data filter or a call filter. The following describes each type:

- Data filter

  Affects the flow of data. Packets are dropped or forwarded as specified in the filter conditions. Mainly used for network security.

- Call filter

  Determines which packets can initiate a connection or reset the idle timer for an established connection. Mainly used to prevent unnecessary connections.

Note: Packets can pass through more than one filter. If both a data filter and call filter are applied, the data filter takes precedence.

Data filters for dropping or forwarding certain packets

Data filters are commonly used for security, but they can be used for any purpose that requires the DSLPipe to drop or forward specific packets. For example, you can use data filters to drop packets addressed to particular hosts, or to prevent broadcasts from going across the WAN. You can also use data filters to allow only specified devices to be accessed by users across the WAN.

Data filters do not affect the idle timer, and a data filter applied to a Connection profile does not affect the answering process.

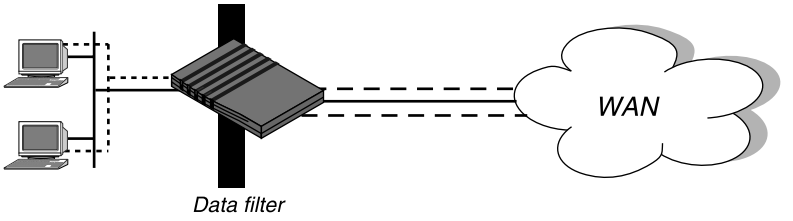


Figure 10-1. Data filters can drop or forward certain packets

To define which packets will be allowed to cross the WAN interface, apply a data filter to a Connection profile or the Answer profile using the following steps:

1. Open a Connection profile or the Answer profile.
2. Open the Session Options submenu.
3. Apply a data filter.

   For example:

   ```
   Data Filter=4
   ```

   If this parameter is set to zero, the default, no filter is applied. To apply a filter, specify its profile number. You can view the profile number by opening the Filters menu. You don't have to specify the whole number, just the unique portion of it, for example, 1, 2, 3,...
4. Close the Connection profile or Answer profile.

A filter applied to a Connection or Answer profile takes effect only when the connection goes from an offline state to a call-placed state.

To define which packets will be allowed to cross the Ethernet interface, apply a data filter to a connecton profile or the Answer profile using the following steps:

1. Open the Ethernet profile.
2. Open the Ether Options submenu.
3. Apply the data filter.

   For example:

   ```
   Data Filter=4
   ```

   If this parameter is set to zero, the default, no filter is applied. To apply a filter, specify its profile number. You can view the profile number by opening the Filters menu. You don't have to specify the whole number, just the unique portion of it, for example, 1, 2, 3,...
4. Close the Ethernet profile.

A filter applied to the Ethernet interface takes effect immediately. If you change any of the conditions in the Filter profile definition, new or changed conditions are applied as soon as you save the Filter profile.

For an example data filter, see "Example filters" on page 10-12.

Call filters for managing connections

Call filters are used to prevent unnecessary connections and to help the DSLPipe distinguish active traffic from "noise." By default, any traffic to a remote site triggers a call to that site, and any traffic across an active connection resets the connection's idle timer.

Note: The idle timer is set to 120 seconds by default. If a connection is inactive for two minutes, the idle timer expires and the DSLPipe terminates the connection.

Call filters define which packets are not considered active traffic on a particular connection. They identify which packets should not originate a connection or reset the idle timer. Call filters do not affect which packets are transmitted or received across active connections.

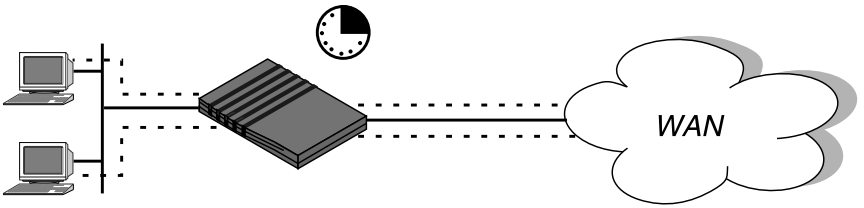


Figure 10-2. Call filters can prevent certain packets from resetting the timer

To define which packets will not reset the idle timer or keep a connection active, apply a call filter to a Connection profile or the Answer profile using the following steps:

1 Open a Connection profile or the Answer profile.

2 Open the Session Options submenu.

3 Apply the call filter.

For example:

```
Call Filter=5
```

If this parameter is set to zero, the default, no filter is applied.

If it is set to any other value, the value must be a valid Filter profile number. The Filter profile number is the number in the Filters menu. You don't have to specify the whole number, just the unique portion of it.

4 Close the Connection profile or Answer profile.

When you apply a filter to the WAN interface, it takes effect only when a connection goes from an offline state to a call-placed state.

To reset the idle timer, perform the following steps:

1 Open a Connection profile.

2 Open the Session Options submenu.

3 Specify the number of seconds to wait before clearing an inactive connection.

For example:

```
Idle=15
```

If this parameter is set to zero, an idle connection stays open indefinitely.

For example, if you specify 15, an idle connection is terminated after 15 seconds.

4 Close the Connection profile.

Predefined call filters

The DSLPipe ships with the following predefined Filter profiles:

- IP Call, for IP connections.
- NetWare Call, for IPX connections.
- AppleTalk Call, for bridged AppleTalk connections.

These filters are basic call filters that prevent the most common traffic in each kind of packet stream from initiating or maintaining a connection. (For information about predefined-filter settings, see “Working with predefined call filters” on page 10-21.)

Note: For information about IPX SAP filters, pertaining to NetWare services the DSLPipe adds to its service table, see Chapter 8, “Setting up IPX Routing.”

Overview of Filter profiles

You apply a filter to an interface by specifying its profile number. The DSLPipe applies all filter conditions defined in a filter profile to the Connecton or Answer profile where it is specified.

Figure 10-3 shows how filters are organized in the menu interface, and the terminology used to describe each part of a filter.

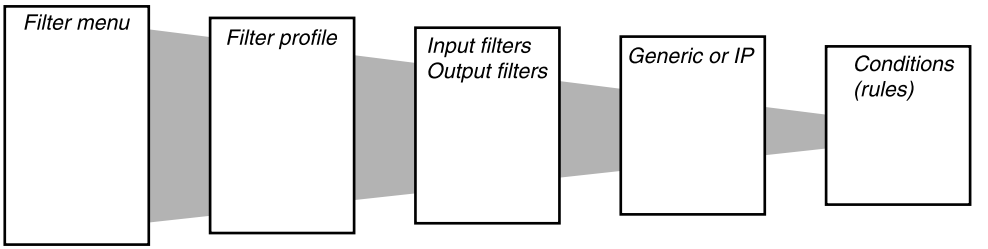


Figure 10-3. Filter organization and terminology

The menus shown in Figure 10-3 are nested, beginning with the Filters menu. That is, the numbered Filter profile menus are found under the Filters menu; the Input or Output filter menus are found under each numbered Filter profile menu, and so forth. Each level of the Filters menu is described as follows:

- Filters menu

  The Filters menu contains a list of numbered profiles. When applying a filter, you identify it by the unique portion of its Filter profile number, for example, you would use 1, 2, or 3, rather than 20-401, 20-402, or 20-403.

- Filter profile

  A Filter profile is a set of filter conditions.

- Input or Output filters

  At the top level of a Filter profile are two submenus: Input Filters and Output Filters. The Input submenu allows you to define 12 In-filter conditions to apply to incoming data. The Output submen allows you to define 12 Out-filter conditions to apply to outgoing data. The conditions are applied to the data stream in filter order, starting with 01.

- Generic or IP filters

  Each In filter and Out filter can be one of two types: “Generic” or “IP.” After assigning a type, you define filter conditions applicable to that type of packet in its corresponding submenu.

- Filter conditions

  Filter conditions specify the actual packet characteristics that will be examined in the data stream. Generic filter conditions specify locations and values that may be found within any packet. IP filter conditions specify packet characteristics that apply only to TCP/IP/UDP packets, such as address, mask, and port.

Filtering inbound and outbound packets

At the top level of a Filter profile, you can assign a name and open the Input filters or Output filters submenu.

```
20-401 IP Call
>Name=IP Call
 Input filters...
 Output filters...
```

Input filters cause the DSLPipe to examine incoming packets, and Output filters cause it to examine outgoing packets. If the filter is applied as a data filter on the Ethernet, it affects packets from the Ethernet *into* the DSLPipe or from the DSLPipe *out* to the Ethernet. If applied as a data or call filter on a WAN interface defined in a Connection profile, it affects packets from that WAN interface *into* the DSLPipe or from the DSLPipe *out* to that interface.

You can specify up to 12 In filters" and 12 Out filters in a Filter profile. These filters are applied in filter-number order, beginning with In filter 01.

```
20-401 IP Call
 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
```

By default, all packets are forwarded. So if a packet does not match any of the defined conditions in a filter, it is forwarded as usual.

Note: If only Input filters are defined, all outbound packets are forwarded or allowed to reset the idle timer. If you define only Output filters, all inbound packets are forwarded or alloed to reset the idle timer.

Selecting filter type and activating the filter

The “In filters” and “Out 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.

When you open an “In filter” or an “Out filter,” set the Valid parameter to Yes and select the type of filter conditions to be defined, Generic or IP.

```
20-401 IP Call
 In filter 01
 >Valid=Yes
  Type=GENERIC
  Generic...
  IP...
```

Generic filter conditions define bits and bytes within a packet. They are applied to all packet types, including TCP and IP. IP filter conditions are related only to TCP/IP/UDP packets.

Defining generic filter conditions

If the Type parameter in a filter is set to GENERIC, you can define generic conditions. Table 10-1 shows the generic filter conditions.

Table 10-1. Generic filter conditions

Location	Parameters with example values
Ethernet > Filters > *any profile* > Input filters > 01 to 12 > Generic Ethernet > Filters > *any profile* > Output filters > 01 to 12 > Generic (Filter profile)	Forward=No Offset=14 Length=8 Mask=ffffffffffffffff Value=aaa030000000080f3 Compare=Equals More=No

For details on each parameter, see the *Reference Guide.*

- Forward

  The Forward parameter determines whether the DSLPipe will forward a packet if it matches the definition, where Forward=Yes, or drop the packet if it matches, where Forward=No.

  If a filter is applied as a data filter, the “forward” action determines which packets will be transmitted and received. If a filter is applied as a call filter, the “forward” action determines which packets can either initiate a connection or reset the timer for an established connection.

- Offset, Length, Mask, and Value

  The Offset, Length, Mask, and Value parameters are used to define the exact location of certain bytes within a packet and the value of those bytes.

- Compare

  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.

- More

  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.

Defining IP filter conditions

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 10-2 shows the filter conditions you may specify in an IP filter.

Table 10-2. IP filter conditions

Location	Parameters with example values
Ethernet > Filters > *any profile* > Input filters > 01 to 12 > Ip Ethernet > Filters > *any profile* > Output filters > 01 to 12 > Ip	Forward=Yes Src Mask=255.255.255.192 Src Adrs=192.100.40.128 Dst Mask=0.0.0.0 Dst Adrs=0.0.0.0 Protocol=0 Src Port Cmp=None Src Port #=N/A Dst Port Cmp=None Dst Port #=N/A TCP Estab=N/A

For details on each parameter, see the *Reference Guide*.

- Forward

  The Forward parameter determines whether the DSLPipe will forward a packet if it matches the definition, where Forward=Yes, or drop the packet if it matches, where Forward=No.

  If a filter is applied as a data filter, the “forward” action determines which packets will be transmitted and received. If a filter is applied as a call filter, the “forward” action determines which packets can either initiate a connection or reset the timer for an established connection.

- Source and destination address and mask

  The source and destination Mask and Adrs parameters specify the contents of the source or destination fields in a packet. Use the Mask parameter to mask out portions of the source or destination address, for example, to mask out the host number.

- Protocol

  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.

  – 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

- Source and destination ports and comparison method

  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 comparison may match a protocol port number that is less-than, greater-than, equal, or not-equal.

- TCP Estab

  The TCP Estab parameter can be set to match a packet only if a TCP session is already established.

Example filters

This section provides a step-by-step examples of defining filters. It shows how to specify both generic and IP filter conditions.

This section shows how to create Filter profiles. Some sites modify the predefined call filters to make them more full-featured for the types of packets commonly seen at that site. See “Working with predefined call filters” on page 10-21 for details.

An example generic filter to handle AppleTalk broadcasts

This section shows how to define a generic data filter whose purpose is to prevent local AppleTalk AEP and NBP traffic from going across the WAN. The data filter first defines the types of packets that should *not* be filtered:

- AppleTalk Address Resolution Protocol (AARP) packets
- AppleTalk packets that are not addressed to the AppleTalk multicast address, such as regular traffic related to an actual AppleTalk File Server connection
- All non-AppleTalk traffic

The filter then defines the packets that should be dropped:

- AppleTalk Echo Protocol (AEP)
- Name Binding Protocol (NBP)

To define a generic data filter:

1 Select an unnamed Filter profile in the Filters menu and press Enter.

For example, select 20-403.

2 Assign a name to the Filter profile.

For example:

```
Name=AppleTalk Data
```

```
20-403
>Name=AppleTalk Data
 Input filters...
 Output filters...
```

3 Open the Output Filters submenu.

4 Open Out filter 01.

```
20-403
 Out filter 01
 >Valid=Yes
  Type=GENERIC
  Generic...
  IP...
```

5 Set Valid=Yes and Type=GENERIC, and then open the Generic submenu and specify the following conditions:

```
Generic...
  >Forward=No
   Offset=14
   Length=8
   Mask=ffffffffffffffff
   Value=aaaa0300000080f3
   Compare=Equals
   More=No
```

These conditions define a location within a packet and the hexadecimal value that AARP packets contain within that location, protocol type 0x80f3. Outbound AARP packets will not be forwarded.

6 Close Out filter 01, and then open Out filter 02.

7 Set Valid=Yes and Type=GENERIC, and then open the Generic submenu and specify the following conditions:

```
Generic...
  >Forward=Yes
   Offset=14
   Length=8
```

```
   Mask=ffffffffffffffff
   Value=aaaa03080007809b
   Compare=NotEquals
   More=No
```

These conditions define non-AppleTalk traffic. Note that AppleTalk has the protocol type 0x809b. Outbound packets that are not AppleTalk packets will be forwarded. Because all non-AppleTalk packets have now been forwarded, subsequent filters can assume that a packet is AppleTalk.

8 Close Out filter 02, then open Out filter 03.

9 Set Valid=Yes and Type=GENERIC, and then open the Generic submenu and specify the following conditions:

```
Generic...
  >Forward=Yes
   Offset=32
   Length=3
   Mask=ffffff0000000000
   Value=0404040000000000
   Compare=Equals
   More=No
```

These conditions filter AEP packets.

10 Close Out filter 03, then open Out filter 04.

11 Set Valid=Yes and Type=GENERIC, and then open the Generic submenu and specify the following conditions:

```
Generic...
  >Forward=Yes
   Offset=32
   Length=6
   Mask=ffffffffffff0000
   Value=090007ffffff0000
   Compare=NotEquals
   More=No
```

AppleTalk “broadcast” traffic uses a multicast address. These conditions specify the multicast address. Any AppleTalk packet that does not use the multicast address will be forwarded.

12 Close Out filter 04, then open Out filter 05.

13 Set Valid=Yes and Type=GENERIC, and then open the Generic submenu and specify the following conditions:

```
Generic...
  >Forward=Yes
   Offset=32
   Length=4
   Mask=ff00fff000000000
   Value=0200022000000000
   Compare=Equals
   More=Yes
```

Together, Out filters 05 and 06 specify NBP lookup packets with a wildcard entity name. NBP lookups are transmitted by the Chooser and other applications that look up entities on AppleTalk networks.

14 Close Out filter 05, then open Out filter 06.

15 Set Valid=Yes and Type=GENERIC, and then open the Generic submenu and specify the following conditions:

```
Generic...
  >Forward=Yes
   Offset=42
   Length=2
   Mask=ffff000000000000
   Value=013d000000000000
   Compare=Equals
   More=No
```

16 Close Out filter 06, then open Out filter 07.

17 Set Valid=Yes.

To discard everything else, just set Valid to Yes. This causes the default settings shown below:

```
Generic...
  >Forward=No
   Offset=0
   Length=0
   Mask=0000000000000000
   Value=0000000000000000
```

```
Compare=Equals
More=No
```

18 Close the Filter profile.

An example IP filter to prevent address spoofing

This section shows how to define an IP data filter whose purpose is to prevent "spoofing" of local 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.

The filter first defines Input filters that drop packets whose source address is on the local IP network or the loopback address (127.0.0.0). In effect, these filters say: "If you see an inbound packet with one of these source addresses, drop the packet." The third Input filter defines every other source address (0.0.0.0) and specifies "Forward everything else to the local network."

The data filter then defines an Output filter that specifies: "If an 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'll use your own local IP address and netmask when defining a Filter profile.

Note: Because the Pipeline only supports 3 filters, this example modifies the predefined IP Call filter. See "Working with predefined call filters" on page 10-21 for information about predefined filters.

To define an IP data filter:

1 Select an unnamed Filter profile in the Filters menu and press Enter.
For example, select 20-401.

```
20-400 Filters
 20-401 IP Call
 20-402 NetWare Call
 20-403 AppleTalk Call
```

2 Assign a name to the Filter profile.

For example:

```
Name=no spoofing
```

```
20-401
>Name=no spoofing
 Input filters...
 Output filters...
```

3 Open the Input Filters submenu

4 Open In filter 01.

```
20-401
 In filter 01
 >Valid=Yes
  Type=IP
  Generic...
  IP...
```

5 Set Valid=Yes and Type=IP, and then open the IP submenu

6 Specify the following conditions:

```
 Ip...
 >Forward=No
  Src Mask=255.255.255.192
  Src Adrs=192.100.50.128
  Dst Mask=0.0.0.0
  Dst Adrs=0.0.0.0
  Protocol=0
  Src Port Cmp=None
  Src Port #=N/A
  Dst Port Cmp=None
  Dst Port #=N/A
  TCP Estab=N/A
```

These conditions specify 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.

7 Close the current Input filter, and then open In filter 02.

8 Set Valid=Yes and Type=IP, and then open the IP submenu and specify the following conditions:

```
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
```

These conditions specify the loopback address in the Src Mask and Src Adrs fields. If an incoming packet has this address, it will not be forwarded onto the Ethernet.

9 Close the current Input filter, and then open In filter 03.

10 Set Valid=Yes and Type=IP, and then open the IP submenu and specify the following conditions:

```
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
```

These conditions specify every other source address (0.0.0.0) If an incoming packet has any non-local source address, it will not be forwarded onto the Ethernet.

11 Close the Input filter, and then return to the top level of the “no spoofing” Filter profile.

12 Open the Output Filters submenu, and select Out filter 01.

13 Set Valid=Yes and Type=IP, and then open the IP submenu and specify the following conditions:

```
Ip...
>Forward=Yes
 Src Mask=255.255.255.192
 Src Adrs=192.100.40.128
 Dst Mask=0.0.0.0
 Dst Adrs=0.0.0.0
 Protocol=0
 Src Port Cmp=None
 Src Port #=N/A
 Dst Port Cmp=None
 Dst Port #=N/A
 TCP Estab=N/A
```

These conditions specify the local net mask and IP address in the Src Mask and Src Adrs fields. If an outbound packet has a local source address, it will be forwarded.

14 Close the Filter profile.

An example IP filter for more complex security issues

This section describes an IP data filter that illustrates some of the issues you may need to consider when writing your own IP filters. The sample filter does not address fine points of network security. You may want to use this sample 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 is unnecessary.

Working with predefined call filters

The DSLPipe ships with three predefined Filter profiles, one for each commonly used protocol suite.

- IP Call, for IP connections.
- NetWare Call, for IPX connections.
- AppleTalk Call, for bridged AppleTalk connections.

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 DSLPipe handles routine traffic on your network.

Note: You can modify the predefined Filter profiles to make them more full-featured for the types of packets commonly seen on your network that you want to prevent form initiating or maintaining connections.

NetWare Call filter

The predefined NetWare Call filter is designed to prevent Service Advertising Protocol (SAP) packets originating on the local IPX network from resetting the idle timer or initiating a call.

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.

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=ffffffffffffff
Out filter 02...Generic...Value=ffffffffffff0452
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=ffffffffffff0452
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=ffffffffffffffff
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 11...Generic...Compare=Equals
Out filter 11...Generic...More=No
```

Defining a SNEP data filter for Ethernet

NetWare’s copy-protection scheme makes use of Serialization Number Exchange Protocol (SNEP) 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 DSLPipe, 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, when you don't extend the filter to include RIP as described in "Extending the predefined filter for RIP packets" on page 10-23, 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.

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
```

AppleTalk Call filter

The AppleTalk Call filter instructs the DSLPipe 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 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 DSLPipe 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=000000000000000000
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=32
Out filter 02...Generic...Length=3
Out filter 02...Generic...Mask=ffffff0000000000
Out filter 02...Generic...Value=0404040000000000
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=809b0000000000000
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
```

Managing the DSLPipe

11

Introduction to Ascend administration

This introduction gives an overview of the Pipeline unit's administrative features and tells you where to find more detailed information.

Administration features in the VT100 interface

The DSLPipe VT100 interface provides the following administrative features:

- Security Profiles

  The DSLPipe has password security to protect the box itself from unauthorized access. see "Activating administrative privileges" on page 11-3. For details on Security Profiles, see the Chapter 9, "Setting up Security."

- System administration commands

  The DSLPipe provides commands for rebooting the device, saving or restoring configuration information, and performing other administrative functions. The DSLPipe 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 "Performing system administration operations" on page 11-8.

- DO commands

  Pressing Ctrl-D in the vt100 interface displays the DO menu, which contains commands for changing security levels in the DSLPipe, 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.

- Terminal server command-line interface

The DSLPipe'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 "Using the terminal server interface" on page 11-13.

- Status windows

  The status windows in the vt100 interface provide information about what is currently happening in the DSLPipe. For example, one status window displays up to 31 of the most recent system events that have occurred since the DSLPipe 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.

- Interaction with syslog for ASCII log files

  If a Windows or UNIX host on the local network is running the Syslog daemon, you can configure the DSLPipe to write log messages to an ASCII file on that host. See "Configuring the DSLPipe to interact with syslog" on page 11-6.

Security features

Security is one of the most important factors in managing the Pipeline. The many security features you can use are discussed in detail in the Chapter 9, "Setting up Security."

SNMP management

The DSLPipe supports SNMP on a TCP/IP network. An SNMP management station that uses the Ascend Enterprise MIB can query the DSLPipe, set some parameters, sound alarms when certain conditions appear in the DSLPipe, and so forth. An SNMP manager must be running on a host on the local IP network, and the Pipeline must be able to find that host, either via static route or RIP.

In addition, SNMP has its own password security, which you should set up to protect the Pipeline from being reconfigured from an SNMP station.

Remote management via Telnet

The DSLPipe can be remotely configured and managed by establishing a Telnet session from any Telnet workstation and viewing the configuration menus in a Telnet vt100 window.

You can use this feature to manage the DSLPipe from a local or remote computer. You can also use it to manage remote Ascend units. From a Telnet session you can perform all of the configuration, diagnostic, management, and other functions that could be performed from a computer connected to the DSLPipe Terminal port.

See “Using the terminal server interface” on page 11-13.

Activating administrative privileges

This section assumes that you have taken the recommended steps to secure the DSLPipe box, as described in the Chapter 9, “Setting up Security.”

After you have taken the recommended steps, you cannot perform any system administration operations without first supplying the required password. To specify that password:

1 Press Ctrl-D to display the DO menu.

```
50-101 brian-gw
DO...
>0=ESC
 P=Password
```

2 Press P (or select P=Password) to invoke Password command.
A menu of Security Profiles opens.

3 Select Full Access.
The DSLPipe prompts for the password for the Full Access Profile.

```
00-300 Security
Enter Password:
 []

 Press > to accept
```

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 DSLPipe is using the new security level. If the password you enter is incorrect, you are prompted again to enter the password.

Configuring administration options

This section describes the following system administration configurations:

- Setting a system name
- Specifying administrative information in the System Profile
- Setting the Telnet password
- Configuring the DSLPipe to interact with a Syslog daemon

Table 11-1 shows related parameters.

Table 11-1. System management information

Location	Parameters with example values
System > Sys Config (System Profile)	Name=LAB10GW Location=LAB10 Contact=MIS Term Rate=9600 Console=Standard Remote Mgmt=No
Ethernet > Mod Config (Ethernet Profile)	Telnet PW=*SECURE*

Table 11-1. System management information (Continued)

Location	Parameters with example values
Ethernet > Mod Config > Log...	Syslog=Yes Log Host=10.23.45.111 Log Facility=Local5

For details on parameters, see the *Reference Guide.*

Setting the system name

The system name is used in negotiating bridged PPP connections. To set the DSLPipe unit's system name:

1. Open the System Profile.
2. Specify a system name up to 16 characters long.
   For example:
   `Name=LAB10GW`
3. Close the System Profile.

Specifying management information

To configure management information in the System Profile:

1. Open the System Profile.
2. Enter the physical location of the DSLPipe.
   For example:
   `Location=LAB10`
   You can enter up to 80 characters. An SNMP manager can read this field, but its value does not affect the operation of the DSLPipe.
3. Specify a person to contact in case of error conditions.
   For example:
   `Contact=MIS`
   You can enter up to 80 characters. An SNMP manager can read this field, but its value does not affect the operation of the DSLPipe.

4 Specify the data transfer rate of the DSLPipe Terminal port.

For example:

```
Term Rate=9600
```

The default 9600 is appropriate if you are accessing the vt100 interface from a PC connected to the DSLPipe Terminal port. If you are managing a remote Ascend unit, you may want to increase the baud rate on the local terminal to a higher speed for improved performance.

Note: Make sure the Term Rate setting matches the speed configured for your Com Port.

5 Specify the type of console interface to be displayed at power-up.

For example:

```
Console=Standard
```

Currently this is the only value the DSLPipe supports.

6 Specify whether a remote device (across the WAN) will be allowed to operate the DSLPipe.

For example:

```
Remote Mgmt=No
```

Remote management only applies to MPP calls.

7 Close the System Profile.

Setting the Telnet password

To set a Telnet password that will be required of all incoming Telnet connections, including administrative logins to the DSLPipe:

1 Open the Ethernet Profile.

2 Enter a Telnet password up to 20 characters long.

For example:

```
Telnet PW=*SECURE*
```

3 Close the Ethernet Profile.

Configuring the DSLPipe to interact with syslog

To maintain a permanent log of DSLPipe system events and send Call Detail Reporting (CDR) reports to a host that can record and process them, configure

the DSLPipe to report events to a syslog host on the local IP network. Note that syslog reports are only sent out through the Ethernet interface.

To configure the DSLPipe to send messages to a Syslog daemon:

1 Open the Ethernet Profile.

1 Open the Log submenu.

2 Turn on Syslog.

```
Syslog=Yes
```

3 Specify the IP address of the host running the Syslog daemon.

For example:

```
Log Host=10.1.3.7
```

The host running a Syslog daemon is typically a UNIX host, but it may also be a Windows system. If the log host is not on the same subnet as the DSLPipe, the DSLPipe must have a route to that host, either via RIP or a static route.

Note: Do not configure the DSLPipe to send reports to a syslog host that can only be reached by a dial-up connection. That would cause the DSLPipe to dial the log host for every logged action, including hang ups.

4 Set the log facility level.

For example:

```
Log Facility=Local0
```

This parameter is used to flag messages from the DSLPipe. After you set a log facility number, you need to configure the Syslog daemon to write all messages containing that facility number to a particular log file. (That will be the DSLPipe log file.)

5 Close the Ethernet Profile.

To configure the Syslog daemon, you need to modify /etc/syslog.conf on the log host. This file specifies which action the daemon will perform when it receives messages from a particular log facility number (which represents the DSLPipe). For example, if you set Log Facility to Local5 in the DSLPipe, and you want to log its messages in /var/log/DSLPipe, add this line to /etc/syslog.conf:

```
local5.info<tab>/var/log/DSLPipe
```

Note: The Syslog daemon must reread /etc/syslog.conf after it has been changed.

Performing system administration operations

This section describes the following system administration operations:

- Using DO commands to manually place and clear calls
- Restoring and saving a configuration
- Resetting the DSLPipe
- Invoking the terminal server interface

Table 11-2 shows the related system administration commands.

Table 11-2. System administration commands

Location	Commands
System > Sys Diag	Restore Cfg Save Cfg Sys Reset Term Serv

For details on each of these parameters, see the *Reference Guide.*

Using DO commands

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

```
50-101 brian-gw
DO...
>0=ESC
 1=Dial
 P=Password
```

To type a DO command, press and release the vt100 interface Ctrl-D combination, and then press and release the next key in the sequence; for example, press 1 to invoke the DO 1 (Dial) command.

The PF1 function key on a VT-100 monitor is equivalent to the DO key or Ctrl-D.

This is a complete list of DO commands:

- 0=ESC — Abort and exit the DO menu.
- 1=Dial — Dial the selected or current profile (N/A for nailed connections)
- 2=Hang Up— Hang up from a call in progress (N/A for nailed connections)
- 3=Answer — Answer an incoming call. (N/A for nailed connections)
- 4=Extend BW — Increase bandwidth. (N/A for nailed connections)
- 5=Contract BW — Decrease bandwidth. (N/A for nailed connections)
- 8=Beg/End Rem Mgm — Begin/End remote management.
- C=Close TELNET — Close the current Telnet session.
- R=Resynchronize — Resynchronize a call in progress. (N/A for nailed connections)
- L=Load — Load parameter values into the current profile.
- P=Password — Log into or out of a DSLPipe security profile.
- S=Save — Save parameter values into the specified profile.

For details on each of these commands, see the *Reference Guide*.

Saving the DSLPipe configuration

To save the DSLPipe configuration, you must have administrative privileges that include Field Service (such as the Full Access Profile, for example).

Note: When you save the DSLPipe configuration, the configuration data is written to a text file on the disk of the accessing host (the computer connected to the DSLPipe Terminal 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, 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 DSLPipe configuration (except passwords) to disk:

1 Open the Sys Diag menu.

2 Select Save Config and press Enter.

The following message appears:

```
Ready to download - type any key to start...
```

3 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.

4 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.

5 Turn off the Capture feature of your communications program.

6 Print a copy of your configured profiles for later reference.

If you examine the saved DSLPipe 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. Make sure that there are no extra lines of text or characters either before START= or after END=. If there are, delete them; they could cause problems when you try upload the file to the DSLPipe.

Restoring the DSLPipe configuration

To restore the DSLPipe configuration, you must have administrative privileges that include Field Service (such as the Full Access Profile, for example).

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:

1 Connect the backup device to the DSLPipe Terminal port.

The backup device is typically the PC through which you access the vt100 interface.

2 Open the Sys Diag menu.

3 Select Restore Cfg and press Enter.

The following message appears:

```
Waiting for upload data...
```

4 Use the Send ASCII File feature of the communications software to send the DSLPipe 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
```

5 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 the passwords:

6 Press Ctrl-D to invoke the DO menu, select Password, and choose the Full Access profile.

7 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.

See Appendix D, "Upgrading System Software," for related information.

Resetting the DSLPipe

When you reset the DSLPipe, the unit restarts and all active connections are terminated. All users are logged out and the default security level is reactivated. In addition, a system reset can cause a WAN line to temporarily be shut down due to momentary loss of signaling or framing information.

To reset the unit:

1 Open the Sys Diag menu.

2 Select Sys Reset and press Enter.

The DSLPipe asks you to verify that you want to reset.

```
0=ESC
1=Reset
```

3 To confirm, type 1.

During a reset, the DSLPipe clears active connections and runs its Power-On Self Test (POST), just as it would if the unit were power-cycled. If you do not see the POST display, press Ctrl-L.

While the yellow FAULT LED on the front panel is ON, the DSLPipe checks its memory, configuration, installed modules, and lines. If any of the tests fail, the FAULT LED remains on or blinking.

The alarm relay remains closed while the POST is running and opens when the POST completes successfully. When you see this message:

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

Press any key to display the Main Edit Menu.

Using the terminal server interface

This section describes how to use the administrative commands that are available in the terminal server command-line interface. It describes these tasks:

- Invoking and quitting the terminal server interface
- Initiating self-test calls
- Starting a remote management session with a device at the far end of an MP+ connection
- Setting parameters such as terminal type
- Displaying information such as the ARP cache, statistics about specific protocols, or ISDN events.
- Working with IP routes
- Pinging an IP or IPX host
- Logging into an IP host using TELNET

Invoking and quitting the terminal server interface

To invoke the terminal server command-line interface, you must have administrative privileges. See “Activating administrative privileges” on page 11-3.

To open the command-line:

1 Open the Sys Diag menu.

2 Select Term Serv and press Enter.

The command-line prompt will be displayed at the bottom of the vt100 window:

```
ascend%
```

3 To close the command-line, use the QUIT command at the prompt.

For example:

```
ascend% quit
```

The command-line interface closes and the cursor is returned to the vt100 menus.

Note: You could also use the HANGUP or LOCAL command to end the session. When a dial-in user enters the LOCAL command, it begins a Telnet session to the DSLPipe.

The HELP command

To display the list of terminal server commands, type:

```
ascend% ?
```

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
telnet       telnet [ -a|-b ] <hostname> [<port-number>]
tcp          tcp <hostname> <port-number>
ping         ping [-qv] [-c count] [-i wait] [-s packetsize]
ipxping      ipxping <server-name>
```

For help on a particular command, type that command followed by a question mark. For example:

```
show ?
```

Enabling password challenges

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

```
ascend% set all
term = vt100
dynamic password serving = disabled
```

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

```
ascend% set password
```

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

Note: Note that each channel of a connection to a secure site requires a separate password challenge, so for multichannel connections to a secure site, you must leave the terminal server in password mode until all channels have been established. The APP Server utility is an alternative way to allow users to respond to dynamic password challenges obtained from hand-held security cards. For details, see the Chapter 9, “Setting up Security.”

Viewing the ARP cache

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

```
ascend% show arp
```

The output looks similar to this:

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

The output contains these fields:

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 DSLPipe received the ARP packet. ie0 is the Ethernet interface, wanN represents an active WAN interface.
Ref Count	The number of times the address was used.

Viewing interface statistics

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

```
ascend% show if stats
```

The output looks similar to this:

```
Interface  Name      Status  Type   Speed     MTU   InPackets   Outpacket
ie0        ethernet  Up      6      10000000  1500       7385       85384
wan0                 Down    1             0  1500          0           0
wan1                 Down    1             0  1500          0           0
wan2                 Down    1             0  1500          0           0
wanidle0             Up      6      10000000  1500          0           0
lo0        loopback  Up     24      10000000  1500          0           0
```

The output contains these fields:

Interface	ie0 is the Ethernet interface, lo0 is the loopback interface, “wanN” represents each of the active WAN interfaces in the order in which they became active, and wanidle0 is the inactive interface. The inactive interface is the special interface where all routes point when their WAN connections are down.
Name	The name of the profile associated with the interface, or a text name for the interface
Status	The interface status.Up means the interface is functional, but is not necessarily handling an active call. Down means the interface is not functional.

Type	The type of application being used on the interface, as specified in RFC 1213 (MIB-2). For example, 23 indicates PPP and 28 indicates SLIP.
Speed	The data rate in bits per second.
MTU	The maximum packet size allowed on the interface. MTU stands for Maximum Transmission Unit.
InPackets	The number of packets the interface has received.
OutPackets	The number of packets the interface has transmitted.

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

```
ascend% show if totals
```

The output looks similar to this:

```
Name        --Octets-- --Ucast---NonUcast-Discard -Error-Unknown-Same IF-
ie0      i:   7813606   85121      22383       0       0       0        0
         o: 101529978   85306        149       0       0       0        0
wan0     i:          0       0          0       0       0       0        0
         o:          0       0          0       0       0       0        0
wan1     i:          0       0          0       0       0       0        0
         o:          0       0          0       0       0       0        0
wan2     i:          0       0          0       0       0       0        0
         o:          0       0          0       0       0       0        0
wanidle0 i:          0       0          0       0       0       0        0
         o:          0       0          0       0       0       0        0
lo0      i:          0       0          0       0       0       0        0
         o:          0       0          0       0       0       0        0
```

The output contains these fields:

Name	The interface name (same as described immediately above).
Octets	The total number of bytes processed by the interface.
Ucast	Packets with a unicast destination address.
NonUcast	Packets with a multicast address or a broadcast address.
Discard	The number of packets that the interface could not process.
Error	The number of packets with CRC errors, header errors, or collisions.

Unknown	The number of packets the DSLPipe 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.

Viewing TCP/IP information

This section shows how to display information about the following protocols:

- ICMP
- IP
- TCP
- UDP

ICMP statistics

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

```
ascend% show icmp
```

The output looks similar to this:

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

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

IP statistics

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

```
ascend% show ip stats
```

The output looks similar to this:

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

IP address information

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

```
ascend% show ip address
```

The output looks similar to this:

```
Interface   IP Address    Dest IP Address   Netmask          MTU  Status
ie0          10.2.3.4     N/A               255.255.255.224  1500    Up
wan0         0.0.0.0      N/A               0.0.0.0          1500    Down
wan1         0.0.0.0      N/A               0.0.0.0          1500    Down
wan2         0.0.0.0      N/A               0.0.0.0          1500    Down
wanidle0     10.5.7.9     N/A               255.255.255.224  1500    Up
lo0          127.0.0.1    N/A               255.255.255.255  1500    Up
```

The output contains these fields:

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

IP routing information

To display the DSLPipe unit’s entire IP routing table, enter this command:

```
ascend% show ip routes
```

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

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

where <hostname> is a hostname or IP address.

The output looks similar to this:

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

The output contains these fields:

Destination	The target address of a route. To send a packet to this address, the Pipeline will use this route. Note that the router will use the most specific route (having the largest netmask) that matches a given destination.
Gateway	The address of the next hop router that can forward packets to the given destination. Direct routes (without a gateway) do not show a gateway address in the gateway column.
IF	ie0 is the Ethernet interface, lo0 is the loopback interface, "wanN" specifies each of the active WAN interfaces, and wanidle0 is the inactive interface (the special interface where all routes point when their WAN connections are down).
Flg	One of the following characters: • C=Connected (A directly connected route, for example, the Ethernet.) • I=ICMP (ICMP Redirect dynamic route.) • N=NetMgt (Placed in the table via SNMP MIB II.) • R (A RIP dynamic route.) • S=Static (A local IP Route profile or Connection Profile route.) • ?=Unknown (A route of unknown error, which indicates an error.) • G=Gateway (A gateway is required in order to reach this route.) • P=Private (This route will not be advertised via RIP.) • T=Temporary (This route will be destroyed when its interface goes down. • *=Hidden (A hidden route means that there is a better route in the table, so this route is hidden "behind" the better route. If the better route should go away, then this route may be used.)
Pref	The preference value of the route. Note that all routes that come from RIP will have a preference value of 100, while the preference value of each individual static route may be set independently.
Met	The RIP-style metric for the route, with a valid range of 0-16.

Use	This is a count of the number of times the route was referenced since it was created. (Many of these references are internal, so this is not a count of the number of packets sent using this route.)
Age	This is the age of the route in seconds. It is used for troubleshooting, to determine when routes are changing rapidly or flapping.

UDP statistics

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

```
ascend% show udp stats
```

The output looks similar to this:

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

UDP port information

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

```
ascend% show udp listen
```

The output looks similar to this:

```
Socket       Local Port      InQLen
     0              520           0
     1              7             0
     2              123           0
     3              514           0
     4              161           0
     5              162           0
```

The output contains these fields:

Socket	The socket number associated with the port.

Local Port	The UDP port on which the DSLPipe is listening.
InQLen	The input queue length for the port.

TCP statistics

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

```
ascend% show tcp stats
```

The output looks similar to this:

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

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

TCP connection information

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

```
ascend% show tcp connection
```

The output looks similar to this:

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

The output contains these fields:

Socket	The socket associated with the port.
Local	The local IP address and port associated with the connection. For example, if the DSLPipe 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 DSLPipe is listening for a connection, or ESTABLISHED if it has already established one.

Viewing NetWare information

This section shows how to display information about the IPX packets and to view the IPX routing and server tables.

IPX statistics

To display IPX packet statistics, enter this command:

```
ascend% show netware stats
```

The output looks similar to this:

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

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

IPX service information

To display the IPX service table, enter this command:

```
ascend% show netware servers
```

The output looks similar to this:

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

The output contains these fields:

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

IPX routing information

To display the IPX routing table, enter this command:

```
ascend% show netware networks
```

The output looks similar to this:

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

The output contains these fields:

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

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

IPX ping statistics

To display statistics related to the IPXPING command, type:

```
ascend% show netware pings
```

The output looks similar to this:

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

The output shows how many NetWare stations have pinged the Pipeline (InPing requests and replies) and how many times the IPXPING command has been executed in the Pipeline. See “Pinging a NetWare system” on page 11-32.

Viewing frame relay information

This section shows how to display information related to frame relay interfaces.

Frame relay statistics

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

```
ascend% show fr stats
```

The output looks similar to this:

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

The output contains these fields:

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

DLCI status

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

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

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

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

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

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

Link management information

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

```
ascend% show fr lmi
```

The output looks similar to this:

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

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

Viewing system uptime

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

```
ascend% show uptime
```

The output looks similar to this:

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

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

Working with IP routes

In addition to displaying the routing table, you can add or delete routes from the table using terminal server commands.

Note: The IPROUTE SHOW command is an alias to SHOW IPROUTES. See "IP routing information" on page 11-20 for details on the information it displays.

Adding a static route

To add a static route to the DSLPipe unit's routing table, enter the IPROUTE ADD command in this format:

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

iproute add command arguments

The arguments to the IPROUTE ADD command are as follows:

- destination/size

  The destination network address and the subnet mask in Ascend netmask notation. Refer to "Netmask notation" on page 7-2 for more information on the subnet masks.

- gateway
  The IP address of the router that can forward packets to that network.
- pref
  The preference value for the route. When choosing which routes should be put in the routing table, the router first compares the Preference value, preferring the lower number. If the Preference values are equal, the router then compares the Metric field, using the route with the lower Metric.
- metric
  The virtual hop count to the destination network (default 7).
- proto
  The protocol of the route.

For example, enter this command:

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

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

If you try to add a route to a destination that already exists in the routing table, the DSLPipe 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 DSLPipe rejected your attempt to add a route because the routing table already contained the same route with a lower metric. Note that RIP updates can change the metric for the route.

Note: The IPROUTE ADD command adds a static route that is a lost whenever the DSLPipe is reset. For detailed information about IP routing, see Chapter 7, "Setting up IP Routing."

Deleting a route

To remove a route from the DSLPipe unit's routing table, enter the IPROUTE DELETE command in this format:

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

For example:

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

Note: RIP updates can add back any route you remove with IPROUTE DELETE. Also, the DSLPipe restores all routes listed in the Static Route Profile after a system reset.

iproute delete command arguments

The arguments to the IPROUTE DELETE command are as follows:

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

Pinging an IP host

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

The PING command uses this format:

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

For example:

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

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

```
PING 10.1.2.3 (10.1.2.3): 56 data bytes
64 bytes from 10.1.2.3: icmp_seq=0 ttl=255 time=30 ms
64 bytes from 10.1.2.3: icmp_seq=1 ttl=255 time=0 ms
64 bytes from 10.1.2.3: icmp_seq=2 ttl=255 time=0 ms
64 bytes from 10.1.2.3: icmp_seq=3 ttl=255 time=10 ms
64 bytes from 10.1.2.3: icmp_seq=4 ttl=255 time=0 ms
^ C
```

```
--- 10.1.2.3 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0/1/30 ms
```

The output contains this information:

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

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

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

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

PING command arguments

The arguments to the PING command are:

- hostname

  The IP address or name of the host.
- [-q]

  (Optional.) Use quiet input. Do not display any informational messages, except the summary lines at the beginning and end of the command.
- [-v]

  (Optional.) Use verbose output. The DSLPipe lists all ICMP packets received, except echo_response packets.
- [-c count]

  (Optional.) Stop the test after sending and receiving the number of packets specified by count.
- [-i delay]

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

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

Pinging a NetWare system

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

Enter the IPXPING command in this format:

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

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

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

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

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

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

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

During the IPXPING exchange, the DSLPipe calculates and reports this information:

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

These statistics include the following information:

- The IPX address of the source and destination nodes.
- The byte counts of the request and response packets.
- The PING ID of the command. (The PING Request # replied to by target host.)
- The number of milliseconds required to send the IPXPING and receive a response.
- The number of packets transmitted and received.
- Duplicate or damaged packets, if applicable.
- Average round-trip times for the PING request and reply.
  In some cases, round-trip times cannot be calculated.

IPXPING command arguments

The arguments to the IPXPING command are:

- servername
  The advertised name of the IPX server.
- [-c count]
  (Optional.) Stop the test after sending and receiving the number of packets specified by count.
- [-i delay]
  (Optional.) Wait the number of seconds specified by wait before sending the next packet. The default is one second.
- [-s packet-size]
  (Optional.) Send the number of data bytes specified by packet-size. The default is 56 bytes. packet-size does not include the 8-byte ICMP header.
- [net#:node#]
  The IPX network and node number of an IPX host.
  - The network number can be 0x00000000 (the local network) to 0xfffffffe
  - The node number can be 0x0000000001 to 0xfffffffffe

Logging into an IP host using TELNET

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

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

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

```
ascend% telnet myhost
```

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

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

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

In the example commands in this section, the Telnet prompt is the word "telnet" followed by a greater-than sign (telnet>). When you see that prompt, you can enter any of the TELNET commands described in "Telnet session commands" on page 11-35.

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

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

```
telnet> quit
```

TELNET command arguments

The arguments to the TELNET command are as follows:

- <hostname>

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

- [–a]

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

- [–b]

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

  Note: Note that the Telnet escape sequence does not operate in 8-bit binary mode. The Telnet session can close only if one end of the connection quits the session. Therefore, a local user not connected through a dial up connection cannot quit the session; he or she must wait for the remote user to close the session.

- [<port-number>]

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

Telnet session commands

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

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

```
telnet> ?
```

or

```
telnet> help
```

To open a Telnet connection after invoking TELNET, use the OPEN command. The arguments you specify are exactly the same as those for opening a connection from the TELNET command-line, except for that the OPEN command does not support the -a and -b options. See “TELNET command arguments” on page 11-34. For example:

```
telnet> open myhost
```

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

```
telnet> send susp
```

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

```
telnet> send ?
```

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

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

To display current settings, type:

```
telnet> set all
```

To see a list of SET commands, type:

```
telnet> set ?
```

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

```
telnet> close
```

or:

```
telnet> quit
```

TELNET error messages

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

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

Opening a raw TCP connection to an IP host

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

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

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

```
ascend% tcp myhost
```

TCP command arguments

The arguments to the TCP command are as follows:

- <hostname>

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

- [<port-number>]

  (Optional.) You can specifies the port to use for the session. The port number typically indicates a custom application that runs on top of the TCP session. For example, port number 23 starts a Telnet session. However, terminating the Telnet session does not terminate the raw TCP session.

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

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

TCP error messages

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

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

`no connection: host unreachable`	The destination host is unreachable.
`no connection: net unreachable`	The destination network is unreachable.

Safety and Warranty Information

A

FCC Part 15

Caution: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. The limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and, if not installed and used in accordance with the instruction manual, might cause harmful interference to radio communications. Operation in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his or her own expense.

The authority to operate this equipment is conditioned by the requirement that no modifications will be made to the equipment unless the changes or modifications are expressly approved by Ascend.

Canadian Notice

Note: The Canadian Department of Communications label identifies certified equipment. The certification means that the equipment meets certain telecommunications network protective, operational and safety requirements. The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should make sure that its connection to the facilities of the local telecommunications company is permissible and that the method used for connection is acceptable. In some cases, the company's inside

wiring associated with a single line individual service may be extended by means of a certified connector assembly (telephone extension cord). The customer should be aware that compliance with the above conditions might not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Equipment malfunctions or any repairs or alterations made by the user might give the telecommunications company cause to request that the user disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution can be particularly important in rural areas.

Warning: Users should not attempt to make such connections themselves, but should contact the electric inspection authority or an electrician, as appropriate.

A *Load Number (LN)* is assigned to each terminal device to help prevent overloading. The LN denotes a percentage of the total load to be connected to a telephone loop used by the device. The termination on a loop may consist of any combination of devices so long as the total of the Load Numbers of all the devices does not exceed 100.

Caution: THE DIGITAL APPARATUS DOES NOT EXCEED THE CLASS A LIMITS FOR RADIO NOISE EMISSIONS FROM DIGITAL APPARATUS SET OUT IN THE RADIO INTERFERENCE REGULATIONS OF THE CANADIAN DEPARTMENT OF COMMUNICATIONS.

LE PRESENT APPAREIL NUMERIQUE N'EMET PAS DE BRUITS RADIOELECTRIQUES DEPASSANT LES LIMITES APPLICABLES AUX APPAREILS NUMERIQUES DE LA CLASSE A PRESCRITES DANS LE REGLEMENT SUR LE BROUILLAGE RADIOELECTRIQUE EDICTE PAR LE MINISTERE DES COMMUNICATIONS DU CANADA.

Product warranty

1. Ascend warrants that the DSLPipe will be free from defects in material and workmanship for a period of twelve (12) months from date of shipment.
2. Ascend shall incur no liability under this warranty if
   - the allegedly defective goods are not returned prepaid to Ascend within thirty (30) days of the discovery of the alleged defect and in accordance with Ascend's repair procedures; or
   - Ascend's tests disclose that the alleged defect is not due to defects in material or workmanship.
3. Ascend's liability shall be limited to either repair or replacement of the defective goods, at Ascend's option.
4. Ascend MAKES NO EXPRESS OR IMPLIED WARRANTIES REGARDING THE QUALITY, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE BEYOND THOSE THAT APPEAR IN THE APPLICABLE Ascend USER'S DOCUMENTATION. Ascend SHALL NOT BE RESPONSIBLE FOR CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGE, INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFITS OR DAMAGES TO BUSINESS OR BUSINESS RELATIONS. THIS WARRANTY IS IN LIEU OF ALL OTHER WARRANTIES.

Warranty repair

1. During the first three (3) months of ownership, Ascend will repair or replace a defective product covered under warranty within twenty-four (24) hours of receipt of the product. During the fourth (4th) through twelfth (12th) months of ownership, Ascend will repair or replace a defective product covered under warranty within ten (10) days of receipt of the product. The warranty period for the replaced product shall be ninety (90) days or the remainder of the warranty period of the original unit, whichever is greater. Ascend will ship surface freight. Expedited freight is at the customer's expense.
2. The customer must return the defective product to Ascend within fourteen (14) days after the request for replacement. If the defective product is not returned within this time period, Ascend will bill the customer for the product at list price.

Out-of-warranty repair

Ascend will either repair or, at its option, replace a defective product not covered under warranty within ten (10) working days of its receipt. Repair charges are available from the Repair Facility upon request. The warranty on a serviced product is thirty (30) days measured from date of service. Out-of-warranty repair charges are based upon the prices in effect at the time of return.

Hardware Specifications

B

DSLPipe specifications

This section provides the specifications for the DSLPipe.

Table 11-3. Physical specifications

Physical connectors	RJ11 for RADSL 10 Base-T for Ethernet
Connector requirements	Must meet JIS C 5973 standards
Dimensions	5.6 in high x 10.7 in long (14.2 cm x 27 cm)
Weight	~2 pounds (0.9 kg)
Operating humidity	0-90%, non-condensing
Operating temperature	32-104˚ F (0-40˚ C)

How to convert a DSLPipe-S to a COE unit

Each DSLPipe is designed to be used for a very specific purpose, including whether or not it functions as Customer Premises Equipment (CPE) or Central Office Equipment (COE). The facilities performed by the unit at either end are different. The unit at the central office is the ‘master’ unit.

The DSLPipe-S is configured for use at the customer's premises at the factory, but you can change the DSLPipe-S (not the DSLPipe-C) to central office equipment by opening the case and setting a jumper.

To make the conversion, do the following tasks:

1 Open the case of the DSLPipe-S.

2 On the circuit board, locate the three jumpers above U19. (U19 is clearly silk screened on the board.)

3 There are three jumpers above U19. Put a jumper on P2 (which also has a silk screened label identifying it).

You can now use this DSLPipe-S to perform COE facilities.

SDSL Central Office Setup

C

Introduction

The central-office setup of the SDSL uses a MAX TNT with an SDSL slot card. The configuration is described below.

Installing the SDSL card

The SDSL card is illustrated in Figure 12.

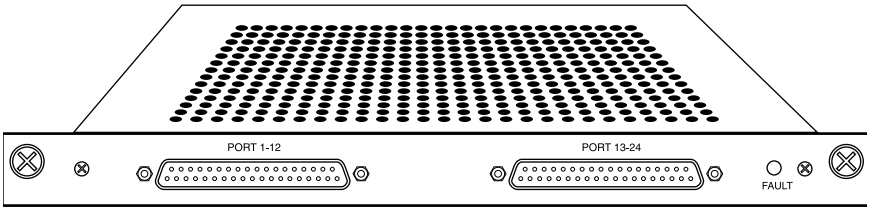


Figure 12. DSLPipe SDSL card

To install the SDSL card:

1 Hold the expansion card with the thumbscrew facing you and insert the card into the open slot as shown in Figure 13.

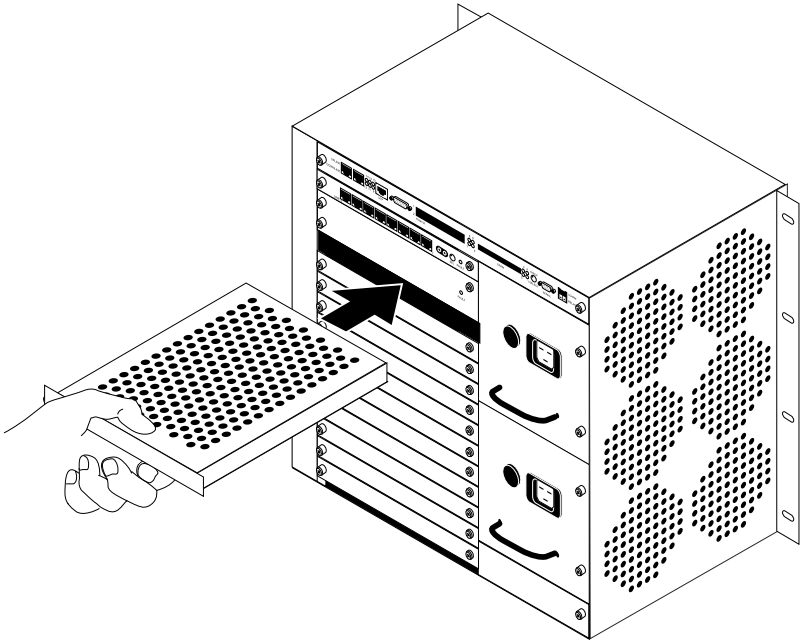


Figure 13. Inserting an expansion card into a DSLPipe slot

2 Push the card along the internal card guides until the thumbscrew on the right side of the card is seated in the hole in the backpanel. The panel of the expansion card should touch the back panel of the DSLPipe.

Caution: Do not force the expansion card into the slot. Doing so can damage the card or slot connector.

3 Tighten the thumbscrews on the card, as shown in Figure 14.

Note: All DSLPipe expansion cards are hot-swappable, meaning that you can safely insert or remove cards while the DSLPipe power is on.

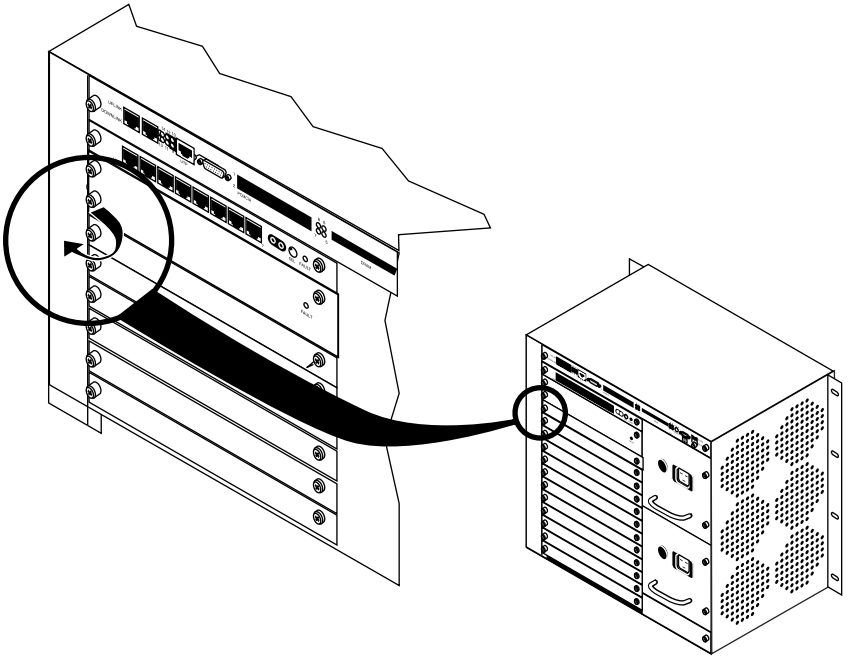


Figure 14. Tightening expansion card thumbscrews

The next section provides an example SDSL configuration.

Example central office SDSL configuration

Configuring an SDSL connection requires these general steps:

- Configuring the SDSL profile on the MAX TNT
- Configuring the Connection profile
- Configuring the Frame Relay profile
- Configuring the DSLPipe

Configuring the SDSL profile on the MAX TNT

To configure the SDSL profile:

1 Read in the SDSL profile. For example, if the SDSL card is installed in slot 11 of shelf 1 and the remote DSLPipe is connected to port 1, enter:

```
admin> read sdsl {1 11 1}
```

2 List the profile:

```
admin> list
```

3 Enable the port:

```
admin> set enabled=yes
```

4 List the contents of the line config profile:

```
admin> list line-config
```

5 Assign this port to a nailed group:

```
admin> set nailed-up-group=1
```

This nailed group points the Frame Relay profile you will create later. The nailed group must be unique for each active WAN interface.

6 Move up to the top-level profile:

```
admin> list..
```

7 Write the profile:

```
admin> write
```

Configuring the Connection profile

To configure the Connection profile:

1 Create a new Connection profile:

```
admin> new con coe-11-1
```

2 List the profile:

```
admin> list
```

3 Enable the profile:

```
admin> set active=yes
```

4 Set the encapsulation type to Frame Relay:

```
admin> set encapsulation-protocol=frame relay
```

5 List the IP options submenu:

```
admin> list ip-options
```

6 Set the IP address of the DSLPipe connecting to the DSLPipe.

```
admin> set remote-address=192.168.216.141/24
```

7 Set the IP address of the DSLPipe SDSL port.

```
admin> set local-address=192.168.215.135/24
```

8 Move up to the higher-level profile:

```
admin> list..
```

9 List the Frame Relay options submenu:

```
admin> list fr-options
```

10 Link this Connection profile to the Frame Relay profile you will create in the next section:

```
admin> set frame-relay-profile=fr-prof-1
```

11 Set the DLCI to the same value as the DSLPipe:

```
admin> set dlci=16
```

12 Write the profile:

```
admin> write
```

Configuring the Frame Relay profile

To configure the Frame Relay profile:

1 Create a new Connection profile:

```
admin> new frame-relay fr-prof-1
```

2 List the profile:

```
admin> list
```

3 Enable the profile:

```
admin> set active=yes
```

4 Assign the Frame Relay profile to a nailed-up group:

```
admin> set nailed-up-group=1
```

This must be the same as the SDSL nailed group number you configured in the SDSL profile. The nailed group must be unique for each active WAN interface.

5 Write the profile:

```
admin> write
```

Configuring the DSLPipe

Before you configure the Pipeline, make sure:

- the PC connected to the Pipeline has an IP address on the same subnet as the Pipeline
- the IP address of the Pipeline is configured as the default gateway for the PC

To configure the Pipeline:

1 From the Main Edit menu, select Configure.

2 Specify the following values:

- Chan Usage=**Leased/Unused**
- My Name=**cpe**
- My Addr=**192.168.216.141/24**
- Rem Name=**coe-11-1**
- Rem Addr=**192.168.215.135/24**

- Route=**IP**

3 Exit and save the Configure profile.

4 From the Main Edit menu, select Ethernet>Connections>coe-11-1.

5 Specify the following values:

- Active=**Yes**
- Encaps=**FR**
- Route IP=**Yes**

6 Open the Encaps Options submenu.

7 Specify the DLCI used for this profile:

- FR Prof=**16**

8 Exit and save the Connection profile.

Troubleshooting

If the SDSL link between the DSLPipe and the DSLPipe does not come up after a few seconds, try these troubleshooting steps:

Action	Example
Check that the card is active.	admin> **read sdsl-statistics {1 11 1}** admin> **list** Verify that active=yes.
Check that the card passed POST.	admin> **read sdsl-statistics {1 11 1}** admin> **list** Verify that self test=passed.
Check the data transfer rates.	admin> **read sdsl-status {1 11 1}** admin> **list** Verify that self up-stream-rate=784000 and down-stream-rate=784000.

SDSL line card specifications

This section provides the specifications for the SDSL line card.

Transfer rate	768 Kbps (symmetric)
Transmission distance	12,000 feet (3.7 km)
Interfaces per card	16 ports per card, up to 15 cards per system
Physical connectors	2 DB37 to 50-pin telco connectors
Connector requirements	Must meet JIS C 5973 standards
Card dimensions	8.8 in high x 10.6 in long (22.35 cm x 26.92 cm)
Card weight	~3 pounds (1.37 kg)
Operating humidity	0-90%, non-condensing
Operating temperature	32-104˚ F (0-40˚ C)

Cabling specifications

This section provides the cable specifications for the DB37 to 50-pin telco cable that ships with the SDSL card.

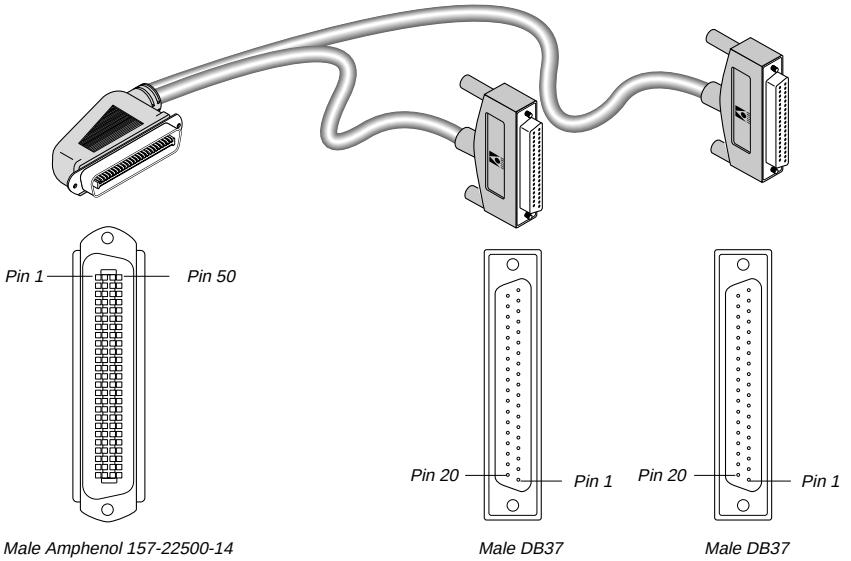


Figure 15. DB37 to 50-pin telco cable

Table 15-1. DB37 to 50-pin telco cable pinouts

P1 Pin	P2 Pin	J1 Pin	Signal
36		1	Tip1
37		26	Ring 1
18		2	Tip 2
19		27	Ring 2
16		3	Tip 3
17		28	Ring 3
14		4	Tip 4

Table 15-1. DB37 to 50-pin telco cable pinouts (Continued)

P1 Pin	P2 Pin	J1 Pin	Signal
15		29	Ring 4
12		5	Tip 5
13		30	Ring 5
10		6	Tip 6
11		31	Ring 6
8		7	Tip 7
9		32	Ring 7
6		8	Tip 8
7		33	Ring 8
4		9	Tip 9
5		34	Ring 9
2		10	Tip 10
3		35	Ring 10
1		11	Tip 11
20		36	Ring 11
21		12	Tip 12
22		37	Ring 12
	36	13	Tip 13
	37	38	Ring 13

Table 15-1. DB37 to 50-pin telco cable pinouts (Continued)

P1 Pin	P2 Pin	J1 Pin	Signal
	18	14	Tip 14
	19	39	Ring 14
	16	15	Tip 15
	17	40	Ring 15
	14	16	Tip 16
	15	41	Ring 16
	12	17	Tip 17
	13	42	Ring 17
	10	18	Tip 18
	11	43	Ring 18
	8	19	Tip19
	9	44	Ring 19
	6	20	Tip 20
	7	45	Ring 20
	4	21	Tip 21
	5	46	Ring 21
	2	22	Tip 22
	3	47	Ring 22
	1	23	Tip 23

Table 15-1. DB37 to 50-pin telco cable pinouts (Continued)

P1 Pin	P2 Pin	J1 Pin	Signal
	20	48	Ring 23
	21	24	Tip 24
	22	49	Tip 24

Upgrading System Software

D

What you need to upgrade system software

Ascend system software is continually being enhanced to support new features and improve performance. The DSLPipe 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 DSLPipe 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 DSLPipe.

4 Restore your DSLPipe 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 DSLPipe and which Security profile is activated.

To see which software version is currently running on the DSLPipe, look in the Sys Option status window. See “The DSLPipe menus and status displays” on page 3-1 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).

```
Main Edit Menu
DO...
>0=ESC
 P=Password
```

```
Main Edit Menu
 Security Profile...?
 00-301 Default
 00-302
 00-301 Full Access
```

The DSLPipe then prompts for that profile’s password.

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

```
00-300 Security
Enter Password:
 []

 Press > to accept
```

If you enter the right password, a message states that the password was accepted and the DSLPipe 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 DSLPipe configuration

Before you overwrite the software in the DSLPipe, make sure that you save your existing configuration to disk.

Note: When you backup the DSLPipe configuration, the configuration data is written to a text file on the disk of the accessing host (the computer connected to the DSLPipe 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 DSLPipe 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 DSLPipe 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 DSLPipe in boot mode:

1. From any menu in the DSLPipe 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 DSLPipe. Your communications program begins sending the binary file to your DSLPipe. 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 DSLPipe 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 DSLPipe. Continue to the next section.

Restoring the DSLPipe 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 DSLPipe 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 DSLPipe 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 DSLPipe, re-activate the appropriate Security profile. Use the procedure explained in “Activating a Security Profile” on page D-2 and select the appropriate Security Profile.

Index

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

W

X