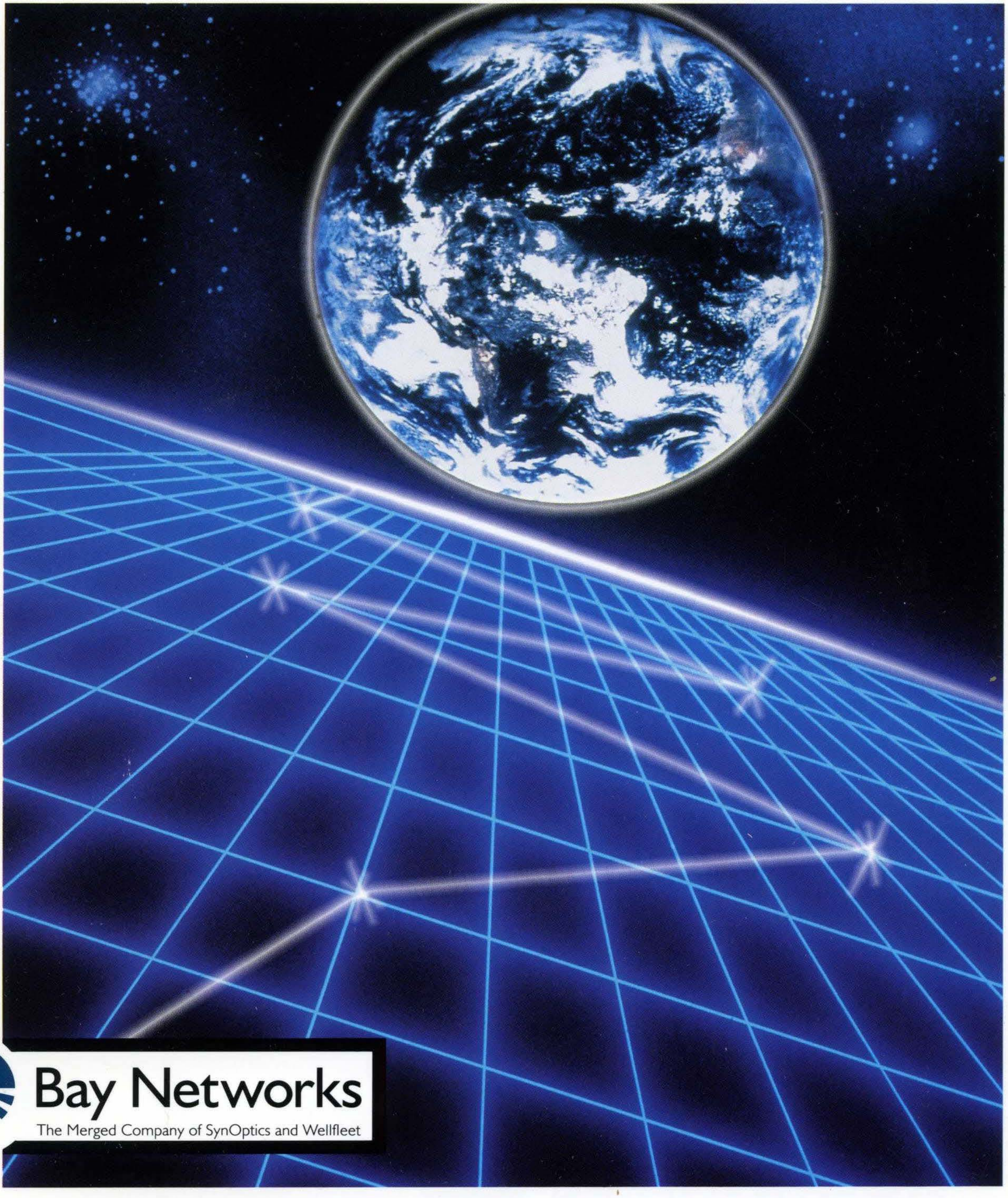


Bay Networks

The Merged Company of SynOptics and Wellfleet

Customizing PPP Services

Part No. 110060 A

Customizing PPP Services

Router Software Version 8.10
Site Manager Software Version 2.10

Part No. 110060 Rev. A
February 1995

Bay Networks
The Merged Company of SynOptics and Wellfleet

Restricted Rights Legend

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notice for All Other Executive Agencies

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Trademarks of Bay Networks, Inc.

ACE, BLN, BN, and Wellfleet are registered trademarks and AFN, AN, ASN, BCN, BCNX, BLNX, BNX, CN, FN, FRE, LN, PPX, Bay Networks, and the Bay Networks logo are trademarks of Bay Networks, Inc.

Third-Party Trademarks

3Com is a registered trademark of 3Com Corporation.

AIX, NetView, and IBM are registered trademarks of International Business Machines Corporation.

AppleTalk and EtherTalk are registered trademarks of Apple Computer, Inc.

AT&T and ST are registered trademarks of American Telephone and Telegraph Company.

DEC, DECnet, VAX, and VT100 are trademarks of Digital Equipment Corporation.

Distinct is a registered trademark and Distinct TCP/IP is a trademark of Distinct Corporation.

Fastmac and MADGE are trademarks of Madge Networks, Ltd.

Hayes is a registered trademark of Hayes Microcomputer Products, Inc.

HP is a registered trademark of Hewlett-Packard Company.

Intel is a registered trademark of Intel Corporation.

IPX, NetWare, and Novell are registered trademarks of Novell, Inc.

MCI is a registered trademark of MCI Communications Corporation.

Microsoft, MS, and MS-DOS are registered trademarks and Windows is a trademark of Microsoft Corporation.

Motif and OSF/Motif are registered trademarks of Open Software Foundation, Inc.

Motorola is a registered trademark of Motorola, Inc.

NetBIOS is a trademark of Micro Computer Systems, Inc.

Open Look and UNIX are registered trademarks of UNIX System Laboratories, Inc.

Sun and Solaris are registered trademarks and SPARCstation is a trademark of Sun Microsystems, Inc.

VINES is a registered trademark of Banyan Systems Incorporated.

X Window System is a trademark of the Massachusetts Institute of Technology.

Xerox is a registered trademark and XNS is a trademark of Xerox Corporation.

All other trademarks and registered trademarks are the property of their respective owners.

Bay Networks, Inc., 8 Federal Street, Billerica, MA 01821

Bay Networks Software License

This Software License shall govern the licensing of all software provided to licensee by Bay Networks ("Software"). Bay Networks will provide licensee with Software in machine-readable form and related documentation ("Documentation"). The Software provided under this license is proprietary to Bay Networks and to third parties from whom Bay Networks has acquired license rights. Bay Networks will not grant any Software license whatsoever, either explicitly or implicitly, except by acceptance of an order for either Software or for a Bay Networks product ("Equipment") that is packaged with Software. Each such license is subject to the following restrictions:

1. Upon delivery of the Software, Bay Networks grants to licensee a personal, nontransferable, nonexclusive license to use the Software with the Equipment with which or for which it was originally acquired, including use at any of licensee's facilities to which the Equipment may be transferred, for the useful life of the Equipment unless earlier terminated by default or cancellation. Use of the Software shall be limited to such Equipment and to such facility. Software which is licensed for use on hardware not offered by Bay Networks is not subject to restricted use on any Equipment, however, unless otherwise specified on the Documentation, each licensed copy of such Software may only be installed on one hardware item at any time.

2. Licensee may use the Software with backup Equipment only if the Equipment with which or for which it was acquired is inoperative.

3. Licensee may make a single copy of the Software (but not firmware) for safekeeping (archives) or backup purposes.

4. Licensee may modify Software (but not firmware), or combine it with other software, subject to the provision that those portions of the resulting software which incorporate Software are subject to the restrictions of this license. Licensee shall not make the resulting software available for use by any third party.

5. Neither title nor ownership to Software passes to licensee.

6. Licensee shall not provide, or otherwise make available, any Software, in whole or in part, in any form, to any third party. Third parties do not include consultants, subcontractors, or agents of licensee who have licensee's permission to use the Software at licensee's facility, and who have agreed in writing to use the Software only in accordance with the restrictions of this license.

7. Third-party owners from whom Bay Networks has acquired license rights to software that is incorporated into Bay Networks products shall have the right to enforce the provisions of this license against licensee.

8. Licensee shall not remove or obscure any copyright, patent, trademark, trade secret, or similar intellectual property or restricted rights notice within or affixed to any Software and shall reproduce and affix such notice on any backup copy of Software or copies of software resulting from modification or combination performed by licensee as permitted by this license.

9. Licensee shall not reverse assemble, reverse compile, or in any way reverse engineer the Software. [Note: For licensees in the European Community, the Software Directive dated 14 May 1991 (as may be amended from time to time) shall apply for interoperability purposes. Licensee must notify Bay Networks in writing of any such intended examination of the Software and Bay Networks may provide review and assistance.]

10. Notwithstanding any foregoing terms to the contrary, if licensee licenses the Bay Networks product "Site Manager," licensee may duplicate and install the Site Manager product as specified in the Documentation. This right is granted solely as necessary for use of Site Manager on hardware installed with licensee's network.

11. This license will automatically terminate upon improper handling of Software, such as by disclosure, or Bay Networks may terminate this license by written notice to licensee if licensee fails to comply with any of the material provisions of this license and fails to cure such failure within thirty (30) days after the receipt of written notice from Bay Networks. Upon termination of this license, licensee shall discontinue all use of the Software and return the Software and Documentation, including all copies, to Bay Networks.

12. Licensee's obligations under this license shall survive expiration or termination of this license.

Contents

Chapter 1
PPP Overview

Chapter 2
Implementation Notes

Chapter 3
Editing PPP Parameters

Figures

Tables

About This Guide

If you are responsible for configuring and managing Wellfleet® routers running over Point-to-Point links, you need to read this guide.

This guide describes Point-to-Point Protocol (PPP) services and provides instructions for using Site Manager to configure PPP parameters for your network.

Refer to this guide for

- ❐ An overview of Point-to-Point Protocol services (Chapter 1)
- ❐ Information about the Bay Networks implementation of PPP services (Chapter 2)
- ❐ Descriptions of PPP parameters and instructions for editing those parameters (Chapter 3)

For information and instructions about the following topics, see *Configuring Wellfleet Routers*.

- ❐ Initially configuring and saving a WAN interface
- ❐ Retrieving a configuration file
- ❐ Rebooting the router with a configuration file

Before You Begin

Before using this guide, you must complete the following procedures:

- ❒ Create and save a configuration file that contains at least one PPP interface.
- ❒ Retrieve the configuration file in local, remote, or dynamic mode.

Refer to *Configuring Bay Networks Routers* for instructions.

How to Get Help

For additional information or advice, contact the Bay Networks Help Desk in your area:

United States	1-800-2LAN-WAN
Valbonne, France	(33) 92-966-968
Sydney, Australia	(61) 2-903-5800
Tokyo, Japan	(81) 3-328-0052

Conventions

arrow character (➔)

Separates menu and option names in instructions. Example: Protocols➔AppleTalk identifies the AppleTalk option in the Protocols menu.

user entry text

Denotes text that you need to enter. Example: Start up the Windows environment by entering the following after the prompt: **win**

command text

Denotes command names in text. Example: Use the **xmodem** command.

italic text

Indicates variable values in command syntax descriptions, new terms, file and directory names, and book titles.

`screen text`

Indicates data that appears on the screen. Example: `Set Trap Monitor Filters`

quotation marks (" ")

Indicate the title of a chapter or section within a book.

vertical line (|)

Indicates that you enter only one of the parts of the command. The vertical line separates choices. Do not type the vertical line when entering the command.

Example: If the command syntax is

show at routes | nets, you enter either

show at routes or **show at nets**, but not both.

Acronyms

ATCP	AppleTalk Control Protocol
BNCP	Bridge Network Control Protocol
BOFL	Breath of Life (message)
CHAP	Challenge Handshake Authentication Protocol
DNCP	DECnet Network Control Protocol
FDDI	Fiber Distributed Data Interface
HDLC	High-level Data Link Control
HSSI	high speed synchronous links
IP	Internet Protocol
IPCP	IP Control Protocol
IPX	Internet Packet Exchange
IPXCP	IPX Control Protocol
LCP	Link Control Protocol
LQM	Link Quality Monitoring
LQR	Link Quality Report
MAC	media access control
MIB	Management Information Base
MTU	maximum transmission unit
NCP	Network Control Protocol
OSI	Open Systems Interconnection
OSINLCP	OSI Network Layer Control Protocol
PAP	Password Authentication Protocol
SMDS	Switched Multimegabit Data Services
SNMP	Simple Network Management Protocol
VNCP	Vines Network Control Protocol
WAN	wide area network
XNSCP	Xerox Network System Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol

Chapter 1
PPP Overview

This chapter provides an overview of Wellfleet Point-to-Point Protocol (PPP) services.

PPP Functions

PPP provides a standard method to route or bridge datagrams between peer routers over serial point-to-point links (Figure 1-1).

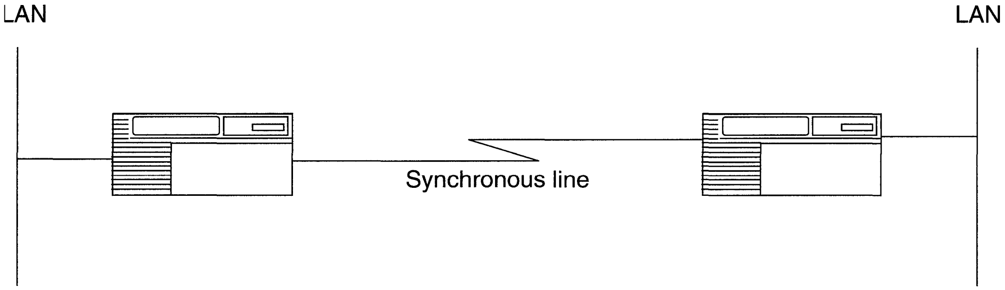


Figure 1-1. Point-to-Point Network Connection

PPP provides three major functions:

- Data link layer connection and management
- Network layer connection and management
- Datagram encapsulation

PPP uses a suite of data link and network control protocols to connect peer routers. PPP also allows peer routers to negotiate and determine data link and network layer options (see Table 1-1 and Table 1-2). When negotiations successfully complete, PPP encapsulates the data and transmits it over the link.

Table 1-1. Data Link Control Protocol Options

Option	Function or Values
Maximum Receive Unit	Specifies the Maximum Transmission Unit (MTU) size for the line.
Authentication protocol: Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP)	Imposes network security by requiring an authentication process that identifies the caller and receiver to each other.
Chap Name	Establishes data link layer connection for dial-on-demand and dial backup lines without requirement to configure IP or IPX Network Control Protocols (NCPs).
Quality Protocol	Specifies the link quality reporting period.

Table 1-2. Network Control Protocols and Options

Protocol	Negotiable Options
IP Control Protocol (IPCP)	IP Addresses (for backward compatibility), IP Address (default)
Internet Package Exchange Control Protocol (IPXCP)	IPX Network Number, IPX Node Number, IPX Routing Protocol, IPX Router Name, IPX Configuration Complete
AppleTalk® Control Protocol (ATCP)	AppleTalk Network Number, AppleTalk Node Number, AppleTalk Routing Protocol
DECnet™ Phase IV Control Protocol (DNCP)	None
OSI Network Layer Control Protocol (OSINLCP)	None
Xerox® Network System Control Protocol (XNSCP)	None
VINES® Network Control Protocol (VNCP)	None
Bridge Network Control Protocol (BNCP)	MAC Type Selection

Routing over a PPP Link

PPP allows you to enable the following routing protocols over PPP interfaces:

- AppleTalk
- DECnet Phase IV
- Internet Packet Exchange Protocol (IPX)®
- Internet Protocol (IP)
- Open System Integration (OSI)
- XNS™
- VINES

Transparent/Translation Bridge and Source Routing Bridge are other routing media that you can enable over any PPP interface. The PPP bridge accepts incoming traffic from any media (Ethernet, FDDI, Token Ring) and forwards data transparently (or translates when necessary).

Initializing a PPP Interface

PPP creates an interface between peer routers that allows the routers to exchange data. Interface initialization consists of three phases:

- Link establishment
- Authentication
- Network layer protocol negotiations

The following sections describe each phase.

Establishing the PPP Link

PPP's Link Control Protocol (LCP) helps establish a link. LCP generates three types of packets:

- Link Configuration packets, including Configure-Request, Configure-ACK, Configure-NAK, and Configure-Reject packets
- Link Termination packets, including Terminate-Request and Terminate-ACK packets
- Link Maintenance packets, including Code-Reject, Protocol-Reject, Echo-Request, and Echo-Reply packets

When two routers initialize a PPP dialogue, each of them sends a Configure-Request packet to the other (peer) router. Each Configure-Request packet contains a list of LCP options and corresponding values that the sending router wants to use to define its end of the link. For example, a Configure-Request packet may specify the link's MTU size and whether the sender wants to use Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP). The Configure-Request packet contains the user-configured values, which the sender and its peer router may need to negotiate.

Each router receives a Configure-Request packet from its peer. Each router responds with one of three types of packets:

- Configure-ACK

  If a router accepts the proposed LCP options, it responds with a Configure Acknowledgment (ACK) packet.

  When the routers on each side of the link send and receive Configure-ACK packets, the LCP advances to an "open state," meaning that the PPP interface can advance to the next phase.

- Configure-Reject

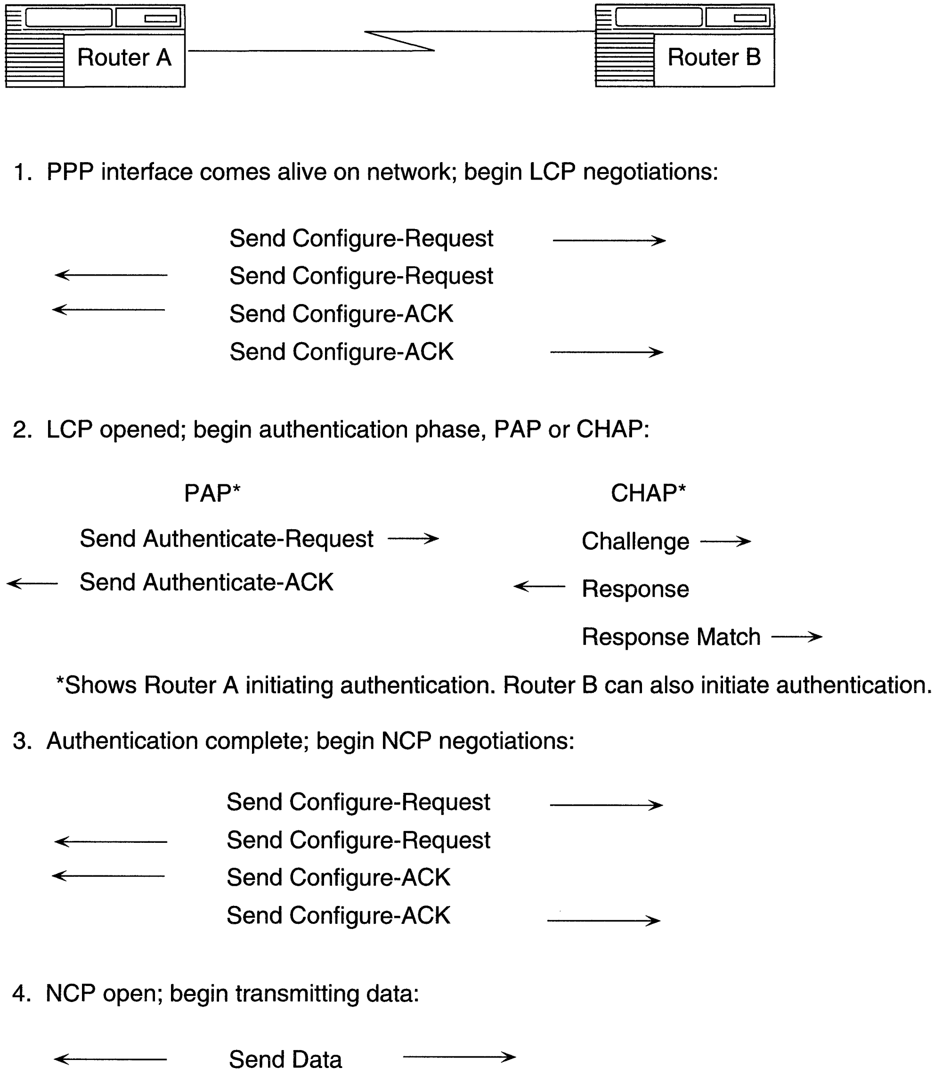
  If the Configure-Request packet contains options that the peer router is not willing to negotiate, the peer router sends back a Configure-Reject packet specifying the non-negotiable options. From that point on, Configuration-Request packets the originating router sends should no longer specify the unacceptable options.

- Configure-NAK

  If the Configure-Request packet contains proposed values for options that the peer disagrees with, it responds with a Configure Negative Acknowledgment (NAK) packet. The Configure-NAK packet notes the values that the peer disagrees with and includes the corresponding values that the peer would like to see in subsequent Configure-Request packets.

LCP negotiations between peers continue until either the routers converge (reach an agreement regarding the Configure Request) and PPP advances to the next phase, or the peer router transmits a user-specified number of Configure-NAK packets before sending a Configure Reject packet. When the originating router receives a Configure Reject packet, the originating router removes the offending options. The routers should then converge.

Figure 1-2 demonstrates how a PPP interface initializes.



1. PPP interface comes alive on network; begin LCP negotiations:

Send Configure-Request →

← Send Configure-Request

← Send Configure-ACK

Send Configure-ACK →

2. LCP opened; begin authentication phase, PAP or CHAP:

PAP*

Send Authenticate-Request →

← Send Authenticate-ACK

CHAP*

Challenge →

← Response

Response Match →

*Shows Router A initiating authentication. Router B can also initiate authentication.

3. Authentication complete; begin NCP negotiations:

Send Configure-Request →

← Send Configure-Request

← Send Configure-ACK

Send Configure-ACK →

4. NCP open; begin transmitting data:

← Send Data →

Figure 1-2. PPP Interface Initialization

Authenticating the PPP Link: PAP and CHAP

The second phase of PPP initialization, authentication, is optional. Authentication occurs only if one or both of the peer routers enables either Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP).

Password Authentication Protocol (PAP)

PAP imposes network security by requiring the peer router to send a PAP packet that contains a plain-text user identifier and password to the originating router before the interface can advance to the network layer protocol phase.

If PAP fails, the network administrator must change the identifier and password on both peer routers and disable and re-enable LCP so that line initialization starts over.

Challenge Handshake Authentication Protocol (CHAP)

CHAP imposes network security by requiring that the peer routers share a plain-text secret. The originating router sends a challenge message to its peer. The peer responds with a value it calculates on the basis of knowing the secret. The first router then matches the response against its own calculation of what the response should be. If the values match, the LCP establishes the link.

CHAP uses an incrementally changing identifier and a variable challenge value to provide network security. It also allows for repeated challenges at intervals that either router on a link can specify. A router may transmit challenge packets not only during the link establishment phase, but also at any time during the network layer protocol phase to ensure that the connection retains its integrity.

If CHAP fails, the network administrator must change the identifiers and secret on both peer routers, and disable and re-enable LCP to re-initialize the line.

Note: If you implement CHAP, you must use Chap Name for router identification on dial-on-demand and dial backup circuits. Conversely, if you configure a dial-on-demand or dial backup circuit using IP or IPX for identification, you cannot use CHAP for authentication.

Establishing Network Connections

PPP uses the services of various network control protocols (NCPs) to determine the values of parameters during the third phase of PPP initialization, network layer negotiations.

Like the LCP, each NCP allows peer routers to negotiate various network options over the data link (by transmitting Configure-Request, Configure-ACK, Configure-NAK, and Configure-Reject packets). Network options include which network addresses to use, which media types to bridge, and which authentication protocol to use. Once both peer routers agree upon network options, the NCP reaches the "opened" state. The routers then begin transmitting user data packets for any upper-layer protocols over the link.

Datagram Encapsulation

Before transmitting data across the link, PPP encapsulates data in a frame that is similar to a High-level Data Link Control (HDLC) frame (see Figure 1-3).

PPP Frame

Flag	Address	Control	Protocol	Data	FCS	Flag
1 byte	1 byte	1 byte	2 bytes	Variable	2 or 4 bytes	1 byte

Figure 1-3. PPP Encapsulated Frame

The parts of the PPP frame function as follows:

- The Flag fields delimit the beginning and end of a frame. Peer routers on synchronous lines exchange flags continuously when there are no frames to transmit.
- The Address field indicates which device originated the frame.
- The Control field indicates what type of frame this is (information or administrative).
- The Protocol field indicates the operative network layer protocol.
- The Data field contains the data one link sends to the other. Its length is less than or equal to the MTU line size. The default maximum length is 1500 bytes; LCP negotiations determine the actual length.
- The Frame Check Sequence (FCS) shows the sequence order of the frame; router hardware computes FCS. A 16- or 32-bit Cyclic Redundancy Check (CRC) is at the end of each frame.

Monitoring the PPP Link

To ensure that the router can successfully transfer data, PPP monitors the quality of the point-to-point link by using Link Quality Monitoring (LQM) and Link Quality Report (LQR) packets. PPP supports link quality monitoring over standard synchronous interfaces only. It does not support link quality monitoring over high speed synchronous interfaces (HSSI) or sync interfaces configured in a Multi-line.

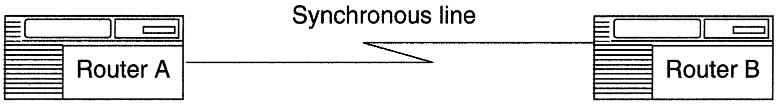
LQR packets contain counters of incoming and outgoing data packets for the routers on each side of the link. Each time a router receives an LQR packet, it uses it to calculate the outbound link quality (the percentage of packets the router transmitted that its peer successfully receives) and the inbound link quality (the percentage of packets that the peer transmitted that the originating router successfully receives).

After 5 LQR reporting periods, the router averages the inbound link quality and the outbound link quality, and compares these values against a user-specified threshold. (Note that this is a rolling average; the router computes the link quality average each time 5 LQR periods have passed.)

If either the inbound link quality average or the outbound link quality average drops below the threshold, the router disables each NCP on the interface. The router re-enables each NCP when the link quality improves, or when the user reconfigures the line.

For example, in Figure 1-4, the acceptable outbound and inbound link quality configured on Router A for the PPP interface is 100%. After 5 LQR periods, Router A calculates the outbound and inbound link quality averages, and determines that the inbound link quality average is below the 100% threshold (in this case, 90%). As a result, Router A disables all NCPs on the interface.

In addition to LQR packets, PPP transmits Echo Request packets periodically. If the router transmits a user-specified number of Echo requests before receiving an Echo reply from its peer router, then the router disables each NCP on the interface.



LQR Period	Packets Router A Transmitted	Packets Router B Received	Outbound Link Quality Router A
1	100	100	100%
2	100	100	100%
3	100	100	100%
4	100	100	100%
5	100	100	100%

Outbound average after 5 LQR periods = 100%

LQR Period	Packets Router A Received	Packets Router B Transmitted	Inbound Link Quality Router A
1	90	100	90%
2	90	100	90%
3	90	100	90%
4	90	100	90%
5	90	100	90%

Inbound average after 5 LQR periods = 90%

Figure 1-4. Link Quality Monitoring from Router A's Perspective

Chapter 2
Implementation Notes

This chapter contains basic guidelines on configuring PPP interfaces. It also addresses special configuration features.

PPP Data Compression

The Wellfleet data compression software enables you to reduce line costs and improve response times over wide area networks running PPP.

Wellfleet data compression eliminates redundancies in data streams. When you use compression on your network, bandwidth efficiency improves, and you can transmit more data over a given amount of network bandwidth.

For a more complete discussion of data compression, descriptions of Wellfleet Compression Protocol parameters, and instructions for configuring compression over a PPP interface, see the manual *Customizing Data Compression Services*.

PPP Dial-on-Demand Support

PPP allows you to configure dial-on-demand services. Dial-on-demand enables you to establish a circuit “on demand” as opposed to having a leased line connection, which is always available. By using a circuit on a demand basis, you can significantly reduce your line costs.

Site Manager automatically configures PPP on the lines that you select for dial-on-demand. PPP, with Chap Name, IP, or IPX, implements a router identification mechanism that dial-on-demand and dial backup services require.

If you configure CHAP as an authentication protocol, you must use Chap Name for router identification on all dial-on-demand or dial backup lines in a pool. You must also use the same Chap Secret for all lines in a pool. Conversely, if you configure a dial-on-demand or dial backup pool using IP or IPX for identification, you cannot use CHAP for authentication.

For more information on dial-on-demand and dial backup, see the manual *Customizing Dial Services*.

PPP Dial Backup Support

PPP allows you to configure a dial backup feature. If a primary PPP line fails and you have enabled dial backup, the router automatically establishes a backup line.

See the manual *Customizing Dial Services* for more information and instructions on how to enable a dial backup circuit.

Disabling Network Control Protocols

To stop traffic from routing over a PPP interface, either

❒ Disable the NCP for the upper-level routing protocol.

For example, if you disable the NCP for IP, then even though IP is still enabled on the interface, it is no longer able to route traffic over the interface.

To disable the NCP for IP, you set the IP Enable parameter to Disable. See “Editing PPP Interface Parameters” in Chapter 3 for instructions on disabling NCP parameters.

❒ Disable the upper-level routing protocol itself.

Note that if you disable the routing protocol running on top of the PPP interface, then Site Manager disables the NCP for the routing protocol automatically. For example, if you disable IP on an interface, Site Manager disables the NCP for IP as well.

However, this is a one-way dependency — that is, disabling the NCP does *not* disable the upper-level routing protocol.

Configuring Synchronous Lines with PPP

If you enable PPP on a circuit, PPP automatically sets the following synchronous line parameters as follows:

Parameter	Value
BOFL	Disable
Promiscuous	Enable
Service	Transparent
WAN Protocol	PPP

For more information on these parameters, refer to the manual *Configuring Wellfleet Routers*.

Protocol Prioritization

When you configure your router, you can prioritize the different types of traffic sent across a synchronous line. This process is called protocol prioritization. The ability to prioritize traffic is important because some types of operations require faster responses than do other types. For example, a user in a Telnet session requires a more immediate response than does a user performing a file transfer.

When you select PPP on a circuit, protocol prioritization is automatically enabled, so PPP data has precedence over other types of data. For more information about protocol prioritization, see *Configuring Wellfleet Routers*.

Chapter 3
Editing PPP Parameters

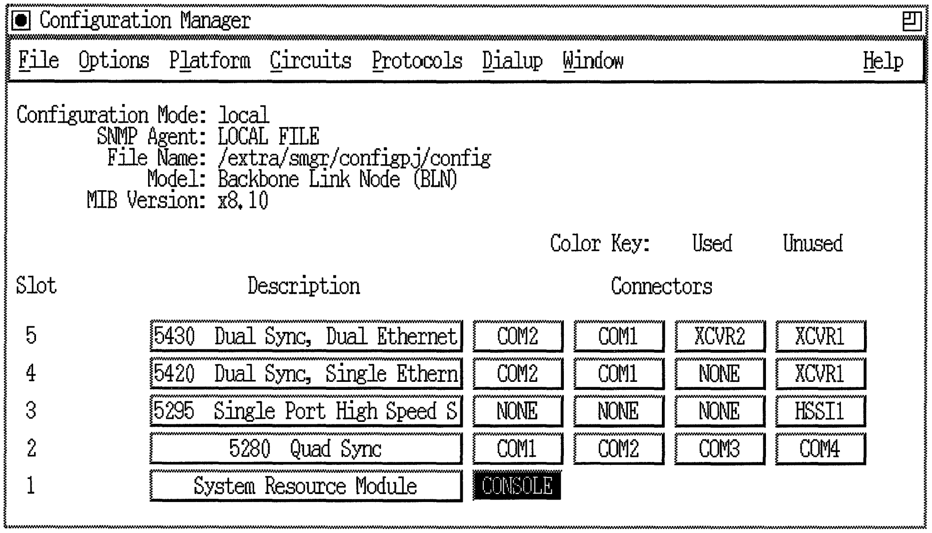
This chapter provides information on how you can edit, or customize, the parameters for the PPP interfaces that you configure on the router.

Note: You must have already configured at least one PPP interface on the router to edit PPP parameters. If you have *not* yet configured a PPP interface, or want to add additional PPP interfaces, see *Configuring Wellfleet Routers* for instructions.

You access all PPP parameters from the Configuration Manager window shown in Figure 3-1. (Refer to *Configuring Wellfleet Routers* for instructions on accessing this window.)

For each PPP parameter that you configure, this chapter gives the default setting, all valid setting options, the parameter function, instructions for setting the parameter, and the Management Information Base (MIB) object ID.

The Technician Interface allows you to modify parameters by issuing **set** and **commi**t commands with the MIB object ID. This process is equivalent to modifying parameters using Site Manager. For more information about using the Technician Interface to access the MIB, refer to *Using Technician Interface Software*.



```
Configuration Mode: local
        SNMP Agent: LOCAL FILE
         File Name: /extra/smgr/configpj/config
             Model: Backbone Link Node (BLN)
       MIB Version: x8.10
```

Color Key: Used Unused

Slot	Description	Connectors			
5	5430 Dual Sync, Dual Ethernet	COM2	COM1	XCVR2	XCVR1
4	5420 Dual Sync, Single Ethern	COM2	COM1	NONE	XCVR1
3	5295 Single Port High Speed S	NONE	NONE	NONE	HSSI1
2	5280 Quad Sync	COM1	COM2	COM3	COM4
1	System Resource Module	CONSOLE			

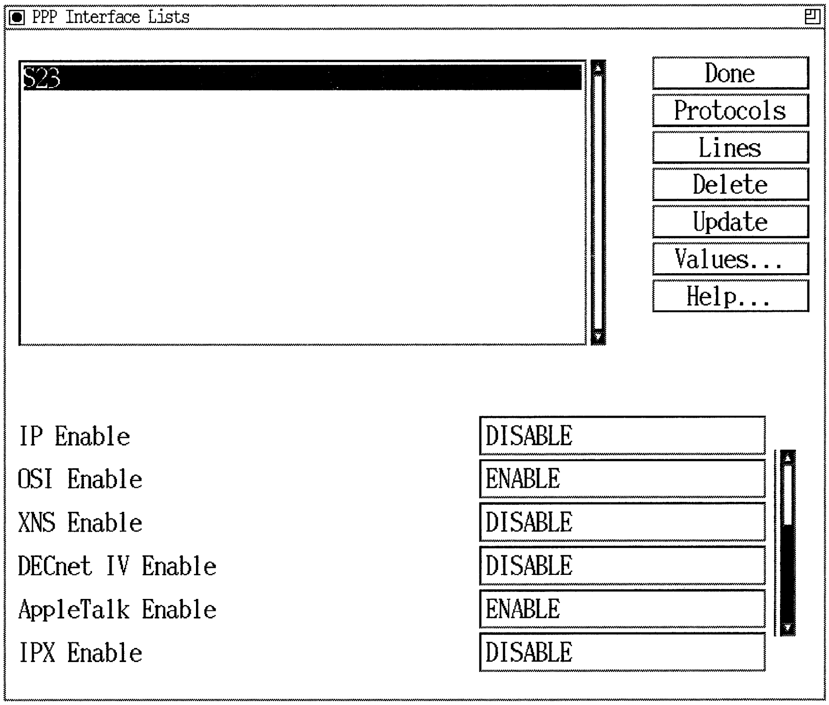
Figure 3-1. Configuration Manager Window

Editing PPP Interface Parameters

To edit the PPP interface-specific parameters, begin at the Configuration Manager window shown in Figure 3-1 and proceed as follows:

1. Select the Protocols→PPP→Interfaces option.

The PPP Interface Lists window appears (see Figure 3-2).



IP Enable DISABLE

OSI Enable ENABLE

XNS Enable DISABLE

DECnet IV Enable DISABLE

AppleTalk Enable ENABLE

IPX Enable DISABLE

Figure 3-2. PPP Interface Lists Window

2. Click on the PPP interface that you want to edit.
3. Edit those parameters you want to change, referring to the descriptions following this procedure for guidelines.

If you change any of the following parameters, you must force LCP re-negotiation on the interface for your changes to take effect:

Remote IP Address

IPX Remote Node Number

Remote AppleTalk Node

Bridge Enet

AppleTalk Routing Protocol

Bridge FDDI

Bridge Token Ring

You must disable, and then re-enable, the corresponding network control protocol to implement your changes. Therefore, after making all of your changes to any of the parameters listed above, but *before* proceeding to step 4, do the following:

— Set the corresponding network control protocol parameter(s) to Disable.

For example, if you change the Remote IP Address parameter, set the IP Enable parameter to Disable; if you change the Remote AppleTalk Node parameter, set the AppleTalk Enable parameter to Disable.

— Click on the Apply button.

— Reset the corresponding network control protocol parameter(s) to Enable.

4. Click on the Apply button to implement your changes.
5. Click on the Done button to exit the window.

If you configure dial-on-demand or dial backup services, you see a special PPP record for demand or backup circuits in the PPP Interface Lists screen that reads:

```
Special PPP for Switch Services
```

This is a generic PPP record that demand and backup circuits use for identification purposes.

PPP Interface Parameter Descriptions

Use the following guidelines when you configure the parameters on the PPP Interface List window.

Parameter:	**IP Enable**
Default:	If you enable IP support on this interface, Site Manager automatically sets IP Enable to Enable. Otherwise, the default is Disable.
Options:	Enable | Disable
Function:	Enables or disables the network control protocol (NCP) for IP. Note that this parameter does *not* enable or disable IP routing services for the interface; it affects the NCP for IP. However, disabling the NCP for IP stops IP traffic from being routed over this interface.
Instructions:	To stop IP traffic from being routed over this interface, set IP Enable to Disable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.2.1.12

Parameter: OSI Enable

Default: If you enable OSI support on this interface, Site Manager automatically sets OSI Enable to Enable. Otherwise, the default is Disable.

Options: Enable | Disable

Function: Enables or disables the network control protocol (NCP) for OSI.

OSI Enable does *not* enable or disable OSI routing for the interface; it affects the NCP for OSI. However, disabling the NCP for OSI stops OSI traffic from being routed over this interface.

Instructions: To stop OSI traffic from being routed over this interface, set OSI Enable to Disable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.13

Parameter: XNS Enable

Default: If you enable XNS support on this interface, Site Manager automatically sets XNS Enable to Enable. Otherwise, the default is Disable.

Options: Enable | Disable

Function: Enables or disables the network control protocol (NCP) for XNS.

Note that this parameter does *not* enable or disable XNS routing services for the interface; it affects the NCP for XNS. However, disabling the NCP for XNS stops XNS traffic from being routed over this interface.

Instructions: To stop XNS traffic from being routed over this interface, set XNS Enable to Disable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.14

Parameter: **DECnet IV Enable**

Default: If you enable DECnet IV support on this interface, Site Manager automatically sets DECnet IV Enable to Enable. Otherwise, the default is Disable.

Options: Enable | Disable

Function: Enables or disables the network control protocol (NCP) for DECnet IV.

This parameter does *not* enable or disable DECnet IV routing services for the interface; it affects the NCP for DECnet IV. However, disabling the NCP for DECnet IV stops DECnet IV traffic from being routed over this interface.

Instructions: To stop DECnet IV traffic from being routed over this interface, set DECnet IV Enable to Disable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.15

Parameter:	**AppleTalk Enable**
Default:	If you enable AppleTalk support on this interface, Site Manager automatically sets AppleTalk Enable to Enable. Otherwise, the default is Disable.
Options:	Enable | Disable
Function:	Enables or disables the network control protocol (NCP) for AppleTalk. Note that this parameter does *not* enable or disable AppleTalk routing services for the interface; it affects the NCP for AppleTalk. However, disabling the NCP for AppleTalk stops AppleTalk traffic from being routed over this interface.
Instructions:	To stop AppleTalk traffic from being routed over this interface, set AppleTalk Enable to Disable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.2.1.16

Parameter:	**IPX Enable**
Default:	If you enable IPX support on this interface, Site Manager automatically sets IPX Enable to Enable. Otherwise, the default is Disable.
Options:	Enable | Disable
Function:	Enables or disables the network control protocol (NCP) for IPX. Note that this parameter does *not* enable or disable IPX routing services for the interface; it affects the NCP for IPX. However, disabling the NCP for IPX stops IPX traffic from being routed over this interface.
Instructions:	To stop IPX traffic from being routed over this interface, set IPX Enable to Disable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.2.1.17

Parameter: **Bridge Enable**

Default: If you enable the Bridge on this interface, Site Manager automatically sets this parameter to Enable. Otherwise, the default is Disable.

Options: Enable | Disable

Function: Enables or disables the network control protocol (NCP) for the bridge.

Note that this parameter does *not* enable or disable bridging services for the interface; it affects the NCP for the bridge. However, by disabling the NCP for the bridge, it stops traffic from being bridged over this interface.

Instructions: To stop traffic from being bridged over this interface, set this parameter to Disable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.18

Parameter: **VINES Enable**

Default: If you enable VINES support on this interface, Site Manager automatically sets VINES Enable to Enable. Otherwise, the default is Disable.

Options: Enable | Disable

Function: Enables or disables the network control protocol (NCP) for VINES.

Note that this parameter does *not* enable or disable VINES routing services for the interface. However, setting this parameter to Disable stops VINES traffic from being routed over this interface.

Instructions: To stop VINES traffic from being routed over this interface, set VINES Enable to Disable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.19

Parameter: **CCP Enable**

Default: Disable

Options: Enable | Disable

Function: Enables or disables compression.

Instructions: You enable compression according to the instructions in *Customizing Data Compression Services*. When you do so, Site Manager automatically sets the CCP Enable parameter to Enable. Note that this parameter does *not* enable or disable compression for the interface. However, setting this parameter to Disable stops compression over this interface.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.49

Parameter: **Remote IP Address**

Default: 0.0.0.0

Options: Any valid IP address

Function: Specifies the IP address the peer router should use. This interface includes this IP address in NCP negotiations.

Instructions: If you want to specify an IP address for the peer router, enter it here. Note that if this circuit is a dial-on-demand or dial backup circuit, you *must* enter an IP address for this parameter. PPP uses this address to identify the router to its peer.

If this interface has been up and running, you must also set the IP Enable parameter to Disable, click on the Apply button, and then reset the IP Enable parameter to Enable to implement your changes.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.22

Parameter: IPX Network Number

Default: None

Options: A valid, unique, unreserved network number. This number must be a string of up to eight hexadecimal characters. (0xffffffff is invalid.)

Function: Specifies a network number used to negotiate the link. The negotiated number must be unique. It cannot be a previously assigned network number.

Note that both sides of the link do not have to have the same network number. PPP negotiates the higher of the two numbers. Note also that the negotiated number may be zero (that is, the IPX network number is zero on both sides of the link). In this case, IPX defines the link's network number.

Instructions: Enter a valid IPX network number for each PPP interface.

Be aware that the value for this parameter depends on the IPX configuration for this interface. For information about IPX and PPP interaction, see *Customizing IPX Services*.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.24

Parameter: **IPX Remote Node Number**

Default: None

Options: Any valid IPX node number

Function: Specifies the IPX node number the peer router should use. This interface includes this IPX remote node number in NCP negotiations.

Instructions: If you want to specify an IPX node number for the peer router, enter it here.

If this interface has been up and running, you must also set the IPX Enable parameter to Disable, click on the Apply button, and then reset the IPX Enable parameter to Enable to implement your changes.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.26

Parameter: **Remote AppleTalk Node**

Default: None

Options: Any valid AppleTalk node number

Function: Specifies the AppleTalk node number the peer router should use. This interface includes this AppleTalk node number in NCP negotiations.

Instructions: If you want to specify an AppleTalk node number for the peer router, enter it here.

If this interface has been up and running, you must also set the AppleTalk Enable parameter to Disable, click on the Apply button, and then reset the AppleTalk Enable parameter to Enable to implement your changes.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.36

Parameter: **AppleTalk Routing Protocol**

Default: RTMP

Options: RTMP (Routing Table Maintenance Protocol)

Function: Specifies the AppleTalk routing update protocol that this interface wants the peer router to use. This interface specifies AppleTalk RTMP as the routing update protocol in NCP negotiations.

Instructions: Accept the default, RTMP.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.38

Parameter: **Bridge Ethernet**

Default: Enable

Options: Enable | Disable

Function: Specifies whether this PPP interface accepts bridged traffic that is Ethernet encapsulated, and then forwards it over the PPP network.

Instructions: Reset to Disable if you do not want the PPP interface to accept bridged, Ethernet-encapsulated frames.

If this interface has been up and running, you must also set the Bridge Enable parameter to Disable, click on the Apply button, and then reset the Bridge Enable parameter to Enable to implement your changes.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.40

Parameter: **Bridge FDDI**

Default: Enable

Options: Enable | Disable

Function: Specifies whether this PPP interface accepts bridged traffic that is FDDI encapsulated, and then forwards it over the PPP network.

Instructions: Reset to Disable to refuse bridged, FDDI-encapsulated frames on this PPP interface.

If this interface has been up and running, you must also set the Bridge Enable parameter to Disable, click on the Apply button, and then reset the Bridge Enable parameter to Enable to implement your changes.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.42

Parameter: **Bridge Token Ring**

Default: Enable

Options: Enable | Disable

Function: Specifies if this PPP interface accepts bridged traffic that is Token Ring encapsulated, and then forwards it over the PPP network. The Token Ring network must support source routing; the router expects all Token Ring-bridged frames to be source routed.

Instructions: Reset to Disable if you do not want the PPP interface to accept bridged, Token Ring-encapsulated frames.

If this interface has been up and running, you must also set the Bridge Enable parameter to Disable, click on the Apply button, and then reset the Bridge Enable parameter to Enable to implement your changes.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.44

Editing PPP Line Parameters

To edit the PPP line-specific parameters, begin at the Configuration Manager window shown in Figure 3-1 and proceed as follows:

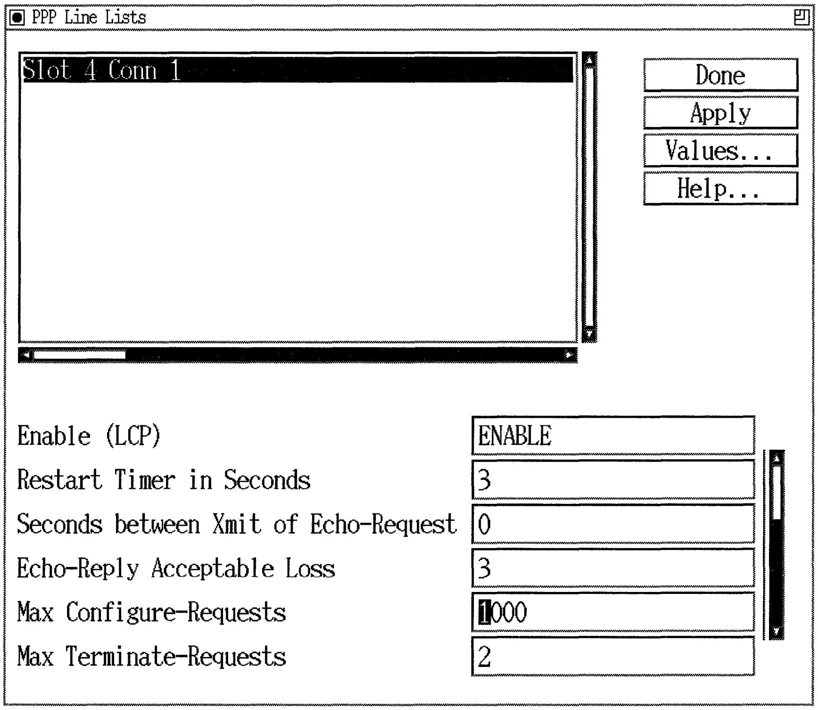
1. Select the Protocols→PPP→Interfaces option.

   The PPP Interface Lists window appears (see Figure 3-2).

   If you are configuring a dial-on-demand or dial backup pool, select the interface, Special PPP for Switched Services, if you want to configure Chap Local Name for identification purposes.

2. Click on the Lines button.

   The PPP Line Lists window appears (see Figure 3-3).



Slot 4 Conn 1

Enable (LCP)	ENABLE
Restart Timer in Seconds	3
Seconds between Xmit of Echo-Request	0
Echo-Reply Acceptable Loss	3
Max Configure-Requests	1000
Max Terminate-Requests	2

Figure 3-3. PPP Line Lists Window

3. Click on the PPP line that you want to edit.
4. Edit those line parameters that you want to change, referring to the descriptions following this procedure for guidelines.

Note: If you change any of the following parameters you must force LCP re-negotiation on the interface for your changes to take effect.

Local Authentication Protocol

Local PAP ID

Local PAP Password

Remote PAP ID

Remote PAP Password

Link Quality Protocol

Peer Link Quality Report Timer

LQR Reporting Period

Chap Secret

Chap Local Name

Chap Periodic Timer

You must disable, and then re-enable, the corresponding network control protocol to implement your changes. Therefore, after making all of your changes to any of the parameters listed above, but *before* proceeding to step 5, do the following:

— Set the Enable (LCP) parameter to Disable.

— Click on the Apply button.

— Reset the Enable (LCP) parameter to Enable.

5. Click on the Apply button to implement all of your changes.
6. Click on the Done button to exit the window when you are finished.

PPP Line Lists Parameter Descriptions

Use the following guidelines to configure the parameters on the PPP Line Lists window.

Parameter:	**Enable (LCP)**
Default:	Enable
Options:	Enable | Disable
Function:	Enables or disables the Link Control Protocol on the PPP interface. Disabling this parameter generates a “close” event to LCP. Similarly, enabling this parameter generates an “open” event to LCP.
Instructions:	To disable LCP on this interface, reset this parameter to Disable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.1.1.2

Parameter:	**Restart Timer in Seconds**
Default:	3 seconds
Range:	1 to 100 seconds
Function:	Specifies the number of seconds that the Restart Timer waits before retransmitting data.
Instructions:	Accept the default value of 3.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.1.1.7

Parameter:	**Seconds between Xmit of Echo-Request**
Default:	0
Range:	0 to 100
Function:	Specifies the number of seconds that the router waits between the transmission of Echo-Request packets. A value of 0 seconds implies that this parameter is turned off.
Instructions:	Accept the default value of 0.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.1.1.8

Parameter:	**Echo-Reply Acceptable Loss**
Default:	3
Range:	1 to 100
Function:	Specifies the maximum number of unacknowledged Echo-Reply packets that the router will transmit before declaring the point-to-point link down.
Instructions:	Accept the default value of 3.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.1.1.9

Parameter: **Max Configure-Requests**

Default: 1000

Range: 1 to 100000

Function: Specifies the maximum number of unacknowledged Configure-Request packets that the router will transmit before assuming that the peer router on the other end of the link is unable to respond. The link is then brought down. Valid acknowledgments include Configure-ACK, Configure-NAK, or Configure-Reject packets.

To initialize the link, set the Enable (LCP) parameter to Disable, click on the Apply button, and then reset the parameter to Enable.

Instructions: Accept the default value of 1000.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.10

Parameter: **Max Terminate-Requests**

Default: 2

Range: 1 to 100

Function: Specifies the maximum number of unacknowledged Terminate-Request packets that the router transmits before assuming that the peer router on the other end of the link is unable to respond. The valid acknowledgment is a Terminate-ACK packet.

Instructions: Accept the default value of 2.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.11

Parameter: Max Configuration Failure Count

Default: 10

Range: 1 to 100

Function: Specifies the maximum number of Configure-NAK packets the router sends before sending a Configure-Reject packet for those options that it does not agree with.

To restart link initialization, set the Enable (LCP) parameter to Disable, click on the Apply button, and then reset the parameter to Enable.

Instructions: Accept the default value of 10.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.12

Parameter: **Local Authentication Protocol**

Default: None

Options: None | PAPAUTH (Password Authentication Protocol) | CHAP (Challenge Handshake Authentication Protocol)

Function: Specifies the type of authentication protocol that this interface uses: none, PAP, or CHAP.

Instructions: If you do not want to enable security features on this interface, accept the default, None.

To enable Password Authentication Protocol, select PAPAUTH. Then do the following:

— Define the Local PAP ID and Local PAP Password parameters for this interface.

— Set the Enable (LCP) parameter to Disable, click on the Apply button, and then reset the parameter to Enable.

To enable Challenge Handshake Authentication Protocol, select CHAP. Then do the following:

— Define the CHAP Secret, CHAP Local Name, and CHAP Periodic Timer parameters for this interface. Find these parameters by scrolling further through the list of line parameters.

— Set the Enable (LCP) parameter to Disable, click on the Apply button, and then reset the parameter to Enable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.15

Parameter: Local PAP ID

Default: None

Range: Any text string; maximum 25 characters

Function: Specifies the PAP ID assigned to this interface. During the interface's authentication phase, all Password Authenticate-Request messages the peer router sends to this interface must include the correct PAP ID or the interface sends a NAK and the link is not created.

Instructions: If you set the Local Authentication Protocol parameter to None, ignore this field.

If you set the Local Authentication Protocol to PAPAUTH, then specify a unique local PAP ID for this interface. To implement your changes, set the Enable (LCP) parameter to Disable, click on the Apply button, and then reset the parameter to Enable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.17

Parameter: Local PAP Password

Default: None

Range: Any text string; maximum 25 characters

Function: Specifies the PAP password assigned to this interface. During the interface's authentication phase, all Authenticate-Request messages sent to this interface by the peer router must include the correct PAP password or the peer router sends a NAK and the link is not brought up.

Instructions: If you set the Local Authentication Protocol parameter to None, ignore this field.

If you set the Local Authentication Protocol to PAPAUTH, then specify a unique local PAP password for this interface. To implement your changes, set the Enable (LCP) parameter to Disable, click on the Apply button, and then reset the parameter to Enable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.18

Parameter:	**Remote PAP ID**
Default:	None
Range:	Any text string; maximum 25 characters
Function:	Specifies the PAP ID assigned to the peer router. During the interface's authentication phase, this interface must include the correct Remote PAP ID in all password Authenticate-Request messages it sends to the peer router or the peer router sends a NAK and the link is not brought up.
Instructions:	If the remote peer does not enable PAP, ignore this field. If the remote peer enables PAP, specify the remote PAP ID that identifies the remote peer. To implement your changes, set the Enable (LCP) parameter to Disable, click on the Apply button, and then reset the parameter to Enable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.1.1.19

Parameter: **Remote PAP Password**

Default: None

Range: Any text string; maximum 25 characters

Function: Specifies the PAP password assigned to the peer router. During the interface's authentication phase, this interface must include the correct remote PAP password in all password Authenticate-Request messages it sends to the peer router, or the peer router sends a NAK and the link is not created.

Instructions: If the remote peer does not enable PAP, ignore this field.

If the remote peer enables PAP, specify the remote PAP password that identifies the remote peer. To implement your changes, set the Enable (LCP) parameter to Disable, click on the Apply button, and then reset the parameter to Enable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.20

Parameter: **Link Quality Protocol**

Default: None

Options: None | Link Quality Report

Function: Enables or disables the Link Quality Protocol for this interface.

Instructions: To enable LQR, reset this parameter to Link Quality Report. To implement your changes, remember to set the Enable (LCP) parameter to Disable, click on the Apply button, and then reset the parameter to Enable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.21

Parameter: **Peer Link Quality Report Timer**

Default: Enable

Options: Enable | Disable

Function: Enables or disables the peer router's Link Quality Report (LQR) Timer.

When you enable this parameter, the peer router maintains its own LQR timer for this interface. When you disable this parameter, this router is responsible for maintaining the LQR timer for this interface.

Instructions: Accept the default, Enable, if you want the peer router to maintain an LQR timer for the interface.

Reset this parameter to Disable if you want this router to maintain the LQR timer for the interface. To implement your changes, set the Enable (LCP) parameter to Disable, click on the Apply button, and then reset the parameter to Enable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.22

Parameter: **LQR Reporting Period**

Default: 3 seconds

Range: 1 to 120 seconds

Function: Specifies the maximum number of seconds between the transmission of LQR packets.

Instructions: Enter a number representing the interval between the transmission of LQR packets. Make certain to specify the same LQR reporting period for both this interface and the peer router. To implement your changes, set the Enable (LCP) parameter to Disable, click on the Apply button, and then reset the parameter to Enable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.23

Parameter: Inbound Link Quality

Default: 90 (percent)

Range: 1 to 100 (percent)

Function: Specifies the minimum acceptable success rate (percentage) of packets the peer router transmits and this router receives on this interface over the last 5 LQR reporting periods.

If the percentage drops below the inbound link quality you specify, the router brings down the NCPs until the percentage increases to an acceptable level.

See “Monitoring the PPP Link” in Chapter 1 for more information.

Instructions: Accept the default value, 90.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.25

Parameter: Outbound Link Quality

Default: 90 (percent)

Range: 1 to 100 (percent)

Function: Specifies the minimum acceptable success rate (percentage) of packets the router transmits and the peer router receives on this interface.

If the percentage drops below the outbound link quality you specify, the router brings down NCPs until the percentage increases to an acceptable level.

See “Monitoring the PPP Link” for more information.

Instructions: Accept the default, 90.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.27

Parameter: **Chap Secret**

Default: None

Range: Any text string; maximum 20 characters

Function: Specifies the CHAP Secret you assign to this interface. The CHAP Secret must be the same on both sides of the link. Both routers on a link must have the same secret to correctly calculate responses to challenges either one of them may send to the other during the authentication process and/or the network layer negotiation phase.

Note: If you are configuring a dial-on-demand or dial backup pool, you must use the same secret for all lines in the pool.

Instructions: If you have not enabled CHAP, ignore this field.

If you have enabled CHAP, specify the secret. To implement your changes, set the Enable (LCP) parameter to Disable, click on the Apply button, and then reset the parameter to Enable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.31

Parameter: **Chap Local Name**

Default: None

Range: Any text string; maximum 20 characters

Function: A local Chap Name informs the peers of each other's identity.

Instructions: If you configure CHAP as an authentication protocol, you *must* use Chap Local Name for router identification on a dial-on-demand or dial backup line. If you do not configure CHAP, you *cannot* use Chap Local Name for identification; instead you must configure IP or IPX.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.33

Parameter:	**Chap Periodic Timer**
Default:	None
Options:	Options are in seconds. Setting this value to 0 disables Periodic Chap. A reasonable value for this parameter is 60 seconds.
Function:	Allows for repeated authentication challenges at an interval (in seconds) that either router on the link can specify. The timer begins counting when an authentication phase has completed. A new challenge does not begin until the amount of time you specify elapses.
Instructions:	Set to 60.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.1.1.35

Deleting PPP from the Router

To delete PPP from *all* circuits on which it is currently configured, complete the following steps:

1. From the Configuration Manager window (Figure 3-1), select Protocols→PPP→Delete PPP. A window pops up and asks

   ```
   Do you REALLY want to delete PPP?
   ```

2. Click on the OK button.

   Site Manager returns you to the Configuration Manager window. PPP is no longer operating on the router.

Index