Configuring PPP Services

Router Software Version 11.0
Site Manager Software Version 5.0

Part No. 114068 Rev. A
August 1996

Bay Networks

Bay Networks

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

Copyright © 1988–1996 Bay Networks, Inc.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Bay Networks, Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

Restricted Rights Legend

Use, duplication, or disclosure by the United States 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 United States 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, AFN, BCN, BLN, BN, CN, FRE, LN, Optivity, SynOptics, SynOptics Communications, Wellfleet and the Wellfleet logo are registered trademarks and AN, ANH, ASN, BaySIS, BayStack, BCNX, BLNX, BNX, EZ Internetwork, EZ LAN, FN, PathMan, PhonePlus, PPX, Quick2Config, RouterMan, SPEX, Bay Networks, Bay Networks Press, the Bay Networks logo and the SynOptics logo are trademarks of Bay Networks, Inc.

Third-Party Trademarks

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

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Bay Networks, Inc. reserves the right to make changes to the products described in this document without notice.

Bay Networks, Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product are Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Bay Networks Software License

Note: This is Bay Networks basic license document. In the absence of a software license agreement specifying varying terms, this license -- or the license included with the particular product -- shall govern licensee's use of Bay Networks software.

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

Configuring PPP Services

About This Guide

Technical Support and Online Services

Chapter 1
Starting PPP

Chapter 2
PPP Concepts

Chapter 3
Customizing PPP

Appendix A
PPP Parameters

Appendix B
Default PPP Configuration

Appendix C
PPP Statistics

Index

Figures

Tables

About This Guide

This manual describes Point-to-Point Protocol (PPP) services and guides you in configuring PPP parameters for your network. If you are responsible for configuring and managing Bay Networks™ routers or BNX™ switching platforms running over point-to-point links, you need to read this manual.

This task-oriented manual focuses on what you, as a network manager, have to do to get PPP up, running, and customized for your network. Refer to this guide for

- A guide to starting PPP using all default values (Chapter 1)
- Conceptual information to help you decide how you want to configure PPP on your network (Chapter 2)
- Instructions on customizing PPP (Chapter 3)
- Descriptions of PPP parameters (Appendix A)
- Default parameter settings (Appendix B)
- PPP statistics (Appendix C)

See *Configuring Routers* or *Configuring Customer Access and Trunks (BNX Software)*, depending on your platform, for information and instructions about the following topics:

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

Before You Begin

Before using this guide, you must create and save a configuration file that contains at least one WAN interface, then retrieve the configuration file in local, remote, or dynamic mode

Refer to *Configuring Routers* or *Configuring Customer Access and Trunks (BNX Software)*, depending on your platform, for instructions on how to do these tasks.

Conventions

angle brackets (< >) — Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command.
Example: if command syntax is **ping** *<ip_address>*, you enter **ping 192.32.10.12**

bold text — Indicates text that you need to enter, command names, and buttons in menu paths.
Example: Enter **wfsm &**

Example: Use the **dinfo** command.

Example: Protocols > PPP > Interfaces > **Lines** identifies the Lines button on the PPP Interfaces window.

brackets ([ ]) — Indicate optional elements. You can choose none, one, or all of the options.

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

quotation marks (“ ”) — Indicate the title of a chapter or section within a book.

`screen text` — Indicates data that appears on the screen.
Example: `Set Bay Networks Trap Monitor Filters`

separator (>) — Separates menu and option names in instructions and internal pin-to-pin wire connections.
Example: Protocols > AppleTalk identifies the AppleTalk option in the Protocols menu.

Example: Pin 7 > 19 > 20

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

BNCP	Bridge Network Control Protocol
BNX	Backbone Node Switch
BOFL	Breath of Life (message)
CCP	Compression Control Protocol
CHAP	Challenge Handshake Authentication Protocol
CRC	cyclic redundancy check
DNCP	DECnet Phase IV Control Protocol
FCS	Frame Check Sequence
FDDI	Fiber Distributed Data Interface
HDLC	high-level data link control
HSSI	High-Speed Serial Interface
IP	Internet Protocol
IPCP	IP Control Protocol
IPX	Internet Packet Exchange
IPXCP	IPX Control Protocol
LAN	local area network
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
RFC	Request for Comment
SMDS	Switched Multimegabit Data Service
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol
VINES	Virtual Networking System
VNCP	VINES Network Control Protocol
WAN	wide area network
XNS	Xerox Networking System
XNSCP	Xerox Networking System Control Protocol

Ordering Bay Networks Publications

To purchase additional copies of this document or other Bay Networks publications, order by part number from the Bay Networks Press™ at the following telephone or fax numbers:

• Telephone - U.S./Canada	1-888-4BAYPRESS
• Telephone - International	1-510-490-4752
• Fax	1-510-498-2609

You can also use these numbers to request a free catalog of Bay Networks Press product publications.

Technical Support and Online Services

To ensure comprehensive network support to our customers and partners worldwide, Bay Networks Customer Service has Technical Response Centers in key locations around the globe:

- Billerica, Massachusetts
- Santa Clara, California
- Sydney, Australia
- Tokyo, Japan
- Valbonne, France

The Technical Response Centers are connected via a redundant Frame Relay Network to a Common Problem Resolution system, enabling them to transmit and share information, and to provide live, around-the-clock support 365 days a year.

Bay Networks Information Services complement the Bay Networks Service program portfolio by giving customers and partners access to the most current technical and support information through a choice of access/retrieval means. These include the World Wide Web, CompuServe, Support Source CD, Customer Support FTP, and InfoFACTS document fax service.

Bay Networks Customer Service

If you purchased your Bay Networks product from a distributor or authorized reseller, contact that distributor's or reseller's technical support staff for assistance with installation, configuration, troubleshooting, or integration issues.

Customers can also purchase direct support from Bay Networks through a variety of service programs. As part of our PhonePlus™ program, Bay Networks Service sets the industry standard, with 24-hour, 7-days-a-week telephone support available worldwide at no extra cost. Our complete range of contract and noncontract services also includes equipment staging and integration, installation support, on-site services, and replacement parts delivery -- within approximately 4 hours.

To purchase any of the Bay Networks support programs, or if you have questions on program features, use the following numbers:

Region	Telephone Number	Fax Number
United States and Canada	1-800-2LANWAN; enter Express Routing Code (ERC) 290 when prompted (508) 436-8880 (direct)	(508) 670-8766
Europe	(33) 92-968-300	(33) 92-968-301
Asia/Pacific Region	(612) 9927-8800	(612) 9927-8811
Latin America	(407) 997-1713	(407) 997-1714

In addition, you can receive information on support programs from your local Bay Networks field sales office, or purchase Bay Networks support directly from your authorized partner.

Bay Networks Information Services

Bay Networks Information Services provide up-to-date support information as a first-line resource for network administration, expansion, and maintenance. This information is available from a variety of sources.

World Wide Web

The Bay Networks Customer Support Web Server offers a diverse library of technical documents, software agents, and other important technical information to Bay Networks customers and partners.

A special benefit for contracted customers and resellers is the ability to access the Web Server to perform Case Management. This feature enables your support staff to interact directly with the network experts in our worldwide Technical Response Centers. A registered contact with a valid Site ID can

- View a listing of support cases and determine the current status of any open case. Case history data includes severity designation, and telephone, e-mail, or other logs associated with the case.
- Customize the listing of cases according to a variety of criteria, including date, severity, status, and case ID.
- Log notes to existing open cases.
- Create new cases for rapid, efficient handling of noncritical network situations.
- Communicate directly via e-mail with the specific technical resources assigned to your case.

The Bay Networks URL is *http://www.baynetworks.com*. Customer Service is a menu item on that home page.

Customer Service FTP

Accessible via URL *ftp://support.baynetworks.com* (134.177.3.26), this site combines and organizes support files and documentation from across the Bay Networks product suite, including switching products from our Centillion™ and Xylogics® business units. Central management and sponsorship of this FTP site lets you quickly locate information on any of your Bay Networks products.

Support Source CD

This CD-ROM -- sent quarterly to all contracted customers -- is a complete Bay Networks Service troubleshooting knowledge database with an intelligent text search engine.

The Support Source CD contains extracts from our problem-tracking database; information from the Bay Networks Forum on CompuServe; comprehensive technical documentation, such as Customer Support Bulletins, Release Notes, software patches and fixes; and complete information on all Bay Networks Service programs.

You can run a single version on Macintosh Windows 3.1, Windows 95, Windows NT, DOS, or UNIX computing platforms. A Web links feature enables you to go directly from the CD to various Bay Networks Web pages.

CompuServe

For assistance with noncritical network support issues, Bay Networks Information Services maintain an active forum on CompuServe, a global bulletin-board system. This forum provides file services, technology conferences, and a message section to get assistance from other users.

The message section is monitored by Bay Networks engineers, who provide assistance wherever possible. Customers and resellers holding Bay Networks service contracts also have access to special libraries for advanced levels of support documentation and software. To take advantage of CompuServe's recently enhanced menu options, the Bay Networks Forum has been re-engineered to allow links to our Web sites and FTP sites.

We recommend the use of CompuServe Information Manager software to access these Bay Networks Information Services resources. To open an account and receive a local dial-up number in the United States, call CompuServe at 1-800-524-3388. Outside the United States, call 1-614-529-1349, or your nearest CompuServe office. Ask for Representative No. 591. When you are on line with your CompuServe account, you can reach us with the command **GO BAYNET**.

InfoFACTS

InfoFACTS is the Bay Networks free 24-hour fax-on-demand service. This automated system has libraries of technical and product documents designed to help you manage and troubleshoot your Bay Networks products. The system responds to a fax from the caller or to a third party within minutes of being accessed.

To use InfoFACTS in the United States or Canada, call toll-free 1-800-786-3228. Outside North America, toll calls can be made to 1-408-764-1002. In Europe, toll-free numbers are also available for contacting both InfoFACTS and CompuServe. Please check our Web page for the listing in your country.

How to Get Help

Use the following numbers to reach your Bay Networks Technical Response Center:

Technical Response Center	Telephone Number	Fax Number
Billerica, MA	1-800-2LANWAN	(508) 670-8765
Santa Clara, CA	1-800-2LANWAN	(408) 764-1188
Valbonne, France	(33) 92-968-968	(33) 92-966-998
Sydney, Australia	(612) 9927-8800	(612) 9927-8811
Tokyo, Japan	(81) 3-5402-0180	(81) 3-5402-0173

Chapter 1
Starting PPP

PPP is a standard point-to-point protocol for sending data packets over serial synchronous and asynchronous lines.

This chapter tells you how to configure PPP on a circuit using all default values. Once you've done that, you can customize the configuration as needed. Chapter 2, "PPP Concepts," gives you detailed background information on PPP to help you make appropriate customizing choices. Chapter 3, "Customizing PPP," describes how to change the default settings after you've configured the circuit.

Configuring PPP on a Circuit

To configure PPP on a circuit, using default values for all parameters:

1. **Prepare the configuration file.**

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

2. **Select the circuit you want to configure.**

   - If this is a local mode configuration file, specify the router hardware.
   - Select the link or net module connector on which you are enabling PPP.

3. **Enable PPP on the interface.**

   If you are using Site Manager:

   a. **Select PPP from the WAN Protocols menu.**

This menu appears after you select a link or net module connector that requires a WAN circuit.

b. **Click on OK to enable default PPP service.**

The Configuration Manager displays the Select Protocols window.

If you are running router (as opposed to BNX) software, selecting PPP automatically enables protocol prioritization. For detailed information on protocol prioritization, refer to *Configuring Traffic Filters and Protocol Prioritization.*

4. **Select the routing protocol that you want to run on this interface.**

PPP is the WAN protocol for the interface. You also need to enable an upper-level routing protocol (such as IP, IPX, or AppleTalk) to run on top of PPP. Enabling this protocol allows the routing of traffic over this interface. Refer to the appropriate protocol-specific guides for information on these protocols.

When you've finished these steps, you'll have a fully operational PPP connection configured with all default values. For a list of the default values, see Appendix B. Refer to *Configuring Routers* or *Configuring Customer Access and Trunks (BNX Software)*, depending on your platform, for instructions on how to do these tasks.

PPP Tasks

You can configure PPP to perform the following functions:

- Route data over a PPP link
- Perform data compression
- Run PPP over dial-up lines
- Run PPP over multiple lines
- Run PPP over a multilink circuit
- Set up protocol prioritization on a multiline circuit

In addition, you can

- Configure IP to run over PPP interfaces
- Enable and disable network control protocols
- Use PPP with asynchronous modems

- Calculate and view line and circuit statistics
- Configure authentication protocols
- Set up link quality monitoring
- Configure echo requests

The following chapters describe how to do all of these tasks.

Where to Go Next

Go to Chapter 2 to learn more about PPP concepts and characteristics.

Go to Chapter 3 for instructions on how to customize a PPP interface.

Go to Appendix A for a description of PPP parameters.

Go to Appendix B for a list of PPP parameter default values.

Go to Appendix C for a list of the PPP statistics that you can view.

Chapter 2
PPP Concepts

This chapter describes PPP concepts that may help you decide how to customize the PPP parameters for your system. This chapter also addresses special configuration features of Bay Networks Point-to-Point Protocol (PPP) services. It contains basic guidelines on configuring PPP interfaces.

PPP Overview

Point-to-Point Protocol (PPP) is a standard method of routing or bridging datagrams between peer routers or other devices over serial point-to-point links (Figure 2-1).

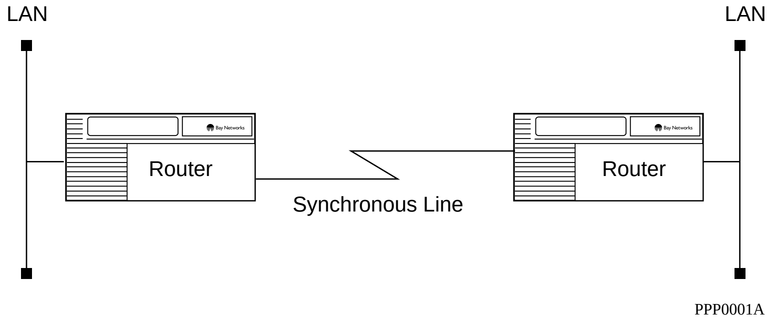


Figure 2-1. Point-to-Point Network Connection

PPP serves 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 peers to negotiate and determine data link and network layer options, such as those listed in Table 2-1 and Table 2-2. When negotiations complete successfully, PPP encapsulates the data and transmits it over the link.

Table 2-1. Sample Data Link Control Protocol Options

Option	Function
Maximum Receive Unit	Specifies the maximum transmission unit (MTU) size for the line.
Authentication Protocol: • Password Authentication Protocol (PAP) • Challenge Handshake Authentication Protocol (CHAP)	Imposes network security by requiring an authentication process.
Link Quality Protocol	Enables or disables link quality monitoring and reporting.
Multilink Endpoint Discriminator	Enables the PPP mulitlink protocol and specifies the identity of the sender of the option.

Table 2-2. Network Control Protocols and Options

Protocol	**Negotiable Options**
IP Control Protocol (IPCP)	IP Addresses (for backward compatibility), IP Address (default)
Internet Packet 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 Networking System Control Protocol (XNSCP)	None
VINES Network Control Protocol (VNCP)	None
Bridge Network Control Protocol (BNCP)	MAC Type Selection

Routing over a PPP Link

You can enable the following protocols over PPP interfaces:

- AppleTalk
- DECnet Phase IV
- Internet Packet Exchange (IPX)
- Internet Protocol (IP)
- Open Systems Interconnection (OSI)
- Virtual Networking System (VINES)
- Xerox Networking System (XNS)

The protocol that you selected when you first enabled PPP on the circuit is enabled by default. You can enable a different protocol by editing PPP protocol parameters, as described in Chapter 3.

Transparent/Translation Bridge and Source Route 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 to allow them to exchange data. The routers initialize the interface in three phases:

1. Establishing the PPP link
2. Authenticating the link (optional for leased lines)
3. Negotiating network layer protocols

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 uses to define its end of the link.

For example, a Configure-Request packet may specify the link's maximum transmission unit (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,* which means that the PPP interface can advance to the next phase.

- Configure-Reject

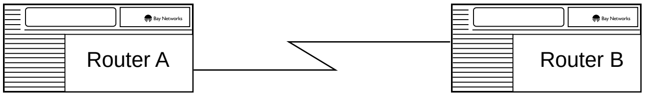
  If the Configure-Request packet contains options that the peer router is not willing to negotiate, the peer router sends back a Configure-Reject packet specifying the nonnegotiable options. From that point on, Configure-Request packets that the originating router sends should eliminate the unacceptable options.

- Configure-NAK

  If the peer disagrees with some or all of the values of the proposed options in the Configure-Request packet, it responds with a Configure Negative Acknowledgment (NAK) packet. The Configure-NAK packet notes the values that the peer disagrees with, and it 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, until the peer router transmits a user-specified number of Configure-NAK packets before sending a Configure-Reject packet, or until the configurable convergence timer expires. When the originating router receives a Configure-Reject packet, the originating router removes the offending options. The routers should then converge.

Figure 2-2 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*	**CHAP***
Send Authenticate-Request →	Challenge →
← Send Authenticate-ACK	← 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 2-2. Initializing the PPP Interface

Authenticating the PPP Link: PAP and CHAP

In the authentication phase of PPP initialization, one or both peer routers enable either Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP). Authentication is optional for leased lines but required for switched (dial-up) lines. You can optionally specify a time limit for authentication on switched lines.

Password Authentication Protocol

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 to reinitialize the line.

Challenge Handshake Authentication Protocol

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

➡ **Note:** For all dial services, you must use PAP or CHAP, either of which provides an identification mechanism that is essential to bringing up dial-on-demand, bandwidth-on-demand, and dial backup lines. Failure of either authentication protocol causes the connection to be dropped, without the network administrator's intervention.

One-Way Authentication

One-way authentication uses an authentication protocol on only one side of a dial-up connection. The router placing the call disables the authentication protocol for a circuit, while the router on the receiving side enables authentication. Disabling the outbound authentication lets the router interoperate with other devices that may not allow two-way authentication or support CHAP.

The receiving router can use both PAP and CHAP in the same line pool. When the router receives a call, it authenticates using the user-configured protocol. If the calling router rejects the authentication protocol CHAP, the receiving router switches to PAP.

One-way authenticationrequires that PAP and CHAP be enabled in the same line pool. Set the PPP Local Authentication Protocol parameter to CHAP and enable PAP Fallback. You must also configure certain options for the switched circuit itself. See *Configuring Dial Services* for a description of how you must set up dial services to enable one-way authentication.

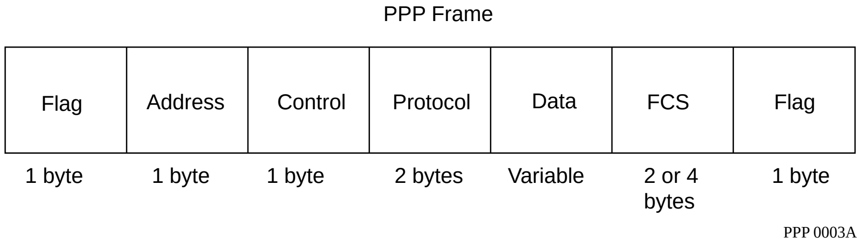
Negotiating Network Layer Protocols

PPP uses various network control protocols to determine the values of parameters during network layer negotiations, the final phase of PPP initialization. Like the LCP, each network control protocol 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 and which media types to bridge. Once both peer routers agree upon network options, the network control protocol reaches the open 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 similar to a high-level data link control (HDLC) frame (Figure 2-3).



PPP Frame

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

PPP 0003A

Figure 2-3. PPP-Encapsulated Frame

The parts of the PPP frame function as follows:

- The Flag field marks the beginning and end of a frame. Peers 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 shows the frame type (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 1594 bytes; LCP negotiations determine the actual length.
- The Frame Check Sequence (FCS) field shows the sequence order of the frame; router hardware computes the FCS. A 16- or 32-bit cyclic redundancy check (CRC) is at the end of each frame.

PPP Dial Services Support

Bay Networks dial services offer access to switched networks through dial-up line connections (also called *switched lines*) that are active only when you choose to use them. In contrast, a leased line is always available. If you transmit limited amounts of data, or if your data transmission is intermittent, dial services may let you run your network more effectively and economically.

PPP is automatically configured on lines that you select for dial services. PPP, with either CHAP or PAP, implements a router identification mechanism that dial services require.

Bay Networks provides three types of dial services: dial-on-demand, bandwidth-on-demand, and dial backup. For information on how to configure dial-on-demand, bandwidth-on-demand, and dial backup lines, see *Configuring Dial Services*.

Dial-on-Demand

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 have a network connection only when you need it and significantly reduce your line costs.

Bandwidth-on-Demand

Bandwidth-on-demand uses secondary, dial-up lines to augment a primary, leased line (or lines) or an initial dial-on-demand line when the primary line experiences congestion. Congestion occurs when traffic volume exceeds the configured congestion threshold. Bandwidth-on-demand brings up these secondary lines one at a time, as needed, up to a maximum of 30 lines, including the primary lines. Up to 30 lines can be combined into a multilink bundle, depending upon platform constraints, total bundle speed, variance in member links speeds, and traffic characteristics. When congestion abates, the secondary lines become inactive.

Please consult the Bay Networks Technical Response Center in your area for design guidelines.

Dial Backup

If a primary PPP, Frame Relay, or standard line fails and you have enabled dial backup, the router automatically establishes a backup line and data transmission continues.

PPP Multiline

Bay Networks PPP services include support for the multiline feature, which lets you configure a single circuit that consists of one or more WAN data paths. A data path is a logical point-to-point channel that is a permanent (leased) line. Multiline provides both increased fault tolerance and greater bandwidth between two sites.

Refer to the section “Differences between Multi*line* and Multi*link*” on page 2-16 for a comparison of these features. For more information about the Bay Networks multiline feature, see *Configuring Line Services*. For information on configuring PPP multiline over HSSI interfaces within the BNX environment, refer to *Configuring Customer Access and Trunks (BNX Software)*.

PPP Multilink

Note: BNX software does not support the PPP multilink feature. If you use BNX, ignore this and the following sections relating to multilink.

The multilink feature of PPP provides capabilities beyond those of multiline circuits. The major characteristics of multilink include the ability to

- Use lines that have different speeds, proportionally distributing traffic over those lines
- Balance traffic load and maintain packet sequence
- Use switched lines (such as ISDN-B channels) as well as leased lines
- Monitor traffic volume

Configurations with bandwidth-on-demand, which can activate additional lines in response to increased traffic, can find these features particularly useful.

Multilink is available on all platforms that have more than one WAN line, including the following platforms:

- BLN®/BCN®
- LN®/CN®
- AFN®
- AN™
- ASN™

Using PPP Multilink

The routers at each end of a PPP link (that is, a logical communications line) are called *peers*. A link is an individual communication channel between two peers. Typical links include one ISDN-B channel, an aggregation of T1 DS0s, one dial-up modem connection, and one leased T1 line.

Links can be either leased or switched lines. All links must have the same data link encapsulation (PPP), and all links must have the same maximum transmission unit (MTU). On non-ISDN lines, you must configure the clock speed.

When you enable multilink, you can configure a set of links between two peers into a single “bundle,” which can consist of up to 30 links, possibly of different bandwidths. (The practical maximum number of lines depends on factors such as the amount of memory, the number of lines configured, the speed of those lines, the packet sizes, and the traffic patterns.) With multilink configured, leased lines in a bundle can be on different router slots. Multilink distributes traffic over each logical line in a bundle in an amount roughly proportional to the effective bandwidth of the link.

With multilink and bandwidth-on-demand enabled, you can configure one side of the link as the congestion monitor. This router monitors network traffic and line usage. When the traffic exceeds a user-specified threshold, the bandwidth-on-demand monitor can bring up a secondary line.

Figure 2-4 shows a configuration that uses the multilink feature.

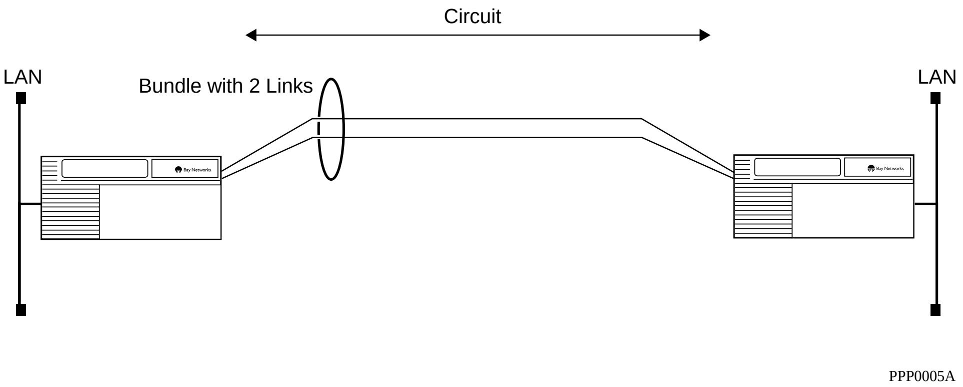


Figure 2-4. Multilink Circuit

As Figure 2-4 shows, a bundle is a logical connection between two routers. Once you have configured a circuit for multilink or bandwidth-on-demand operation, it always uses PPP multilink encapsulation.

All lines in a circuit must negotiate and perform multilink. You cannot pair non-multilink lines with multilink lines in a circuit. Multilink can resequence packets sent over different lines of the link. Starting with Version 11.0, PPP supports packet fragmentation and reassembly, as described in the section "Using Multilink Fragmentation" on page 2-14.

You can use the multilink feature over the following physical media:

- V.35
- MCT1/MCE1
- ISDN-B channel drivers
- Raise-DTR modems
- V.25bis modems

Compatibility with Previous Versions

A multi*line* circuit using PPP cannot communicate with a router running a software version earlier than 9.0. Pre-9.0*x* versions use a multiline circuit with LCP running on only one line. In this situation, you must use uniline PPP.

A multi*link* circuit can communicate only with a router running Version 10.0 or later software (because earlier versions do not support the multilink feature). Attempting to run multilink on a pre-10.0 version results in the multilink circuit dropping back to multiline.

Configuring Multilink Operation

You configure a PPP multilink circuit by selecting the appropriate value in the PPP Mode parameter for the intended circuit. This parameter controls whether the local side of the bundle attempts to negotiate the multilink protocol, and whether the local circuit operates as the congestion monitor for bandwidth-on-demand. The congestion monitor locally monitors traffic congestion on the circuit. Only one side of any connection should be the congestion monitor.

Balancing Traffic Loads

In a configuration with multilink enabled, a sending router divides the outbound traffic among all the lines in the bundle. The configured external clock speed of each line determines the proportion of the total traffic each receives. For example, pairing a 9600-bit/second line with an ISDN-B channel yields a clock-speed ratio of roughly 1:6.8, assuming same-size packets. That is, for every packet sent on the slower link, the router can send about seven packets on the faster link.

On the receiving end, multilink resequences packets arriving on different links using the sequence number from the multilink header. Gaps in the ordering may occur, however, when packets are corrupted or otherwise lost or when they arrive after packets with later sequence numbers. To minimize this situation, multilink buffers out-of-sequence packets in case the preceding sequence-numbered packets arrive shortly after the later-numbered packets.

Using Multilink Fragmentation

By default, PPP multilink allows packet fragmentation. With fragmentation enabled, PPP splits large datagrams into smaller packets and sends these packets across links in a multilink bundle. Enabling fragmentation means that PPP can split packets when necessary for better performance. PPP does not arbitrarily split all the packets it transmits. Fragmentation improves the distribution of data across multilink lines and uses buffer resources more efficiently, thereby improving the flow of data over multilink circuits. By default, multilink fragmentation is enabled. Bay Networks routers comply with RFC 1717, which defines PPP multilink.

Without multilink fragmentation, when PPP sends packets over a multilink bundle, it sends one packet over each line in sequence in a round-robin fashion. To optimize performance, PPP does attempt to send fewer packets on the slower lines. However, some packets with higher sequence numbers sent over faster lines *could* be received earlier than packets with lower sequence numbers sent over slower lines. Since PPP maintains the sequence of received packets, the receiving peer must store the out-of-sequence packets until the delayed packet arrives, and this can result in slower network performance. If the number of packets needing to be resequenced is greater than the available allowed buffer space, some packets could be considered late and discarded.

When you enable fragmentation, you can specify the minimum-size packet that you want PPP to consider fragmenting. (The default minimum size is 256 bytes.) Even with fragmentation enabled, PPP generally avoids splitting packets unless network performance considerations warrant it.

When necessary, PPP splits packets into fragments and then sends the fragments over the lines in the bundle, reassembling them on the receiving peer into the proper sequence. PPP discards all fragments of an incomplete reassembly. The number of fragments is equal to or less than the number of lines available. For bundles containing lines of different speeds, PPP tries to send the smaller fragments over the slower lines. This mechanism ensures a more even flow of data.

Packets sent over a multilink bundle have an outer header packet that contains a unique packet sequence number and allows for

- Fragmentation of the original packets
- Assignment of sequence numbers to each fragment
- Transmission over a number of links in the bundle
- Reassembly of the original sequence and packet size at the receiving peer

Using Protocol Prioritization with Multiline and Multilink

Note: BNX software uses a different protocol prioritization mechanism from that described in this section. For information on BNX traffic prioritization and congestion control mechanisms, refer to *Configuring Customer Access and Trunks (BNX Software)*.

When you configure a 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 other types. For example, PPP control messages must have precedence over other types of data.

Selecting PPP on a circuit automatically enables protocol prioritization without specifying any filters.

With the multi*line* feature, you can configure both priorities and filters. For more information about protocol prioritization, see *Configuring Traffic Filters and Protocol Prioritization.*

The multi*link* feature uses the automatically enabled functions of protocol prioritization, but only for interrupt queuing. You cannot specify either traffic filters or priorities. Multilink assigns the highest (that is, interrupt-level) priority to link control packets, treating all other traffic as normal priority. This gives PPP control messages precedence over other types of data while preserving the packet sequencing.

Differences between Multiline and Multilink

Both multiline and multilink use circuits consisting of one or more data paths between two peer routers. Each has its special characteristics and advantages, described in the following paragraphs and summarized in Table 2-3.

Table 2-3. Comparing Multiline and Multilink

Feature	**Multiline**	**Multilink**
Advantages	• Fault tolerance • Bandwidth availability	• Fault tolerance • Bandwidth availability • Uses all lines in the bundle for greatest speed and efficiency
Number of physical lines/ circuit	• Up to 31 concurrent data paths/group • Data paths can either be physical or logical lines (multiple independent data paths running over a single physical interface)	Up to 30 lines/bundle, depending on platform constraints, total bundle speed, variance in member links speeds, and traffic characteristics. Please consult the Bay Networks Technical Response Center in your area for design guidelines.
Grouped/bundled data paths	The data paths that together make up a multiline circuit must share the same speed, MTU, and encapsulation method	Lines in a bundle can have different speeds
Line types	Can use leased lines	Can use leased as well as switched lines
Protocol prioritization	• Automatically enabled • User can specify protocol priority and/or traffic filters	• Automatically enabled • Not user configurable • Automatically assigns highest (interrupt) priority to LCP packets and assigns all others normal priority

(continued)

Table 2-3. Comparing Multiline and Multilink *(continued)*

Feature	**Multiline**	**Multilink**
Used with these data link types	• Bay Networks standard synchronous • Frame Relay direct mode • PPP	PPP (only)
Media supported	• Synchronous • T1/E1 • MCE1/MCT1 • HSSI	• Synchronous • T1/E1 • MCE1/MCT1 • ISDN B-channel drivers • Raise-DTR/V.25bis modems
Packet resequencing	Depends on the path selection: • With address-based selection (the default), packets always arrive in sequence. • With random path selection, packets traveling on different paths can arrive at their destination out of sequence.	Multilink maintains the sequence of packets sent over different lines of the link.
Support for bandwidth-on-demand	No	Yes
Miscellaneous	• Address-based selection does not always result in even traffic distribution across all data paths. • Random selection provides for even traffic distribution.	• All lines in a circuit must negotiate and perform multilink. • You cannot use nonmultilink lines in a circuit with multilink lines. • All data packets sent over a PPP multilink circuit travel as multilink packets.

Monitoring PPP Link Quality

To ensure that the router can successfully transfer data, PPP monitors the quality of the point-to-point link with Link Quality Monitoring (LQM) and Link Quality Report (LQR) packets. PPP supports LQM over standard synchronous interfaces only. PPP does not support LQM over High-speed Serial Interfaces (HSSI). BNX software, however, *does* support LQM and LQR over HSSI interfaces.

Note: PPP uses LQM and LQR only if you set the Link Quality Protocol parameter to LINKQR. The default is None.

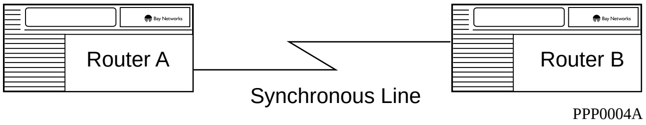
When you enable link quality monitoring through the Link Quality Protocol, you are turning on monitoring only for the local router. For link quality monitoring to be operational, it only has to be enabled on one side of the link. If two routers are configured for different link quality reporting periods, they negotiate to the lower value, so that the LQR period will be the same on both sides of the link.

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, PPP uses that packet 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 this router successfully receives).

After five LQR reporting periods, PPP averages the inbound and outbound link quality and compares these values against a user-specified threshold. This is a rolling average. After the first five LQR reporting periods, PPP acquires the data from the next period and drops the oldest data. Then it computes the link quality average for that set of five LQR periods, and so on.

If either the inbound or outbound link quality average drops below the threshold, PPP brings down the link. The driver software automatically brings the link back up and renegotiates the connection. PPP monitors the link control packets flowing over the connection and resumes network control protocol packet traffic when the link quality improves.

For example, in Figure 2-5, the acceptable outbound and inbound link quality configured on Router A for the PPP interface is 100 percent. After five LQR periods, Router A calculates the outbound and inbound link quality averages and determines that the inbound link quality average is below the 100 percent threshold (in this case, 90 percent). As a result, Router A disables the link.



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 2-5. Link Quality Monitoring from Router A’s Perspective

In addition to LQR packets, PPP periodically transmits Echo-Request packets (when Echo-Request is enabled). If the peer transmits a user-specified number of Echo requests before receiving an Echo reply from its peer router, the router disables the link and restarts.

Note: Echo-Requests are disabled by default and are in no way related to link quality reporting.

PPP Data Compression

The Bay Networks data compression feature lets you reduce line costs and improve response times over wide area networks (WANs) running PPP.

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.

Bay Networks data compression services for PPP include

- Software-based compression for all platforms and all serial interfaces
- Hardware-based data compression for PPP networks that use the octal synchronous link module for the Backbone Node (BN®), using only FRE®-2 processors. Bay Networks provides hardware compression as an optional daughterboard that attaches to the octal synchronous link module.
- Hardware-based data compression for PPP networks that use the octal synchronous link module for the Access Stack Node (ASN™), using any link module. Bay Networks provides hardware compression as an optional daughterboard.

You can use data compression on all PPP circuits, including multiline, multilink, bandwidth-on-demand, dial-on-demand, and dial backup lines. You can use compression separately on each member of a multilink bundle. When you use compression on a bandwidth-on-demand, dial-on-demand, or dial backup circuit, the data compression feature automatically configures or deletes compression as lines are added to or removed from the circuit.

For complete descriptions of hardware and software data compression, descriptions of compression parameters, and instructions for configuring compression over a PPP interface, see *Configuring Data Compression Services*.

Synchronous versus Asynchronous Connections

When you configure a dial (switched) circuit, you can specify whether you want transmission on that circuit to be synchronous or asynchronous. Switched services include dial-on-demand, bandwidth-on-demand, and dial backup. These function independently of the physical modem communication method.

In synchronous transmissions, the timing of each data transfer has a specific time relationship to the previous and next data transfer. Synchronous data transfers are fast because of the low network overhead relative to the amount of data transferred in each block, but they require more expensive, clock-driven data transmission equipment. In general, you might use synchronous data transmission for large data transfers.

Asynchronous communication, on the other hand, does not rely on a clock to define the beginning and end of a transmission. It uses lower-cost, asynchronous modems and appends a start and a stop bit to each transmission. This adds overhead to each data transfer, but it is often acceptable in lower-speed (less than 56KB, for example) and lower-volume data transfers. You can, for example, use an asynchronous modem connected to either a router or a PC to dial into a Bay Networks AN™, ASN, BN, or BCN® router or terminal server (such as a Xylogics 5390) with asynchronous modem banks.

You configure most of the synchronous/asynchronous parameters when you set up dial services on a circuit and configure your modem pools. A modem pool can contain synchronous lines, asynchronous, or ISDN lines.

When you create or add a line to a dial services modem pool for a line configured to use PPP, the parameters that you must supply differ, depending on whether it is a synchronous or an asynchronous line. Refer to *Configuring Dial Services* for details on setting up and configuring both synchronous and asynchronous lines.

Recognizing Asynchronous Modem Control Characters

For a link that uses asynchronous modems, you can configure PPP to recognize and “escape” specified control characters that may occur in data packets. An example of such control characters is the XON/XOFF flow control mechanism that asynchronous modems use. The escape mechanism removes spurious control characters that external hardware may have introduced on the link.

During LCP negotiation, both peers negotiate the characters that they will recognize as modem control characters. PPP calculates and displays a map value based on this negotiation. Each end of the link maintains an asynchronous control character map for both sending and receiving.

When sending data, PPP inserts the escape character 0x7D in front of the control character and does a logical XOR operation, combining the control character with the value 0x20. When the receiving peer encounters these characters in the data stream, it strips off the escape character and converts the next character to the original asynchronous modem control character.

The async control character map consists of 32 bits. Each bit corresponds to one control character, 0x00 (the right end of the map) through 0x1F (the left end of the map); that is, 0 through 31, decimal. The actual map is a value used essentially as a mask. For example, the default map value, 0xA0000 (655360 decimal) allows the escaping of the control characters 0x11 (XON) and 0x13 (XOFF) if they occur in the data stream. Almost all modems need only this default value. The characters 0x7D and 0x7E are special characters that are always escaped in asynchronous data transmission. Chapter 3 describes how to build a customized async control character map.

PPP Line Parameters

When you enable PPP on a circuit (the default), PPP automatically sets the line parameters shown in Table 2-4. These parameters are the same for both synchronous and asynchronous connections.

Table 2-4. PPP Line Parameter Values

Parameter	Value
BOFL	Disable
Promiscuous	Enable
Service	Transparent
WAN Protocol	PPP

Depending on the configuration, you may have to specify explicitly certain other parameters. For more information on these parameters, refer to *Configuring Routers* or *Configuring Customer Access and Trunks (BNX Software),* as appropriate for your platform.

Configuring IP to Run over PPP Interfaces

When you enable numbered Internet Protocol (IP) support on a PPP interface, you must also configure an adjacent host entry for the peer router. See *Configuring IP Services* for instructions on configuring an adjacent host entry.

Detecting Loopback Conditions

As part of its network integrity checking, PPP tests for a loopback condition in which, effectively, it is talking to itself and not communicating with the network. Normally, you would want this feature enabled. For test purposes, however, you can disable this loopback detection feature by using the Technician Interface. After disabling this parameter, you must explicitly set it to Enable to re-enable loopback checking. See “Disabling Loopback Detection” in Chapter 3 for instructions on how to set this parameter.

PPP Software Compatibility Issues

If you need to configure PPP to run over a point-to-point connection between a Version 5.*x* and a Version 11.0 router, read this section.

➡ **Note:** This section is not relevant for BNX software.

The features introduced in Version 11.0, namely asynchronous PPP and multilink fragmentation, are available only with this version.

Version 5.*x* router software uses a Bay Networks proprietary implementation of PPP. Version 7.*x*, Version 8.*x*, Version 9.*x*, Version 10.0, and Version 11.0 routers support a new implementation of PPP. The new implementation complies with the established requirements of the following Internet RFCs: 1332, 1333, 1334, 1378, 1552, 1638, 1661, 1662, 1762, 1763, and 1764. Version 10.0 and 11.0 routers also support the multilink feature, described in RFC 1717.

With the different implementations of PPP, each adhering to a different set of RFCs, the following functions will not work between a Version 5.*x* and a Version 9.*x*, Version 10.0, or Version 11.0 router:

- Link Quality Monitoring (LQM)
- Source-routing over Token Ring networks

For communication over a synchronous line between a Version 5.*x* and a Version 9.*x*, Version 10.0, or Version 11.0 router, each running PPP, make the following configuration checks:

- On the Version 9.*x*, Version 10.0, or Version 11.0 router

  - -- The type of synchronous line service (MIB object ID 1.3.6.1.4.1.18.3.4.5.1.18, *wfSyncService*) must have a value of *Transparent*. (This is the default setting for the Service parameter in the Edit Sync Parameters window. To access the parameter through the Configuration Manager, click on the appropriate sync connector and select Edit Line Details.)

- On the Version 5.*x* router
  - -- The LQM Time parameter must have a value of 0, which disables Link Quality Monitoring on the Version 5.*x* router.
  - -- The Quality of Service parameter must have a value of LLC1, the default setting.

For information on how to check these Version 5.*x* parameters, refer to your Version 5.*x* configuration guide.

For further information on configuring different versions of routers to assure software compatibility, see *Upgrading Routers from Version 7-10.xx to Version 11*.

PPP Interoperability

Bay Networks implementation of PPP conforms to the RFCs listed in the previous section; therefore it can interoperate with routers that also conform to the same standards. If you have questions about whether a particular router can interoperate with your Bay Networks router running PPP Version 11.0, please contact the Bay Networks Technical Response Center for your area, as listed in “About This Guide.”

Stopping the Flow of Traffic over a PPP Interface

To stop traffic from routing over a PPP interface, either disable the Network Control Protocol (NCP) for the upper-level routing protocol or disable the upper-level protocol itself.

For example, if you disable the NCP for IP, even though IP is still enabled on the interface, it is no longer able to route traffic over the interface. See “Disabling Network Control Protocols” in Chapter 3 for instructions on disabling NCP parameters.

Disabling the routing protocol running on top of the PPP interface also automatically disables the NCP for the routing protocol. For example, if you disable IP on an interface, you disable the NCP for IP as well.

Where to Go Next

Go to Chapter 1 for instructions on how to start PPP on your router.

Go to Chapter 3 for instructions on how to customize a PPP interface.

Go to Appendix A for a description of PPP parameters.

Go to Appendix B for a list of PPP parameter default values.

Go to Appendix C for a list of the PPP statistics that you can view.

Chapter 3
Customizing PPP

This chapter describes how to customize and enable PPP services. It assumes you have configured PPP on the interface using the default parameters, as described in Chapter 1 and that you understand the PPP concepts in Chapter 2. You should have read *Configuring Routers* or *Configuring Customer Access and Trunks (BNX Software)*, as appropriate for your platform, and have

1. Opened a configuration file
2. Specified router hardware, if this is a local mode configuration file
3. Selected the link or net module connector on which you are enabling PPP

You can enable PPP services most easily by accepting all the default parameter values that the Configuration Manager supplies. You do not have to configure any PPP parameters for PPP to run on your system.

If, however, you choose to change some or all of the default parameters, you'll find the information you need in this chapter. For a list of all PPP parameters, see Appendix A, "PPP Parameters."

Enabling PPP on an Interface

If you have already enabled PPP on the circuit that you want to configure, go to "Setting Up Remote Addresses" on page 3-2. If you haven't already done so, you must enable PPP on the interface. To do this, refer to Chapter 1.

By default, the protocol that you selected when you first configured this interface is enabled. If you want to enable a different protocol, you can do so as part of the customization.

The rest of this chapter describes how to configure and customize PPP for your system. Follow the instructions that apply to your network requirements.

➡ **Note:** If you are dynamically configuring a router that has already negotiated its Link Control Protocol, you must force LCP renegotiation on the interface to implement your changes. To do this, disable and then re-enable the corresponding network control protocol(s).You can change as many parameters as you need to before forcing the renegotiation.

After making all your changes to any of the addressing or routing protocol enabling parameters:

1. **Set the corresponding network control protocol parameter (for example, IP Enable) to Disable and, if necessary, apply the changes.**
2. **Reset the same parameter to Enable and, if necessary, apply the changes.**

Refer to the description of enabling specific protocols for details.

Setting Up Remote Addresses

You can define an address and node number (depending on the requirements of the protocol you've chosen) that you want the remote peer to use. That is, you can define an

- IP address
- IPX network number and node number
- AppleTalk node number

depending on the protocol you enable. After enabling the protocol, specify the appropriate parameter(s) as described in the following sections.

Defining an IP Address for a Remote Peer

1. **Enter the IP address, in dotted decimal notation, that you want the remote peer to use.**

The default is 0.0.0.0, indicating that this is an unnumbered interface. You can enter any valid IP address. (For information about unnumbered IP interfaces, refer to *Configuring IP Services*.)

Site Manager: Remote IP Address parameter: page A-7

2. **Configure IP to run over PPP interfaces.**

   When you enable numbered Internet Protocol (IP) support on a PPP interface, you must also configure an adjacent host entry for the peer router. See *Configuring IP Services* for instructions on configuring an adjacent host entry.

Defining an IPX Network Number and Node Number for a Remote Peer

You can specify an IPX network number and an IPX node number that you want the remote peer to use. The interface uses these numbers in its NCP negotiations. To specify an IPX network number and remote node number, do the following:

1. **Enter the IPX network number, in hexadecimal notation, for the remote peer to use.**

Site Manager: IPX Network Number parameter: page A-7

   There is no default value; you can enter any unique, valid, unreserved IPX network number, consisting of a string of up to eight hexadecimal characters. The value 0xffffffff is invalid.

   The *negotiated* network 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. In addition, the negotiated IPX network number can be 0 on both sides of the link. In this case, IPX defines the link’s network number.

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

2. **Enter the IPX node number for the remote node to use.**

Site Manager: IPX Remote Node Number parameter: page A-8

If you want to specify an IPX node number for the remote peer to use, enter it here. The interface uses this IPX remote node number in its NCP negotiations.

Configuring AppleTalk

To enable AppleTalk on the interface, configure an AppleTalk node number and the AppleTalk routing update protocol for the remote peer to use.

Defining a Remote AppleTalk Node Number for a Remote Peer

If you want to specify an AppleTalk node number that the peer router should use, enter it here. This interface includes this AppleTalk node number in its Network Control Protocol negotiations.

Enter the AppleTalk node number for the remote peer to use. There is no default value; you can enter any valid AppleTalk node number.

Site Manager: Remote AppleTalk Node parameter: page A-8

Defining the AppleTalk Routing Protocol

You can specify the AppleTalk routing update protocol for the peer router to use.

Site Manager: AppleTalk Routing Protocol parameter: page A-9

Since the only option for the AppleTalk Routing Protocol is the Routing Table Management Protocol (RTMP), you can simply accept the default value. This interface specifies AppleTalk RTMP as the routing update protocol in NCP negotiations.

Enabling Bridging on an Interface

When bridging is enabled for an interface, PPP accepts bridged traffic in the specified encapsulation and forwards it over the PPP network. You can enable or disable bridging for Ethernet, FDDI, and/or Token Ring encapsulated packets. By default, all these parameters are enabled. If you change any of these parameters dynamically (that is, for a router that has already completed its negotiations), you must force LCP renegotiation on the interface, as previously described.

Enabling Bridging

Before you can enable a particular type of encapsulated bridged traffic, you must enable bridging on the interface. You do this by default if you enabled bridging when you initially set up the PPP interface, but you can disable or re-enable it here. To stop traffic from being bridged over this interface, set this parameter to Disable.

Site Manager: Bridge Enable parameter: page A-5

This parameter enables or disables the network control protocol for the bridge. It does *not* enable or disable bridging services for the interface. However, disabling the network control protocol for the bridge stops traffic from being bridged over this interface.

Enabling Ethernet Bridging

If you want PPP to accept and forward Ethernet-encapsulated bridged traffic, set this parameter to Enable (the default).

Set this parameter to Disable if you do not want PPP to accept and forward Ethernet encapsulated frames.

Site Manager: Bridge Ethernet parameter: page A-9

Enabling FDDI Bridging

If you want PPP to accept and forward FDDI encapsulated bridged traffic, set this parameter to Enable (the default).

Set this parameter to Disable if you do not want PPP to accept and forward FDDI encapsulated frames.

Site Manager: Bridge FDDI parameter: page A-10

Enabling Token Ring Bridging

If you want PPP to accept and forward Token Ring encapsulated bridged traffic, set this parameter to Enable (the default).

Set this parameter to Disable if you do not want PPP to accept and forward Token Ring encapsulated frames.

Site Manager: Bridge FDDI parameter: page A-10

Enabling VINES Support on This Interface

If you enabled VINES support when you first configured PPP on this interface, this parameter defaults to Enable; otherwise, the default is Disable. To stop VINES traffic from being routed over this interface, set this parameter to Disable.

Site Manager: VINES Enable parameter: page A-6

This parameter enables or disables the network control protocol for VINES. It does not enable or disable VINES routing services for the interface. However, disabling the network control protocol for VINES stops VINES traffic from being routed over this interface.

Enabling DECnet IV Support on This Interface

If you enabled DECnet IV support when you first configured PPP on this interface, this parameter defaults to Enable; otherwise, the default is Disable. To stop DECnet IV traffic from being routed over this interface, set this parameter to Disable.

Site Manager: DECnet IV Enable parameter: page A-4

This parameter enables or disables the network control protocol for DECnet IV. It does not enable or disable DECnet IV routing services for the interface. However, disabling the network control protocol for DECnet IV stops DECnet IV traffic from being routed over this interface.

Enabling Data Compression on This Interface

If you enabled data compression when you initially configured this interface, then data compression is configured by default for PPP; otherwise, the default is Disable. To stop compression over this interface, set this parameter to Disable.

Site Manager: CCP Enable parameter: page A-6

This parameter allows or stops data compression. It does not enable or disable data compression for the interface, but disabling the Compression Control Protocol (CCP) stops data compression over this interface.

Specifying the Type of Connection - PPP Mode

The PPP Mode parameter indicates the type of connection on this interface: single-line, multiline, multilink, or multilink monitor. This section deals with how you set up each of these PPP modes.

Setting Up a PPP Single-Line Connection

Your choice of options depends on the type of circuit you’re configuring.

Site Manager: PPP Mode parameter: page A-11

For any nonmultilink circuit, use Normal as the parameter value. This is the default for any nonmultilink circuit.

Setting Up a PPP Multiline Connection

As for a single-line connection, use Normal as the parameter value for a multiline connection. This is the default for any nonmultilink circuit.

Site Manager: PPP Mode parameter: page A-11

For a description of the differences between multiline and multilink connections, see “Differences between Multiline and Multilink” in Chapter 2. For more information about multiline connections, refer to *Configuring Dial Services*.

Setting Up a PPP Multilink Connection

For a multilink connection, you have more options.

Site Manager: PPP Mode parameter: page A-11

Set the PPP Mode parameter to Multilink to configure the circuit for multilink operation. Set it to Monitor if you want the local router to serve as the congestion monitor for the multilink circuit. Only one side of any connection should be the monitor.

Configuring the Maximum Number of Links in a Multilink Bundle

You can specify the maximum number of links that you want included in any multilink circuit bundle.

Site Manager: Max Links parameter: page A-12

The links in a bundle can be either leased or switched lines and can have different transmission speeds.

Configuring the Maximum Number of Storage Buffers

You can specify the maximum number of buffers to allocate for storing packets for this multilink circuit.

Site Manager: Max Buffers parameter: page A-13

The optimum number of buffers depends on factors such as

- Amount of memory available for buffers
- Likelihood of delays in the arrival of packets
- Amount and characteristics of network traffic received

In general, a higher number of buffers uses more memory but allows more latitude for late-arriving packets.

Configuring Multilink Fragmentation

For multilink circuits that include different speed links and that may carry both large and small packets, you can enable multilink fragmentation.

Site Manager: Multilink Fragmentation parameter: page A-11

PPP fragments packets only if doing so will improve the flow of data over the circuit. When necessary, PPP splits packets into encapsulated fragments and then sends the fragments over the lines in the multilink bundle, reassembling them on the receiving peer into the proper sequence. PPP discards all fragments of an incomplete reassembly. The number of fragments is always equal to or less than the number of lines in the bundle. Multilink fragmentation is enabled by default.

When you enable fragmentation, you can specify the minimum size packet that you want PPP to consider fragmenting. The default minimum size is 256 bytes.

Site Manager: Fragmentation Min Size parameter: page A-12

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 (by setting the IP Enable parameter to Disable), even though IP is still enabled on the interface, it is no longer able to route traffic over the interface.

- Disable the upper-level routing protocol itself.

  If you disable the routing protocol running on top of the PPP interface, you also automatically disable the NCP for the routing protocol. For example, disabling IP on an interface disables the NCP for IP as well.

Customizing PPP Lines

The PPP line parameters specify the characteristics of individual lines within the interface. You can edit the default PPP line parameters to fit your particular system requirements. Appendix B lists the default PPP line parameters. The following sections describe how to customize those parameters.

Editing PPP Line Parameters

If you change any of the parameters in the following list and you are dynamically configuring a router that has already negotiated its Link Control Protocol, you must force LCP renegotiation on the interface to implement your changes. To do this, disable and then re-enable the Enable (LCP) parameter.

- Echo-Reply Acceptable Loss
- Max Configure-Requests
- Max Terminate-Requests
- Max Configuration Failure Count
- 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
- Asynchronous Control Character Map
- Authentication Timer
- Convergence Timer
- Magic Num Disable

You can change as many parameters as necessary before forcing the renegotiation. After making all your changes to these parameters:

1. **Set the Enable (LCP) parameter to Disable and, if necessary, apply the changes.**

2. **Reset the Enable (LCP) parameter to Enable and, if necessary, apply the changes.**

Enabling Link Control on a Line

The Link Control Protocol (LCP) is enabled by default on the interface. Disabling the Enable (LCP) parameter generates a "close" event to the LCP, and enabling this event generates an "open" event to the LCP. A major use of this sequence is to force LCP renegotiation on the interface during dynamic reconfiguration. Doing so means that any changes you have made to the line parameters are included in the negotiations.

Site Manager: Enable (LCP) parameter: page A-14

To disable LCP on this interface, set Enable (LCP) parameter to Disable. To re-enable LCP, set this parameter to Enable.

Setting Transmission Parameters

You can specify the timing of transmissions and the threshold for considering the link to be down using the parameters described in the following sections.

Setting the Restart Timer

The value of the Restart Timer in Seconds parameter specifies the number of seconds that the restart timer waits before retransmitting data. The default value is 3 seconds, and the range is 1 through 1000 seconds.

Site Manager: Restart Timer in Seconds parameter: page A-14

Specifying the Interval between Echo-Request Packets

The value of the Seconds between Xmit of Echo-Request parameter specifies the number of seconds that the router waits between the transmission of Echo-Request packets. A value of 0 (the default) means that this parameter is turned off.

Site Manager: Seconds between Xmit of Echo-Request parameter: page A-14

Specifying the Acceptable Level of Echo-Reply Packet Loss

The Echo-Reply Acceptable Loss parameter specifies the maximum number of unacknowledged Echo-Request packets that the router will transmit before declaring the point-to-point link down. The default value is 3 packets.

Site Manager: Echo-Reply Acceptable Loss parameter: page A-15

Specifying the Maximum Number of Configure-Request Packets

The Max Configure-Requests parameter specifies the maximum number of unacknowledged Configure-Request packets that the router transmits 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. The default value is 10 packets.

Site Manager: Max Configure-Requests parameter: page A-15

Specifying the Maximum Number of Terminate-Request Packets

PPP uses the Maximum Terminate-Requests parameter to specify 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. The default value is 2 packets.

Site Manager: Max Terminate-Requests parameter: page A-16

Specifying the Maximum Configuration Failure Count

The Max Configuration Failure Count parameter specifies the maximum number of Configure-NAK packets that the router sends before sending a Configure-Reject packet for those options that it does not agree with. The default value is 10 packets.

Site Manager: Max Configuration Failure Count parameter: page A-16

Setting a Time Limit for Convergence

Convergence occurs when the peers have negotiated all the parameters needed to establish a dial services connection. You can limit the amount of time that PPP attempts to negotiate a switched PPP interface by setting the Convergence Timer parameter.

Site Manager: Convergence Timer parameter: page A-26

This parameter applies only to a switched PPP interface. The convergence timer specifies the maximum number of seconds allowed for the completed negotiations. It limits the LCP negotiations and requires at least one NCP to negotiate within the configured amount of time. The default value is 300 seconds. If the timer expires before the negotiation completes, the connection is dropped.

The convergence timer allots the configured number of seconds for the LCP to negotiate and allots the same period for one NCP to complete negotiations.

Customizing PPP Authentication Parameters

PPP imposes network security by offering support for two types of authentication protocols: Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP). The following sections describe how to configure PPP to implement PAP and CHAP.

➡ **Note:** For all dial services, you must use PAP or CHAP, either of which provides an identification mechanism that is essential to bring up demand, backup, and bandwidth lines. You must configure the CHAP local name, CHAP secret, PAP ID, and PAP password through the Dial menu. See *Configuring Dial Services* for details.

In addition, for all dial services, failure of either authentication protocol causes the connection to be dropped, and no intervention from the network administrator is needed.

For leased lines, the authentication phase is optional.

You must first specify what, if any, local authentication protocol this interface uses.

Site Manager: Local Authentication Protocol parameter: page A-17

The Local Authentication Protocol parameter specifies the type of authentication protocol that this interface uses: None, PAP, or CHAP.

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

To enable Password Authentication Protocol, select PAPAUTH. Then define the Local PAP ID and Local PAP Password parameters for this interface.

To enable Challenge Handshake Authentication Protocol, select CHAP. Then define the CHAP Secret, CHAP Local Name, and CHAP Periodic Timer parameters for this interface.

Setting a Time Limit for Authentication

You can specify the maximum number of seconds the router waits for a response to its authentication messages by setting the Authentication Timer parameter.

Site Manager: Authentication Timer parameter: page A-26

If the timer expires before the negotiation completes, the router drops the connection. The default value is 10 seconds.

Customizing PAP

When PAP is the authentication protocol, you must also specify a local PAP ID, a local PAP Password, and a remote PAP ID and remote PAP password for the peer. During the authentication phase of link creation, PPP uses these parameters to verify the peer's right to communicate with the local router.

➡ **Note:** For dial services that use PAP, you must configure the local PAP ID, the local PAP password, the remote PAP ID, and the remote PAP password through the Dial menu. See *Configuring Dial Services* for details.

Specifying Local PAP Parameters

If you did not enable PAP on the local peer, ignore the local PAP parameters that follow. If you set the Local Authentication Protocol to PAPAUTH, specify a unique local PAP identifier and local PAP password for 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 and PAP password. Otherwise, the interface sends an Authenticate-NAK message and the link is not created.

The Local PAP ID parameter specifies the identifier assigned to this interface. The identifier can consist of any text string, up to 25 characters long. There is no default value.

Site Manager: Local PAP ID parameter: page A-18

Now set the local PAP password.

Site Manager: Local PAP Password parameter: page A-18

The Local PAP Password parameter specifies the password assigned to this interface. The password can consist of any text string, up to 25 characters long. There is no default value.

Specifying PAP Parameters for the Remote Peer

If the remote peer does not have PAP enabled, ignore the remote PAP parameters that follow.

During the authentication phase of link creation, PPP uses the remote PAP ID and remote password to verify the local peer’s right to communicate with the remote router. During the authentication phase, this interface must include the correct remote PAP ID and remote PAP password in all Password Authenticate-Request messages it sends to the local peer router; otherwise, the peer router sends an Authenticate-NAK message and the link is not created.

If the remote peer has PAP enabled, specify the Remote PAP ID parameter, which assigns a PAP identifier to the remote peer. There is no default value.

Site Manager: Remote PAP ID parameter: page A-19

Now set the remote PAP password.

Site Manager: Remote PAP Password parameter: page A-19

The Remote PAP Password parameter specifies the password assigned to the remote peer router. The password can consist of any text string, up to 25 characters long. There is no default value.

Allowing PAP Rejection

Some peers do not use PAP. If you set the Allow PAP Reject parameter to Enable, your router accepts the Reject message from such a peer and removes PAP from the LCP Configure-Request.

Site Manager: Allow PAP Reject parameter: page A-24

The default value is Disable.

Customizing CHAP

The Challenge Handshake Authentication Protocol imposes network security by requiring that the peers share a plain-text secret. You specify that secret, as well as other CHAP parameters, by configuring the parameters described in the next sections. If you have not enabled CHAP, ignore these parameters.

➡ **Note:** For dial services that use CHAP, you must configure the CHAP secret and the CHAP local name through the Dial menu. See *Configuring Dial Services* for details.

Specifying the CHAP Secret

The function of the CHAP secret is similar to a password, but its use is slightly different. Both peers 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 network-layer negotiation phase. You can assign a text string up to 20 characters long as the CHAP secret for this interface.

Site Manager: CHAP Secret parameter: page A-23

If you have enabled CHAP, specify the secret. There is no default value.

Specifying the CHAP Local Name

A local CHAP name informs the peers of each other’s identity. Specify the CHAP local name as a text string of up to 20 characters. There is no default value.

Site Manager: CHAP Local Name parameter: page A-23

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

Specifying the CHAP Authentication Challenge Interval

The CHAP Periodic Timer parameter indicates the interval (in seconds) that must elapse between CHAP challenges. You can specify any number of seconds. Setting this value to 0 (the default) disables the timer. A reasonable value for this parameter is 60.

Site Manager: CHAP Periodic Timer parameter: page A-24

PPP allows repeated authentication challenges at an interval (in seconds) that either peer 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.

Enabling PAP Fallback

If the peer sends a Configure-NAK packet , rejecting CHAP as the authentication protocol, and if you have enabled PAP fallback, the router offers PAP as the authentication protocol.You must also have enabled PAP and provided a PAP password.

Site Manager: Enable PAP Fallback parameter: page A-20

Setting the Enable PAP Fallback parameter to Enable causes a fallback to PAP if you have selected CHAP as the authentication protocol, but the peer rejects CHAP. The default value is Disable.

Set this parameter to Enable if you mix authentication types in the same pool.

Setting Up Link Quality Monitoring

When you turn on the link quality monitoring and reporting function for an interface, PPP monitors the quality of the point-to-point link as a percentage of sent packets received on each end of the link. When the average quality falls below the threshold you specify, PPP brings down the link. The driver software automatically brings the link back up and renegotiates the connection.

By default, link quality monitoring is disabled. If you do not want to enable this feature, accept the default value.

Note: PPP supports link quality monitoring over standard synchronous interfaces only. PPP does not support link quality monitoring over asynchronous or High-Speed Serial Interfaces (HSSI). BNX software, however, does support both link quality monitoring and link quality reporting over HSSI interfaces.

If two routers are configured for different link quality reporting periods, they negotiate to the lower value, so that the period is the same on both sides of the link.

Enabling Link Quality Monitoring and Reporting

To turn on link quality monitoring and reporting for the interface, set the Link Quality Protocol parameter to LINKQR.

Site Manager: Link Quality Protocol parameter: page A-20

When you enable link quality monitoring and reporting through the link quality protocol, you are turning on monitoring only for the local router. The router on which you enable it is responsible for monitoring link quality for the connection. By default, link quality monitoring and reporting is disabled.

If you do not enable link quality monitoring and reporting, ignore the rest of the link quality parameters.

Establishing the Timing of Link Quality Reports

You can specify which peer is responsible for running the Link Quality Report Timer and set the maximum interval between the transmission of Link Quality Report packets.

Designating the Link Quality Report Timekeeper

This parameter deals with the *remote* peer, not the local one. The setting determines whether the remote peer runs the Link Quality Report (LQR) timer for the connection. Setting this parameter enables or disables the remote peer’s LQR timer.

The peer whose timer is enabled generates one LQR packet for each interval specified in the LQR Reporting Period parameter. The peer whose timer is disabled verifies that the other peer did, in fact, send an LQR. If three successive LQRs are not received, the receiving peer disables the connection.

Site Manager: Peer Link Quality Report Timer parameter: page A-21

Accept the default, Enable, if you want the remote peer router to maintain an LQR timer for the interface. Reset this parameter to Disable if you do not want the peer to maintain the LQR timer for the interface.

Specifying the Link Quality Reporting Period

The LQR Reporting Period parameter specifies the maximum number of seconds between the transmission of LQR packets.

Site Manager: LQR Reporting Period parameter: page A-21

Enter a number representing the interval between the transmission of LQR packets. The value of this parameter can be from 1 through 120 seconds. The default value is 3 seconds.

Specifying the Inbound Link Quality

The Inbound Link Quality parameter 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.

Site Manager: Inbound Link Quality parameter: page A-22

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

The default value for this parameter is 90 (percent). You can specify values in the range 1 through 100 (percent).

Specifying the Outbound Link Quality

The Outbound Link Quality parameter specifies the minimum acceptable success rate (percentage) of packets the router transmits and the peer router receives on this interface.

Site Manager: Outbound Link Quality parameter: page A-22

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

The default value for this parameter is 90 (percent). You can specify values in the range 1 through 100 (percent).

Specifying the Asynchronous Modem Control Character Map

During LCP negotiations, the peers negotiate the characters that they will recognize as asynchronous modem control characters. PPP creates a 32-bit map that represents the negotiated control characters. Both routers use this map in sending and receiving data packets. While the default value serves for almost all modems, you can configure the map for other modem control characters if necessary.

The async control character map specifies a value representing one or more asynchronous modem control characters for the peer to recognize ("escape") and that may occur in the data packet. Each bit in the map corresponds to one control character, 0x00 (the right end of the map) through 0x1F (the left end of the map); that is, 0 through 31, decimal. The actual map is a value used essentially as a mask. For example, the default map value, 0xA0000 (655360 decimal) allows the escaping of the control characters 0x11 (XON) and 0x13 (XOFF) if they occur in the data stream. The values 0x7D and 0x7E are always escaped.

If you have a modem that requires control characters different from the default, you can build your own async control character map. Determine the corresponding bit for each character by converting the hex value of the control character to decimal. For example, 0x1F = 31 decimal; so to escape that character, set the leftmost bit in the map. Do the same thing for each control character. Once you've decided what bits in the map to set, you can enter either the hex character equivalent to the bit string or the decimal equivalent. To set escape all control characters in the packet, set the map to 0xFFFFFFFF. For a description of how PPP encodes escaped control characters in the data stream, refer to Chapter 2.

PPP displays the decimal number equivalent to the string and uses that value in its link negotiations.

Site Manager: Async Control Character Map parameter: page A-25

Viewing Line Statistics for Multilink Circuits

To view the statistics that PPP collects for multilink circuits, use the Technician Interface software to access the PPP MIB. For instructions on how to use this software, refer to *Using Technician Interface Software.* Appendix C lists the PPP multilink statistics and describes the data that they record. The key statistics to check are the following:

- In the *wfPppCircuitEntry* MIB:
  - -- *wfPppCircuitMlFragPerm* indicates that fragmentation is enabled.
  - -- *wfPppCircuitMlFragTriggerSize* indicates the smallest-size packet that PPP may fragment.
  - -- *wfPppCircuitMaxBuffers* is the maximum allowable number of buffers for this circuit.
  - -- *wfPppCircuitMaxLinks* is the maximum number of links allowed in the multilink bundle for this circuit at any one time.

- In the *wfPppMlStatsEntry* MIB:
  - *wfPppMlStatsReSeqBufferCnt* is the current count of packets (not fragments) that the receiver has buffered because they arrived out of order. To analyze the effects of fragmentation, periodically observe this value under a typical traffic load *without* fragmentation enabled on the peer router, and then observe the value *with* fragmentation enabled on the peer router. Typically, this number is higher in configurations with greatly differing line speeds. This number should go down when fragmentation is enabled. If this number is constantly at or near the maximum number of buffers allowed, as indicated in *wfPppCircuitMaxBuffers*, reset the maximum number of buffers allowed to a higher number. In addition, the higher the value of *wfPppCircuitMaxLinks*s, the more likely it is you'll need to increase *wfPppCircuitMaxBuffers*.
  - *wfPppMlStatsReSeqBufferMax* is the maximum that *wfPppMlStatsReSeqBufferCnt* ever reached.
  - *wfPppMlStatsNumPktsFragmented* counts the number of packets that have been fragmented (transmit only). This indicates how often the router judges that fragmentation is necessary.
  - *wfPppMlStatsTxPkts* counts the total number of packets transmitted by multilink. Comparing this to the numberof packets fragmented (*wfPppMlStatsNumPktsFragmented*) helps you see how well the link is doing and whether you need to adjust parameters such as the minimum size of packets to be considered for fragmentation.
  - *wfPppMlStatsReasmFails* is an event counter of failures to reassemble a fragmented packet. If this number is high, either you're losing fragments or your reassembly buffer count is at or near the maximum number of buffers allowed, as indicated in *wfPppCircuitMaxBuffers*. Reset the maximum number of buffers allowed to a higher number.
  - *wfPppMlStatsReassmBufferCnt* is the number of fragments that the receiver has stored pending reassembly. Typically, this number is higher in configurations with greatly differing line speeds. If this number is constantly at or near the maximum number of buffers allowed, as indicated in *wfPppCircuitMaxBuffers*, reset the maximum number of buffers allowed to a higher number.
  - *wfPppMlStatsReassmBufferMax* is the maximum number that *wfPppMlStatsReassmBufferCnt* ever reached.

- -- *wfPppMlStatsExceededBufferMax* indicates the number of times the sum of *wfPppMlStatsReassmBufferCnt* and *wfPppMlStatsReSeqBufferCnt* exceeded the specified maximum allowable number of buffers, as indicated in *wfPppCircuitMaxBuffers*. As a side effect of reaching or exceeding *wfPppMlStatsExceededBufferMax,* you may see the value of *wfPppMlStatsSeqNumberArrived Late* increase. If so, it may indicate that you should increase *wfPppCircuitMaxBuffers*.

- In the *wfSyncEntry* MIB:

  -- *wfSyncRejectsRx* counts the number of times a packet arrives that is larger than a receive buffer. *wfSyncRejectsTx* counts the number of times a packet grows larger than its transmit buffer. If either of these conditions occurs, lower the size of the maximum transmission unit (MTU), *wfSyncMtu*, on both the local and remote peers.

Disabling Loopback Checking

For test purposes, you can disable the loopback test that the peer normally performs as part of its network integrity checking. The loopback test ensures that a peer is talking to the network, not to itself.

Site Manager: Magic Num Disable parameter: page A-26

To disable loopback detection, set the Magic Num Disable parameter to Disable. After disabling this parameter, you must explicitly set it to Enable to re-enable loopback checking.

Deleting PPP

You can delete PPP from a specific circuit by simply reconfiguring that circuit with a different configuration file that does not use PPP.

The way you delete PPP from *all* circuits on which it is currently configured depends on the tool you are using. For detailed information, refer to *Configuring Routers*, *Configuring Customer Access and Trunks (BNX Software)*, or *Using Technician Interface Software*, as appropriate.

Site Manager: Protocols > PPP > Delete PPP > **OK**

When you delete PPP globally, PPP no longer operates on the router. Be aware that the Technician Interface software does not ask you to confirm your deletions.

➡ **Note:** Site Manager does not let you delete PPP globally from a router running dial-on-demand, bandwidth-on-demand, or dial backup.

Where to Go Next

Go to Chapter 1 for instructions on how to start PPP on your router.

Go to Chapter 2 to learn more about PPP concepts and characteristics.

Go to Appendix A for a list of all PPP parameters.

Go to Appendix B for a list of PPP parameter default values.

Go to Appendix C for a list of the PPP statistics that you can view.

Appendix A
PPP Parameters

This appendix lists the parameters for the PPP interfaces that you can configure on the router. For each PPP parameter, this appendix gives the Site Manager path, the default setting, all valid parameter options or ranges, the parameter function, instructions for setting the parameter, and the Management Information Base (MIB) object ID. Refer to Chapter 3 for a full description of the tasks to which these parameters pertain.

After you enable PPP, you can edit all PPP parameters. For instructions on using Site Manager to edit PPP parameters, refer to *Configuring Routers* or *Configuring Customer Access and Trunks (BNX Software)*, as appropriate for your platform. Alternatively, you can use Technician Interface **set** and **commit** commands to modify parameter values in the MIB object ID. This process is equivalent to modifying parameters using Site Manager.

Caution: The Technician Interface does not verify the validity of the parameter values that you enter. Entering an invalid value can corrupt your configuration.

The following sections deal with the parameters in two groups: those that pertain to configuring PPP on the interface and those that you use to configure PPP on individual lines on the interface. These correspond to Site Manager's PPP Interfaces and PPP Line Lists windows, respectively.

PPP Interface Parameter Descriptions

Use the following guidelines to configure the PPP Interface parameters. The order of presentation corresponds to the order of fields in the PPP Interfaces window, and also (approximately) to the order of items in the *wfPppCircuitEntry* MIB.

Note: In BNX software environments, only the IP Enable parameter is meaningful. In the BNX environment, ignore all other PPP interface parameters.

Parameter: IP Enable

Path: Protocols > PPP > Interfaces

Default: If you enable IP support when you configure PPP on this interface, this parameter is automatically set to Enable. Otherwise, the default is Disable.

Options: Enable | Disable

Function: Enables or disables the Network Control Protocol for IP.

This parameter does *not* enable or disable IP routing services for the interface; it affects the Network Control Protocol for IP. However, disabling the Network Control Protocol for IP stops IP traffic from being routed over this interface.

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

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.12

Parameter: OSI Enable

Path: Protocols > PPP > Interfaces

Default: If you enable Open Systems Interconnect (OSI) support when you configure PPP on this interface, this parameter is automatically set to Enable. Otherwise, the default is Disable.

Options: Enable | Disable

Function: Enables or disables the Network Control Protocol for OSI.

This parameter does *not* enable or disable OSI routing services for the interface; it affects the Network Control Protocol for OSI. However, disabling the Network Control Protocol for OSI stops OSI traffic from being routed over this interface.

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

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.13

Parameter: XNS Enable

Path: Protocols > PPP > Interfaces

Default: If you enable XNS support when you configure PPP on this interface, this parameter is automatically set to Enable. Otherwise, the default is Disable.

Options: Enable | Disable

Function: Enables or disables the Network Control Protocol for XNS.

This parameter does *not* enable or disable XNS routing services for the interface; it affects the Network Control Protocol for XNS. However, disabling the Network Control Protocol for XNS stops XNS traffic from being routed over this interface.

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

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.14

Parameter:	**DECnet IV Enable**
Path:	Protocols > PPP > Interfaces
Default:	If you enable DECnet IV support when you configure PPP on this interface, this parameter is automatically set to Enable. Otherwise, the default is Disable.
Options:	Enable | Disable
Function:	Enables or disables the Network Control Protocol for DECnet IV. This parameter does *not* enable or disable DECnet IV routing services for the interface; it affects the Network Control Protocol for DECnet IV. However, disabling the Network Control Protocol 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 this parameter to Disable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.2.1.15

Parameter:	**AppleTalk Enable**
Path:	Protocols > PPP > Interfaces
Default:	If you enable AppleTalk support when you configure PPP on this interface, this parameter is automatically set to Enable. Otherwise, the default is Disable.
Options:	Enable | Disable
Function:	Enables or disables the Network Control Protocol for AppleTalk. This parameter does *not* enable or disable AppleTalk routing services for the interface; it affects the Network Control Protocol for AppleTalk. However, disabling the Network Control Protocol for AppleTalk stops AppleTalk traffic from being routed over this interface.
Instructions:	To stop AppleTalk traffic from being routed over this interface, set this parameter to Disable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.2.1.16

Parameter: IPX Enable

Path: Protocols > PPP > Interfaces

Default: If you enable Internet Packet Exchange (IPX) support when you configure PPP on this interface, this parameter is automatically set to Enable. Otherwise, the default is Disable.

Options: Enable | Disable

Function: Enables or disables the Network Control Protocol for IPX.

This parameter does *not* enable or disable IPX routing services for the interface; it affects the Network Control Protocol for IPX. However, disabling the Network Control Protocol for IPX stops IPX traffic from being routed over this interface.

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

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.17

Parameter: Bridge Enable

Path: Protocols > PPP > Interfaces

Default: If you enable the bridge when you configure PPP on this interface, this parameter is automatically set to Enable. Otherwise, the default is Disable.

Options: Enable | Disable

Function: Enables or disables the Network Control Protocol for the bridge.

This parameter does *not* enable or disable bridging services for the interface; it affects the Network Control Protocol for the bridge. However, disabling the Network Control Protocol for the bridge 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

Path: Protocols > PPP > Interfaces

Default: If you enable VINES support when you configure PPP on this interface, this parameter is automatically set to Enable. Otherwise, the default is Disable.

Options: Enable | Disable

Function: Enables or disables the Network Control Protocol for VINES.

This parameter does *not* enable or disable VINES routing services for the interface; it affects the Network Control Protocol for VINES. However, disabling the Network Control Protocol for VINES stops VINES traffic from being routed over this interface.

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

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.19

Parameter: CCP Enable

Path: Protocols > PPP > Interfaces

Default: If you enable data compression when you configure PPP on this interface, this parameter is automatically set to Enable. Otherwise, the default is Disable.

Options: Enable | Disable

Function: Enables or disables data compression.

This parameter does *not* enable or disable data compression for the interface. However, disabling the Compression Control Protocol (CCP) stops data compression over this interface.

Instructions: To stop compression over this interface, set this parameter to Disable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.49

Parameter: Remote IP Address

Path: Protocols > PPP > Interfaces

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.

If this interface has been up and running, you must also set the IP Enable parameter to Disable, apply the change, 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

Path: Protocols > PPP > Interfaces

Default: None

Options: Any 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.

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

The network number does not have to be the same on both sides of the link; PPP negotiates the higher of the two numbers. Note also that the negotiated IPX network number may be 0 on both sides of the link. In this case, IPX defines the link’s network number.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.24

Parameter: IPX Remote Node Number

Path: Protocols > PPP > Interfaces

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, apply the change, 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

Path: Protocols > PPP > Interfaces

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, apply the change, 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**

Path: Protocols > PPP > Interfaces

Default: RTMP

Options: RTMP (Routing Table Management 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**

Path: Protocols > PPP > Interfaces

Default: Enable

Options: Enable | Disable

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

Instructions: Set 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, apply the change, 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

Path: Protocols > PPP > Interfaces

Default: Enable

Options: Enable | Disable

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

Instructions: Set 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, apply the change, 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

Path: Protocols > PPP > Interfaces

Default: Enable

Options: Enable | Disable

Function: Specifies whether this PPP interface accepts bridged traffic that is Token Ring encapsulated, 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: Set 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, apply the change, 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

Parameter: PPP Mode

Path: Protocols > PPP > Interfaces

Default: Multilink for a dial-on-demand or bandwidth-on-demand circuit

Normal for a nonmultilink circuit

Options: Normal for a nonmultilink circuit

Multilink | Monitor for a dial-on-demand or bandwidth-on-demand circuit

Normal | Multilink for all other circuit types

Function: Specifies the type of multiline or multilink connection on this interface.

Instructions: The set of available options depends on the type of circuit you’re configuring. Select one of the following values:

Normal - to configure a nonmultilink circuit

Multilink - to enable the multilink feature

Monitor - to designate the local router as the multilink monitor

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.50

Parameter: Multilink Fragmentation

Path: Protocols > PPP > Interfaces

Default: Permitted

Options: Permitted | Prohibited

Function: This parameter is active only for multilink. Allows packet fragmentation on multilink circuits, when needed.

Instructions: Accept the default, Permitted, if you want to allow multilink packet fragmentation. Otherwise, specify Prohibited.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.51

Parameter: Fragmentation Min Size

Path: Protocols > PPP > Interfaces

Default: 256 (bytes)

Range: 64 through the maximum transmission unit for the circuit

Function: This parameter is active only for multilink. Specifies the minimum size of a packet that multilink will fragment.

Instructions: When packet fragmentation over multilink is permitted, accept the default or specify the minimum packet size that PPP will consider fragmenting.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.57

Parameter: Max Links

Path: Protocols > PPP > Interfaces

Default: 4 (links)

Range: 1 through 30

Function: This parameter is active only for multilink. It specifies the maximum number of links (both leased and switched lines) allowed in the multilink bundle for this circuit at any one time.

Instructions: Accept the default, 4, or enter a value in the range 1 through 30. If this is not a multilink circuit, leave this parameter blank. Up to 30 lines can be combined into a Multilink bundle, depending upon platform constraints, total bundle speed, variance in member links speeds, and traffic characteristics.

Please consult the Bay Networks Technical Response Center in your area for design guidelines for your particular network needs.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.58

Parameter: **Max Buffers**

Path: Protocols > PPP > Interfaces

Default: 30 (buffers)

Range: 10 through 60 (buffers)

Function: This parameter is active only for multilink. It specifies the maximum allowable number of buffers stored by multilink for this circuit. The choice depends on such factors as the amount of memory available for buffers, the likelihood of delays in the arrival of packets, and the amount of total network traffic, among other variables. In general, a higher number uses more memory but allows more latitude for late-arriving packets.

Instructions: Accept the default, 30, or specify a value in the range 10 through 60.

If you experience buffer resource problems (not enough memory allocated for buffers), set this parameter to a lower value.

If you experience packet loss because of an inadequate number of buffers, increase this value.

You can determine whether buffer resource problems exist by using either the Site Manager Statistics feature or the Technician Interface. Check the number of times the number of buffers needing to be stored exceeded the number of buffers available. The MIB object *wfPppMlStatsExceededBufferMax* counts these occurrences.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.64

PPP Line Parameter Descriptions

Use the following guidelines to configure the PPP Lines parameters. The order of presentation corresponds to the order of fields in the PPP Lines window, and also (approximately) to the order of items in the *wfPppLineEntry* MIB. In the path names that follow, bold text indicates that in Site Manager, you invoke the PPP Line Lists window by clicking on the **Lines** button on the PPP Interfaces window.

Parameter: Enable (LCP)

Path: Protocols > PPP > Interfaces > **Lines**

Default: Enable

Options: Enable | Disable

Function: Enables or disables the Link Control Protocol (LCP) on the PPP interface. Disabling this parameter generates a “close” event to LCP. Similarly, enabling this parameter generates an “open” event to LCP.

Disabling, then re-enabling this parameter forces the interface to renegotiate the link.

Instructions: To disable LCP on this interface, set 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

Path: Protocols > PPP > Interfaces > **Lines**

Default: 3 (seconds)

Range: 1 through 1000

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

Path: Protocols > PPP > Interfaces > **Lines**

Default: 0 (seconds)

Range: 0 through 100

Function: Specifies the number of seconds that the router waits between the transmission of Echo-Request packets. A value of 0 means that this parameter is turned off.

Instructions: Accept the default value of 0 or enter an integer value in the range 0 through 100.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.8

Parameter: Echo-Reply Acceptable Loss

Path: Protocols > PPP > Interfaces > **Lines**

Default: 3 (packets)

Range: 1 through 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.

If you enter a different value, you must set the Enable (LCP) parameter to Disable, apply the change, and then reset the parameter to Enable to implement your change.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.9

Parameter: Max Configure-Requests

Path: Protocols > PPP > Interfaces > **Lines**

Default: 10 (packets)

Range: 1 through 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.

Instructions: Accept the default value of 10.
If you enter a different value, you must set the Enable (LCP) parameter to Disable, apply the change, and then reset the parameter to Enable to implement your change.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.10

Parameter: **Max Terminate-Requests**

Path: Protocols > PPP > Interfaces > **Lines**

Default: 2 (packets)

Range: 1 through 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.

If you enter a different value, you must set the Enable (LCP) parameter to Disable, apply the change, and then reset the parameter to Enable to implement your change.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.11

Parameter: **Max Configuration Failure Count**

Path: Protocols > PPP > Interfaces > **Lines**

Default: 10

Range: 1 through 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.

Instructions: Accept the default value of 10.

If you enter a different value, you must set the Enable (LCP) parameter to Disable, apply the change, and then reset the parameter to Enable to implement your change.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.12

Parameter: Local Authentication Protocol

Path: Protocols > PPP > Interfaces > **Lines**

Default: CHAP for dial services
None for all others

Options: None | PAPAUTH | CHAP

Function: Specifies the type of authentication protocol that this interface uses: none, PAP (Password Authentication Protocol), or CHAP (Challenge Handshake Authentication Protocol).

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, apply the change, 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, apply the change, and then reset the parameter to Enable.

For all dial services, you must use PAP or CHAP, either of which provides an identification mechanism that is essential to bring up demand, backup, and bandwidth lines. You must configure CHAP Local Name, CHAP Secret, PAP ID, and PAP Password through the Dial menu. See *Configuring Dial Services* for details.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.15

Parameter: Local PAP ID

Path: Protocols > PPP > Interfaces > **Lines**

Default: None

Options: 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. Otherwise, the interface sends an Authenticate-NAK message and the link is not created.

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

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

For dial services that use PAP, you must configure the local PAP ID through the Dial menu. See *Configuring Dial Services* for details.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.17

Parameter: Local PAP Password

Path: Protocols > PPP > Interfaces > **Lines**

Default: None

Options: Any text string; maximum 25 characters

Function: Specifies the PAP password assigned to this interface. During the interface’s authentication phase, all Password Authenticate-Request messages sent to this interface by the peer router must include the correct PAP password. Otherwise, the peer router sends an Authenticate-NAK message and the link is not created.

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

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

For dial services that use PAP, you must configure the local PAP Password through the Dial menu. See *Configuring Dial Services* for details.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.18

Parameter: **Remote PAP ID**

Path: Protocols > PPP > Interfaces > **Lines**

Default: None

Options: Any text string; maximum 25 characters

Function: Specifies the PAP ID assigned to the remote 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 an Authenticate-NAK message and the link is not created.

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

If the remote peer has PAP enabled, specify the remote PAP ID that identifies the remote peer. To implement your changes, set the Enable (LCP) parameter to Disable, apply the change, and then reset the parameter to Enable.

For dial services that use PAP, you must configure the remote PAP ID through the Dial menu. See *Configuring Dial Services* for details.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.19

Parameter: **Remote PAP Password**

Path: Protocols > PPP > Interfaces > **Lines**

Default: None

Options: Any text string; maximum 25 characters

Function: Specifies the PAP password assigned to the remote 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. Otherwise, the peer router sends an Authenticate-NAK message and the link is not created.

Instructions: If the remote peer has PAP enabled, specify the remote PAP password that identifies the remote peer. To implement your changes, set the Enable (LCP) parameter to Disable, apply the change, and then reset the parameter to Enable.

For all dial services, you must configure the remote PAP password through the Dial menu. See *Configuring Dial Services* for details.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.20

Parameter: Enable PAP Fallback

Path: Protocols > PPP > Interfaces > **Lines**

Default: Disable

Options: Enable | Disable

Function: Enabling this parameter causes a fallback to PAP if you have selected CHAP as the authentication protocol, and an attempt to negotiate CHAP fails.

Instructions: Select Enable or Disable. Set this parameter to Enable if you mix authentication types in a pool. Remember that you must use an authentication protocol if you are using dial-on-demand, bandwidth-on-demand, or dial backup.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.32

Parameter: Link Quality Protocol

Path: Protocols > PPP > Interfaces > **Lines**

Default: None

Options: None | LINKQR

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

Instructions: To enable link quality reporting, set this parameter to LINKQR. When you enable link quality reporting on one side of the connection, the router on which you enable it is responsible for monitoring link quality for the connection. To implement your changes, set the Enable (LCP) parameter to Disable, apply the change, 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

Path: Protocols > PPP > Interfaces > **Lines**

Default: Enable

Options: Enable | Disable

Function: This parameter deals with the *remote* peer, not the local one. The setting determines whether the remote peer runs the Link Quality Report Timer (LQR) for the connection. Setting this parameter enables or disables the remote peer's LQR Timer.

The peer whose timer is enabled generates one LQR packet for each interval specified in the LQR Reporting Period parameter. The peer whose timer is disabled verifies that the other peer did, in fact, send an LQR. If the receiving peer does not receive three successive LQRs, it disables the connection.

Instructions: Use this parameter only when you have set the Link Quality Protocol parameter to LINKQR.

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 do not want the peer to maintain the LQR timer for the interface. To implement your changes, set the Enable (LCP) parameter to Disable, apply the change, 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

Path: Protocols > PPP > Interfaces > **Lines**

Default: 3 (seconds)

Range: 1 through 120

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

Instructions: Use this parameter only when you set the Link Quality Protocol parameter to LINKQR.

Enter a number representing the interval between the transmission of LQR packets. To implement your changes, set the Enable (LCP) parameter to Disable, apply the change, 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

Path: Protocols > PPP > Interfaces > **Lines**

Default: 90 (percent)

Range: 0 through 100

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. Use this parameter only when you enable the Link Quality Protocol parameter.

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

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.25

Parameter: Outbound Link Quality

Path: Protocols > PPP > Interfaces > **Lines**

Default: 90 (percent)

Range: 0 through 100

Function: Specifies the minimum acceptable success rate (percentage) of packets the router transmits and the peer router receives on this interface. Use this parameter only when you enable the Link Quality Protocol parameter.

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

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.27

Parameter: CHAP Secret

Path: Protocols > PPP > Interfaces > **Lines**

Default: None

Options: 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 the network layer negotiation phase.

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, apply the change, and then reset the parameter to Enable.

For all dial services, you must configure CHAP Secret through the Dial menu. See *Configuring Dial Services* for details.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.31

Parameter: CHAP Local Name

Path: Protocols > PPP > Interfaces > **Lines**

Default: None

Options: 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 bandwidth-on-demand, 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 PAP.

For all dial services, you must configure CHAP Local Name through the Dial menu. See *Configuring Dial Services* for details.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.33

Parameter:	**CHAP Periodic Timer**
Path:	Protocols > PPP > Interfaces > **Lines**
Default:	0 (disabled)
Options:	Any number of seconds. Setting this value to 0 disables the timer. A reasonable value for this parameter is 60.
Function:	Allows for repeated authentication challenges at an interval (in seconds) that either peer 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:	Accept the default or set this parameter to 60. If you have not configured CHAP, ignore this field.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.1.1.35

Parameter:	**Allow PAP Reject**
Path:	Protocols > PPP > Interfaces > **Lines**
Default:	Disable
Options:	Enable | Disable
Function:	Some peers do not use PAP. If you set this parameter to Enable, your router accepts the Reject message from such a peer and removes PAP from the LCP Configure-Request.
Instructions:	Select Enable or Disable. If you have not configured PAP, ignore this field.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.1.1.39

Parameter: **Async Control Character Map**

Path: Protocols > PPP > Interfaces > **Lines**

Default: 655360

Range: 0 through 4294967295 (0x00 through 0xFFFFFFFF)

Function: This parameter is relevant only if you use an asynchronous modem. During LCP negotiations, the peers negotiate the characters that they will recognize as modem control characters.

The async control character map specifies a value representing one or more asynchronous modem control characters for the peer to recognize (“escape”) and that may occur in the data packet. Each bit in the map represents a control character from 0x00 through 0x1F. The default value serves for almost all modems. It escapes the asynchronous modem control sequence XON/XOFF (0x11 and 0x13) if they occur in the data stream. The values 0x7D and 0x7E are always escaped.

PPP displays the decimal number equivalent to the string and uses that value in its link negotiations.

Instructions: Accept the default value 655360 (0x000A0000) or enter the value corresponding to the asynchronous control character map for the character(s) that you want recognized (“escaped”) in the data stream. It is unusual to require a value other than the default.

If you must create a different map, here’s how to do it. The map consists of 32 bits. Each bit corresponds to one control character, 0x00 (the right end of the map) through 0x1F (the left end of the map); that is, 0 through 31, decimal.

If you have a modem that requires control characters different from the default, determine the corresponding bit for each character by converting the hex value of the control character to decimal. For example, 0x1F = 31 decimal, so to escape that character, set the leftmost bit in the map. Do the same thing for each control character to be escaped. Once you’ve decided what bits in the map to set, enter either the hex character equivalent to the bit string or the decimal equivalent. To set escape all control characters in a packet, set the map to 0xFFFFFFFF.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.41

Parameter:	**Authentication Timer**
Path:	Protocols > PPP > Interfaces > **Lines**
Default:	10
Range:	1 through 1000 (seconds)
Function:	Sets the time limit the router waits for a response to its authentication messages.
Instructions:	Accept the default value, 10 (seconds) or enter an integer in the range 1 through 1000. If you have not configured PAP or CHAP, ignore this field.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.1.1.43

Parameter:	**Convergence Timer**
Path:	Protocols > PPP > Interfaces > **Lines**
Default:	300 (seconds)
Range:	1 through 5000 (seconds)
Function:	Limits the amount of time PPP attempts to negotiate a dial-up connection. If the timer expires, the connection is dropped. This parameter is valid only for switched PPP interfaces.
Instructions:	Accept the default value, 10 (seconds) or enter an integer in the range 1 through 1000.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.1.1.44

Parameter:	**Magic Num Disable**
Path:	Protocols > PPP > Interfaces > **Lines**
Default:	Enable
Options:	Enable | Disable
Function:	Disables the loopback test that the peer normally performs as part of its network integrity checking. The loopback test ensures that a peer is talking to the network, not to itself.
Instructions:	Accept the default value, Enable, unless you are testing the connection. After disabling this parameter, you must explicitly set it to Enable to re-enable loopback checking.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.1.1.45

Appendix B
Default PPP Configuration

The PPP default configuration depends on which protocols you enable for the interface. Tables B-1 and B-2 list the default PPP parameter settings.

Table B-1. Point-to-Point (PPP) Interface Parameters

Parameter	Default
IP Enable OSI Enable XNS Enable DECnet IV Enable AppleTalk Enable IPX Enable Bridge Enable VINES Enable	Enabling support for any of these protocols when you configure PPP on this interface, automatically sets the protocol’s corresponding Enable parameter to Enable. Otherwise, the default is Disable.
CCP Enable	If you enabled data compression on this interface, Site Manager automatically sets this parameter to Enable. Otherwise, the default is Disable.
Remote IP Address	0.0.0.0
IPX Network Number	None
IPX Remote Node Number	None
Remote AppleTalk Node	None
AppleTalk Routing Protocol	RTMP
Bridge Ethernet	Enable
Bridge FDDI	Enable

(continued)

Table B-1. Point-to-Point (PPP) Interface Parameters *(continued)*

Parameter	**Default**
Bridge Token Ring	Enable
PPP Mode	Normal for a nonmultilink circuit Multilink for a multilink circuit
Multilink Fragmentation	Permitted
Fragmentation Min Size	256
Max Links	4
Max Buffers	30

Table B-2. Point-to-Point (PPP) Line Parameters

Parameter	**Default**
Enable (LCP)	Enable
Restart Timer in Seconds	3
Seconds between Xmit of Echo-Request	0
Echo-Reply Acceptable Loss	3
Max Configure-Requests	10
Max Terminate-Requests	2
Max Configuration Failure Count	10
Local Authentication Protocol	CHAP for dial services None for all others
Local PAP ID	None
Local PAP Password	None
Remote PAP ID	None
Remote PAP Password	None

(continued)

Table B-2. Point-to-Point (PPP) Line Parameters *(continued)*

Parameter	**Default**
Enable PAP Fallback	Disable
Link Quality Protocol	None
Peer Link Quality Report Timer	Enable
LQR Reporting Period	3
Inbound Link Quality	90
Outbound Link Quality	90
CHAP Secret	None
CHAP Local Name	None
CHAP Periodic Timer	None
Allow PAP Reject	Disable
Async Control Character Map	655360 (0x000A000)
Authentication Timer	10
Convergence Timer	300
Magic Num Disable	Enable

Appendix C
PPP Statistics

Table C-1 summarizes the PPP statistics you can view from the Site Manager Statistics Manager tool or from the Technician Interface.

Table C-1. PPP Statistics

MIB object name	**What it tells you**
wfPppMlStatsCircuitID	Circuit number for this instance
wfPppMlStatsHomeSlot	Slot on which this multilink control subsystem exists
wfPppMlStatsLineCnt	Current count of lines in the multilink bundle
wfPppMlStatsBundleSpd	Current total bandwidth of the multilink bundle
wfPppMlStatsTxOctets	Number of octets transmitted by multilink
wfPppMlStatsTxPkts	Number of packets transmitted by multilink
wfPppMlStatsAvgTxListLen	Average number of packets received in the transient list by the Multilink Transmit gate
wfPppMlStatsRxOctets	Number of octets received without error
wfPppMlStatsRxPkts	Number of packets received by multilink
wfPppMlStatsReasmFails	Number of packet reassembly failures
wfPppMlStatsSeqNumberLost	Number of multilink packets considered to be lost on the wire
wfPppMlStatsSeqNumberArrivedLate	Number of multilink packets that arrive containing an old sequence number; that is, packets with a more current sequence number have already been sent up to NCP

(continued)

Table C-1. PPP Statistics *(continued)*

MIB object name	What it tells you
wfPppMlStatsReSeqBufferCnt	Number of multilink packets currently stored in the ReSequencing buffer pool
wfPppMlStatsReSeqBufferMax	The maximum number of multilink packets stored in the ReSequencing buffer pool
wfPppMlStatsExceededBufferMax	The number of times a buffer needed to be stored by the Multilink Receive logic when the count of buffers stored, wfPppMlStatsReSeqBufferMax, was equal to the maximum allowable for this circuit,wfPppCircuitMaxBuffers
wfPppMlStatsLinkIdleEvents	The number of times the Multilink Receive logic detected a stored buffer received on a line what has been declared idle
wfPppMlStatsCalcPercent	Enable/disable calculating the percentage of multilink octets received on the line
wfPppMlStatsReassmBufferCnt	The number of multilink packets currently stored in the Reassembling buffer pools
wfPppMlStatsReassmBufferMax	The maximum number of multilink packets stored in the Reassembling buffer pools
wfPppMlStatsNumPktsFragmented	The number of multilink packets that were fragmented

Index