



Operator's Reference

Dictionary of Configuring,
Operating, and
Reporting Features

HP AdvanceStack Routers

Hewlett-Packard Series 200, 400, and 600 Routers

Operator's Reference

© Copyright Hewlett-Packard Company 1994.
All rights reserved.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard.

Publication Number
5962-8305
E0794

Edition 1, July 1994

Printed in Singapore

Product Numbers and Software Version

This guide provides information for Hewlett-Packard routers running software with the following version numbers:

A.08 series

B.08 series

C.08 series

Earlier and later software versions may operate differently than described in this manual.

Warranty

The information contained in this document is subject to change without notice

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

Preface

When To Use This Guide

Part I of this guide provides an alphabetical listing of Configuration Editor parameters and their descriptions, grouped according to their corresponding entries in the Configuration Menu of the Configuration Editor.

```
                                DEFAULT_CONFIG
=====-- SESSION 1 - MGR MODE -----
Configuration Editor

1.  System (1)
2.  Software (1)
3.  Lines (4)
4.  Circuits (4)
5.  Circuit Groups (4)
6.  Bridge (1)
7.  DoD Internet Router (0)
8.  DECNET IV Routing Service (0)
9.  SNMP Sessions (0)
10. Xerox Routing Service (0)
11. IPX Routing Service (0)
12. AppleTalk Router (0)
13. X.25 Network Service (0)
14. U.25 bis Network Mapping (0)

Enter Selection (0 for Previous Menu) : ____
```

The Configuration Menu of the Configuration Guide

Refer to Part I when you need information on a parameter in order to better understand how to use it in your router's configuration.

Part II of this guide provides detailed descriptions of the following:

- The router statistics screens
- The Network Command Language Interpreter (NCL) commands
- The Event Log messages
- The Management Information Base (MIB) variables

Preface

Refer to Part II when you need to learn the meanings of features in these areas. (To learn *how to use* statistics screens, NCL commands, the Event Log, and the MIB variables, refer to the *User's Guide*.)

Coverage Note	This manual addresses the entire range of parameters and other software features found in Hewlett-Packard routers, including features that are not found on all router models. Thus, for some routers, such as the HP Router PR (J2540), certain features described in this manual are not available in the router. For information on the features available in your router, refer to the release notes you received with the router or most recent software upgrade.
----------------------	--

Audience

This guide is intended for network managers and other technicians who install, configure, and manage routers.

Organization

Part I: Dictionary of Configuration Parameters logically groups the Configuration Editor parameters into chapters, according to the options in the Configuration menu. Each chapter contains an alphabetical listing of the indicated parameters, along with their corresponding options and descriptions. The individual chapters are:

- Chapter 1, "Global and Session Parameters"
- Chapter 2, "Software Parameters"
- Chapter 3, "Lines Parameters"
- Chapter 4, "Circuits Parameters"
- Chapter 5, "Circuit Group Parameters"
- Chapter 6, "Bridge Parameters"
- Chapter 7, "Internet Protocol (IP) Parameters"
- Chapter 8, "DECnet Parameters"
- Chapter 9, "SNMP Parameters"

- Chapter 10, "Xerox Network System (XNS) Parameters"
- Chapter 11, "IPX Protocol Parameters"
- Chapter 12, "AppleTalk Parameters"
- Chapter 13, "X.25 Service Parameters"
- Chapter 14, "V.25 bis Network Mapping Parameters"

Part II: General Operating Reference provides detailed reference information on the router's statistics output, NCL command usage, event messages, and MIB variables. The individual chapters are:

- Chapter 15, "Statistics"
- Chapter 16, "Network Command Language (NCL) Commands"
- Chapter 17, "Event Log Messages"
- Chapter 18, "Management Information Base (MIB) Variables"

Appendix A, "Public Ethernet Type Field Values", lists Ethernet packet types found in the 13th and 14th octets of an Ethernet packet.

Appendix B, "TCP and UDP Well-Known Port Numbers", lists well-known port numbers used by TCP and UDP.

Appendix C, "Parameter Locator", is an aid to locating individual parameters in the Configuration Editor Structure.

The Index includes references to terms and parameters described in this manual.

Other HP Router Manuals

For a current listing of manuals designed for use with your Hewlett-Packard router, refer to the *Hewlett-Packard Router Products Release Notes* shipped with your router or most recent software update.

Operator's Reference
Preface

Contents

Operator's Reference

Preface	3
When To Use This Guide	3
Audience	4
Organization	4
Other HP Router Manuals	5

Introduction

Part 1 Dictionary of Configuration Parameters

1 Global and Session Parameters

Overview	1-2
Parameters and Options	1-4

2 Software Parameters

Overview	2-2
Parameters and Options	2-3

3 Lines Parameters

Overview	3-2
Parameters and Options	3-3

4 Circuit Parameters

Overview	4-2
Parameters and Options	4-5

5 Circuit Group Parameters

Overview	5-2
Parameters and Options	5-3

6 Bridge Parameters

Overview	6-2
Parameters and Options	6-5

7	Internet Protocol (IP) Parameters	
	Overview	7-2
	Parameters and Options	7-6
8	DECnet Parameters	
	Overview	8-2
	Parameters and Options	8-4
9	SNMP Agent Parameters	
	Overview	9-2
	Parameters and Options	9-3
10	Xerox Network Systems (XNS) Router Parameters	
	Overview	10-2
	Parameters and Options	10-4
11	IPX Protocol Parameters	
	Overview	11-2
	Parameters and Options	11-5
12	AppleTalk Parameters	
	Overview	12-2
	Parameters and Options	12-5
13	X.25 Service Parameters	
	Overview	13-2
	Parameters and Options	13-4
14	V.25 bis Network Mapping	
	Overview	14-2
	Parameters and Options	14-3

Part II General Operating Reference

15 Using the Statistic Screens

AppleTalk Router Statistics Screen	15-4
Bridge Statistics Screen	15-6
Buffers Usage Statistics Screen	15-8
Circuit Statistics Screen	15-10
DECnet Router Statistics Screen	15-12
DoD IP Router Statistics Screen	15-14
IPX Router Statistics Screen	15-16
Per Second Statistics Screen	15-18
XNS Router Statistics Screen	15-20

16 Using the Network Control Language

Managing Router Operations and Resources	16-2
Accessing the Management Information Base	16-30
Accessing the Internet Management Information Base	16-40
Accessing a Remote Management Information Base	16-48
Accessing a Foreign Management Information Base	16-51
Accessing Bridging and Routing Tables	16-54
Managing the Open Shortest Path First Protocol	16-72
Blocking and Unblocking Spanning Tree Explorer Frames	16-84
Controlling IP-Mapped Circuits for V.25 bis	16-87
Using TFTP To Transfer Operating Code, Configuration, and NCL Display	16-93
Using ZModem to Transfer Configuration and NCL Display	16-98

17 Event Log Messages

How To Use This Chapter	17-2
at: AppleTalk Event Messages	17-4
boot: Boot Event Messages	17-15
bootp: Network Boot Protocol Event Messages	17-16
cct: Circuit Event Messages	17-18

dev: Device Event Messages	17-60
dls: Data Link Services Event Messages	17-69
drs: DECnet Event Messages	17-74
egp: Exterior Gateway Protocol Event Messages	17-79
ip: IP Event Messages	17-86
ipx: IPX Router Event Messages	17-92
lb: Bridge Event Messages	17-96
line: Lines Event Messages	17-101
mgr: Manager Event Messages	17-103
ospf: OSPF Event Messages	17-105
pm: Port Module Manager Event Messages	17-112
ppp: Point-to-Point Protocol	17-117
rok: Router Operating Kernel Event Messages	17-120
SMDS Event Messages	17-122
tcp: Transmission Control Protocol Event Messages	17-124
telnet: Telnet Event Messages	17-125
tftp: TFTP and Fget Event Messages	17-126
timep: Time Protocol Event Messages	17-133
X.25 Event Messages	17-135
xrx: XNS Router Event Messages	17-147
zmodem: Zmodem Event Messages	17-149

18 Management Information Base Variables

alarm: Alarm Information Base	18-3
at: AppleTalk Information Base	18-4
atmib: AppleTalk MIB Information Base	18-9
buf: Buffers Information Base	18-12
cct: Circuits Information Base	18-14
chassis: Chassis Information Base	18-43
config: Configuration Information Base	18-47
dev: Device Information Base	18-52

decnet: DECnet Configuration Information Base	18-53
dls: Data Link Services Information Base	18-55
drs: DECnet Circuit Group Information Base	18-58
echo: Echo Service Information Base	18-60
egp: EGP Information Base	18-61
hw: Hardware Information Base	18-63
ip: IP Information Base	18-64
ipx: IPX Information Base	18-68
isdn: ISDN (V.25 bis) Information Base	18-70
key: Key Information Base	18-74
lb: Bridge Information Base	18-75
lbmib: Bridge Address Table Information Base	18-79
log: Event Log Information Base	18-81
mem: Memory Information Base	18-82
mgr: Manager Information Base	18-83
mib: Internet MIB	18-84
name: Name Information Base	18-85
pm: Port Module Manager Information Base	18-86
proprietary: Proprietary Information Base	18-88
rok: Router Operating Kernel Information Base	18-89
snmp: SNMP Information Base	18-90
svc: System Services Information Base	18-91
tcp: TCP Information Base	18-92
telnet: Telnet Information Base	18-95
tftp: TFTP Information Base	18-97
timep: Time Protocol Information Base	18-99
timer: Timer Information Base	18-100
xrx: Xerox XNS Information Base	18-101
x25: X.25 Information Base	18-105

A Parameter Finder

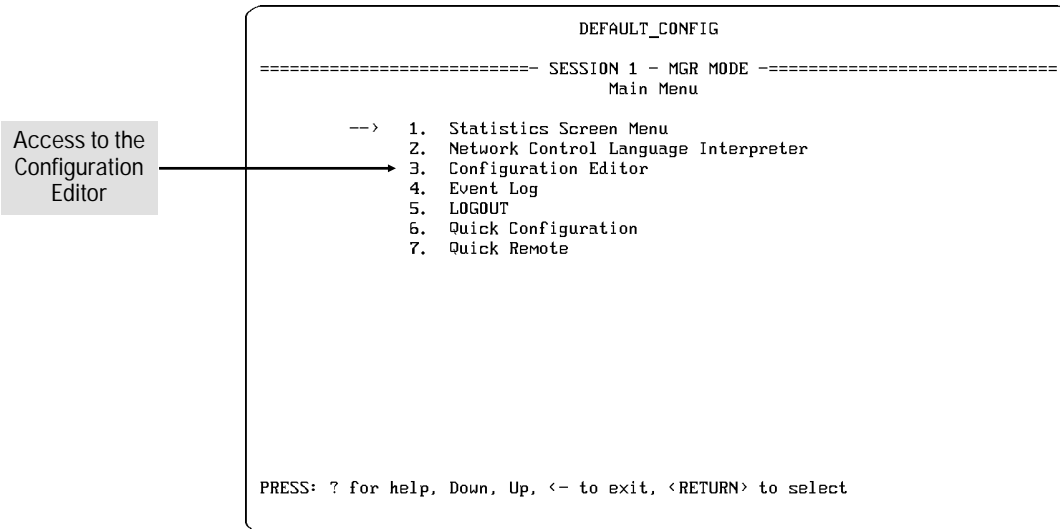
How To Use the Parameter Finder	A-2
1. System	A-4
2. Software & 3. Lines	A-5
4. Circuits	A-6
5. Circuit Groups	A-12
6. Bridge	A-13
7. DoD Internet Router	A-16
8. DECNET IV Routing Service	A-23
9. SNMP Sessions	A-25
10. Xerox Routing Service	A-26
11. IPX Routing Service	A-28
12. AppleTalk Router	A-31
13. X.25 Network Service	A-33
14. V.25 bis Network Mapping	A-35

Index

Introduction: How To Use the Dictionary of Configuration Parameters

Introduction

Part I is a dictionary reference of the Parameters found in the Configuration Editor, which is accessible from the Main menu (or by using the **[F] [M]** hot-key combination in Quick Configuration).



Accessing the Configuration Editor from the Main Menu

Part I is divided into fourteen chapters corresponding to the options listed in the Configuration menu:

```
                                DEFAULT_CONFIG
=====-- SESSION 1 - MGR MODE -----
Configuration Editor

1. System (1)
2. Software (1)
3. Lines (4)
4. Circuits (4)
5. Circuit Groups (4)
6. Bridge (1)
7. DoD Internet Router (0)
8. DECNET IV Routing Service (0)
9. SNMP Sessions (0)
10. Xerox Routing Service (0)
11. IPX Routing Service (0)
12. AppleTalk Router (0)
13. X.25 Network Service (0)
14. U.25 bis Network Mapping (0)

Enter Selection (0 for Previous Menu) : ____
```

Figure 1-1. The Configuration Menu

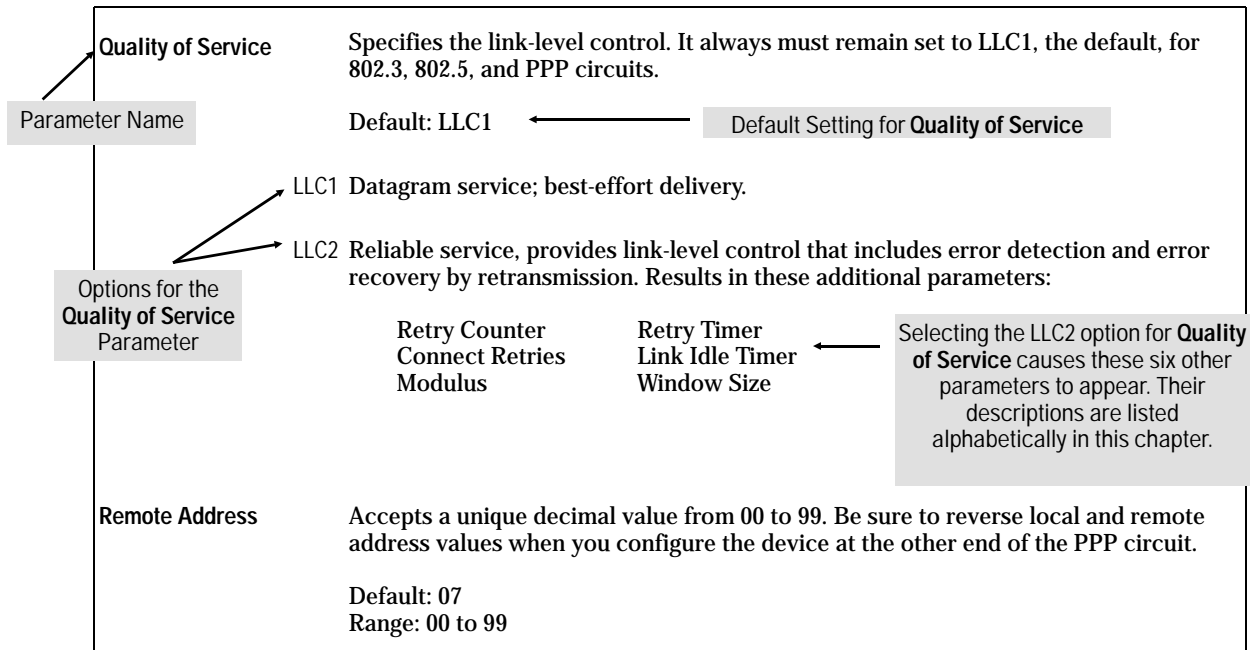
Operator's Reference

To find a parameter description, turn to the chapter corresponding to the Configuration menu option containing that parameter. Then locate the parameter by finding it in its alphabetic order. (You can also locate the parameter description by using the page/parameter listing at the beginning of each chapter.)

Within each chapter, the parameters are listed alphabetically, with descriptions of their functions and associated options. For example, the following sample of dictionary entries describes the Quality of Service and Remote Address parameters, and include:

- The parameter names
- Any applicable options for parameter settings
- A description of each parameter and each parameter option
- Any default settings

Example of Dictionary Entries in Operator's Reference



Part I

Part I

Dictionary of Configuration Parameters

Part I

Global and Session Parameters

Overview

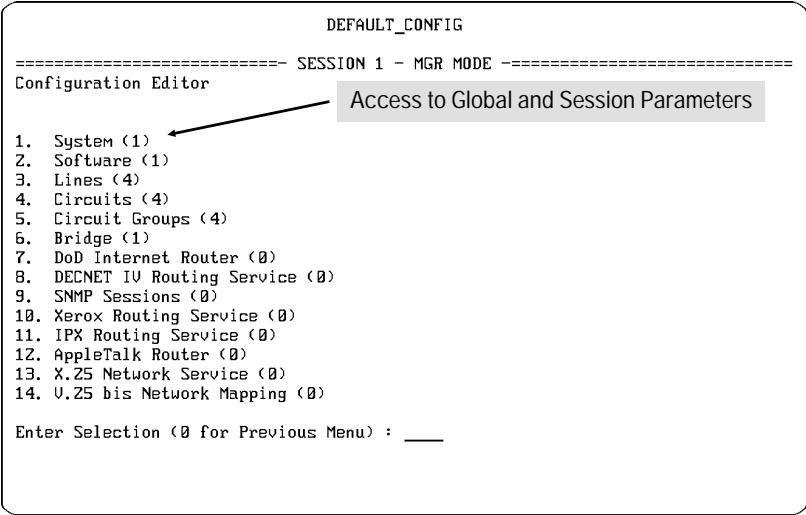


Figure 1-1. Access to Global Parameters in the Configuration Menu

Global Parameters: These specify how the router initializes its services.

Page	Global Parameters
1-4	Auto Enable
1-4	Automatic Reboot
1-5	Daylight Time Rule
1-8	Screen Refresh Rate
1-9	System Contact
1-9	System Name
1-9	System Location
1-9	Timezone

Session Parameters: Define the interface between the router and I/O devices, such as a console, modem, and Telnet.

Page	Session Parameters
1-4	Baud Rate
1-5	Bit / Char.
1-5	Connection inactivity time (min)
1-6	Event Filter Level
1-7	Flow Control
1-7	Modem connection time (sec)
1-7	Modem disconnection time (sec)
1-8	Modem lost receive ready time (msec)
1-8	Parity
1-8	Session Mode
1-8	Screen Refresh Rate
1-8	Stop Bits
1-9	Terminal
1-9	Timezone

Parameters and Options

Auto Enable		Determines whether various system services and application modules initialize automatically when the router boots.
		Default: Yes
	No	Disables all protocol-specific Auto Enable parameters for all software modules and system services. You will need to enable each service or software module with the NCL (Network Control Language Interpreter) Enable command after the router boots.
	Yes	Conditionally enables all protocol-specific Auto Enable parameters for all software modules and system services.
Automatic Reboot		Enables or disables automatic router booting after a software crash.
		Default: No
	No	Disables automatic rebooting—the router must be rebooted manually.
	Yes	Enables automatic rebooting—the router starts operation with its bridging and routing applications enabled if booting is successful. Your console screen stops at the copyright screen, displays “crash” information about the cause of the crash, and waits for you to type the customary password or any key before you can use the console.
Baud Rate		Sets the data transmission speed (baud rate) for router connect sessions initiated through the Console port.
		Default: Speed Sense
	Speed Sense	Automatically detects the baud rate of the remote terminal device and sets the router to the same baud rate.
	Other Options	300, 600, 1200, 2400, 4800, 9600, 19200, 38400
		Note: If the router is set to a fixed baud rate, the terminal device connected to the router must be set to the same baud rate.
Beginning day		Assigns a day of the week to apply the time adjustment when preparing a user-defined daylight savings time rule.
		Default: Sunday

Options: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday

Note: If `Beginning Day` is set to Sunday, the router compensates for daylight savings time at 2 a.m. on that Sunday. If `Beginning day` is not set to Sunday, the router makes the time correction at 2 a.m. on the first Sunday following the specified day.

Beginning month Assigns the month of the year to correct for daylight savings time when preparing a user-defined daylight savings time rule.

Default: April

Options January, February, March, April, May, June, July, August, September, October, November, December

Bit / Char. Sets the number of data bits in each ASCII character received or transmitted over the Console port by the router. The terminal device or remote modem connected to the Console port must be set to a matching number of data bits.

Default: 8

8 8 data bits

7 7 data bits

Connection Inactivity Time Sets the number of minutes of no activity detected on the Console port before the router terminates a communication session. When the time period elapses, the router logs off the user if a terminal device is connected to the port or sends a hang-up string if a modem is connected to the port.

Default: 0 (The router ignores inactivity on the Console port)

Options 0, 1, 5, 10, 15, 20, 30, 60, 120, 1080.

Daylight Time Rule Applies the daylight savings time rule used by the Internet RFC 868 Time protocol. If the Time protocol is enabled with IP routing and a timeserver is available, the daylight savings time correction is applied after the router is powered on or booted.

Default: None

Alaska Applies the daylight savings time rule observed in Alaska local time.

None Disables corrections for daylight savings time.

Global and Session Parameters

Parameters and Options

Canada and Continental US	Applies the daylight savings time rule observed in Canada and the continental U.S.A..										
Middle Europe and Portugal	Applies the daylight savings rule observed in middle Europe and Portugal.										
Southern Hemisphere	Applies the daylight savings time rule observed in the southern hemisphere.										
User defined	Displays a screen with four parameters for defining a custom daylight savings time rule. Use this option to define a daylight savings time rule if one of the other parameter options does not meet your requirements. For additional information, refer to "Beginning Month," "Beginning Day," "Ending Month," and "Ending Day."										
Western Europe	Applies the daylight savings rule observed in western Europe.										
Ending month	Assigns the month in which to return to standard local time when defining a custom daylight savings time rule. Default: October Options January, February, March, April, May, June, July, August, September, October, November, December										
Ending day	Assigns the day on which to return to standard local time when defining a custom daylight savings time rule. Default: Sunday Options Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday Note: If Ending day is set to Sunday, the router makes the correction at 2 a.m. on that day. If Ending day is not set to Sunday, the router makes the correction at 2 a.m. on the first Sunday after the specified day.										
Event Filter Level	Determines which event messages are automatically displayed on the console. <table><tr><td>Major</td><td>A service has appeared or disappeared.</td></tr><tr><td>Performance</td><td>A service has upgraded or degraded.</td></tr><tr><td>Warning</td><td>A service has behaved unexpectedly.</td></tr><tr><td>Information</td><td>General system information</td></tr><tr><td>Debug</td><td>Installation and diagnostic information</td></tr></table> Default: Show All Events	Major	A service has appeared or disappeared.	Performance	A service has upgraded or degraded.	Warning	A service has behaved unexpectedly.	Information	General system information	Debug	Installation and diagnostic information
Major	A service has appeared or disappeared.										
Performance	A service has upgraded or degraded.										
Warning	A service has behaved unexpectedly.										
Information	General system information										
Debug	Installation and diagnostic information										
Debug Events	Sends all event messages.										

Drop All	Sends no event messages.
Just MAJOR	Sends major event messages only.
Not INFO	Sends major, performance, and warning event messages.
PERF and MAJOR	Sends major and performance event messages.
Show All Events	Sends major, performance, warning, and information event messages.
Flow Control	<p>Enables XON/XOFF flow control and sets the type of XON/XOFF flow control for connect sessions made through the router Console port.</p> <p>XON/XOFF flow control is a software method of controlling flow control negotiation, and CTS/RTS is the hardware method of controlling flow control negotiation. The flow control negotiation method used by the remote device must match the router setting.</p> <p>Default: XON/XOFF</p>
None	Disables XON/XOFF software flow control and uses CTS/RTS hardware flow control instead.
XON/OFF	Enables XON/XOFF software flow control.
Robust XON/XOFF	Enables XON/XOFF software flow control and sends out periodic XON signals when the flow of data stops and the router expects to receive more data (checksum failure). For example, the remote connection might have dropped (lost) an XON signal sent by the router and could be waiting for the arrival of the lost signal before transmitting more data. In this case, data transmission resumes when the remote end of the connection receives the next XON signal.
Modem Connection Time	<p>Sets the number of seconds to wait for data mode and clear to send and receiver ready signals after asserting request to send and terminal ready signals.</p> <p>Default: 60</p>
Options	0, 1, 5, 10, 15, 20, 25, 30, 60, 120, 255
	Note: The router waits forever for the modem to connect when the parameter setting is 0 (zero).
Modem Disconnection Time	Sets the wait period, in seconds, for the Console port after the modem disconnects and before the modem reconnects.

Global and Session Parameters

Parameters and Options

Default: 0.5

Options 0.5, 1, 5, 10, 15, 20, 30, 60

Modem Lost Receive Ready Time Sets the number of milliseconds the receiver ready signal drops before the router disconnects the modem attached to the Console port. This is a form of debouncing the receiver ready signal.

Default: 400

Options 0, 25, 50, 100, 200, 400, 800, 1600, 2550

Note: The modem waits forever when the time period is set to 0 (zero)

Parity Assigns a value to the eighth bit of each ASCII character transmitted by the router. Match your console's requirements.

Default: None (no parity)

Options None, Even, Odd

Note: Most terminals do not operate with an odd or even parity if Bit/Char is set to 8.

Screen Refresh Rate Matches the vertical frequency rate (Hz) of the router end of the connection to the vertical frequency rate of the terminal device connected to Console port or remote modem.

Default: 3 (Hz)

Options 1, 3, 5, 10, 20, 30, 45, 60

Session Mode Toggles the Console port connection between standard User mode and Telnet mode.

Default: User

Telnet Places the Console port connection in Telnet mode.

User Places the Console port in standard User mode.

Stop Bits Specifies the number of bits following each ASCII character received or transmitted by the router. Match your console requirements.

Default: 2

Options 1, 1.5, 2

System Contact Accepts an ASCII character string identifying the person responsible for the router. For example: John Smith, Building 6.

System Location Accepts an ASCII character string identifying the physical location of the router. For example: Technology Center, Engineering Lab.

System Name Accepts a 15 character string (with no spaces) naming the router as a node in the network.

Default: DEFAULT_CONFIG

System Session Optional selection for displaying additional parameters for configuring the Console port connection. Remote users can enable this option to display the session parameters when they want to optimize the connection with the router. For example, the user might want to change the baud rate of the Console port.

Default: 0

0 Displays no parameters.

1 Displays these additional parameters:

Baud Rate	Bit/Char
Connection Inactivity Time	Event Filter
Flow Control	Modem Connection Time
Modem Disconnection Time	Modem Lost Receive Ready Time
Parity	Screen Refresh Rate
Session Mode	Stop Bits
Terminal	

Note: A smaller set of parameters are displayed if you later toggle to Telnet Session Mode.

Terminal Sets the router to match the type of terminal emulation supported by the remote device connected to the Console port.

Default: VT100

ANSI ANSI terminal emulation.

VT100 VT100 terminal emulation.

Timezone Sets the local time offset from GMT (Greenwich Mean Time) for the time protocol, which automatically sets the clock when the router boots.

Software Parameters

Overview

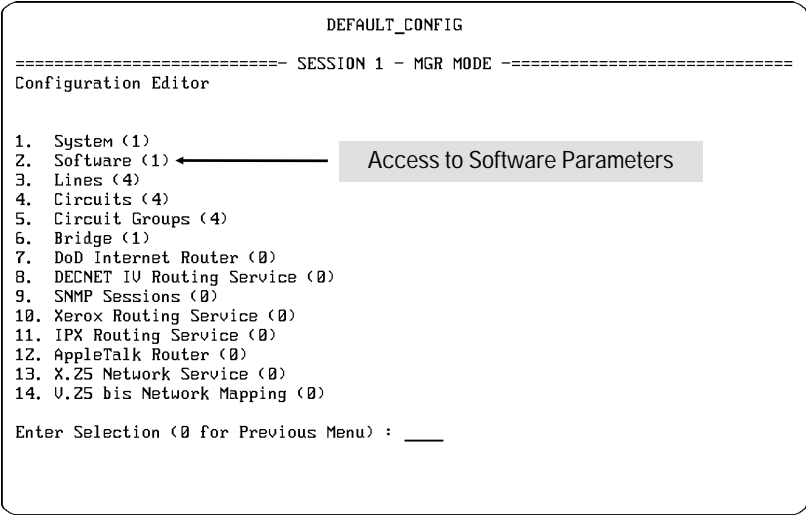


Figure 2-1. Access to Software Parameters in the Configuration Menu

Software Parameter: Enables the application modules--the bridging and specific routing services on the router. You must enable each application to be used. Any service that you enable can be used on any port.

Page	Software Parameter
2-3	Protocol

Parameters and Options

Protocol	Adds or deletes the protocol (service) you want to enable or disable on the router. Default: Bridge
Options	Bridge, DoD IP Router, DECnet Router, Xerox (XNS) Router, IPX Router, AppleTalk Router



Lines Parameters

Overview

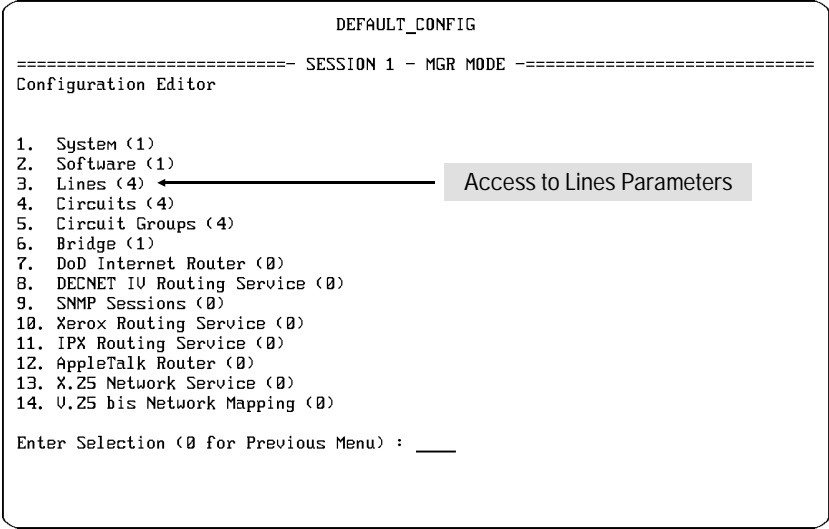


Figure 3-1. Access to Lines, Circuits, and Circuit Group Parameters

Line Parameters: Describe the physical (level 1) connections between the router and local area networks and/or long-haul transmission facilities. The lines for the ports are initially established with default attributes configured.

Page	Line Parameters
3-3	Bridge Type
3-3	Circuit Name
3-3	Clock Source
3-4	Clock Speed
3-4	Connector
3-4	Physical Access Method
3-5	Ring Interface

Parameters and Options

Bridge Type	Specifies the FDDI bridge type when FDDI is selected as the Physical Access Method. Default: Encapsulating Encapsulating Translating
Circuit Name	Identifies the circuit for the associated connector. The default startup and default Quick Configuration set this parameter to the name of the connector. This name should also appear on your network map. In HP Series 200 and 400 routers, the default circuit name includes the circuit type and related port number (1 – 4). For example: ETHER1 The first 802.3/Ethernet port configured WAN2 The second WAN port configured In HP Series 600 routers, the default circuit name also includes the number of the slot in which the associated port is installed. For example: ETHER21 The first 802.3/Ethernet port in the second slot WAN32: The second WAN port in the third slot Note: You can change a circuit name to nearly any character sequence you want, but it is recommended that you use names that identify the associated slot (if any) and port numbers for each circuit.
Clock Source	Identifies the origin of synchronous timing signals. Default: External External Select this option if an external network device supplies the timing signals over synchronous lines. In virtually all field applications, another network device supplies the timing signals. The send timing (ST) signal is looped back through the transmit timing (TT) output line. The upper range for external clocking is 2 megabits per second, and the aggregate throughput is 4 megabits per second. Internal Select this option if the router has to supply the timing signals. Some test environments do require an external clock. The internal clock signal drives the transmit timing (TT) output line. If you set Clock Source to Internal, also set the Clock Speed parameter.

Lines Parameters
Parameters and Options

Clock Speed	Sets the speed on the internal clock if the Clock Source parameter is set to Internal. Choose one of the following options: Default: 56 K (bits per second) Options 1.2 K, 2.4 K, 4.8 K, 7.2 K, 9.6 K, 19.2 K, 32 K, 38.4 K, 56 K, 64 K, 125 K, 230.4 K, 420 K, 625 K, 833 K, 1.25 M Note: The Clock Speed limit for RS-232 cables connected to the router's WAN ports is 230.4Kbps.																	
Connector	Identifies the physical port interfaced to a synchronous line. Examples of defaults: <table><tr><td>Line Type</td><td>Series 200/400 (First Port of Type)</td><td>Series 600 (First Port of Type)</td></tr><tr><td>Ethernet/802.3:</td><td>ETHER1</td><td>ETHER21 (slot 2, port 1)</td></tr><tr><td>Synchronous:</td><td>WAN1</td><td>WAN31 (slot 3, port 1)</td></tr><tr><td>Token Ring:</td><td>TOKEN1</td><td>TOKEN41 (slot 4, port 1)</td></tr><tr><td>FDDI:</td><td>FDDI1</td><td></td></tr></table> Note: The options displayed for Connector vary depending on the type of line you are configuring.			Line Type	Series 200/400 (First Port of Type)	Series 600 (First Port of Type)	Ethernet/802.3:	ETHER1	ETHER21 (slot 2, port 1)	Synchronous:	WAN1	WAN31 (slot 3, port 1)	Token Ring:	TOKEN1	TOKEN41 (slot 4, port 1)	FDDI:	FDDI1	
Line Type	Series 200/400 (First Port of Type)	Series 600 (First Port of Type)																
Ethernet/802.3:	ETHER1	ETHER21 (slot 2, port 1)																
Synchronous:	WAN1	WAN31 (slot 3, port 1)																
Token Ring:	TOKEN1	TOKEN41 (slot 4, port 1)																
FDDI:	FDDI1																	
Physical Access Method	Specifies the type of physical line connected to the indicated port (and, on HP Series 600 routers, the Slot Number). Note: Any option listed below is available, regardless of whether the router you are configuring has the corresponding port type. If the router does not have a particular port type, do not select the corresponding option. Default: CSMA/CD CSMA/CD Specifies an Ethernet/802.3 LAN port. For additional information, refer to the Connector parameter. Token Ring Specifies a Token Ring / 802.5 ring port. Results in these additional parameters: <table><tr><td>Connector</td><td>Ring Interface</td></tr></table>			Connector	Ring Interface													
Connector	Ring Interface																	

SYNC Specifies a synchronous WAN port. Results in these additional parameters:

Connector Clock Speed
Clock Source

FDDI Specifies an FDDI dual-attach port. For additional information, refer to the Bridge Type parameter.

X.25 Directs the router to use the link-level control associated with X.25. This should be set in conjunction with a circuit type of LAPB (X.25).

Ring Interface Specifies the type of token ring service when the Physical Access Method is set to Token Ring.

Default: 16 Mbps

4 Mbps

16 Mbps

16 Mbps ETR

Circuit Parameters

Overview

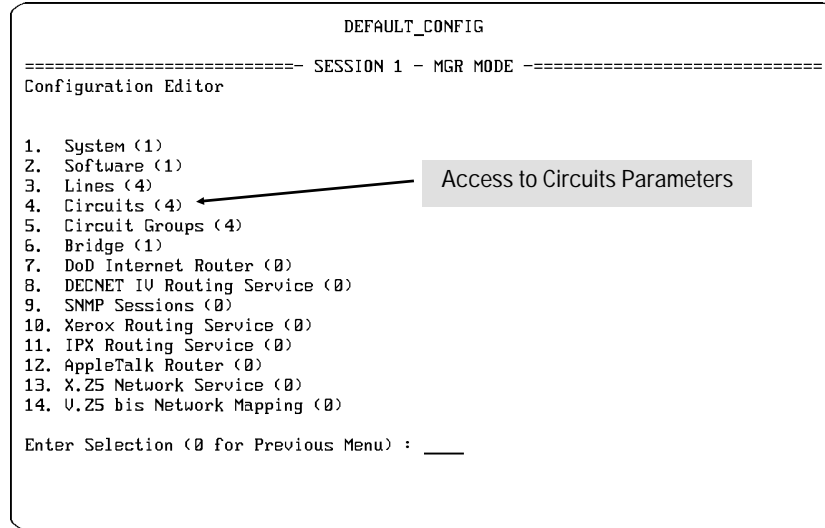


Figure 4-1. Access to Circuit Parameters

Circuit Parameters: Describe the data-link layer (level 2) transmission channels between the router and the extended network. Circuits condition the bandwidth provided by lines to provide a reliable transmission medium.

Page	Circuits Parameters
4-5	AppleTalk multicast DLCI
4-5	ARP multicast DLCI
4-5	Auto Enable
4-6	Bridge Flood multicast DLCI
4-7	Circuit Name
4-7	Circuit Type
4-10	Connect Retry
4-11	Data Link Layer protocol
4-11	DECNet multicast DLCI
4-12	Desired Link Quality
4-14	Echo Request Time (secs)
4-14	Extended (32-bit) CRC
4-15	General multicast DLCI
4-15	IP Address
4-15	LAN Address
4-17	LCP Active-Open
4-17	LCP Auto-Restart
4-17	Link Idle Timer (T3)
4-17	Local Address
4-17	Local LAN Address
4-17	LQM Time (secs)
4-20	Max Pkt Size
4-20	Min Frame Spacing (Pt to Pt Protocol--PPP)
4-21	Minimum connect duration (sec)
4-21	Minimum Frame Spacing (HP Point To Point)
4-21	Modulus
4-23	OSI multicast DLCI
4-23	Quality of Service
4-23	Point To Point Address
4-27	Remote Address
4-25	Remote LAN Address
4-25	Remote signal and sense
4-26	Retry Counter (N2)
<i>—Continued Next Page—</i>	

Circuit Parameters

Overview

Page	Circuits Parameters
<i>—Continued From Previous Page—</i>	
4-26	Retry Timer (T1)
4-28	Use UPAP
4-28	Window Size
4-29	XCVR signal polling

Parameters and Options

Adapter Record	Displays a screen with parameters for configuring a V.25bis circuit. For additional information, refer to Connect When.
Alarm Timer	<p>Sets the time interval between issuing a Status Enquiry or Full Status Enquiry message and the receipt of a Link Verification or Full Status Report from a Frame Relay DCE. The timer value must be less than or equal to the value selected for Poll Interval.</p> <p>Default: 10 Range: 5 to 30</p>
AppleTalk multicast DLCI	Refer to "Multicast Support" on page 4-22.
ARP Group Address	Accepts an IP address resolution multicast address. Enter a 10-digit decimal address to be used for IP address resolution broadcasts or leave blank if the SMDS circuit does not carry IP traffic.
ARP multicast DLCI	Refer to "Multicast Support" on page 4-22.
Auto Enable	<p>Enables or disables the initial state of the LAN circuit.</p> <p>This circuit-specific Auto Enable parameter works in conjunction with the global Auto Enable parameter found on the Global Parameters screen in the System configuration menu to enable or disable the LAN circuit when the router boots.</p> <ul style="list-style-type: none">■ When the global Auto Enable parameter is set to No, the setting of the circuit-specific Auto Enable parameter is unconditionally disabled.■ When the global Auto Enable parameter is set to Yes, the setting of the circuit-specific Auto Enable parameter determines whether the circuit is automatically enabled. <p>Default: Yes</p> <p>No Disables the circuit. (To enable the circuit after the router boots, you must use the NCL Interpreter's Enable command.)</p> <p>Yes Automatically enables the circuit if the global Auto Enable parameter is enabled.</p>

Circuit Parameters
Parameters and Options

Bandwidth Reservation Reserves percentages of the total available bandwidth on a WAN circuit for the transmission of high, normal, and low priority packets. Use this feature to prevent any one priority from taking over the entire bandwidth of a circuit.

Default: High Priority (34%)

High Priority Reserves 34% of the total available bandwidth.

Normal Priority Reserves 33% of the total available bandwidth.

Low Reserves 33% of the available total bandwidth.

Bridge Flood multicast DLCI Refer to "Multicast Support" on page 4-22.

Call restrictions Specifies which inbound phone numbers will be accepted via V.25 bis media from other routers.

Default: Allows all incoming calls.

Allow all incoming calls Accepts all incoming calls.

Allow defined inbound call number Accepts inbound calls only from the telephone numbers listed with the Allowed inbound call numbers option. If you don't want to allow any inbound calls, use this option and leave the Allowed inbound call numbers empty.

Channel Management Selects the type of channel management.

Default: Not Used

Disable Management Turns off the channel management capability in a terminal adapter with configured channel management. Use this value only when your terminal adapter has channel management capability that you don't want it to use.

Delta Management Causes a terminal adapter with channel management capability to use the maximum bandwidth allowed for channel management. Refer to the manual for your terminal adapter for more information.

Minimal Management Causes a terminal adapter with channel management capability to use a minimal portion of its channel bandwidth for channel management. Refer to the manual for your terminal adapter for more information.

Not Used Tells the terminal adapter to operate on its preprogrammed channel management parameters. (Refer to the manual for your adapter.) Use this option if your terminal adapter doesn't have v.25 bis extension features or hasn't been configured to use them.

Circuit Name Identifies the circuit for the associated connector. The default startup and default Quick Configuration set this parameter to the name of the Connector. This name should also appear on your network map. In HP Series 200 and 400 routers, the default circuit name includes the circuit type and related port number (1 -- 4). For example:

ETHER1 The first 802.3/Ethernet port configured
WAN2 The second WAN port configured

In HP Series 600 routers, the default circuit name also includes the number of the slot in which the associated port is installed. For example:

ETHER21 The first 802.3/Ethernet port in the second slot
WAN32: The second WAN port in the third slot

Note: You can change a circuit name to nearly any character sequence you want, but it is recommended that you use names that identify the associated slot (if any) and port numbers for each circuit.

Circuit Type Specifies the circuit type.

Ether/802.3 Provides a transmission channel over CSMA/CD or IEEE 802.3 Ethernet network media.

802.5 Provides a transmission channel over IEEE 802.5 Token Ring network media. Results in these additional parameters:

LAN Address Xcvr Signal Polling

FDDI Provides a transmission channel over FDDI (Fiber-Optic Data Distribution Interface) network media.

Frame Relay Provides a transmission channel over a Frame Relay network. Results in these additional parameters:

DLCI Encoding Length DLCI Encoding Type
Management Type Maximum Packet Size
Max Link Latency Provide InARP

Circuit Parameters

Parameters and Options

HP Point-to-Point Provides a transmission channel over a single long-haul medium terminated by a router peer at a remote site. Uses HDLC (High-level Data Link Control) protocol to exchange data and control packets. Displays a screen with parameters for configuring an HP Point-to-Point Protocol circuit. Results in these additional parameters:

Bandwidth Reservation	Compression
Data Link Layer Protocol	Max Link Latency
Minimum Frame Spacing	Point-to-Point Address
Remote Signal and Sense	

LAPB (X.25) Provides a transmission channel over a public or private packet-switched X.25 network. Results in these additional parameters:

Bandwidth Reservation	Max Link Latency
-----------------------	------------------

For additional information about other LAPB parameters, refer to Chapter 10, "X.25 Service Parameters."

Point-to-Point Protocol (PPP) Provides a transmission channel over synchronous (WAN) media between the router and a remote Point-to-Point peer device. The transmission channel supports the Point-to-Point Protocol service as defined in Internet Request for Comments (RFC) 1171, 1172, and 1220. Displays a screen with parameters for configuring a Point-to-Point circuit. Results in these additional parameters:

Bandwidth Reservation	Compression
Desired Link Quality	Echo Request Time (sec)
Extended (32-bit) CRC	IP Address
LCP Active-Open	LCP Auto Restart
LQM Time (sec)	Max Link Latency
Max Packet Size	Min Frame Spacing
Use UPAP	

PPP over V.25 bis Provides a transmission channel using automatic dialup and Point-to-Point over a v.25 bis circuit to a remote Point-to-Point peer device. Displays a screen with parameters for configuring a Point-to-Point over V.25 bis circuit. Results in these additional parameters:

Bandwidth Reservation	Compression
Desired Link Quality	Echo Request Time (secs)
Extended (32-bit) CRC	LCP Active-Open
LCP Auto-Restart	LQM Time (secs)
Max Link Latency	Max Pkt Size
Min Frame Spacing	IP Address
Use UPAP	

Circuit Parameters Parameters and Options

SMDS Provides a transmission channel over V.35 (synchronous media) between the router and an SMDS (Switched Multi-megabit Data Service) data service unit (DSU) or switch. Displays a screen with parameters for configuring an SMDS (Switched Multi-megabit Data Service) circuit. Results in these additional parameters:

ARP Group Address	Extended (32-bit) CRC
Group Address	Heartbeat Down Count
Heartbeat Polling Interval	Individual Address
Max Link Latency	Max Pkt Size
Min Frame Spacing	Use DXI v3.2
Use Heartbeat Poll	Use SNAP

V.25 bis Adapter Provides a transmission channel for automatic dialup over a V.25 bis circuit. Results in these additional parameters:

Adapter Record	Bandwidth Reservation
Max Link Latency	Min Frame Spacing

Compression Enables or disables packet compression to enable increased throughput over HP Point-to-Point WAN links connecting two Hewlett-Packard routers. Compression reduces or eliminates the need to move to higher-speed (and more expensive) synchronous lines. In operation, individual packets are compressed in the source router, transmitted to the destination router over the Point-to-Point circuit, and decompressed. Compression operates with the following three circuit types:

HP Point to Point
Pt to Pt Protocol (PPP)
PPP over V.25 bis

Note: To operate properly, compression must be configured on both the source and destination routers for the interconnecting circuit.

Limitations: On any HP series 200 or 400 router, there should be no more than than two WAN links running with Compression enabled.

Default:

HP Point to Point:	Auto
Pt to Pt Protocol (PPP):	No Compression
PPP over V.25 bis:	No Compression

Auto Lets the router automatically sense the compression setting used by the remote device and resets local compression accordingly.

HP PPC (Packet-by-Packet) Enables packet compression.

No Compression Disables packet compression.

Circuit Parameters

Parameters and Options

Connect inactivity time (sec) Sets a time interval, in seconds, for determining how long to incrementally maintain a connection after no activity is detected in either direction. This parameter is typically set to the incremental charge rate of the local phone system. The parameter does not become active until the Minimum connect duration (sec) parameter elapses. Thus, if you want the inactivity time to be the sole reason for disconnecting, set the a wait time period here and leave the Minimum connect duration (sec) parameter set to zero.

Default: 60

Disable: 0

Range: 10 to 64800 (seconds), or Infinity

Infinity Connection inactivity does not cause the router to terminate the call.

Other choices 0 (zero) disables the timer.

Connect Retries Determines the number of times to try to reconnect an idle LLC2 connection. After the Retry Time period elapses, the router broadcasts control messages based on the value set for the Retry Counter and waits for a response from the remote end of the circuit. If an acknowledgment is not returned, the router repeats the loop the number of times set here for Connect Retries.

Default: 0 (infinity)

Range: 0-9999

Connect retry count Sets the number of times the router tries to establish a connection if the initial call attempt fails. The range is 1 (try only once for each available phone number) to 30. For example, if you set Connect retry count to 3, the router makes up to three call attempts for each outbound phone number you provide (by cycling through the set of provided phone numbers three times). If the router is unsuccessful in establishing a connection, the internal record of connect attempts is reset to zero and an error log message is sent to the error log file.

Default: 3

Range: 1 to 30

Connect wait time(sec) Sets how long to wait after trying to make a connection (call) for the connection to be established. If the connection is not established within the specified time, the router drops DTR and retries the call. (In this case, retry means to bring the DTR line back up.) This pattern is repeated until either the router make the connection or the specified number of retries is reached.

Default: 60.

Note: If a call fails due to a "busy signal," then the next available outbound phone number (if configured) is used immediately. However, none of the phone numbers are repeated before the connect wait time expires.

Connect when	Determines when to attempt a connection with the remote router via V.25 bis. Default: Data is available or on incoming calls														
Circuit is enabled	Initiates a call attempt when the circuit is enabled (that is, either when the subject circuit is configured and the router reboots or when the subject circuit is a backup circuit that will be called when all primary circuits are down). Results in these additional parameters: <table><tr><td>Allowed Inbound Call Numbers</td><td>Call Restrictions</td></tr><tr><td>Connect Retry Count</td><td>Connect Wait Time (sec)</td></tr><tr><td>Delay after Connect Failure (min)</td><td>Local Number</td></tr><tr><td>Max Channels to Aggregate</td><td>Min Channels to Aggregate</td></tr><tr><td>Outbound Call Number</td><td>Per Channel Bandwidth</td></tr><tr><td>Send CIC on all allowed INC's</td><td></td></tr></table>	Allowed Inbound Call Numbers	Call Restrictions	Connect Retry Count	Connect Wait Time (sec)	Delay after Connect Failure (min)	Local Number	Max Channels to Aggregate	Min Channels to Aggregate	Outbound Call Number	Per Channel Bandwidth	Send CIC on all allowed INC's			
Allowed Inbound Call Numbers	Call Restrictions														
Connect Retry Count	Connect Wait Time (sec)														
Delay after Connect Failure (min)	Local Number														
Max Channels to Aggregate	Min Channels to Aggregate														
Outbound Call Number	Per Channel Bandwidth														
Send CIC on all allowed INC's															
Data is available or on incoming calls	Initiates call attempts whenever there is data to transmit or there is an incoming call from another router via V.25 bis. Results in these additional parameters: <table><tr><td>Allowed Inbound Call Numbers</td><td>Call Restrictions</td></tr><tr><td>Channel Management</td><td>Connect Inactivity Time</td></tr><tr><td>Connect Retry Count</td><td>Connect Wait Time (sec)</td></tr><tr><td>Delay after Connect Failure</td><td>Local Number</td></tr><tr><td>Max Channels to Aggregate</td><td>Min Channels to Aggregate</td></tr><tr><td>Minimum Connect Duration</td><td>Per Channel Bandwidth</td></tr><tr><td>Send CIC on Allowed INC's</td><td></td></tr></table> <p>Note: If the V.25 bis circuit is configured as a backup circuit, then the connection will not be enabled unless all primary circuits become disabled.</p>	Allowed Inbound Call Numbers	Call Restrictions	Channel Management	Connect Inactivity Time	Connect Retry Count	Connect Wait Time (sec)	Delay after Connect Failure	Local Number	Max Channels to Aggregate	Min Channels to Aggregate	Minimum Connect Duration	Per Channel Bandwidth	Send CIC on Allowed INC's	
Allowed Inbound Call Numbers	Call Restrictions														
Channel Management	Connect Inactivity Time														
Connect Retry Count	Connect Wait Time (sec)														
Delay after Connect Failure	Local Number														
Max Channels to Aggregate	Min Channels to Aggregate														
Minimum Connect Duration	Per Channel Bandwidth														
Send CIC on Allowed INC's															
Data Link Layer Protocol	Enables a standard link-layer protocol or a Wellfleet-proprietary protocol (Pass Thru). Default: Standard Standard Required for a circuit connecting to an HP remote bridge. Pass Thru Displays a screen with parameters for allowing any type of synchronous protocol (SDLC, HDLC, or LAPB) to be bridged from the pass-through circuit to a predefined destination station (MAC) address that terminates the point-to-point link. For additional information, refer to "Local LAN Address" and "Remote LAN Address."														
DECnet multicast DLCI	Refer to "Multicast Support" on page 4-22.														

Circuit Parameters

Parameters and Options

- Delay after connect failure (min)** Sets the time, in minutes, elapsing before the router attempts to make another outbound connection. This time interval comes into effect only when the router fails to establish a connection, and only after the Connect retry count has been exhausted. The parameter has no effect on a connection failing after successfully connecting.)
- Default: Retry immediately
Range: 0.1 to 30 (minutes)
Other options: DON't Retry on connect failure, Disable on connect failure
- DON't Retry on connect failure** Prevents the router from trying to open an outbound connection if the initial attempt failed. In this case, if you want the router to try again, you must use the Network Command Language (NCL) disable and denable commands to disable, then re-enable the circuit. (Even if the router will no longer try to open an outbound connection, it will still accept inbound calls.)
- Disable on connect failure** Disables the circuit when a connect failure occurs. In this case, if you want the router to try again, you must use the Network Command Language (NCL) enable command to re-enable the circuit.
- Desired Link Quality** Provides a metric for measuring circuit reliability. The link-quality-report packets exchanged by Point-to-Point peers contain counts of received and transmitted octets and packets, thus allowing both Point-to-Point implementations to monitor data loss across the link. Desired Link Quality specifies an "acceptable" percentage of data loss. The percentage is determined by dividing the constant 1 by the value for Desired Link Quality. For example, the default value, 99, specifies an acceptable loss of approximately 1% ($1/99 = .0101$).
- Default: 99
- Options** The range of Desired Link Quality parameter values along with the resulting data loss percentages are as follows:

Desired Link Quality Value	"Acceptable" Loss Percentage
1	100
2	50
4	25
5	20
10	10
20	5
50	2
100	1
200	0.5

Desired Link Quality Value	"Acceptable" Loss Percentage
250	0.4
300	0.3
500	0.2
999	0.1
0	0

DLCI Encoding Length Sets the length of the Frame Relay address field.

Default: Two Bytes

Four Bytes Sets the DLCI encoding length for four-byte extended address fields. Use this value only if your Frame Relay service supports extended four-byte address fields.

Three Bytes Sets three-byte extended address fields. Use this value only if your Frame Relay services supports extended three-byte address fields.

Three + Control Sets Q922 encoding (not yet completely standardized). While this value can be selected with the Q922 encoding type, the control field is undefined.

Two Bytes Sets the length of the address field to two bytes.

Two + Control Sets Two + Control Q922 encoding (not yet completely standardized). While this value can be selected with the Q922 encoding type, the control field is undefined.

DLCI Encoding Type Selects the DLCI encoding format.

Default: Q.922

Q921 Q.921 is a virtually obsolete method of setting a 13-bit DLCI within a two-byte address field. It drops the FECN, BECN, and DE bits from the second byte of the address field. Select DLCI encoding on the basis of the encoding format used by the attached Frame Relay DCE device.

Q922 Selects DLCI encoding as described in CCITT draft standard Q.922. This standard specifies a 10-bit DLCI. While the DLCI is most often contained within a two-byte address field, the Q.922 standard allows for three-byte and four-byte address fields. Regardless of the address field length, Q.922 encoding provides for forward explicit congestion notification (FECN), backward explicit congestion notification (BECN), discard eligibility (DE), and address field extension (EA) within the second byte of the address field.

Q922 March Defines a 11-bit DLC and drops the DE bit from the second byte of the address field.

Circuit Parameters
Parameters and Options

Q922 November	Identical to Q922 encoding except in the extended forms (three-byte and four-byte address fields). Q922 November encoding lacks a control indicator (D/C) bit in the least significant byte.
Yes	Disables the circuit when a connect failure occurs.
No	Allows the circuit to continue operating when a connect failure occurs.
Echo Request Time (sec)	<p>Sets the interval, in seconds, between the transmission of Point-to-Point echo request packets. The default time (zero seconds) disables echo requests. When PPP Echo Request Times is enabled (set to a not zero value), the router sends a Point-to-Point echo request with every packet and expects to receive a reply from the destination to confirm arrival of the packet. The link between the router and destination is considered down if the destination fails to echo a reply after five echo request times elapse. The router automatically attempts to restart the link control protocol if the link goes down and the LCP restart option is enabled.</p> <p>Default: 0 Range:</p>
Events for Error	<p>Works in conjunction with Monitored Events parameter to define a quality of service metric for the Frame Relay DCE/DTE connection.</p> <p>Default: 3 Range: 1 to 10</p> <p>The Events for Error and Monitored Events parameters work together to form a j out of k relationship for measuring circuit reliability. If the number of faulty status exchanges (Status Inquiry, Link Integrity Verification, Full Status Inquiry, and/or Full Status Report messages) in a continuous sequence of k events (Monitored Events), equals or exceeds j (Events for Error), the interface is declared down. While the connection is down, status exchanges continue. Once j consecutive status exchanges are transferred without error, the connection is restored to the active state.</p>
Extended (32-bit) CRC	<p>Determines the error detection scheme for encapsulated packets. Point-to-Point or SMDS circuits can use either a 16-bit (standard) or 32-bit (extended) encapsulation scheme and a corresponding cyclic redundancy check (CRC) to detect errors in the encapsulated packet.</p> <p>Point-to-Point Default: No SMDS Default: Yes</p> <p>Yes Enables extended 32-bit encapsulation and CRC.</p> <p>No Enables standard 16-bit encapsulation and CRC.</p>

Note: To use the 32-bit encapsulation scheme, all interfaces on the network must have sufficient memory resources to handle 32-bit encapsulation. An interface with sufficient memory resources to handle 32-bit encapsulation can unpack packets with 16-bit and 32-bit encapsulation. An interface that supports only 16-bit encapsulation cannot unpack 32-bit encapsulated packets.

General multicast DLCI	Refer to "Multicast Support" on page 4-22.
Group Address	Accepts the broadcast address for an SMDS circuit.
Heartbeat Down Count	<p>Sets the number of unacknowledged heartbeat polling messages to be consecutively counted before declaring the SMDS circuit down due to lack of communication with the DSU.</p> <p>Default: 6 (messages)</p> <p>Note: If DXI version 2.1 is selected (Use DXI v3.2 set to No), this parameter is ignored.</p>
Heartbeat Polling Interval	<p>Sets the number of seconds to wait between sending heartbeat poll messages to the DSU.</p> <p>Default: 10</p>
Individual Address	Specifies the 10-digit SMDS address. SMDS addresses mirror the North American Plan (NANP).
Intervals Between Full Polls	<p>Specifies the interval between Full Status Inquiry messages transmitted by the router to the Frame Relay network. The Full Status Inquiry messages requests the Frame Relay network to respond with a Full Status Report listing all PVCs, the PVC state (active or inactive), and whether the PVC is new or previously established.</p> <p>Default: 6</p> <p>Note: The default response (6) configures the multiprotocol router to send a Full Status Inquiry message every 6 polling intervals; that is, if the polling interval is 10, the router sends a Full Status Inquiry every 60 seconds.</p>
IP Address	Specifies the 32-bit Internet address of the Point-to-Point circuit. Enter the IP address in dotted-decimal notation.
LAN Address	Changes the station address (also called the physical or Ethernet or MAC address) for the port assigned to the circuit.

Circuit Parameters

Parameters and Options

Every HP router is shipped with a unique universally-administered 48-bit station address for each port written in read-only memory (ROM). The first 24 bits are always 080009 (hexadecimal) from Hewlett-Packard, and the second 24 bits are unique to each port on each unit manufactured by Hewlett-Packard. Because each LAN device within your network requires a unique station address, it is imperative that no other device use the same address; the address assigned in the factory guards against duplicate addresses.

The station address of each port is used by the protocol application for routing. Some of the protocols, when enabled, override the currently configured station address for some or all of the ports. DECnet sets its own single station address identically on all ports. IPX and IP host-only routing and spanning tree bridging use the currently configured station address of the WAN1 Port for all ports in the router. IP routing uses the currently configured station address of the WAN1 port.

By default, the LAN Address field on the Circuit Parameters screen is blank, which leaves the factory default unchanged. This setting is recommended.

To assign a different station address, enter it in 12-character hexadecimal format. (The user-configured address is also be ignored by some protocols, as described earlier.)

The nodes ignores the value of the LAN Address on circuits supporting the Bridge (with the spanning tree algorithm enabled). In such instances, the bridging/routing software asserts an internally generated LAN address.

If the node uses only the IP Router, or if it uses the IP Router in conjunction with the Bridge (with the spanning tree algorithm disabled), you can assigned an Ethernet address of your choosing. Because each LAN device within you network requests a unique 48-bit address, it is imperative that you guard against duplicated addresses.

Note: When assigning a user-supplied LAN address, ensure that the least significant bit of the most significant byte is clear (equal to zero). When the LAN address is transmitted their bit order is reversed. Consequently, the least significant bit of the most significant byte is transmitted first. A local one in the first bit position of a destination address designated a broadcast or multicast address.

During router operation, you can see what station address is actually being used on a circuit by entering the following NCL command:

```
get cct.circuit-name.mac_addr
```

circuit-name is the name of the circuit. The character between mac and addr is an underline character.

LCP Active-Open	<p>Determines whether Point-to-Point establishes the LCP connection.</p> <p>Note: At least one of the Point-to-Point peers must be configured to “actively” open the LCP connection.</p> <p>Default: Yes</p> <p>Yes The Point-to-Point circuit attempts to establish the LCP connection as soon as the physical link is ready.</p> <p>No The Point-to-Point circuit waits for the remote peer to establish the LCP connection.</p>
LCP Auto Restart	<p>Determines whether the Point-to-Point protocol attempts to re-establish an LCP connection after the link is declared down.</p> <p>Yes The Point-to-Point circuit attempts to re-establish an LCP connection.</p> <p>No The Point-to-Point circuit does not attempt to re-establish an LCP connection.</p>
Link Idle Timer (T3)	<p>Sets the idle time, in seconds, to wait before disconnecting the Point-to-Point circuit.</p> <p>Default: 3 (seconds)</p> <p>Range:</p>
Local Address	<p>Accepts a unique decimal value from 00 through 99 when entering an explicit Point-to-Point (non x.25) address. For more information, refer to “Point to Point Address,” and specifically, the Explicit option.</p> <p>Default: 07</p> <p>Range: 00 to 99.</p> <p>Note: Avoid the conventional address values of 01 or 03.</p>
Local LAN Address	<p>Accepts the MAC address of the source pass-thru circuit. This parameter appears when the Data Link Layer protocol parameter is set to Pass Thru.</p>
LQM Time (secs)	<p>Sets the link-quality-monitoring report period in seconds.</p> <p>Default: 0 (seconds)</p> <p>Disable: 0</p> <p>Range:</p>

Circuit Parameters

Parameters and Options

Link-quality-monitoring (a Point-to-Point initial configuration option described in RFC 1172) is the process where Point-to-Point determines the frequency and magnitude of data loss across the circuit. With link-quality-monitoring enabled, both ends of a Point-to-Point circuit can exchange Link-Quality-Report packets. These packets serve two functions. First, they provide a “keep-alive” indication to let the local end know that the remote Point-to-Point peer is operational. Second, link-quality-report packets contain a series of counters providing dynamic information on the number of octets and data-link frames received and transmitted.

- Options ■ If you do not want to enable link-quality-monitoring or if the remote Point-to-Point peer does not issue link-quality-report packets, enter 0.
- If you do want to enable link-quality-monitoring, LQM Time (secs) sets the maximum time interval (in seconds) between link-quality-report packets generated by the remote end of the Point-to-Point circuit. Failure to receive a link-quality-report packet within the expected interval indicates Point-to-Point link failure.

Note: The remote Point-to-Point peer is free to generate link-quality-report packets more rapidly than specified by the LQM Time (secs) parameter. However, it must generate packets at least as frequently as specified by LQM Time (secs).

To avoid declaring link failure in the light of a (possibly) single lost link-quality-report packet, the multiprotocol router waits until five link-quality-report periods elapse without the receipt of a link-quality-report packet before declaring the link down. For example, if LQM Time (secs) is set to a value of 3, the multiprotocol router declares the link down after a 15-second interval between the receipt of link-quality-report packets.

Upon declaring the link down, Point-to-Point closes all active network (NCP) and data-link layer (LCP) connections. If LCP Auto-Restart is set to Yes, it then attempts to re-establish the LCP connection. If LCP Auto-Restart is set to No, Point-to-Point makes no attempt to re-establish the LCP connection (thus leaving it up to the remote Point-to-Point peer to restart LCP).

Management Type

Assigns the interface management mode. The between the multiprotocol router and the Frame Relay network is generally defined by one of two commonly implemented standards. Both standards generally specify notification procedures for adding or deleting PVCs, indications of the availability or unavailability of PVCs, and verification of link integrity.

Default: ANSI Annex D

ANSI Annex D Displays a screen with parameters for specifying interface management procedures defined in Annex D to ANSI Standard T1617-1991. Results in these additional parameters:

- | | |
|----------------------------|------------------------------|
| Alarm Timer | Bandwidth Reservation |
| Events for Error | Intervals Between Full Polls |
| Monitored Events | Multicast Support |
| Permanent Virtual Circuits | Poll Interval |

LMI The Local Management Interface option displays a screen with parameters for defining a set of vendor-generated enhancements to the original Annex D procedures. Results in these additional parameters:

- | | |
|----------------------------|------------------------------|
| Alarm Timer | Bandwidth Reservation |
| Events for Error | Intervals Between Full Polls |
| Permanent Virtual Circuits | Poll Interval |
| Monitored Events | Multicast Support |

Unsupported Specifies no management interface between the multiprotocol router and the Frame Relay network. In the instance all PVCs must be manually configured.

Note: Two other parameters, Annex D Switch and LMI Switch are intended to support test/debug environments where two Hewlett Packard (or Wellfleet) multiprotocol routers are directly connected. To use these parameters, configure one router as a DTE (with ANSI Annex D or LMI specified as the Management Type) and the other router as DCE (with Annex D Switch or LMI Switch specified as the Management Type). Both options display additional parameters. For more information, refer to “Provide Update Status,” “Maximum Poll Interval (secs),” “Monitored Events,” and “Events for Error.”

Max channels to aggregate Sets the upper limit for the number of channels your terminal adapter uses to make a connection. (For further channel information, refer to the instruction manual for your terminal adapter.)

Default: Not Used

Max Link Latency (ms) (0=none) Determines how many bytes can be queued on a WAN link (expressed in milliseconds), based on the following equation:

$$bytes\ queued = \frac{latency\ (in\ ms)}{1000} \times link\ speed\ (in\ bits/sec)$$

Default: 1000 (ms)

You can use this parameter for applications that are sensitive to response time in order to avoid connection time-out periods.

Circuit Parameters

Parameters and Options

Note: Because this parameter uses the “Clock Speed” of the WAN circuit configured in the Lines configuration to calculate the maximum number of bytes queued to the WAN circuit, be sure to enter the Clock Speed accurately even when an External Clock source is used. During router boot sequence, an event is logged to show the calculated latency cap and the parameters in effect.

If Max Link Latency is set to zero (0), there is no latency limit. As packets are queued for transmission over the WAN circuit, the router counts the number of bytes in the queued packets. Before a packet is added to the queue, the router checks to make sure that the number of bytes in the packet plus the current number of bytes queued does not exceed the latency cap. If the sum exceeds the cap, the packet is dropped. When a packet is dropped, the “latency_tx” MIB variable is incremented and, on the first drop of a packet, an event is logged.

Max Pkt Size or	Determines the largest packet size handled by the Frame Relay network or the maximum size of an SMDS packet transmitted by the router or the largest packet size accepted by Point-to-Point from the peer router.
Maximum Packet Size	SMDS Default: 1547 Point-to-Point Default: 1578 Frame Relay Default: 1600
Min Channels to Aggregate	Sets the lower limit for the number of channels your terminal adapter uses to make a connection. (For further information, refer to the instruction manual for your terminal adapter).
Min Frame Spacing	Used with Pt to Pt Protocol (PPP) to determine the minimum number of eight-bit flag sequences prefixed to an HDLC packet transmitted by the router. The packet ends with a single instance of the same flag. The total number of flags transmitted between sequential packets includes the trailing flag and the variable number of leading flags. After determining the minimum number of leading flags (not including the trailing flag) needed, select the closest available value. Default: 2 Range: 2 to 62 (in increments of 2)

Minimum connect duration (sec)	<p>Sets the total time to keep the connection open even if no further data is expected. (This parameter is also disabled when you set the Connect when parameter to Circuit is enabled.)</p> <p>Default: 180 Disable: 0 Range: 0 to 64800 (seconds)</p> <p>This parameter lets you keep a line open for the minimum period that you are charged for a call. This reduces overall line charges by keeping a line open for subsequent transmissions at a lower line rate than if an initial call is terminated, then followed by another call. If a data flow interrupts a period of inactivity within the Minimum connect duration time, then the connection remains open for at least one Connect inactivity time period after the Minimum connect duration elapses (that is, after the Minimum connect duration time expires).</p>
Minimum Frame Spacing	<p>Used with the HP Point To Point circuit type to specify the minimum number of 8-bit flag sequences prefixed to an HDLC packet transmitted by the router. You can choose any even-numbered value from 2 to 62. The packet ends with a single instance of the same flag. The total number of flags transmitted between sequential packets includes the trailing flag and the variable number of leading flags.</p> <p>Default: 2 Range: Even numbers from 2 to 62</p> <p>Note: The default setting (2) is the required setting for a circuit connecting to an HP remote bridge.</p>
Modulus	<p>Specifies the length, in bits, of the HDLC packet control field. The size of the control field determines the maximum number of unacknowledged packets that may be pending at any one time. The format of the entire HDLC frame, including the control field, is illustrated in figure 4-2, below.</p> <p>Default: 8</p> <p>8 Selects an 8-bit control field, providing three bits for message sequencing and allowing for a maximum of seven unacknowledged packets.</p> <p>Note: The default of 8 is the required setting for connecting an HP Remote Bridge.</p> <p>128 Selects a 16-bit control field, providing seven bits for sequencing and allowing a maximum of 127 unacknowledged packets.</p>

Circuit Parameters

Parameters and Options

Flag	...	Flag	Address	Control	I	FCS	Flag
Key:	Flag	8-bit sequence (01111110)					
	Address	8/16 bits in length					
	Control	16 bits if Modulus is 123; 8 bits if Modulus is 8					
	I (Information)	Contains <i>n</i> bytes of data					
	FPS	16-bit or 32-bit frame check sequence					

Figure 4-2. HDLC Frame Format

Monitored Events

Works in conjunction with the Events for Error parameter to define the quality of service metric for the Frame Relay DCE/DTE connection.

Default: 4
Range: 1 to 10

The two parameters specify a *j* out of *k* relationship used to measure circuit reliability as follows. If the number of faulty status exchanges (Status Inquiry, Link Integrity Verification, Full Status Inquiry, and/or Full Status Report messages) in a continuous sequence of *k* (Monitored Events) such as events, equals or exceeds *j* (Events for Error), the interface is declared down. While the connection is down, status exchanges continue. Once *j* consecutive status exchanges are transferred without error, the connection is restored to the active state.

Multicast Support

Frame Relay multicast support lets the multiprotocol router take advantage of the multicast functionality offered (or expected to be offered) by some Frame Relay service providers. Frame Relay multicasting reserves certain network-assigned DLCIs as multicast addresses. The Frame Relay network maps multiple recipients (an address group) to this single DLCI and delivers copies of a single Frame Relay packet to each member of the address group. As the packet passes through the Frame Relay network, the DLCI is manipulated so that the packet recipient receives a DLCI indicating the actual packet source (not the multicast DLCI). Multicasting is generally used in certain address resolution techniques and for applications requiring delivery of identical information to multiple recipients. You can configure the following for multicast support:

- ARP multicast DLCI
- AppleTalk multicast DLCI
- Bridge Flood multicast DLCI
- DECnet multicast DLCI
- OSI multicast DLCI
- General multicast DLCI

OSI multicast DLCI	Refer to “Multicast Support”, above.
Password of Remote Station	Accepts the password used by the remote Point-to-Point peer when logging into the local router. Enter the password as an ASCII string of less than 16 characters.
Percent of queue reserved for high priority packets	Default: 34
Percent of queue reserved for low priority packets	Default: 33
Percent of queue reserved for normal priority packets	Default: 33
Per channel bandwidth	Sets the bandwidth (in Hz) for each channel making a connection. The total bandwidth available for a connection is a cumulative value of the Per channel bandwidth parameter setting multiplied by the number of channels. (For further bandwidth information, refer to the instruction manual with your adapter or contact your service provider.) Default: Not Used
Not Used	Ignores the per channel bandwidth.
Other Options 56K, 64K, 384K, 1536K	
Permanent Virtual Circuits	Accepts the network-assigned DLCI value, in decimal format, used in the unlikely absence of Annex D of LMI network management services. When the Management Type parameter is set to Unsupported, you must manually configure all Frame Relay Permanent Virtual Circuits (PVCs) by configuring the DLCI parameter.
Point-to-Point Address	Value used in the address field of the HDLC packet. Conventionally, one end of a HP Point-to-Point circuit is assigned an address of 03 and designated as DCE; the other end of the circuit is assigned an address of 01 and designated as DTE. Default: Auto
Auto	Allows the router to automatically sense the HP Point-to-Point address of the remote device and to set the local HP Point-to-Point address accordingly.

Circuit Parameters

Parameters and Options

Note: The remote device must be either an HP router configured as a HP Point-to-Point circuit for an HP Remote Bridge.

DCE DCE is the required choice for a circuit connecting to an HP Remote Bridge. To use this option, configure the remote device with the address "DTE".

DTE To use this option, configure the remote device with the address DCE.

Explicit Used when multiple communication channels are enabled by a common satellite link. Displays a screen with two additional parameters. For more information, refer to "Local Address" and "Remote Address."

Poll Interval (seconds) Sets the time interval between Status Inquiry messages transmitted by the router to the Frame Relay network.

Default: 10 (seconds)

Range:

The Status Inquiry message requests the Frame Relay network to respond with a Link Integrity Verification to verify the status of the DCE/DTE link.

Provide InARP Enables or disables the Inverse Address Resolution Protocol (InARP).

InARP, an extension to the Address Resolution Protocol, enables the router to resolve a given DLCI to a specific protocol address. Within the Frame Relay environment, new PVCs are announced through the exchange of signaling messages between the Frame Relay DCE and the multiprotocol router. These signaling exchanges provide an indication of the DLCI assigned to the PVC, but provide no information regarding protocol addressing (thus severely limiting the immediate utility of the PVC). InARP enables the multiprotocol router to discover the protocol address of the remote station associated with the newly-announced DLCI (as specified in RFC 1293).

Default: No

No Disables InARP

Yes Enables InARP.

Quality of Service Specifies the link-level control. It always must remain set to LLC1, the default, for 802.3, 802.5, and Point-to-Point circuits.

Default: LLC1

Auto Allows the router to automatically detect the link-level control and to set the link-level control accordingly.

LLC1 Datagram service; best-effort delivery.

LLC2 Reliable service, provides link-level control that includes error detection and error recovery by retransmission. For more information, refer to these parameters:

Retry Counter	Retry Timer
Connect Retries	Link Idle Timer
Modulus	

X.25 Directs the router to use the link-level control associated with X.25. This should be set in conjunction with a circuit type of LAPB (X.25).

Remote Address Accepts a unique decimal value from 00 to 99. Be sure to reverse local and remote address values when you configure the device at the other end of the Point-to-Point circuit.

Default: 07
Range: 00 to 99

Remote LAN Address Accepts the MAC address of the destination pass-thru circuit. This parameter appears when the Data Link Layer protocol parameter is set to Pass Thru.

Remote Signal and Sense Enables transmission of periodic messages by the router software to the remote router. The messages are sent at 10-second intervals to verify end-to-end connectivity on the circuit. This is a proprietary protocol and can be used only between HP or certain Wellfleet routers. When enabled, the port's Net Fail LED indicates the loss of connectivity even if no packets are transmitted, since the messages are sent regularly. Also, when the router is reset and nothing is connected to the port or if carrier detect is lost, the Net Fail LED turns ON and the circuit is brought down. A Warning event message is also recorded.

Default: Inactive

Inactive Disables remote signal and sense, so the loss of the connection is not detected unless LLC type 2 is enabled.

Note: Inactive is the required choice for a circuit connecting to an HP Remote Bridge (HP 28674A).

Active Enables Remote signal and sense, with the effects noted earlier. For more information, refer to "Remote signal & sense timeout (sec)." This option only works if Quality of Service is set to LLC1.

Circuit Parameters
Parameters and Options

Remote signal & sense timeout (sec) Sets the timeout range for the Remote signal & sense feature. Smaller values allow quicker detection of disabled lines and larger values reduce the amount of line bandwidth needed.

Default: 50-60
Range: 5-6 to 165-198 (seconds)

Note: For the specified circuit, set Remote signal & sense timeout (sec) to the same value in both routers connected to the circuit. Otherwise, the line between the two routers may be unintentionally disabled.

Remote Station Number Accepts the telephone number used by the terminal adapter when dialing out to reach the remote router. This number can be up to 20 digits long, depending upon your terminal adapter. You may also be able to include some or all of the following symbols in the number string:

: < < = > > P T &

If you leave this field blank, the router operates as a V.25 bis receive-only unit.

Retry Counter (N2) Determines the number of possible retransmissions of the same frame after the Retry Timer (T1) interval elapses.

Default: 16 (seconds)

Retry Timer (T1) Sets the time interval, in seconds, between issuing a command and receiving an acknowledgment. In the absence of an acknowledgment, the router retransmits the command when the T1 Timer elapses.

Default: 3

Note: This default is the recommended setting for the HP Remote Bridge connection. The bridge and HP router should have the same setting.

Send CIC on all allowed INC's Controls whether to send a "connect incoming call" (CIC) command in response to any incoming call indication. Set this parameter to Yes only if your adapter requires a CIC command.

Default: No

Yes Enables the transmission of a CIC command.

No Disables the transmission of a CIC command.

Here are the required CIC settings for some V.25 bis devices:

Device	Required CIC Setting
Ascend Multiband Adapters	Yes or No
General Datacom 914 ADR	Yes
Hitachi ISDN Adapter	No
Motorola DU170	Yes
NEC ISDN	No
Northern Telecom NT4X25AG	Yes, if device not set for auto answer

Server Password	Assigns the password used by the router when it logs in to the remote Point-to-Point peer. Enter the password as an ASCII string of less than 16 characters.
Server User ID	Assigns the name (user ID) used by the router when logging into the remote Point-to-Point peer. Enter the name as an ASCII string of less than 16 characters.
Slot Number	Identifies the slot in which the port corresponding to the specified Physical Access Method is installed. (Applies only to ports on interface modules installed in an HP Series 600 router. Range: 2 - 5
Subaddress	Accepts a subaddress extension used at the remote site to access the remote router. Leave this field blank if a subaddress is not required. This field can accept up to 40 digits, but the actual number of characters you enter could be limited to your terminal's capabilities. Use only numeric symbols in the subaddress.
Use DXI v3.2	Selects which version of the Data eXchange Interface (DXI) to use Default: No No Selects DXI Version 2.1. Yes Enables DXI Version 3.2.
Use Heartbeat Poll	DXI specifies the interface between the multiprotocol router and a DSU/CSU. DXI version 3.2 includes a "heartbeat polling" mechanism to verify the line from the router to the DSU. Heartbeat polling is implemented by sending a short message on a regular interval to the DSU and verifying that the DSU responds with an acknowledgment. Heartbeat polling does not check the status of the trunk line connected to the DSU. If DXI version 2.1 is selected (Use DXI v3.2 set to No), this parameter is ignored. Default: No

Circuit Parameters
Parameters and Options

No Disables heartbeat polling.

Yes Enables heartbeat polling.

Use SNAP

Identifies the version of IEEE 802.6 to be used.

Default: Yes

Yes Enables the approved version of IEEE 802.6 (D15). With 802.6 (D15), encapsulation as specified by Internet RFC 1209, IP Over SMDS.

No Enables IEEE version(s) D9 and D11. With IEE 802.6 (D9/D11), an At&T proprietary encapsulation is used.

Use UPAP

Enables the User Password Authentication protocol (UPAP). Point-to-Point implementations can require a remote peer to authenticate itself before engaging in NCP negotiation. For more information, refer to the RFC 1172 specification.

Default: No

No Disables UPAP.

Yes Enables UPAP.

User ID of Remote Station

Accepts the name (user ID) used by the remote Point-to-Point peer when logging into the local router. Enter the name as an ASCII string of less than 16 characters

Window Size

Used with HP Point To Point circuits to specify an exact number of packets that may be unacknowledged at any one time. Modulus specifies a maximum number of unacknowledged packets. This toggle option offers different choices for different current settings of Modulus. The options are:

Modulus Setting	Windows Size Options
8	7, 1, or 3
128	1,3,7,15, 31, 63, 127

Xcvr Signal Polling

Enables the transmission of periodic self-addressed messages by the router software. Messages are sent at 5-second intervals to verify proper transceiver operation on the LAN port. When signal polling is enabled, the port's Net Fail LED indicates the loss of the transceiver connection even if no packets are being transmitted, since the signal polling messages are sent regularly. Also, when the router is reset and nothing is connected to the port, the Netfail LED turns ON. An event message with the severity level of the warning is also recorded.

Default: Inactive

Yes Enables the transmission of periodic self-addressed messages.

No Disables the transmission of periodic self-addressed messages.

Circuit Group Parameters

Overview

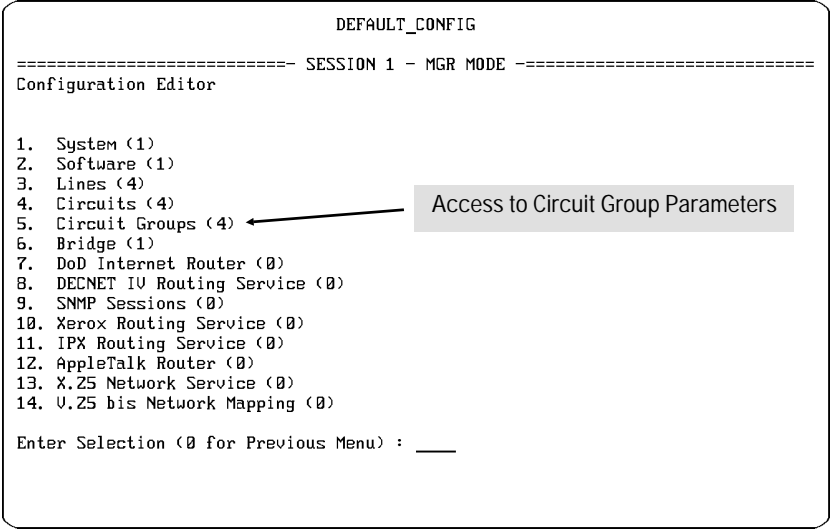


Figure 5-1. Access to Circuit Parameters

Circuit Group Parameters: Complete the communication channels between multiprotocol routers and network devices by forming collections of circuits used by the application modules to bridge and route packets. A circuit group comprises circuits of the same type (such as LAN, WAN, and Frame Relay) that originate at a common point and terminate at another common point. Each individual circuit must be assigned to a circuit group, even if the group consists of only one circuit.

Page	Circuits Parameters
5-3	Circuit Group Name
5-3	Circuit Group Speed
5-3	Circuit Name

Parameters and Options

Circuit Group Name	Accepts a maximum of 12 alphanumeric characters to identify the circuit group.
ETHER1G	The default when configuring an Ethernet LAN port.
WAN1G	The default when configuring a WAN port.
Circuit Group Speed	Used for WAN ports to enable the setting of the MIB interface (“if”) Speed entry in the “if” table by providing this value in response to SNMP “gets” requesting the “if” speed setting. Default: 56000
Circuit Name	Identifies the circuit for the associated connector. The default startup and default Quick Configuration set this parameter to the name of the Connector. This name should also appear on your network map. In HP Series 200 and 400 routers, the default circuit name includes the circuit type and related port number (1 -- 4). For example: ETHER1 The first 802.3/Ethernet port configured WAN2 The second WAN port configured In HP Series 600 routers, the default circuit name also includes the number of the slot in which the associated port is installed. For example: ETHER21 The first 802.3/Ethernet port in the second slot WAN32: The second WAN port in the third slot Note: You can change a circuit name to nearly any character sequence you want, but it is recommended that you use names that identify the associated slot (if any) and port numbers for each circuit.

Bridge Parameters

Overview

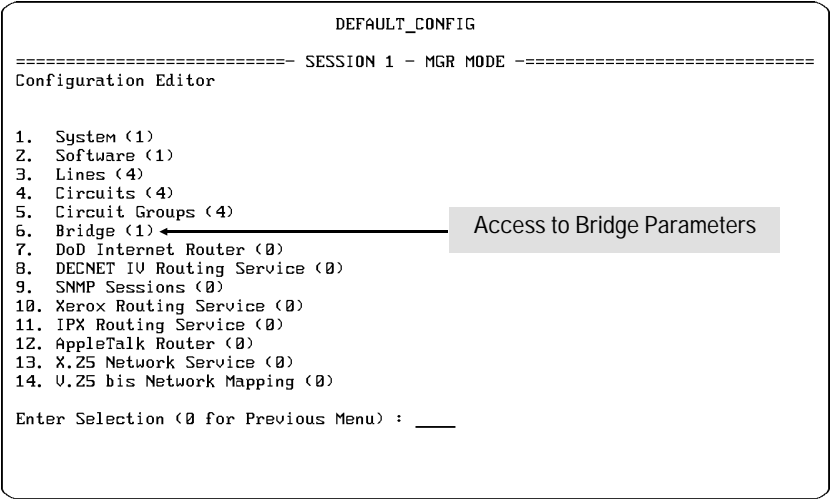


Figure 6-1. Access to Bridge Parameters

Bridge Parameters: Describe the means for filtering and relaying frames at the data-link layer between network and/or point-to-point connections using station (MAC, or Media Access Control) addressing.

Page	Bridge Parameters
6-5	Action
6-5	Aging Timer (min)
6-5	Auto Enable
6-6	Block STE
6-6	Bridge ID (hex)
6-7	Circuit Group Name
6-7	Circuit Name
6-7	Cost
6-7	Default Conversion Type
—Continued Next Page—	

Page	Bridge Parameters
<i>—Continued From Previous Page—</i>	
6-7	Default Conversion Type
6-7	DL Format
6-8	DSAP (high)
6-8	DSAP (low)
6-9	Effect
6-9	Ethernet Type (high)
6-10	Ethernet Type (low)
6-10	Flood Interval (sec)
6-10	Forward Delay
6-11	Forwarding Table Size
6-11	Group LAN ID
6-11	Header
6-12	Hello Time
6-12	High Value (hex)
6-12	Hop Count Reduction
6-12	Internal LAN ID (Hex)
6-13	LAN ID (Hex)
6-13	Length
6-13	List Name
6-13	Loop Detection Time (Hex)
6-13	Low Value (hex)
6-14	MAC Address (high)
6-14	MAC Address (low)
6-14	MAC dest (high)
6-15	MAC dest (low)
6-15	MAC source (high)
6-15	MAC source (low)
6-16	Max Age
6-16	Max Hops
6-16	Offset
6-17	Precedence
6-17	Priority
6-17	Protocol ID/Org. Code (high)
6-17	Protocol ID/Org. Code (low)
<i>—Continued Next Page—</i>	

Bridge Parameters

Overview

Page	Bridge Parameters
<i>—Continued From Previous Page—</i>	
6-18	Protocol Type
6-18	SAP (high)
6-18	SAP (low)
6-18	Set Hop Count Reduction
6-19	Spanning Tree Enable
6-20	Src Rte
6-20	SSAP (high)
6-20	SSAP (low)
6-21	STP Priority
6-21	Table Age Interval
6-22	Traffic Priority
6-22	Transitional Bridge
6-22	Type (high)
6-23	Type (low)

Parameters and Options

Action	<p>Determines the disposition of frames meeting the filter rule.</p> <p>Default: Drop</p> <p>Drop Discards a frame meeting the filter rule.</p> <p>Accept Relays a frame meeting the filter rule.</p> <p>High Priority Assigns the first priority to all incoming bridged packets from the LAN circuit meeting the filter rule. This gives packets a higher priority than bridged and routed packets not meeting the filter rule. To select this option, the Traffic Priority parameter must be set to Normal.</p> <p>Low Priority Assigns last priority to all incoming bridged packets meeting the filter rule. This gives packets a lower priority than any bridged and routed packets from the LAN circuit not meeting the filter rule.</p>
Aging Timer (min)	<p>Sets a time interval, in minutes, for aging the source route (SR) entries in a forwarding table.</p> <p>Default: 5 (minutes) Disable: 0</p> <p>The Aging Timer controls how frequently the source route entries are checked for removal from the bridge forwarding table. Each time a frame is forwarded to a station, its entry in this table is time-stamped. If the entry is not accessed for a time period equaling twice this time, the entry is removed from the table. A value of zero disables the timer and aging is no longer performed.</p> <p>Any source-routing station that is moved from one ring to another must be timed-out before it can again communicate via TRNSB. In most cases, the default (5 minutes) is sufficient. A shorter duration can cause non-functional stations to be removed more quickly, but impacts performance.</p>
Auto Enable	<p>Determines the initial state of the bridge. The bridge-specific Auto Enable parameter works in conjunction with the global Auto Enable parameter to enable or disable the bridge application software when the node boots based on the following criteria.</p>

Bridge Parameters

Parameters and Options

- When the global Auto Enable parameter is set to No, the bridge (as are all other application software modules) is unconditionally disabled. The bridge-specific Auto Enable parameter is disabled when the global Auto Enable parameter is disabled.
- When the global Auto Enable parameter is set to Yes, the bridge (as are all other application software modules) is conditionally enabled. The bridge-specific Auto Enable parameter can be set to enable or disable the bridge.

Default: Yes

No Disables the bridge-specific Auto Enable parameter if the global Auto Enable parameter is enabled. If you choose No, you will subsequently need to enable the bridge manually with the NCL Interpreter after the node boots.

Yes Enables the bridge-specific Auto Enable parameter if the global Auto Enable parameter is also enabled.

Note: Select an applicable value for the bridge-specific Auto Enable parameter regardless of the global Auto Enable parameter setting. If the global Auto Enable parameter is later enabled, the option selected for the bridge-specific Auto Enable parameter takes effect.

Block STE

Determines whether the bridge should drop single-route explorer frames received on the circuit group. Note that this option does not stop single route explorer frames from being transmitted on the circuit group.

Default: No

No Disables Block STE.

Yes Enables Block STE.

Bridge ID (Hex)

Enables source routing. In the initial Bridge screen, identifies a specific source route bridge. If your network does not include parallel source-routing bridges, this is the only instance you should enter. But if your network includes parallel source routing bridges, then you will need to configure a second Bridge ID (Hex) entry under the "Source Route Bridge IDs" menu item. (The second entry specifies a second HP bridge configured in parallel with the bridge you are currently configuring as a source routing bridge.) Both instances of this parameter use a value between 1 and F (hexadecimal). Leave this field blank if you do not want to enable source routing.

Default: 1

Disable: Leave Blank

Range: 1 to F (hexadecimal)

Note: Parallel source routing bridges require unique Bridge ID (hex) values. Non-parallel bridges do not need unique identifiers.

Circuit Group Name	Identifies the circuit group connecting the bridge and the attached LAN or network device. Enter the name of the circuit group providing the connection.																				
Circuit Name	Identifies the circuit (not the circuit group) carrying the traffic specified by Protocol Type.																				
Cost	<p>Assigns a relative cost value to the circuit group. Cost is meaningful only if you have enabled the spanning tree algorithm. Move to the next field to accept the default value (100) if the spanning tree algorithm is not enabled. Cost reflects the relative speed of the media—lower costs are for high-speed media and higher costs are for low-speed media. Use Cost to direct network traffic to higher-speed media. There are 14 options for Cost:</p> <p>Default: 100</p> <table><tr><td>Options</td><td>100</td><td>1</td><td>40</td><td>80</td></tr><tr><td></td><td>250</td><td>10</td><td>50</td><td>90</td></tr><tr><td></td><td>500</td><td>30</td><td>70</td><td></td></tr><tr><td></td><td>65535</td><td>30</td><td>70</td><td></td></tr></table>	Options	100	1	40	80		250	10	50	90		500	30	70			65535	30	70	
Options	100	1	40	80																	
	250	10	50	90																	
	500	30	70																		
	65535	30	70																		
Default Conversion Type	<p>Assigns the default frame type for conversion. This parameter determines whether the TRNSB converts frames to 802.3 or the Ethernet V2 format. (This rule is altered for any stations configured in the Alternate Conversion list). Configure the frame type used by most (if not all) stations on your 802.3/Ethernet LAN.</p> <p>Default: 802.3</p> <p>802.3 Sets the conversion type to 802.3.</p> <p>Ethernet V2 Sets the conversion type to Ethernet V2.</p>																				
DL Format	<p>Enables the construction of more complex filters combining MAC-level source and destination address filtering with protocol-specific filtering.</p> <p>Default: MAC only</p> <p>MAC only Prepares MAC-level source and destination filters. MAC-level source and destination filters drop or forward a frame based of its source and destination addresses. MAC-level filters can filter source addresses only, destination addresses only, or some specified combination of source and destination addresses. You can construct MAC-level source and/or destination filters for any of the four supported encapsulation methods—Ethernet, 802.2 LLC, 802.2 SNAP, or Novell.</p>																				

Bridge Parameters

Parameters and Options

Ethernet Prepares Ethernet filters. Ethernet filters drop a frame on the basis of its Ethernet type. Ethernet filters filter Ethernet type values only, or some specified combination of Ethernet type values in conjunction with MAC-level source and destination addresses.

802.2 LLC Prepares of 802.2 LLC filters. 802.2 LLC filters drop or forward a frame on the basis of its destination and/or source service access points. 802.2 LLC filters filter only source service access points (SSAP), only destination service access points (DSAP), some combination of SSAP and DSAP values, or some specified combination of SSAP/DSAP values in conjunction with MAC-level source and destination addresses.

802.2 SNAP Prepares of 802.2 SNAP filters. 802.2 SNAP filters drop or forward a frame based on the protocol or Ethernet type. 802.2 SNAP filters filter only protocol ID values, only Ethernet values, some combination of protocol ID and Ethernet type values, or some specified combination of protocol ID/Ethernet type values in conjunction with MAC-level source and destination addresses.

Novell Prepares Novell filters. Novell filters drop or forward Novell frames. As an option, you can construct filters to examine Novell-encapsulated frames in conjunction with MAC-level source and destination addresses.

DSAP (high) Sets the upper boundary of the range for filtering 802.2 LLC packets based on the contents of its destination service access point (DSAP) field.

- Options**
- Leave this field blank if you do not want to filter destination service access points.
 - Leave this field blank and enter a DSAP in the DSAP (low) field if you are filtering a single destination service access point.
 - Enter the highest DSAP in the range if you are filtering a range of destination service access points.
 - Leave this field blank and enter the name of the SAP list in the DSAP (low) field if you are establishing a range of destination service access points with a filter list.

For more information, refer to “DSAP (low).” To learn how to create a SAP list, refer to “SAP (low)” and “SAP (high).”

DSAP (low) Sets the lower boundary of the range for filtering 802.2 LLC packets based on the contents of its destination service access point (DSAP) field.

- Options**
- Leave this field blank if you do not want to filter destination service access points.
 - Enter a DSAP in this field if you are filtering a single destination access point.

- Enter a the lowest DSAP in this field and the highest DSAP in the DSAP (high) field if you are filtering a range of destination service access points.
- Enter the name of a SAP list in this field and leave the DSAP (high) field blank if you are establishing a range of destination service access points with a filter list.

For more information, refer to “DSAP (high)”. To learn how to create a SAP list, refer to “SAP (low)” and “SAP (high)” later in this chapter.

Effect

Determines whether frames are dropped or relayed (filtered) based on the contents of a frame field and a range established by a matching set of (low) and (high) filter parameters. The frame field and corresponding (low) and (high) filter parameters are listed in the following table:)

Frame Field	Bridge Parameter
DSAP	DSAP (low) and DSAP () high)
Ethertype	Ethertype (low) and Ethertype (high)
Protocol ID/Org.	
Code	Protocol ID/Org. Code (low) and (high)
MAC dest	MAC dest (low) and MAC dest (high)
MAC source	MAC source (low) and MAC source (high)
SSAP	SSAP (low) and SSAP (high)
Type	Type (low) and Type (high)

Default: Ignore

- Don't Match Applies the filtering action (drop/accept/log) if the contents of the frame field do not fall within the range established by the matching (low) and (high) filter parameters.
- Ignore Applies no filtering action if the contents of the frame field falls within the range established by the matching (low) and (high) parameters.
- Match Applies the filtering action (drop/accept/log) if the contents of the frame field falls within the range established by the matching (low) and (high) filter parameters.

Ethernet Type (high)

Sets the upper boundary of the range for filtering a Ethernet frame based on the contents of its Ethernet Type field.

- Options
- Leave this field blank if you do not want to filter and Ethernet frame based on the contents of its Ethernet Type field.
 - Leave this field blank and enter the Ethernet Type in the Ethernet Type (low) field if you are filtering a single Ethernet Type.

Bridge Parameters

Parameters and Options

- Enter the highest Ethernet Type in the range if you are filtering a range of Ethernet Types.
- Leave this field blank and enter the name of a Ethernet Type list if you want to establish the range of Ethernet Types using a filter list.

For more information, refer to “Ethernet Type (low)” later in this chapter. To learn how to create an Ethernet Type filter list, refer to “Type (low)” and “Type (high)” later in this chapter.

Ethernet Type (low) Sets the lower boundary of the range for filtering a frame based on the contents of its Ethernet Type field.

- Options
- Leave this field blank if you do not want to filter an Ethernet frame based on the contents of its Ethernet Type field.
 - Enter the Ethernet Type in this field and leave the Ethernet Type (high) field blank if you are filtering a single Ethernet Type.
 - Enter the lowest Ethernet Type in this field and enter the highest Ethernet Type in the Ethernet Type (high) field if you are filtering a range of Ethernet Types.
 - Enter the name of an Ethernet Type list in this field blank and end leave the Ethernet Type (high) field blank if you want to establish the range of Ethernet Types using a filter list.

For more information, refer to “Ethernet Type (high)” earlier in this chapter. To learn how to create a Ethernet Type filter list, refer to “Type (low)” and “Type (high)” later in this chapter.

Flood Interval (sec) Sets the time interval in seconds during which (at most) a single frame will be flooded to an unlearned address.

Default: 0 (disables flood limiting)

Forward Delay Sets the time interval spent by a circuit group when in the Listening and Learning states. Setting Forward Delay to the minimum value causes the spanning tree to converge at its fastest rate.

Default: 15
Range: 4 to 30

- Options
- Skip this field if the spanning tree algorithm is disabled.
 - Use the Forward Delay parameter to set a timer value for timing a circuit group as it moves from state to state if the spanning tree algorithm is enabled.

As the algorithm operates, it eventually places all circuit groups in either a forwarding (enabled) or blocking (disabled) state. Later, in response to network topology changes, the algorithm can change the state of specific circuit groups. In order to prevent network looping caused by sudden state changes, the algorithm does not transition circuit groups directly from Blocking to Forwarding. Rather, it places them in two intermediate states—the Listening and Learning state.

While in the Listening (stand-by) state, the circuit group receives network-generated BPDUs, but does not receive end-station-generated message traffic. When the) Forward Delay timer expires, the circuit group is placed in the Learning state. While in Learning state, the circuit group receives network-generated BPDUs, and also receives end-station-generated traffic which is subjected to the learning process but not relayed. When the Forward Delay timer expires, the circuit group is placed in the Forwarding state.

Forwarding Table Size

Specifies the maximum size of the forwarding table.

The forwarding table contains the list of end-station addresses learned by the bridge, plus all source-address filters and destination-address filters. The value that you enter at Forwarding Table Size sets the maximum size of this table.

Default: 1024

Options 0, 64, 512, 1024, 2048, 4096, and 8192

For more discussion on Forwarding Table Size, refer to “Spanning Tree Enable” on page 6-19

Group LAN ID

Accepts the group LAN ID used by the bridge when transmitting SRFs (Specifically Routed Frames) between HP bridges. Together with the other routing designators, Group LAN ID helps intermediate bridges identify the destination end station. The group ID must match the Group LAN ID assigned to all HP bridges running software release 5.74, and differ from all Internal LAN ID (Hex) values and external LAN ID values assigned to any bridges on the network.

Default: 1

Range: 1 to fff.

Header

Used to position the filtered bit pattern within the incoming frame when creating a user-defined filter.

Default: MAC

MAC Find and position the filtered bit patterns within the MAC-level header of the incoming frame.

Data Link Find the pattern within the data-link header of the incoming frame.

Bridge Parameters
Parameters and Options

Hello Time	<p>Sets the time interval in seconds between BPDUs transmitted by the bridge.</p> <p>Default: 2 (seconds) Range: 1 to 10</p> <p>Options</p> <ul style="list-style-type: none">▪ Skip this field if the spanning tree algorithm is not enabled.▪ Enter the Hello Time in seconds. If the spanning tree algorithm is enabled, Hello Time sets the time interval between BPDUs. BPDUs are periodic, formatted transmissions exchanged between bridges in the extended network. They convey configuration and topology change data.
High Value (hex)	<p>Sets the upper boundary of the range for filtering a frame based on a user-defined bit pattern (hexadecimal value) within the MAC or data-link header.</p> <p>Options</p> <ul style="list-style-type: none">▪ If you are filtering a single MAC or data-link header, leave this field blank and enter the MAC or data-link header in the Low Value (hex) field.▪ If you are filtering a range of MAC or data-link headers, enter the highest MAC or data-link header in the range. <p>For more information, refer to “Low Value (hex).”</p>
Hop Count Reduction	<p>Determines whether to limit the bridge hop count to seven hops or to provide infinite hop capability.</p> <p>Default: No</p> <p>Yes Enables infinite hop capability between the source-routing source and destination.</p> <p>No Allows a maximum of seven hops between the source-routing source and destination.</p>
Internal LAN ID (Hex)	<p>Assigns a numeric identifier to the bridge. The bridge uses the identifier when constructing routing designators.</p> <p>Default: 1 Disable: Leave blank Range: 0 to FFF (hexadecimal)</p> <p>Options</p> <ul style="list-style-type: none">▪ Enter a value from 0 to FFF (hexadecimal) to enable global source routing.▪ Leave this field blank to disable source routing. <p>Note: The internal LAN ID must always be network-unique.</p>

LAN ID (Hex)	<p>Sets the LAN ID of a particular interface. You must assign a unique LAN ID to each bridge interface that uses source routing (including non-token ring interfaces).</p> <p>Default: 1 Disable: Leave blank Range: 0 to fff (hexadecimal)</p> <p>Options ■ Leave this field blank if you don't want to enable source routing.</p> <p>■ Enable source routing by entering a value between 0 and FFF (hexadecimal).</p> <p>Note: You must enter LAN ID in hexadecimal format for each node running Release 5.70 software or later. All nodes on a token ring must have equivalent LAN IDs.</p>
Learning Bridge	<p>Enables the bridging service in the router to automatically learn the addresses of the nodes communicating through the service and on which side of the bridge each node is located. The bridge learns the node addresses from the source address field in each packet it receives. It learns which side the node is on by noting which port receives the packet. The bridge adds entries to the bridge address table for each new address it sees.</p> <p>Default: Yes</p> <p>Yes Enables automatic learning of the source address and location from which bridged packets are received.</p> <p>No Disables Learning Bridge operation.</p>
Length	Sets the length of the bit pattern of a filtered field when creating a user-defined filter.
List Name	Accepts the name of a MAC address list, Ethernet Type list, SAP list, or Protocol ID/Organization Code list.
Loop Detection Time (Hex)	<p>Time period for detecting a loop in the network. When the bridge receives an all-routes explorer packet (ARE) for a particular source-destination pair, a time stamp is stored in the appropriate entry in the Source Routing Intermediate Station table. If the bridge receives another ARE for the same source destination pair before the loop loop detection timer expires, a loop exists in the network and the bridge drops the packet to reduce the hop count.</p> <p>Default: 1000 (ms)</p>
Low Value (hex)	Sets the lower boundary of the range for filtering a frame based on a user-defined bit pattern (hexadecimal value) within the MAC or data-link header.

Bridge Parameters

Parameters and Options

- Options ■ If you are filtering a single MAC or data-link header, enter the MAC or data-link header in this field and leave the High Value (hex) field blank.
- If you are filtering a range of MAC or data-link headers, enter the lowest MAC or data-link header in this field and enter highest MAC or data-link header in the High Value (hex) field.

For additional information, refer to “High Value (hex)”.

MAC Address (high) Sets the upper boundary of the MAC address range when creating a MAC Address list.

- Options ■ If you are filtering a single MAC address, leave this field blank and enter the address in the MAC Address (low) field.
- If you are filtering a range of MAC addresses, enter the highest MAC address in the range.

For more information, refer to “MAC Address (low).” To learn how to apply a MAC Address list to a filter, refer to “MAC dest (low)” and “MAC source (low).”

MAC Address (low) Sets the lower boundary of the MAC address range when creating a MAC Address list.

- Options ■ If you are filtering a single MAC address, enter the MAC address in this field and leave the MAC Address (high) field blank.
- If you are filtering a range of MAC addresses, enter the lowest MAC address in this field and enter the highest MAC address in the MAC Address (high) field.

For more information, refer to “MAC Address (low).” To learn how to apply a MAC Address list to a filter, refer to “MAC dest (low)” and “MAC source (low).”

MAC dest (high) Sets the upper boundary of the range for filtering a frame based on the contents of its MAC-level destination address field.

- Options ■ Leave this field blank if you do not want to filter MAC destination addresses.
- Leave this field blank and enter the destination address in the MAC dest (low) field if you are filtering a single MAC destination address.
- Enter the highest MAC destination address in the range if you are filtering a range of MAC destination addresses.
- Leave this field blank and enter the name of the MAC Address list in the MAC dest (low) field if you are establishing a range of MAC destination addresses with a MAC Address list.

For more information, refer to “MAC dest (low).” To learn how to create a MAC Address list, refer to “MAC Address (low)” and “MAC Address (high).”

MAC dest (low)

Sets the lower boundary of the range for filtering a frame based on the contents of its MAC-level destination address field.

- Options
- Leave this field blank if you do not want to filter a frame based on its MAC destination address.
 - Enter the destination address in this field and leave the MAC dest (high) field blank if you are filtering a single MAC destination address.
 - Enter the lowest MAC destination address in this field and enter the highest MAC destination address in the MAC dest (high) field if you are filtering a range of MAC destination addresses.
 - Enter the name of a MAC Address list in this field if you are establishing the range of MAC destination addresses with a filter list.

For more information, refer to “MAC dest (high).” To learn how to create a MAC Address list, refer to “MAC Address (low)” and “MAC Address (high).”

MAC source (high)

Sets the upper boundary of the range for filtering a frame based on the contents of its MAC-level source address field.

- Options
- Leave this field blank if you do not want to filter a frame based on its MAC source address.
 - Leave this field blank and enter the source address in the MAC source (low) field if you are filtering a single MAC source address.
 - Enter the highest MAC source address in the range if you are filtering a range of MAC source addresses.
 - Leave this field blank and enter the name of the MAC Address list in the MAC source (low) field if you are establishing a range of MAC source addresses with a MAC Address list.

For more information, refer to “MAC source (low).” To learn how to create a MAC Address list, refer to “MAC Address (low)” and “MAC Address (high).”

MAC source (low)

Sets the lower boundary of the range for filtering a frame based on the contents of its MAC-level source address field.

- Options
- Leave this field blank if you do not want to filter a frame based on its MAC source address.

Bridge Parameters

Parameters and Options

- Enter the MAC source address in this field and leave the MAC source (high) field blank if you are filtering a single MAC source address.
- Enter the lowest MAC source address in this field and enter the highest MAC source address in the MAC source (high) field if you are filtering a range of MAC source addresses.
- Leave this field blank and enter the name of the MAC Address list in the MAC source (low) field if you are establishing a range of MAC source addresses with a filter list.

For more information, refer to “MAC source (high).” To learn how to create a MAC Address list, refer to “MAC Address (low)” and “MAC Address (high)”.

Max Age

Sets the maximum length of time the bridge stores configuration information. The bridge declares a line down if it does not receive a BPDU for Max Age seconds. After declaring the line down, the bridge sets the port state to Listen. If you have not enabled the spanning tree algorithm, skip this field. If you have enabled the spanning tree algorithm, consult table 6-1 “Suggested Spanning Tree Parameter Values” (page 6-19) to determine an appropriate value for Max Age.

Default: 20 seconds
Range: 6 to 40

Max Hops

Limits the number of hops an ARE frame traverses through the hop route before it is dropped by the receiving circuit group. For example, if a circuit group is configured for Max Hops of 3, then ARE frames arriving on that circuit group with three or more hops are dropped instead of forwarded.

Default: 7
Range: 1 to 7

Offset

Positions the filtered bit pattern within either the MAC-level or data-link-level header. The first (most significant) bit of either the MAC-level or data-link-level header is referenced as bit 0.

Options Enter the starting location of the filtered bit pattern with reference to the most significant bit of the header. For example, an Ethernet multicast address is designated by setting the lowest-order bit in the highest-order byte of the Ethernet address. Consequently, the following are valid Ethernet multicast addresses: 010000009999, 0F0000009999. To filter multicast addresses, you would examine the multicast bit by entering 7 at Offset.

Precedence	<p>Assigns a priority values to a filter—the higher the precedence, the greater the priority. You can construct up to 31 filters per bridge circuit group. The Precedence value is used when an incoming packet meets multiple filter rules. In such an instance, the filter with the highest priority is applied to the frame.</p> <p>Default: 31 Range: 1 to 31</p>
Priority	<p>In the event of identical-cost circuit groups, the spanning tree algorithm select the circuit group with the better (lower) priority value. Priority is only meaningful if the spanning tree algorithm is enabled.</p> <p>Default: 128</p> <p>Options 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 16, 32, 64, 127, 128, 129, 255</p>
Protocol ID/Org. Code (high)	<p>Sets the upper boundary of the range for filtering a frame based on the contents its Protocol ID/Organization Code field.</p> <p>Options</p> <ul style="list-style-type: none">■ Leave this field blank if you do not want to filter a frame based on its Protocol ID/Organization Codes.■ If you are filtering a single Protocol ID/ Organization Code, leave this field blank and enter the Protocol ID/ Organization Code in the Protocol ID/Org. Code (low) field.■ If you are filtering a range of Protocol ID/Organization Codes, enter the highest Protocol ID/Organization Code in the range.■ If you want to establish a range of Protocol ID/Organization Codes with a filter list, leave this field blank and enter the name of a Protocol ID/Organization Code list in the Protocol ID/Org. Code (low) field. <p>For more information, refer to “Protocol ID/Org. Code (low)”.</p> <p>Note: The Protocol ID/Org. Code (high) parameter is also displayed when creating a Protocol ID/Organization Code list.</p>
Protocol ID/Org. Code (low)	<p>Sets the lower boundary of the range for filtering a frame based on the contents of its Protocol ID/Organization Codes.</p> <p>Options</p> <ul style="list-style-type: none">■ If you do not want to filter Protocol ID/Organization Codes, leave this field blank.■ If you are filtering a single Protocol ID/Organization Code, enter the Protocol ID/Organization Code in this field and leave the Protocol ID/Org. Code (high) field blank .

Bridge Parameters

Parameters and Options

- If you are filtering a range of Protocol ID/Organization Codes, enter the lowest Protocol ID/Organization Code in this field and enter the highest Protocol ID/Organization Code in the Protocol ID/Org. Code (high) field .
- If you are establishing the range of Protocol ID/Organization Codes with a filter list, enter the name of a Protocol ID/Organization Code list in this field and leave the Protocol ID/Org. Code (high) field blank .

For more information, refer to “Protocol ID/Org. Code (high)”.

Note: The)Protocol ID/Org. Code (low) parameter is also displayed when creating a Protocol ID/Organization Code list.

Protocol Type	Determines the protocol to filter. Enter the 12-digit hexadecimal protocol-type value identifying the protocol to relay to a specific circuit.
SAP (high)	<p>Sets the upper boundary of the range for filtering a frame based on the contents of its source service access points (SSAP) or destination service access points (DSAP). The SAP (low) and SAP (high) parameters are displayed when creating a SAP filter list.</p> <p>Options</p> <ul style="list-style-type: none">■ Leave this field blank and enter the source or destination service access point in the SAP (low) field if you are filtering a single service access point.■ Enter the highest service access point in the range if you are filtering a range of source or destination service access points. <p>For more information, refer to “SAP (low).” To learn how to apply a SAP list to a filter, refer to “SSAP (low)” and “DSAP (low).”</p>
SAP (low)	<p>Sets the lower boundary of the range for filtering a frame based on the contents of its source service access points (SSAP) or destination service access points (DSAP). The SAP (low) and SAP (high) parameters are displayed when creating a SAP filter list.</p> <p>Options</p> <ul style="list-style-type: none">■ If you are filtering a single source or destination service access point, enter the service access point in this field and leave the SAP (high) field blank.■ Enter the lowest source or destination service access point in this field and enter the highest service access points in the SAP (high) field if you are filtering a range of service access points, . <p>For more information, refer to “SAP (high).” To learn how to apply a SAP list to a filter, refer to “SSAP (low)” and “DSAP (low).”</p>

Spanning
Tree Enable

Enables or disables the spanning tree algorithm.

Default: No

- Yes Enables the spanning tree algorithm if your network topology contains redundant bridge/LAN connections.
- No Disables the spanning tree algorithm if your network topology contains a single bridge or multiple, non-redundant bridges.

Table 6-1. Suggested Spanning Tree Parameter Values

Hello Time	Max Age	Forward Delay
1	>=4	>=3
2	>=6	>=4
3	>=8	>=5
4	>=10	>=6
5	>=12	>=7
6	>=14	>=8
7	>=16	>=9
8	>=18	>=10
9	>=20	>=11
10	>=22	>=13

If you enable source routing, the spanning tree algorithm is always enabled regardless of the value assigned to the Spanning Tree Enable parameter. Forwarding Table Size specifies the maximum size of the forwarding table.

The forwarding table contains the list of end-station addresses learned by the bridge, plus all source-address filters and destination-address filters. The value entered for the Forwarding Table Size parameter sets the maximum size of the table. There are seven options for Forwarding Table Size:

0	2048
64	4096
512	8192
1024 (default)	

Bridge Parameters

Parameters and Options

To specify forwarding table size, refer to your network topology drawing and estimate the number of end-stations serviced by the bridge; then double this figure. Finally, select the next highest value from the available responses. (For more information on the Forwarding Table parameter, refer to page 6-11.)

Src Rte	<p>Enables or disables source routing.</p> <p>Default: No</p> <p>Yes Enables source routing for the current circuit.</p> <p>No Disables source routing for the current circuit.</p>
SSAP (high)	<p>Sets the upper boundary of the range for filtering a 802.2 LLC frame based on the contents of its source service access points (SSAP) field.</p> <p>Options</p> <ul style="list-style-type: none">■ Leave this field blank if you do not want to filter a frame based on the contents of its SSAP field.■ Leave this field blank and enter the SSAP in the SSAP (low) field if you are filtering a single source service access point.■ Enter the highest DSAP in the range if you are filtering a range of source service access points.■ Leave this field blank and enter the name of a SAP list in the SSAP (low) field if you want to establish the range of source service access points with a filter list. <p>For more information, refer to “SSAP (low)” earlier in this chapter. To learn how to create a SAP list, refer to “SAP (low)” and “SAP (high)” earlier in this chapter.</p>
SSAP (low)	<p>Sets the lower boundary of the range for filtering a 802.2 LLC frame based on the contents of its source service access point (SSAP) field.</p> <p>Options</p> <ul style="list-style-type: none">■ Leave this field blank if you do not want to filter a frame based on the contents of its SSAP field.■ Enter a SSAP in this field and leave the SSAP (high) field blank if you are filtering a single source service access point.■ Enter the lowest SSAP in this field and enter the highest SSAP in the SSAP (high) field if you are filtering a range of source service access points.■ Enter the name of a SAP list in this field and leave the SSAP (high) field blank if you are establishing a range of source service access points with a filter list.

For more information, refer to “SSAP (high)” earlier in this chapter. To learn how to create a SAP list, refer to “SAP (low)” and “SAP (high)” earlier in this chapter.

STP Priority

Sets the bridge priority for the spanning tree algorithm.

Default: 32768

- Options
- Skip this field if you have not enabled the spanning tree algorithm.
 - If you have enabled the algorithm, STP Priority supplies the most-significant 16-bits of the unique 64-bit bridge identifier used by the algorithm to identify the root bridge (the bridge with the best priority). The smaller this value, the more likely it is that the bridge will be the root. Choose one of the following options:

1	1023
3	2047
7	4095
15	8191
31	16383
63	32767
127	32768 (default)
255	32769
511	65535

When assigning values to the spanning tree parameters (Hello Time, Max Age, and Forward Delay), you might want to use the values listed in table 6-1 (page 6-19).

Table Age Interval

Sets a time interval, in minutes, for aging the learning bridge entries in the forwarding table.

Default: 60
Disable: 0

Options 0, 5, 30, 60 (default), 120, 180, 240, 300

The Table Age Interval controls how frequently the learning bridge entries are checked for removal from the bridge forwarding table. Each time a frame is forwarded to a station, its entry in this table is time-stamped. If the entry is not accessed for twice this interval, the entry is removed from the table. A value of zero disables the timer and aging is no longer performed.

Note: If the network contains a high number of end stations, a shorter duration can prevent the forwarding table from being filled.

Bridge Parameters

Parameters and Options

The aging algorithm consumes CPU bandwidth that could otherwise be used to forward packets. Therefore, excessive aging of the table can cause occasional dropping of frames. The default should provide the most appropriate time interval for aging in most installations.

Traffic Priority

Prioritizes packets received for bridging to other routers via WAN links, and assures that packets (packets that are sensitive to long response times such as SNA packets) are not delayed or dropped because of delays caused by traffic congestion. Prioritizing is done on a circuit basis on inbound packets that are bridged. You can configure to prioritize all bridged packets or use filtering to prioritize packets based on their encapsulation type.

Default: Normal

High Incoming packet configured for High priority have first priority for outgoing bridged transmission.

Normal Incoming packets configured for Normal priority have second priority for outgoing bridged transmission, and are subject to the same first-in, first-out rule governing outgoing transmission of traffic in other routing protocols. Any packet types for which there is no level specified are automatically assigned to the Normal level.

Low Incoming packets configured for Low priority have third priority for outgoing bridged transmission, and have a lower priority than traffic in other routing protocols.

Note: If you assign differing priorities to different packet types within the same circuit group, then the Traffic Priority filter must be set to Normal. In this case, any packet type that is not assigned to have Low Priority or High Priority will have Normal priority.

Transitional Bridge

Enables or disables TRNSB (Source Route Translation Bridging) on the Bridge Configuration menu. TRNSB translates frames between source route bridging (SRB) circuit groups and transparent bridging (TB) circuit groups.

Default: No

Yes Enables TRNSB.

No Disables TRNSB.

Type (high)

Sets the upper boundary of the range for filtering an Ethernet frame based on the contents of its Ethernet Type field.

Options ■ Leave this field blank and enter the Ethernet Type value in the Type (low) field if you are filtering a single Ethernet Type.

- Enter the highest Ethernet Type in the range if you are filtering a range of Ethernet Types.

For more information, refer to “Type (low)” below. To learn how to apply an Ethernet Type filter list, refer to “Ethernet Type (low)” (page 6-10) and “Ethernet Type (high)” (page 6-9).

Type (low)

Sets the lower boundary of the range for filtering an Ethernet frame based on the contents of its Ethernet Type field.

- Options
- Enter the Ethernet Type in this field and leave the Type (high) field blank if you are filtering a single Ethernet Type.
 - Enter the lowest Ethernet Type value in this field and enter the highest Ethernet Type in the Type (high) field if you are filtering a range of Ethernet Types.

For more information, refer to “Type (high)”, above. To learn how to apply an Ethernet Type list to a filter, refer to “Ethernet Type (low)” and “Ethernet Type (high)” earlier in this chapter.

Internet Protocol (IP) Parameters

Overview

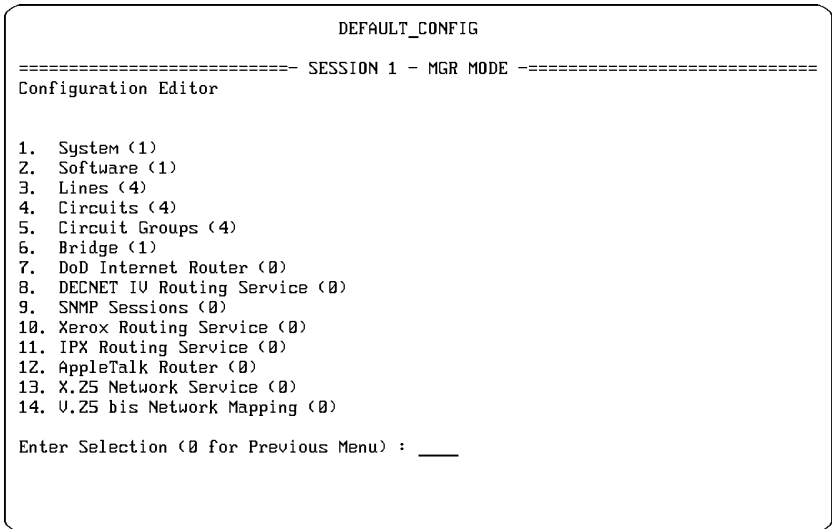


Figure 7-1. Access to IP Parameters

IP Parameters: Enable use of the Internet TCP/IP protocol suite for establishing routing for IP datagrams from a source to a destination over one of several available paths.

Page	IP Parameter
7-6	Action
7-6	Action on circuit group enable/disable
7-6	Acquisition Mode
7-6	Address Mask Reply
7-7	Address Resolution
7-8	Allow Router to Accept Files
7-8	Area ID
7-8	AS Boundary
—Continued Next Page—	

Internet Protocol (IP) Parameters
Overview

Page	IP Parameter
7-8	ASB Flood
7-8	Authentication Type
7-9	Auto Enable
7-9	Circuit Group
7-9	Connection Close Time Out
7-9	Conditional Circuit Group
7-9	Cost
7-9	Dead Interval
7-10	Default Route Listen
7-10	Default Route Supply
7-10	Dest IP Address
7-10	DLCI
7-10	Drop If Next Hop is Down
7-10	Effect
7-11	Encapsulation
7-11	Export Action
7-12	From Autonomous System
7-12	From Gateway
7-12	From Interface
7-12	From Peer
7-12	From Protocol
7-13	Global Broadcast
7-13	Header
7-13	Hello Interval
7-13	Hello Timer
7-13	High Value (hex)
7-14	Host Cache
7-14	Import Action
7-14	Interface Type
7-15	Internet Address
7-15	IP Address
7-15	IP Address (high)
7-15	IP Address (low)
7-15	IP Dest (high)
7-16	IP Dest (low)
—Continued Next Page—	

Internet Protocol (IP) Parameters

Overview

Page	IP Parameter
7-16	IP Port (high)
7-16	IP Port (low)
7-16	IP Source (high)
7-17	IP Source (low)
7-17	LAN Address
7-17	Length
7-17	List Name
7-17	Load Balancing
7-18	Local ASN
7-18	Local Address
7-18	Low Value (hex)
7-18	Make route conditional on an alternate circuit group
7-18	Management Priority
7-19	Max Relay Hops
7-19	Max Retransmissions
7-19	Metric
7-19	Mode (for routing or bridging choice)
7-19	Mode (for time protocol options)
7-19	MTU Discovery Option
7-20	Neighbor ID
7-20	Network Address
7-20	Network Mask
7-20	Next Hop (for static routes)
7-20	Next Hop Address (for IP traffic filters)
7-20	Non Local ARP Source
7-21	Normal ARP
7-21	Offset
7-21	Password
7-21	Poisoned Reverse/ Split Horizon
7-21	Polling Mode
7-22	Polling Timer
7-22	Poll Interval
7-22	Precedence
7-22	Preference
7-23	Priority

Internet Protocol (IP) Parameters
Overview

Page	IP Parameter
7-23	Propagate to EGP
7-23	Propagate to RIP
7-23	Propagate to OSPF
7-23	Protocol
7-24	Proxy ARP
7-24	Receive Broadcast
7-24	Relay Auto Enable
7-25	Remote Address
7-25	Remote ASN
7-25	Retransmission Time Out
7-25	Retransmit Interval
7-25	RIP Interface Cost
7-25	RIP Network Diameter
7-26	RIP Listen
7-26	RIP Supply
7-26	Router ID
7-26	Source Route (Token Ring)
7-26	Stub Area
7-27	Subnet Mask
7-27	Suppress Authentication Traps
7-27	Tag
7-27	To Interface
7-27	To Protocol
7-28	Transit Area
7-28	Transmit Broadcast
7-28	Type (for filtering)
7-28	Type (for static routing)
7-29	UDP Checksum Off
7-29	UDP/TCP Dest Port (high)
7-28	UDP/TCP Dest Port (low)
7-30	UDP/TCP Source Port (high)
7-30	UDP/TCP Source Port (low)

Parameters and Options

Action	Determines the disposition of IP datagrams, UDP datagrams, or TCP segments meeting the filter rule. Default: Drop Accept Relays a packet meeting the filter rule. Drop Discards a packet meeting the filter rule.
Action on circuit group enable/disable	Determines the action taken with the Conditional Circuit Group. Default: disable/enable disable/enable Enables the conditional static routing when the conditional circuit group is disabled. When the conditional circuit group is restored, the conditional route is disabled. enable/disable Enables the conditional static routing when the conditional circuit group is enabled. When the conditional circuit group goes down, the conditional route is disabled.
Acquisition Mode	Specifies which of two neighbors initiates EGP connections. EGP connections are initiated when one neighbor issues an acquisition request message, and finalized when the recipient of the acquisition request message issues an acquisition confirmation response. A neighbor who issues acquisition request messages is said to be active; a neighbor responding to such messages is said to be passive. Although the EGP protocol allows both neighbors to be active, protocol efficiency is enhanced when one neighbor is active and the other is passive. Default: Active Active Assigns the router as an Active neighbor. Passive Assigns the router as an Passive neighbor.
Address Mask Reply	Enables or disables the generation of ICMP address mask reply messages when the router boots and in response to valid address mask request messages. Default: No No Disables address mask reply messages.

Yes Enables address mask reply messages to be generated in compliance with the relevant sections of RFCs 950 and 1009.

Address Resolution Enables or disables address resolution, the mapping of 32-bit IP addresses to 48-bit station addresses. This parameter setting also influences the data-link encapsulation method used at address resolution time.

Default: ARP & HP Probe

ARP Allows the router to conditionally enable IP/Ethernet address mapping using the Address Resolution Protocol (ARP, as described in RFC 826) and the Proxy ARP Protocol.

HP Probe Enables the proprietary Hewlett-Packard Probe Protocol, an address resolution functioning much like ARP. Both Ethernet and IEEE 802.3 encapsulation are used.

The following Probe messages are routed:

Unsolicited Reply (outgoing), transmitted on all IP network IFs when router is booted.

Virtual Address Request (incoming—except on the same circuit—and outgoing)

Virtual Address Reply (incoming and outgoing)

The following HP Probe messages are bridged if bridging is enabled:

Name Request (incoming)

Name Reply (outgoing)

Proxy Name Request (incoming)

Proxy Name Reply (outgoing)

ARP & HP Probe Enables concurrent operation of HP Probe and ARP. With both address resolution protocols enabled, the router uses the first-in resolved media address until the address is modified by subsequent updates. Nodes are contacted with both Ethernet and IEEE 802.3 encapsulation; if a node responds to both, then the encapsulation used for the node is the one with the shortest data-link-layer header.

DDN Enables the DDN address resolution algorithm, a requirement if the network interface provides X.25 DDN service.

None Disables address mapping. With mapping disabled, all station address/IP address relationships must be configured as static routes.

PDN Enables a table-based RFC-877-compliant address resolution mechanism, a requirement if the network interface provides X.25 PDN service.

Internet Protocol (IP) Parameters

Parameters and Options

Allow Router to Accept Files	<p>Enables inbound TFTP by allowing router to accept files via TFTP from other sources.</p> <p>Default: No</p> <p>Yes Enables router to accept files via TFTP from other sources.</p> <p>No Disables acceptance of files via TFTP from other sources.</p>
Area ID	<p>Identifies an OSPF area in dotted-decimal notation.</p> <p>Note: The area ID value of 0.0.0.0 is reserved for the backbone Area ID only, and should not be used to configure other OSPF areas.</p>
AS Boundary	<p>Opens the OSPF routing pool to routing information obtained from sources external to OSPF.</p> <p>No Prevents the OSPF routing pools from including manually configured routes and routes obtained from EGP and OSPF.</p> <p>Yes allows the OSPF routing pool to include manually configured routes and routes obtained from RIP and EGP.</p>
ASB Flood	<p>Enables or disables the all-subnet broadcast (ASB) feature. An ASB datagram is one with a destination IP address equal to the broadcast address for an entire subnet. For example, if a network interface is attached to a subnet with the address 128.10.2.1 and subnet mask 255.255.255.0, any datagram on this network with a destination address of 128.10.255.255 is considered an ASB datagram. When the IP router receives an ASB datagram on one IP network interface, it floods it out on the IP network interface to that subnet. ASB datagrams are flooded one per physical interface, so a port with more than one network interface definition is flooded with one ASB datagram only. This is typically used with HP Data Terminal Concentrator to HP Data Terminal Concentrator communication.</p> <p>Default: No</p> <p>No Disables the ASB Flood feature.</p> <p>Yes Enables the ASB Flood feature.</p>
Authentication Type	<p>Enables or disables password authentication.</p> <p>Default: Simple Password</p> <p>No Authentication Disables password authentication.</p>

Internet Protocol (IP) Parameters Parameters and Options

Simple Password Enables password authentication.

Note: If the Area ID is not specified or is a value other than 0.0.0.0., the Stub Area parameter is displayed.

Auto Enable

Determines the initial state of the IP router. This IP-specific Auto Enable parameter works in conjunction with the global Auto Enable parameter found on the Global Parameters screen in the System configuration menu to enable or disable the IP routing protocol when the router boots.

- When the global Auto Enable parameter is set to No, the IP router (like all other applications) is unconditionally disabled.
- When the global Auto Enable parameter is set to Yes, the setting of the IP-specific Auto Enable parameter determines whether the IP router is automatically enabled.

Default: Yes

No IP routing is disabled. (Then to enable it after the router boots, use the NCL Interpreter's Enable command.)

Yes IP routing is automatically enabled if the global Auto Enable parameter is also enabled.

Circuit Group

Identifies the circuit group associated with the network interface.

Connection Close Time Out

Sets the number of seconds TFTP (Trivial File Transfer Protocol) waits before relinquishing resources after it successfully completes a file transfer.

Default: 25

Conditional Circuit Group

Name of the circuit group whose status (enabled or disabled) determines when to implement or drop the conditional static route.

Cost

Number of router hops that a datagram traverses before the destination is reached (not counting this router).

Range: 1 to 99 (hops)

Dead Interval

Specifies the number of seconds before a "silent" router is declared down.

Default: 20 (seconds)

Options 20, 40, 60, 80, 100, 120, 140, 160, 180, 200, 220, 240, 300, or 360 (seconds)

Internet Protocol (IP) Parameters

Parameters and Options

Note: All routers on the OSPF backbone must be configured with the same values for Hello Interval and Dead Interval.

Default Route Listen Determines whether the IP router adds network and subnet default route information, received in RIP updates from neighboring routers, to its internal routing table.

Default: No

No Prevents the router from adding received default route information to its internal routing table.

Yes Allows the router to add received default route information to its internal routing table.

Note: For Default Route Listen to be enabled, RIP Listen must be set to Yes.

Default Route Supply Determines whether the IP router advertises default routes in RIP updates sent to neighboring routers.

Default: No

No Prevents the router from advertising network or subnet default routes.

Yes Allows the router to advertise default routes.

Note: For Default Route Supply to be enabled, RIP Supply must be set to Yes.

Dest IP Address Accepts the IP destination address used by the relay agent written in dotted-decimal notation.

DLCI Specifies the Frame Relay Data Link Connection Identifier to the target host.

Drop If Next Hop is Down Determines the disposition of a filtered datagram if the next hop is unreachable.

Default: No

No Allows IP to consult its routing table and provide an alternate route for the datagram.

Yes Drops the datagram

Effect Determines whether a packet is dropped or relayed (filtered) based on the contents of a packet field and a range established by a matching set of (low) and (high) parameters. The packet field and corresponding (low) and (high) parameters are listed in the following table:

Internet Protocol (IP) Parameters Parameters and Options

Packet Field	IP Parameters
IP Destination	IP Dest (low) and IP Dest (high)
IP Source	IP Source (low) and IP Source (high)

Default: Ignore

Don't Match Applies the filtering action (drop/accept/log) if the contents of the packet field do not fall within the range established by the matching set of (low) and (high) filter parameters.

Ignore Applies no filtering action if the contents of the packet field falls within the range established by the matching set of (low) and (high) filter parameters.

Match Applies the filtering action (drop/accept/log) if the contents of the packet field falls within the range established by the matching set of (low) and (high) filter parameters.

Encapsulation Type Used with the Adjacent Host type of static route. Assigns one of three encapsulation types.

Default: Ethernet

Ethernet Standard Ethernet 2.0 encapsulation for hosts that support Ethernet. (Required for point-to-point network interface or any type of X.25 interface.) If you are defining a LAN interface (Ethernet or IEEE 802.x), you must specify the encapsulation method supported by the attached network.

802.2 Select this option for hosts supporting 802.2 over 802.3 LAN interfaces. The 802.2 structure is encapsulated as shown, and is further encapsulated within a medium-specific 802.x packet.

SNAP Assigns an extension of 802.2 encapsulation for hosts supporting SNAP. The SNAP structure is encapsulated within a medium-specific 802.x packet.

Export Action Used in export route filters to control the flow of routing information between protocols.

Default: PROPAGATE

IGNORE Suppresses route advertising.

PROPAGATE Advertises the route.

Internet Protocol (IP) Parameters

Parameters and Options

Note: The Metric field appears after selecting PROPAGATE. Metric lets you assign a RIP cost to the propagated route. For more information, refer to “Metric” later in this chapter.

From Autonomous System Lets you identify a specific autonomous system from which RIP updates are received.

- Options
- Leave this field blank if you want the EGP import route filter to be “universal” (that is applicable to all foreign autonomous systems).
 - Enter the system’s NIC-assigned identification number if you want the filter to apply to a specific autonomous system.

From Gateway Assigns a specific gateway for receiving RIP updates.

Yes Enables gateway identification.

No Disables gateway identification.

From Interface Assigns specific interface for receiving RIP updates.

Yes Enables the identification of specific interfaces.

No Disables the identification of specific interfaces.

From Peer Enables the identification of a specific router from which EGP updates are received.

- Options
- Leave this field blank if you wish the EGP import route filter to be “universal” (that is applicable to all foreign EGP routers).
 - Enter the source routers IP address, in dotted-decimal notation, if you want the filter to apply to a specific source of EGP updates.

From Protocol Assigns the source for routing information.

Default: RIP

EGP Assigns EGP (Exterior Gateway Protocol) as the source for routing information.

RIP Assigns RIP (Routing Information Protocol) as the source for routing information.

OSPF Assigns OSPF (Open Shortest Path First Protocol) as the source for the routing information.

Global Broadcast	Determines whether the router accepts or discards a global broadcast message, a message with an IP destination address consisting entirely of 1 digits.
	Default: Yes
	No Allows the router to discard global broadcast messages, effectively disabling the Routing Information Protocol (RIP). Note: Routers use the Routing Information Protocol (RIP) to exchange route information, maintain routing tables, and determine a path by using a distance-vector algorithm. Setting Global Broadcast to No effectively disables RIP, which uses the global broadcast message to propagate periodic routing updates. Yes Lets the router accept the global broadcast message.
Header	Determines whether the IP header or the upper level protocol header is selected when creating a user-defined IP filter.
	Default: Network
	After Network Selects the upper level protocol header. Network Selects the IP header.
Hello Interval	Specifies the number of seconds between the TCP/IP router's transmission of OSPF Hello packets. Hello packets are transmitted across each OSPF interface. On broadcast interfaces, they are used to elect the designated and backup designated router, and to discover and maintain neighbor relationships.
	Default: 5 (seconds)
	Options 10, 15, 20, 30, or 60 seconds Note: All routers connected to the OSPF backbone must be configured with the same values for Hello Interval and Dead Interval.
Hello Timer	Specifies the time interval, in seconds, between EGP Hello commands.
	Default: 60 (seconds) Options 30, 40, 50, 60, 70, 80, 90, 100, 110, and 120 (seconds)
High Value (hex)	Sets the upper boundary range of the hexadecimal bit pattern when creating a user-defined filter.

Internet Protocol (IP) Parameters

Parameters and Options

- Options ■ Leave this field blank and enter the bit pattern in the Low Value (hex) field if you are filtering a single bit pattern.
- Enter the highest bit pattern in the range if you are filtering a range of bit patterns.

For more information, refer to “Low Value (hex)” later in this chapter.

Host Cache Enables or disables the aging of physical-level addresses learned by any of the address resolution protocols. With the address resolution cache disabled (Host Cache is set to No), entries in the address resolution cache are not aged out. With the address resolution cache enabled (Host Cache equal to Yes), cache entries that have not been accessed within two minutes are aged out (removed from the cache). Once an entry has been aged, the TCP/IP router must again acquire the physical level address (via an address resolution protocol) should it be needed in the future.

Default: No

No Disables aging feature.

Yes Enables aging feature.

Import Action Used in import route filters to determine whether the route is transferred to the routing pool.

Default: ACCEPT

ACCEPT Sends information to the routing pool.

IGNORE Drops the routing information.

Note: The Preference parameter is displayed when Import Action is set to ACCEPT. For additional information, refer to “Preference” on page 7-22.

Interface Type Sets the OSPF Interface type.

Default: Broadcast

Broadcast Connects the router to an Ethernet or IEEE 802.x medium and supports multiple (more than two) routers, plus providing the ability to address a single physical message to all of the attached routers. Select this option if the current interface connects to an OSPF broadcast-type media.

Point-to-Point Connects a pair of OSPF routers; that is; it connects the router to a remote peer or to a packet switched network such as Telenet or the DDN. Select this option if the current interface connects to a remote peer.

Non-Broadcast Multi-Access Supports multiple (more than two) routers, but does not provide the ability to address a single physical message to all routers. An example is a public switched packet network.

Internet Address	Accepts the IP (Internet Protocol) address of the remote router port for the destination network. Enter the address in dotted-decimal notation.
IP Address	Identifies the Internet Protocol address for an interface in dotted-decimal notation.
IP Address (high)	Sets the upper boundary of the IP address range when creating an IP address list. Options <ul style="list-style-type: none">■ Leave this field blank and enter the IP address in the IP Address (low) field if you are filtering a single IP address.■ Enter the highest IP address in the range if you are filtering a range of IP addresses. <p>For more information, refer to “IP Address (low)”. To learn how to apply a IP Address list to a filter, refer to “IP Dest (low)” and “IP Source (low).”</p>
IP Address (low)	Sets the lower boundary of the IP address range when creating an IP Address list. Options <ul style="list-style-type: none">■ Enter the IP address in this field and leave the IP Address (high) field blank if you are filtering a single IP address.■ Enter the lowest IP address in this field and enter the highest IP address in the IP Address (high) field if you are filtering a range of IP addresses, <p>For more information, refer to “IP Address (high)” earlier in this chapter. To learn how to apply a IP Address list to a filter, refer to “IP Dest (low)” and “IP Source (low).”</p>
IP Dest (high)	Sets the upper boundary of the range for filtering a packet based on the contents of its IP destination field. Options <ul style="list-style-type: none">■ Leave this field blank if you do not want to filter an IP packet based on the contents of its IP destination field.■ Leave this field blank and enter the IP destination address in the IP Dest (low) field if you are filtering a single IP destination address.■ Enter the highest IP destination address in this field if you are filtering a range of IP destination addresses.■ Leave this field blank and enter the name of a IP Address list in the IP Dest (low) field if you are establishing a range of IP destination addresses with a filter list.

Internet Protocol (IP) Parameters

Parameters and Options

For more information, refer to “IP Dest (low)” later in this chapter. To learn how to create an IP Address list, refer to “IP Address (low)” and “IP Address (high)” earlier in this chapter.

IP Dest (low) Sets the lower boundary of the range for filtering a packet based on the contents of its IP destination field.

Options ■ Leave this field blank if you do not want to filter IP packets based on the contents of their IP destination field.

■ Enter the IP destination address in this field and leave the IP Dest (high) field blank if you are filtering a single IP destination address.

■ Enter the lowest IP destination address in this field and enter the highest IP destination address in the IP Dest (high) field if you are filtering a range of IP destination addresses.

■ Enter the name of an IP Address list in this field if you want to establish a range of IP destination addresses with a filter list.

For more information, refer to “IP Dest (high)” earlier in this chapter. To learn how to create an IP Address list, refer to “IP Address (low)” and “IP Address (high)” earlier in this chapter.

IP Port (high) Sets the upper boundary of the port range when creating an IP Port list.

Options ■ Leave this field blank and enter the IP port in the IP Port (low) field if you are filtering a single IP port.

■ Enter the highest IP port in the range in this field if you are filtering a range of IP ports.

For more information, refer to “IP Port (low)” later in this chapter.

IP Port (low) Sets the lower boundary of the port range when creating an IP Port list.

Options ■ Enter the IP port in this field and leave the IP Port (high) field blank if you are filtering a single IP port.

■ Enter the lowest IP port number in this field and enter the highest IP port number in the IP Port (high) field if you are filtering a range of IP ports.

For more information, refer to “IP Port (high)” earlier in this chapter.

IP Source (high) Sets the upper boundary of the range for filtering a packet based on the contents of its IP source field.

- Options ■ Leave this field blank if you do not want to filter an IP packet based on the contents of its IP source field.
- Leave this field blank and enter the IP source address in the IP Source (low) field if you are filtering a single IP source address.
 - Enter the highest IP source address in this field if you are filtering a range of IP source addresses.
 - Leave this field blank and enter the name of a IP Address list in the IP Source (low) field if you are establishing a range of IP source addresses with a filter list.

For more information, refer to “IP Source (low)” later in this chapter. To learn how to create an IP Address list, refer to “IP Address (low)” and “IP Address (high)” earlier in this chapter.

IP Source (low) Sets the lower boundary of the range for filtering a packet based on the contents of its IP source field.

- Options ■ Leave this field blank if you do not want to filter IP packets based on the contents of their IP source field.
- Enter the IP source address in this field and leave the IP Source (high) field blank if you are filtering a single IP source address.
 - Enter the lowest IP source address in this field and enter the highest IP source address in the IP Source (high) field if you are filtering a range of IP source addresses.
 - Enter the name of an IP Address list in this field if you want to establish a range of IP source addresses with a filter list.

For more information, refer to “IP Source (high)” earlier in this chapter. To learn how to create an IP Address list, refer to “IP Address (low)” and “IP Address (high)” earlier in this chapter.

LAN Address The 48-bit station address (also called the physical or Ethernet or MAC address) of the adjacent host. Enter the 12-digit hexadecimal number.

Length Sets the bit length of the filtered field when creating a user-defined filter.

List Name Accepts the name of the IP address list or IP port list.

Load Balancing Used to balance the network traffic load if more than one circuit is in a circuit group.
Default: No

Internet Protocol (IP) Parameters

Parameters and Options

No Disables load balancing. When disabled, then for a given source IP and destination IP address, the same circuit is used for all packets.

Yes Enables load balancing. When enabled, a circuit is randomly selected from the circuit group for each packet.

Local ASN The NIC-assigned decimal number that identifies the local autonomous system. Enter the local autonomous system number.

Local Address The IP address, in dotted-decimal notation, of the local EGP interface that establishes the connection to the remote autonomous system.

Low Value (hex) Sets the lower boundary range of the bit pattern when creating a user-defined filter.

Options ■ Enter the bit pattern (hexadecimal) in this field and leave the High Value (hex) field blank if you are filtering a single bit pattern.

■ Enter the lowest bit pattern in this field and enter the highest bit pattern in the High Value (hex) field. If you are filtering a range of bit patterns.

For more information, refer to “High Value (hex)” earlier in this chapter.

Make route conditional on an alternate circuit group Determines whether to use conditional static routing.
Default: No

No Disables conditional static routing.

Yes Enables conditional static routing.

Note: When conditional static routing is enabled, the Conditional Circuit Group and Action on circuit group enable/disable parameters are displayed. For more information, refer to “Conditional Circuit Group” and “Action on circuit group enable/disable.”

Management Priority Enables immediate procession of SNMP traffic.

Default: Low

High Causes the router to process all management traffic as it is received.

Note: Setting Management Priority to High can noticeably impact the routing of non-management traffic.

Low Gives priority to the normal routing of incoming non-management traffic.

Internet Protocol (IP) Parameters Parameters and Options

Max Relay Hops	Determines the maximum number of router hops allowed to reach a destination. Default: 4 Range: 1 to 16 (hops)
Max Retransmissions	Determines the number of times TFTP retransmits an unacknowledged data message before abandoning the transfer attempt. Default: 5
Metric	Assigns a cost to the propagated route.
Mode (normal or end-node)	Used in the initial IP display to specify whether the IP router will route or bridge IP datagrams it receives on any circuit group. Default: Router/Host
Host only	Makes the router run in IP end-node mode, as if it is a virtual host on one of the bridged interfaces. If you are bridging IP traffic, select this mode. No IP routing is done in this mode.
Router/Host	Routes IP traffic normally. (The router can also be addressed as a host or node.) If you are not bridging IP traffic, select this mode.
Mode (Time Protocol)	Used in time protocol configuration to access from “8. Time Protocol Configuration” IP menu item. Determines whether the router supplies or receives the time service, or does both. Default: Server only
Client only	Makes the router poll a designated server for the time when the router is initialized.
Server only	Makes router answer time requests made by clients using its address. It provides the time kept on this router (set by the NCL Interpreter's Time command), which is converted by the client to its local time).
Server and Client	Allows the router to send and receive time server updates.
MTU Discovery Option	Enables or disables the Probe MTU and Reply MTU options (IP options number 11 and 12 specified in RFC 1063). These features enable the router to learn the minimum Maximum Transmission Unit (MTU) of all networks traversed by an IP datagram from source to destination. They can significantly decrease network load by eliminating the need for transmit fragmentation and destination reassembly. Default: No
No	Disables MTU discovery.

Internet Protocol (IP) Parameters

Parameters and Options

Yes Enables MTU discovery.

Neighbor ID Identifies the remote end of the virtual link. Enter the router ID of the remote end in dotted-decimal notation.

Network Address Accepts the filtered IP network address, in dotted-decimal notation, when creating an import or export route filter. If you want to filter all destination networks, leave this field blank. If you want to filter a specific IP network, enter that network address.

Network Mask Determines the range of addresses to filter when creating a EGP, RIP, or OSPF export route filter or the IP address of the OSPF backbone network. The address mask directs the filtering process to a specific portion of the IP address.

- Examples
- If Network Mask is set to 255.255.255.0, only the Net_ID portion of the IP address is filtered.
 - If Network Mask is set to 255.255.255.224, the Net_ID and Subnet_ID portions of the IP address are filtered.
 - If Network Mask is set to 255.255.255.255, the entire IP address is filtered.

Next Hop Used with IP static routes to specify the IP address of the router port connected to the next router in the hop sequence. IP addresses are entered in dotted-decimal notation.

Next Hop Address Used with IP traffic filters to set the IP address of the next router in the hop sequence. IP addresses are entered in dotted-decimal notation.

Non Local ARP Source Determines how the IP router responds when receiving ARP requests originating from a non-local network (a network that is not connected directly to the router).

Default: Drop and Log

Accept Adds non-local ARP entries to the local ARP table.

Drop Simply drops non-local ARPs. This option has the least impact on router behavior.

Drop and Log Drops non-local ARPs and logs them.

Note: Because Accept adds nonlocal ARP entries to the local ARP table, it may cause unpredictable results.

Normal ARP	<p>Enables or disables the Address Resolution Protocol (ARP). ARP maps 32-bit IP addresses to 48-bit station addresses. For enabling to take effect, Address Resolution must also be set to ARP or to ARP & HP Probe.</p> <p>Default: Yes</p> <p>No Disables ARP</p> <p>Yes Enables ARP.</p>
Offset	<p>Use to position the filtered bit pattern within the selected header when creating a user-defined filter.</p>
Password	<p>Specifies the authentication key used across an interface.</p>
Poisoned Reverse/ Split Horizon	<p>Determines how IP advertises routes learned from a neighboring router in periodic updates subsequently sent to the router.</p> <p>Default: Poison</p> <p>None Allows the router to advertise all routes learned from a neighbor in subsequent RIP updates using the actual hop count assigned to the routes.</p> <p>Poison Enables Poisoned Reverse—the router advertises routes learned from a neighbor in subsequent RIP updates. The router assigns a hop count of 16 to these routes, thus declaring the destinations unreachable.</p> <p>Split Enables Split Horizon—the router omits routes learned from a neighbor when sending subsequent RIP updates to the neighbor.</p>
Polling Mode	<p>Specifies one of two neighbor-reachability algorithms. In the active mode, the router issues periodic Hello and Poll commands. Neighbor-reachability is verified by receipt of corresponding “I hear you” (I-H-U) and Update responses. In the passive mode, the router does not issue Hello commands; nor does it expect I-H-U responses. Neighbor-reachability is verified by examining the Status field of the received Hello and Poll commands or of Update responses. Although the EGP protocol allows both neighbors to be active, protocol efficiency is enhanced when one neighbor is active and the other is passive.</p> <p>Default: Both</p> <p>Active Places the local router in Active mode.</p> <p>Both Allows the neighboring routers to arbitrate a mutually agreeable neighbor-reachability algorithm.</p>

Internet Protocol (IP) Parameters Parameters and Options

Passive Place the local router in Passive mode.

Polling Timer	<p>Specifies the time interval, in seconds, between EGP Poll commands.</p> <p>Default: 120 (seconds)</p> <p>Options 120, 150, 180, 210, 240, 270, 300, 330, 360, 390, 420, 450, 480 (seconds)</p>
Poll Interval	<p>Allows the router to send additional Hello packets at a reduced rate even though no Hello packets were received for more than the Dead Interval (seconds).</p> <p>Default: 20</p> <p>Options 20, 40, 80, 100, 120, 140, 160, 200 (seconds)</p>
Precedence	<p>Assigns a priority value for filtering a packet. The higher the precedence, the greater the priority.</p> <p>Default: 1</p> <p>You can construct up to 31 filters per IP interface. The Precedence value is used when an incoming IP packet meets multiple filter rules. In such an instance, the filter with the highest priority is applied to the frame. In the event of two filters with equal precedence, the first-configured filter takes precedence.</p>
Preference	<p>Assigns a weighted value used by the TCP/IP router to select from multiple routes to a single destination.</p> <p>Default: 16 Range 1 to 18</p> <p>The TCP/IP router maintains a routing pool containing information supplied by up to three routing protocols (RIP, EGP, OSPF) in addition to manually configured static routes. Consequently, the routing pool can contain multiple routes to the same destination. By default, the TCP/IP router uses manually configured static and/or default routes in preference to routes gathered by protocol exchanges.</p> <p>Preference contains a numeric value within the range from 0 to 16—the higher the value, the greater the preference of the route. That is, routes with higher values are selected (used for routing) by the TCP/IP router in preference to routes with lower values.</p>

Priority	<p>Specifies a weighted value used in the designated router and backup designated router selection algorithm.</p> <p>When two routers attached to the backbone both attempt to become the designated router, the one with the highest Priority value takes precedence. In the case of equal Priority values, the router with the highest Router ID takes precedence.</p> <p>Default: 0 (seconds) Range: 0 to 15 (seconds)</p>
Propagate to EGP	<p>Determines whether the static route is advertised by the EGP protocol.</p> <p>Default: Yes</p> <p>No Prevents the EGP from advertising static routes.</p> <p>Yes Allows the EGP to advertise static routes.</p>
Propagate to RIP	<p>Determines whether the static route is advertised by the RIP protocol.</p> <p>Default: Yes</p> <p>No Prevents the RIP from advertising static routes.</p> <p>Yes Allows the RIP to advertise static routes.</p> <p>Note: The RIP Supply parameter enables the RIP advertising function. If RIP is enabled (RIP Supply is set to Yes), the setting of the Propagate to RIP parameter determines whether an individual static route is advertised. If the RIP Supply parameter is not enabled (RIP Supply is set to No), and the Propagate to RIP parameter is no longer functions.</p>
Propagate to OSPF	<p>Determines whether the static route is advertised by the OSPF protocol.</p> <p>Default: Yes</p> <p>No Prevents the OSPF from advertising static routes.</p> <p>Yes Allows the OSPF to advertise static routes.</p>
Protocol	<p>Enables or disables traffic filtering to and from UDP/TCP ports.</p> <p>Default: Ignore</p> <p>Ignore Disables filtering of UDP/TCP ports.</p>

Internet Protocol (IP) Parameters
Parameters and Options

UDP Enables filtering of UDP ports and displays additional parameters on the screen.

TCP Enables filtering of TCP ports and displays additional parameters on the screen.

Note: For more information about the parameters appearing on the screen when selecting UDP or TCP

Proxy ARP Enables or disables the Proxy ARP protocol. Proxy ARP lets the IP router respond on a local interface to ARP requests for a host on a remote network. This response enables the router to assume responsibility for IP packets destined for that host. Before proxy ARP can be enabled, Address Resolution must also be set to ARP or to ARP & HP Probe.

Default: Yes

Yes Enables Proxy ARP.

No Disables Proxy ARP.

Receive Broadcast Determines the types of broadcast messages received by the IP router.

Default: Network and Subnet

Network Only Sets the router to accept only the network broadcasts. Choose this option only when the network does not have subnets.

Network and Subnet Sets the router to accept both network and subnet broadcast messages. This is appropriate in most applications.

Note: A network broadcast message consists of the network field (the NIC-assigned 8-bit, 16-bit, or 24-bit network address) followed by a string of 8, 16, or 24 logical ones or zeroes.

Note: A subnet broadcast message consists of the network field (the NIC-assigned 8-bit, 16-bit, or 24-bit network address), followed by the locally-assigned subnet field, followed by a string of 8, 16, or 24 logical ones or zeroes.

Relay Auto Enable Determines whether the BOOTP relay agent is automatically enabled by the IP protocol.

Default: No

No Disables the BOOTP Relay agent.

Yes Enables the BOOTP Relay agent.

Note: The BOOTP relay agent does not need to be turned on in all routers between the client and server. The router adjacent to the client must be a relay agent. If the router adjacent to the client has a configured set of BOOTREQUEST destinations that are specific server addresses or subnet addresses, then the adjacent router is the only router requiring relay agent functionality. If the adjacent relay agent does not have either server or subnet addresses configured, then the BOOTREQUEST is sent out through all of the adjacent router interfaces, and is addressed to the ALL HOSTS broadcast for each interface. To allow these BOOTREQUESTS to be forwarded to the server, each router in the path between the client and the server must be a BOOTP relay agent.

Remote Address	The IP address of the remote interface that establishes the connection to the remote autonomous system. Enter the address in dotted-decimal notation.
Remote ASN	The NIC-assigned decimal number identifying the remote autonomous system. Enter the remote autonomous system number.
Retransmission Time Out	Sets the number of seconds TFTP waits for an acknowledgment before retransmitting a data message. Default: 5 (seconds)
Retransmit Interval	Specifies the number of seconds between the TCP/IP router's retransmission of OSPF link state advertisements. Default: 5 (seconds) Options 5, 10, 15, 20, or 30 (seconds) Note: Retransmit Interval should be set to a value greater than the expected round trip delay between any two routers on the backbone.
RIP Interface Cost	Sets the cost for each router hop. Standard RIP implementations assign a cost of 1 to each hop. If you increase this RIP increment, the upper boundary set by RIP Network Diameter (beyond which a network is declared unreachable) is more rapidly attained. Default: 1
RIP Network Diameter	Determines the maximum number of hops for a IP datagram as it moves through an internet from source to destination. Standard Internet usage limits hops to a maximum 15. However, if every router within your internet can be configured to accept the identical number of hops, you can increase the RIP Network Diameter up to a maximum of 127.

Internet Protocol (IP) Parameters

Parameters and Options

Default= 15
Maximum = 127 (hops)

Note: It is strongly recommended that you accept the default value of 15 for RIP Network Diameter. Proper operation of RIP requires that every router within the network use the same network diameter value. Hosts also use the RIP network diameter to determine reachability.

RIP Listen Determines whether the IP router adds routing information, received in RIP updates from neighboring routers, to its internal routing table.

Default: Yes

No Prevents the addition of received routing information to the internal routing table.

Yes Allows the addition of received routing information to the internal routing table.

Note: To enable Default Route Listen, set RIP Listen to Yes; then set RIP Supply. For additional information, refer to "RIP Supply," "Default Route Supply," "Default Route Listen," "Poisoned Reverse," and "RIP Interface Cost."

RIP Supply Determines whether the IP router transmits periodic RIP updates to neighboring routers within the network.

RIP Supply, along with RIP Listen, Default Route Supply, Default Route Listen, Poisoned Reverse, and RIP Interface Cost, implement certain features of the RIP protocol. RIP enables the exchange of routing information between routers in the same autonomous system.

Default: Yes

No Prevents the router from transmitting updates.

Yes Allows the router to transmit RIP updates.

Note: To enable Default Route Supply, RIP Supply must be set to Yes.

Router ID Uniquely identifies the TCP/IP router within the OPSF domain. Accepts the router ID in dotted-decimal notation.

Source Route (Token Ring) Enables or disables source routing over token ring media for the interface being defined. If your router does not have a token ring port, always set this option to No.

Default: No

Stub Area Specifies the area type.

Note: When configuring a stub area, all routers within the stub area should configure the area as a stub. The router connecting to the backbone typically defines the default route onto the backbone.

Subnet Mask Sets the bit mask for determining which portion of the IP address identifies the subnetwork. Subnetworks (called subnets) are two or more physical networks sharing a common network field (the NIC-as signed portion of the 32-bit IP address). If the interface does have subnets, then enter the 32-bit subnet mask in dotted-decimal notation.

Suppress Authentication Traps Suppresses the reporting of SNMP authentication failures to the configured trap community. An authentication failure is the receipt of an SNMP request from an unknown community. This feature informs the network manager of unauthorized attempts to access the router via SNMP.

Default: Yes

No Enables SNMP authentication trapping—SNMP traps the authentication failure and alerts the network management station.

Yes Disables SNMP authentication trapping—the network management station is not alerted about unauthorized attempts to access the router via SNMP.

Tag Enables the further specification of external routes.

Within OSPF external links advertisements, a 32-bit External Route Tag field is attached to each route. The contents of this field are not used by OSPF but can be used by source and destination routers.

- Options ■ If you want to filter the contents of the External Route Tag field, enter the field contents in eight-digit hexadecimal format.
- Leave the field blank if you do not want to filter the contents of the field.

To Interface Assigns a specific interface for receiving EGP, RIP, or OSPF updates when creating a EGP, RIP, or OSPF import route filter.

- Options ■ Enter the IP address of the interface in dotted-decimal notation if you want a single interface to send all EGP, RIP, or OSPF updates to the import route filter.
- Leave the field blank if you want the EGP, RIP, or OSPF filter to universally accept updates from all interfaces.

To Protocol Sets a export or import route filter to recognize EGP, RIP, or OSPF as the protocol used for receiving routing information.

Default: RIP

Internet Protocol (IP) Parameters
Parameters and Options

EGP Exterior Gateway Protocol (EGP).

RIP Routing Information Protocol (RIP).

OSPF Open Shortest Path First Protocol (OSPF).

Transit Area	Identifies the OSPF area through which traffic to Neighbor ID is forwarded. Enter the area ID in dotted-decimal notation.
Transmit Broadcast	Identifies the interface-specific (network and/or subnet) transmit broadcast address. Default: All Ones
All Ones	Uses Subnet Mask (or a default mask if a subnet mask is not defined) and places all ones in the host portion of the address.
All Zeros	Uses Subnet Mask (or a default mask if a subnet mask is not defined) and places all zeroes in the host portion of the address.
Explicit Broadcast	Displays a field for entering a broadcast address in dotted-decimal notation. For more information about entering addresses in dotted-decimal notation, refer to Appendix D, "Network Addresses." Note: When an interface serves multiple networks, use an explicit broadcast address, and set the Broadcast Address to 255.255.255.255.
Type	Used with IP import route filters to enable the filtering of two types of OSPF external metrics. Default: External Type 1
External Type 1	Metrics are equivalent to the standard OSPF link state metric.
External Type 2	Metrics are greater than the cost of any path internal to the autonomous system. Using External Type 2 metrics assumes that the inter-autonomous system routing is the major cost of packet routing.
Type	Specifies the type of static route being configured. Default: Static Route
Static Route	Displays a screen for creating a default static route to another router for a specific network or when creating multiple default routes through different routers to a network. Up to four default routes to a specific network can be defined. All interfaces in the static route must support ARP requests.

Adjacent Host Displays a screen for defining an adjacent host route. Adjacent hosts are systems on a locally-attached network. Select Adjacent Host when the network or a particular host does not respond to ARP requests.

UDP Checksum Off Enables or disables UDP checksum processing for the network interface.

Default: No

No Enables checksum processing to provide backward compatibility with UNIX BSD 4.1.

Yes Disables checksum processing.

UDP/TCP Dest Port (high) Sets the upper boundary of the range for filtering a UDP or TCP destination port.

Options ■ Set the Protocol parameter to Ignore to disable the filtering of UDP and TCP ports.

- Leave this field blank and enter the destination port number in the UDP/TCP Dest Port (low) field if you are filtering a single UDP or TCP destination port.
- Enter the highest port number if you are filtering a range of UDP or TCP destination ports.
- Leave this field blank and enter the name of an IP port list in the UDP/TCP Dest Port (low) field if you want to use an IP port list to establish the lower and upper range of UDP or TCP destination ports.

For more information, refer to “UDP/TCP Dest Port (low)” later in this chapter. To learn how to create a Port list, refer to “Port (low)” and “Port (high)” earlier in this chapter.

UDP/TCP Dest Port (low) Sets the lower boundary of the range for filtering a UDP or TCP destination port.

Options ■ Set the Protocol parameter to Ignore to disable the filtering of UDP and TCP ports.

- Enter the port number in this field and leave the UDP/TCP Dest Port (high) field blank if you are filtering a single UDP or TCP destination port.
- Enter the lowest port number in this field and enter the highest destination port number in the UDP/TCP Dest Port (high) field if you are filtering a range UDP or TCP ports.
- If you want to use an IP port list to establish a range of UDP or TCP destination ports, enter the name of the IP port list in this field and leave the UDP/TCP Dest Port (high) field blank.

Internet Protocol (IP) Parameters

Parameters and Options

For more information, refer to “UDP/TCP Dest Port (high)” earlier in this chapter. To learn how to create a Port list, refer to “Port (low)” and “Port (high)” earlier in this chapter.

UDP/TCP Source Port (high)

Sets the upper boundary of the range for filtering a UDP or TCP source port.

- Options
- Set the Protocol parameter to Ignore to disable the filtering of UDP and TCP source ports.
 - Leave this field blank and enter the source port number in the UDP/TCP Source Port (low) field if you are filtering a single UDP or TCP source port.
 - Enter the highest port number if you are filtering a range of UDP or TCP source ports.
 - Leave this field blank and enter the name of an IP port list in the UDP/TCP Source Port (low) field if you want to use an IP port list to establish the lower and upper range of UDP or TCP source ports.

For more information, refer to “UDP/TCP Source Port (low)” later in this chapter. To learn how to create a Port list, refer to “Port (low)” and “Port (high)” earlier in this chapter.

UDP/TCP Source Port (low)

Sets the lower boundary of the range for filtering a UDP or TCP source port.

- Options
- Set the Protocol parameter to Ignore to disable the filtering of UDP and TCP source ports.
 - Enter the port number in this field and leave the UDP/TCP Source Port (high) field blank if you are filtering a single UDP or TCP source port.
 - Enter the lowest port number in this field and enter the highest source port number in the UDP/TCP Source Port (high) field if you are filtering a range UDP or TCP source ports.
 - If you want to use an IP port list to establish a range of UDP or TCP source ports, enter the name of the IP port list in this field and leave the UDP/TCP Source Port (high) field blank.

For more information, refer to “UDP/TCP Source Port (high)” earlier in this chapter. To learn how to create a Port list, refer to “Port (low)” and “Port (high)” earlier in this chapter.

DECnet Parameters

Overview

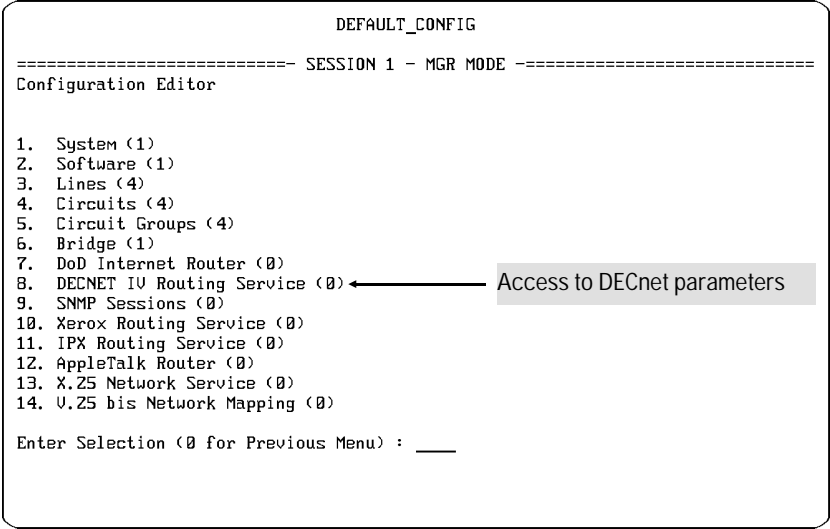


Figure 8-1. Access to DECnet Parameters

DECnet Parameters: Implements the Digital Network Architecture (DNA) session-control layer, which corresponds to the session layer of the International Standards Organization's Open Systems Interconnect (OSI) reference model. (Supports Phase IV DECnet.)

Page	DECnet Parameters
8-4	Action
8-4	Area
8-4	Area (high)
8-4	Area (low)
8-5	Area Max. Cost
8-5	Area Max. Hops
8-5	Auto Enable
8-6	Bcast Routing Timer
—Continued Next Page—	

Page	DECnet Parameters
<i>—Continued From Previous Page—</i>	
8-6	Circuit Group Name
8-6	Cost
8-6	Dest Area (high)
8-7	Dest Area (low)
8-7	Dest Node (high)
8-8	Dest Node (low)
8-8	Effect
8-9	Hello Timer
8-9	List Name
8-9	Max. Area
8-9	Max. Bcast End Nodes
8-9	Max Cost
8-9	Max Hops
8-9	Max. Nodes
8-10	Max. Visits
8-10	Node
8-10	Node (high)
8-10	Node (low)
8-11	Number of Routers
8-11	Packet Type (high)
8-11	Packet Type (low)
8-11	Precedence
8-12	Remote Area
8-12	Remote Node
8-12	Remote WAN Address
8-12	Router Priority
8-12	Source Area (high)
8-12	Source Area (low)
8-13	Source Node (high)
8-13	Source Node (low)
8-14	WAN Protocol

Parameters and Options

Action	<p>Determines the disposition of DECnet packets meeting the conditions set for a filter.</p> <p>Default: Drop</p> <p>Drop Discards a packet meeting the filter rule.</p> <p>Accept Relays a packet meeting the filter rule.</p>
Area	<p>Determines the DECnet ID number of the local area.</p> <p>Default: 1</p> <p>Range: 1 to 63</p>
Area (high)	<p>Sets the upper boundary of the range for filtering DECnet source and destination areas (networks) when creating an Area list.</p> <p>Options</p> <ul style="list-style-type: none">■ Leave this field blank and enter the DECnet ID of the network in the Area (low) field if you are filtering a single DECnet destination or source area.■ Enter the DECnet ID of the highest network in the range if you are filtering a range of DECnet destination or source areas. <p>For more information, refer to “Area (low)” later in this chapter. To learn how to assign an Area list to a filter, refer to “Dest Network (low)” and “Source Area (low)” later in this chapter.</p>
Area (low)	<p>Sets the lower boundary of the range for filtering DECnet source and destination areas (networks) when creating an Area list.</p> <p>Options</p> <ul style="list-style-type: none">■ Enter the DECnet ID of the network in this field and leave the Area (high) field blank if you are filtering a single DECnet destination or source area.■ Enter the DECnet ID in this field and enter the highest DECnet ID in the Area (high) field if you are filtering a range of DECnet destination or source areas. <p>For more information, refer to “Area (high)” earlier in this chapter. To learn how to assign an Area list to a filter, refer to “Dest Network (low)” and “Source Area (low)” later in this chapter.</p>

Area Max. Cost Sets the maximum cost of a path to any area in the network. DECnet determines path costs by summing the individual sequential circuit costs. Circuit costs are decimal values reflecting the relative speed of the transmission media: the faster the media, the lower the cost. Refer to Table 8-1 at the end of this chapter for suggested circuit costs when transmitting media of various clock speeds.

Default: 1008
Range: 1 to 1008

Area Max. Hops Determines the maximum number of DECnet areas (hops) that a packet can pass through before it reaches the area containing its destination end node. In a large network, there are frequently multiple paths to a destination area. The number of routers a packet has to pass through to reach this destination may vary, depending on the path the packet follows. Longer paths mean more routers for the packet to traverse, potentially increasing the packet's travel time. Refer to your network map to determine the longest acceptable path for a packet and count the number of DECnet routers in this path.

Default: 30
Range: 1 to 30

Auto Enable Determines how the DECnet router initializes when the router boots.

The DECnet-specific Auto Enable parameter is protocol-specific and works in conjunction with the global Auto Enable parameter found on the Global Parameters screen. The global Auto Enable parameter influences the DECnet-specific Auto Enable parameter in two ways:

- When the global Auto Enable parameter is set to No, the DECnet router (like all other protocols) is unconditionally disabled; therefore, the DECnet Auto Enable parameter is already disabled.
- When the global Auto Enable parameter is set to Yes, the setting for the DECnet Auto Enable parameter determines whether the DECnet router is automatically enabled or disabled when the router boots.

Default: Yes

Yes Automatically enables DECnet routing if the global Auto Enable parameter is enabled.

No Automatically disables DECnet routing if the global Auto Enable parameter is also enabled. (To enable DECnet routing after the router boots, use the NCL Interpreter's Enable command.)

DECnet Parameters
Parameters and Options

Bcast Routing Timer Sets the maximum number of seconds between routing topology messages issued by the router.

Default: 180

Options 15, 30, 45, 60, 75, 90, 105, 120, 135, 150, 165, 180

Circuit Group Name Identifies the name of a circuit group for DECnet routing. This is one of the circuit groups configured for the Circuit Group menu. For more information about setting circuit group parameters, refer to Chapter 2, "Line, Circuit, and Circuit Group Parameters."

Cost Sets the relative cost of the circuit group. DECnet determines path costs by summing the individual sequential circuit costs. The cost you assign typically should reflect the relative speed of the transmission medium: low costs for high-speed media and high costs for slower media. The DECnet router always selects the circuit(s) with the lowest cost when defining a path, so assigning each circuit a cost is, in effect, a way of assigning it a priority. Assign a higher cost to a circuit not to be used on a regular basis. Your circuit costs should be in line with the settings of the Area Max. Cost and Max. Cost basic parameters. Refer to Table 8-1 at the end of this chapter for suggested circuit costs when transmitting media of various clock speeds.

Default: 10

Range: 1 to 25

Table 8-1. Suggested DECnet Circuit Costs

Transmission Speed	Suggested Circuit Cost	Transmission Speed	Suggested Circuit Cost
10 Mbit/s	3	56 Kbit/s	15
1.54 Mbit/s	7	38.4 Kbit/s	16
1.25 Mbit/s	8	32 Kbit/s	17
833 Kbit/s	9	19.2 Kbit/s	18

Dest Area (high) Sets the upper boundary of the range for filtering a DECnet packet based on the contents of its destination area field.

Options ■ Leave this field blank if you do not want to filter DECnet destination areas.

- Leave this field blank and enter the DECnet ID of the destination area in the Dest Area (low) field if you are filtering a single DECnet destination area.

- Enter the DECnet ID of the highest destination area in the range if you are filtering a range of DECnet destination areas.
- Leave this field blank and enter the name of the Area list in the Dest Area (low) field if you want to use an Area list to establish the upper and lower range of DECnet destination areas.

For additional information, refer to “Dest Area (low)” later in this chapter. For more information about Area lists, refer to “Area (high)” and “Area (low)” earlier in this chapter.

Dest Area (low) Sets the lower boundary of the range for filtering a DECnet packet based on the contents of its destination area field.

- Options
- Leave this field blank if you do not want to filter DECnet destination areas.
 - Enter the DECnet ID of the destination area in this field and leave the Dest Area (high) field blank if you are filtering a single DECnet destination area.
 - Enter the DECnet ID of the lowest destination area in this field and enter the DECnet ID of the highest destination area in the Dest Area (high) field if you are filtering a range of DECnet destination areas.
 - Enter the Area list name in this field and leave the Dest Area (high) field blank if you want to use an Area list to establish the upper and lower range of DECnet destination areas,

For more information, refer to “Dest Area (high)” earlier in this chapter. For more information about Area lists, refer to “Area (high)” and “Area (low)” earlier in this chapter.

Dest Node (high) Sets the upper boundary of the range for filtering a DECnet packet based on the contents of its destination node field.

- Options
- Leave this field blank if you do not want to filter DECnet destination nodes.
 - Leave this field blank and enter the DECnet ID of the destination node in the Dest Node (low) field if you are filtering a single DECnet destination node.
 - Enter the DECnet ID of the highest destination node in the range if you are filtering a range of DECnet destination nodes.
 - Leave this field blank and enter the name of the Node list in the Dest Node (low) field if you want to use a Node list to establish the upper and lower range of DECnet destination nodes,

DECnet Parameters

Parameters and Options

For additional information, refer to “Dest Node (low)” later in this chapter. For more information about Node lists, refer to “Node (high)” and “Node (low)” later in this chapter.

- Dest Node (low)** Sets the lower boundary of the range for filtering a DECnet packet based on the contents of its destination node field.
- Options
- Leave this field blank if you do not want to filter DECnet destination nodes.
 - Enter the DECnet ID of the destination node in this field and leave the Dest Node (high) field blank if you are filtering a single DECnet destination node.
 - Enter the DECnet ID of the lowest destination node in this field and enter the DECnet ID of the highest destination node in the Dest Node (high) field if you are filtering a range of DECnet destination nodes.
 - Enter the Node list name in this field and leave the Dest Node (high) field blank if you want to use a Node list to establish the upper and lower range of DECnet destination nodes.

For more information, refer to “Dest Node (high)” earlier in this chapter. For more information about Node lists, refer to “Node (high)” and “Node (low)” later in this chapter.

Effect Determines whether a packet is dropped or relayed (filtered) based on the contents of a packet field and a range established by a matching set of (low) and (high) parameters. The packet field and corresponding (low) and (high) parameters are listed in the following table:

Packet Field	DECnet Parameter
Destination area	Dest Area (low) and Dest Area (high)
Destination node	Dest Node (low) and Dest Node (high)
Packet Type	Packet Type (low) and Packet Type (high)
Source area	Source Network (low) and (high)
Source node	Source Node (low) and Source Node (high)

Default: Ignore

- Don't Match** Applies the filtering action (drop/accept) if the contents of the packet field do not fall within the range established by the matching set of (low) and (high) filter parameters.
- Ignore** Applies no filtering action if the contents of the packet field falls within the range established by the matching set of (low) and (high) parameters.

DECnet Parameters
Parameters and Options

	Match	Applies the filtering action (drop/accept) if the contents of the packet field falls within the range established by the matching set of (low) and (high) filter parameters.
Hello Timer		Sets the interval in seconds between Hello messages transmitted across the circuit group. Default: 15 Options 15, 30, 45, 60, 600, 1800, 2400, 3600
List Name		Accepts the list name of an Area list, Node list, or Packet Type list.
Max. Area		Determines the number of areas in the extended network. Max. Area identifies the highest area ID number in the extended network. Default: 63 (highly recommended) Range: 1 to 63
Max. Bcast End nodes		Determines the maximum number of end nodes adjacent to (that is, on the same LAN as) a DECnet router on a LAN. The higher the number of adjacent nodes, the greater the impact on network performance and memory utilization. Refer to your network map and find the largest number of adjacent nodes. Default: 95 Range: 1 to 1023 Note: The higher the number of adjacent nodes, the greater the impact on network performance and memory utilization.
Max. Cost		Specifies the maximum cost of a path to any node in the network. This setting must be equal to or greater than Area Max. Cost. Default: 1008 Range: 1 to 1008
Max. Hops		Specifies the maximum number of hops from source to destination. This setting must be equal to or greater than Area Max. Hops. Default: 30 Range: 1 to 30
Max. Nodes		Identifies the highest node number residing in the DECnet area. This setting should be the same for each DECnet router within the network. Default: 1023 (highly recommended) Range: 1 to 1023.

DECnet Parameters

Parameters and Options

Note: All routers within the extended (Phase IV) network must be configured with the same Max. Area and Max. Nodes values.

Max. Visits

Determines packet lifetime by specifying the number of times a packet can pass through the DECnet router. Such a limitation prevents a corrupted packet, or a packet whose destination node has somehow become unreachable, from continuously traveling through the network. This setting must be equal to or greater than Max. Hops.

Default: 63

Range: 1 to 63

Node

Identifies the DECnet ID number (node number) of the router.

Default: 1

Range: 1 to 1023

Note: DECnet Phase IV uses the Area and Node parameters to derive a unique MAC-level address for the DECnet Phase IV router. DECnet first derives a 16-bit binary address by appending Area (expressed as a 6-bit binary value) to Node (expressed as a 10-bit binary value). DECnet then swaps the bytes and converts the resulting 16-bit binary value to 4-digit hexadecimal AA 00 04 (the Digital Equipment Corporation vendor code) 00 (a pad to ensure a 12-digit hexadecimal address). Thus, node 32 in area 256 equates to the MAC address AA 00 04 00 00 81.

Node (high)

Sets the upper boundary of the range for filtering DECnet source and destination nodes when creating an Node list.

- Options
- Leave this field blank and enter the DECnet ID of the node in the Node (low) field if you are filtering a single DECnet destination or source node.
 - Enter the DECnet ID of the highest node in the range if you are filtering a range of DECnet destination or source nodes.

For more information, refer to “Node (low)” later in this chapter. To learn how to assign an Node list to a filter, refer to “Dest Node (low)” and “Source Node (low).”

Node (low)

Sets the lower boundary of the range for filtering DECnet source and destination nodes when creating an Node list.

- Options
- Enter the DECnet ID of the node in this field and leave the Node (high) field blank if you are filtering a single DECnet destination or source node.
 - Enter the DECnet ID of the lowest node in this field and enter the DECnet ID of highest destination or source node (network) in the Node (high) field if you are filtering a range of DECnet destination or source nodes.

For more information, refer to “Node (high)” earlier in this chapter. To learn how to assign an Node list to a filter, refer to “Dest Node (low)” and “Source Node (low).”

Number of Routers Identifies the number of adjacent DECnet routers associated with this circuit group. Refer to your network map to determine this number.

Default: 6
Range: 1 to 33

Packet Type (high) Sets the upper boundary of the range for filtering DECnet Packet Types when creating a Packet Type filter or Packet Type list.

- Options
- Leave this field blank and enter the packet type number in the Packet Type (low) field if you are filtering a single DECnet packet type number,
 - Enter the highest packet type number in the range if you are filtering a range of DECnet packet type numbers.
 - Leave this field blank and enter the name of a Packet Type list in the Packet Type (low) field if you want to establish a range of packet types using a filter list.

For more information, refer to “Packet Type (low)” later in this chapter.

Packet Type (low) Sets the lower boundary of the range for filtering DECnet packet type numbers when creating a Packet Type filter or Packet Type list.

- Options
- Enter the packet type number in this field and leave the Packet Type (high) field blank if you are filtering a single DECnet packet type number.
 - Enter the lowest packet type number in this field and enter the highest packet type number in the Packet Type (high) field if you are filtering a range of DECnet packet type numbers.
 - Enter the name of a Packet Type list in this field and leave the Packet Type (high) field blank if you want to establish the range of Packet Types using a filter list.

For more information, refer to “Packet Type (high)” earlier in this chapter.

Precedence Assigns a priority value to the filter—the higher the precedence, the greater the priority. You can construct up to 31 filters per DECnet circuit group. The Precedence value is used when an incoming packet meets multiple filter rules. In such an instance, the filter with the highest priority is applied to the frame.

Default: 31
Range: 1 to 31

DECnet Parameters

Parameters and Options

Note: In the event of two filters with equal precedence, the first configured filter takes precedence over the second filter.

Remote Area	Identifies the area address of the remote target. Default: 63 Range: 1 to 63
Remote Node	Identifies the node address of the remote target. Default = 1023 Range: 1 to 1023
Remote WAN Address	Identifies the protocol address of the remote target. Enter the remote target's X.25, frame relay, or SMDS address.
Router Priority	Determines the designated router on a LAN segment. The router with the highest priority becomes the designated router. If more than one router shares the same priority, the router with the highest node number becomes the designated router. Default: 64 Range: 1 to 127
Source Area (high)	Sets the upper boundary of the range for filtering a DECnet packet based on the contents of its source area field. Options <ul style="list-style-type: none">■ Leave this field blank if you do not want to filter DECnet packets based on the source area field.■ Leave this field blank and enter the DECnet ID of the source area in the Source Area (low) field if you are filtering a single DECnet source area.■ Enter the DECnet ID of the highest source area in the range if you are filtering a range of DECnet source areas.■ Leave this field blank and enter the name of the Area list in the Source Area (low) field if you want to use an Area list to establish the upper and lower range of DECnet source areas. <p>For additional information, refer to "Source Area (low)" later in this chapter. For more information about Area lists, refer to "Area (high)" and "Area (low)" earlier in this chapter.</p>
Source Area (low)	Sets the lower boundary of the range for filtering a DECnet packet based on the contents of its source area field. Options <ul style="list-style-type: none">■ Leave this field blank if you do not want to filter DECnet source areas.

- Enter the DECnet ID of the source area in this field and leave the Source Area (high) field blank if you are filtering a single DECnet source area.
- Enter the DECnet ID of the lowest source area in this field and enter the DECnet ID of the highest source area in the Source Area (high) field if you are filtering a range of DECnet source areas.
- Enter the Area list name in this field and leave the Source Area (high) field blank if you want to use an Area list to establish the upper and lower range of DECnet source areas.

For more information, refer to “Source Area (high)” earlier in this chapter. For more information about Area lists, refer to “Area (high)” and “Area (low)” earlier in this chapter.

Source Node (high) Sets the upper boundary of the range for filtering a DECnet packet based on the contents of its source node field.

- Options
- Leave this field blank if you do not want to filter DECnet source nodes.
 - Leave this field blank and enter the node number of the source area in the Source Node (low) field if you are filtering a single DECnet source node.
 - Enter the node number of the highest source node in the range if you are filtering a range of DECnet source areas.
 - Leave this field blank and enter the name of the Area list in the Source Node (low) field if you want to use an Area list to establish the upper and lower range of DECnet source nodes.

For additional information, refer to “Source Node (low)” later in this chapter. For more information about Area lists, refer to “Area (high)” and “Area (low)” earlier in this chapter.

Source Node (low) Sets the lower boundary of the range for filtering a DECnet packet based on the contents of its source node field.

- Options
- Leave this field blank if you do not want to filter DECnet source nodes.
 - Enter the node number of the source node in this field and leave the Source Node (high) field blank if you are filtering a single DECnet source node.
 - Enter the node number of the lowest source node in this field and enter the node number of the highest source node in the Source Node (high) field if you are filtering a range of DECnet source nodes.

DECnet Parameters

Parameters and Options

- Enter the Area list name in this field and leave the Source Node (high) field blank if you want to use an Area list to establish the upper and lower range of DECnet source nodes.

For more information, refer to “Source Node (high)” earlier in this chapter. For more information about Area lists, refer to “Area (high)” and “Area (low)” earlier in this chapter.

WAN Protocol

Identifies the WAN protocol for the circuit providing service to the remote target.

Default:

Frame Relay Frame Relay circuits provide a transmission channel between the router and a frame relay network. The transmission channel supports multiple protocols.

SMDS Switched Multi-megabit Data Service (SMDS) circuits provide a transmission channel over V.35 (synchronous media) between the router and an SMDS data service unit (DSU) or switch.

X.25 X.25 packet switched circuits three levels of X.25 service—X.25 DDN, X.25 PDN, and X.25 PPP (Point-to-Point Protocol). For additional information about the services supported by X.25 packet switched circuits, refer to Chapter 13, “X.25 Parameters.”

SNMP Agent Parameters

Overview

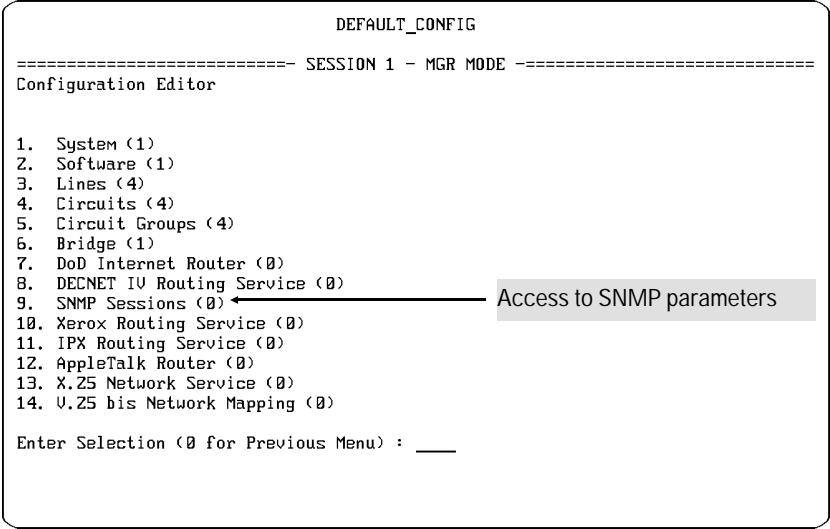


Figure 9-1. Access to SNMP Parameters

SNMP Parameters Enable the Simple Network Management Protocol (SNMP) agent, which allows the router to respond to queries from a network manager, and to report certain router events such as reinitializations and disabled interfaces.

Page	SNMP Parameters
9-3	Community Name
9-3	Event Filter Level
9-3	Node Address
9-4	Send Event Messages As Traps
9-4	Session Mode
9-4	Session Type

Parameters and Options

Community Name

Serves as a password for network managers (“application entities” in SNMP terminology) to have access to the SNMP agent on this router. The SNMP application running on the network management node configures one or more community names the node may use in its queries to agents. Each query uses one name. Other nodes may be configured to use the same community name. A community may have members in common with other communities, and may be a subset or superset of other communities.

Most network management schemes use the community name “Public”. Some schemes set up other specific community names.

- Options ■ If you have SNMP network management stations on your extended network, enter one of the community names used—“Public” or another specific name.
- If you do not have SNMP network management stations on your extended network, HP recommends that you enter a community name even if no other nodes will use it. This allows you to use the Rget commands from the Network Control Language (NCL) Interpreter on this router’s console to check its forwarding and routing tables and other MIB variables. If you enter Public, the Rget commands will default the community name parameter so that you need not type it for every command. Or you can assign some other name—which must be typed for every Rget command—to provide some security against other remote access to the agent.

Note: If you leave the Community Name field blank, as it is by default, there will be no access for queries by either this console or any remote network managers, even if you complete the remainder of this screen so that the agent is “enabled”. You must enter a name to have access.

Event Filter Level

Determines which event messages are transmitted as traps to SNMP application entities. The Event Filter Level parameter is displayed when the Trap option is selected for the Session Type parameter.

- Options ■ Skip this field if enterprise-specific trapping is disabled.
- Select the appropriate filter level if you have enabled enterprise-specific trapping. For information about selecting a filter level, refer to “Filter Level” later in this chapter.

Node Address

Grants SNMP agent access to the member of Community Name whose IP address you specify.

SNMP Agent Parameters

Parameters and Options

- Options
- Leave this field blank if no access of any type is allowed by either this console or any remote network managers, even if other parameters are set to “enable” the agent. You must enter an address to have access.
 - Enter the address of a network management station in dotted-decimal notation. To have access to this router’s agent, a station’s IP address must match the setting of this parameter and, in the case of queries (not receiving trap reports), the community name it uses must match the setting of Community Name.
 - Enter the IP address 0.0.0.0 if you want to permit any network entity using Community Name to query the agent. This setting is valid only for records with Session type of Regular (queries).

Note: In the configuration of a record for a Session type of Trap, you must enter the IP address of the management station to receive trap reports. If you leave the Node Address field blank, as it is by default, no access of any type will be allowed by either this console or any remote network managers, even if other parameters are set to “enable” the agent. You must enter an address to have access.

Send Event Messages As Traps

Enables or disables the generation of enterprise-specific traps. The Send Event Messages As Traps parameter is displayed when the Trap option is selected for the Session Type parameter. With enterprise-specific trapping enabled, some or all of the event messages generated by the node are encapsulated within an SNMP protocol data unit and sent as traps to SNMP application entities.

Default: No

Yes Enables enterprise-specific trapping.

No Disable enterprise-specific trapping.

Session Mode

Determines the SNMP management node’s access privileges to the router’s MIB.

Default: Read

Read Reads MIB data only.

Read/Write Reads and writes MIB data.

Session type

Identifies the types of data exchange—management queries or event reporting—between the SNMP agent and the SNMP management nodes. Some network manager applications provide their users both types of data; in this case you will want to set one of the session types for this access record, and then configure another access record with the other type. The event-reporting types of exchanges are not queries by the managing node, so it doesn’t matter what community name is set for the record using this session type, called “Trap”.

Default: Regular

SNMP Agent Parameters Parameters and Options

Regular Allows the router's agent to respond to queries.

Trap Allows the router's agent to generate unsolicited asynchronous notifications of significant events, such as booting and enabling or disabling interfaces.

Note: Additional fields are displayed when you select the Session Type. For more information about the additional fields, refer to “Send Event Messages As Traps” and “Event Filter Level.”

Xerox Network Systems (XNS) Router Parameters

Overview

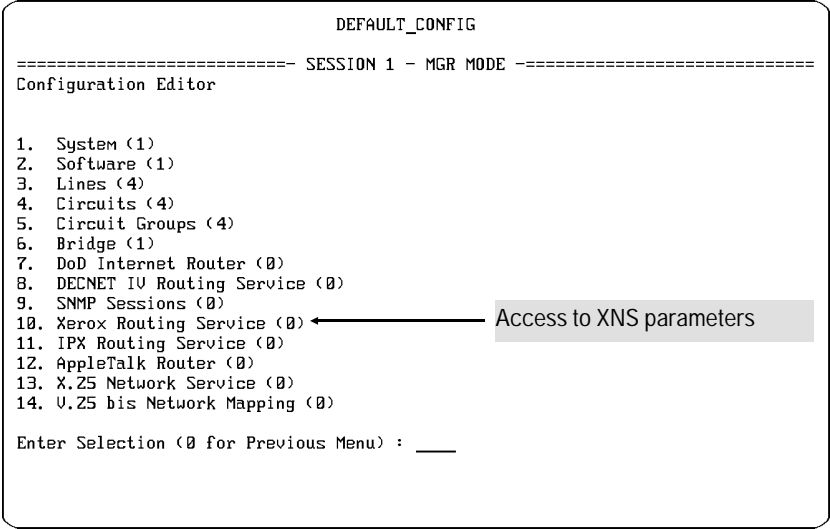


Figure 10-1. Access to XNS Parameters

XNS Parameters: Enable use of the Xerox Network Systems Internet Transport Protocols (XNS) suite for establishing routing over Ethernets and across point-to-point lines.

Page	XNS Parameters
10-4	Action
10-4	Auto Enable
10-4	Circuit Group
10-	Checksums On
10-5	Dest Host (high)
10-5	Dest Host (low)
10-5	Dest Network (high)
10-6	Dest Network (low)
10-6	Dest Socket (high)
10-7	Dest Socket (low)
—Continued on next page—	

Page	XNS Parameters
<i>—Continued from preceeding page—</i>	
10-7	Effect
10-8	Host lists
10-8	Host (high)
10-8	Host (low)
10-8	Host Number
10-8	Network Number (high)
10-9	Network Number (low)
10-9	Network lists
10-9	Network Number
10-9	Next Hop Host
10-9	Next Hop Net
10-9	Packet Type (high)
10-10	Packet Type (low)
10-10	Precedence
10-10	RIP Interface Cost
10-10	RIP Listen
10-11	RIP Supply
10-11	Socket (high)
10-11	Socket (low)
10-11	Source Route (Token Ring)
10-12	Source Host (high)
10-12	Source Host (low)
10-12	Source Network (high)
10-12	Source Network (low)
10-13	Source Socket (high)
10-14	Source Socket (low)
10-14	Target Net
10-14	XNS Filter-rule-B

Parameters and Options

Action	Determines the disposition of packets meeting the filter rule: Default: Drop
	Accept Relays a packet meeting the filter rule.
	Accept and Log Relays a packet meeting the filter rule and records an event message in the event log.
	Drop Discard a packet meeting the filter rule.
Drop and Log Drop	Discards a packet meeting the filter rule and records an events message in the event log.
Auto Enable	Determines the initial state of the XNS router. The XNS-specific Auto Enable parameter works in conjunction with the global Auto Enable parameter found on the Global Parameters screen in the System configuration menu to enable or disable XNS routing when the router boots.
	<ul style="list-style-type: none">■ When the global Auto Enable parameter is set to No, the XNS router (like all other protocols) is unconditionally disabled.■ When the global Auto Enable parameter is set to Yes, the setting of the XNS-specific Auto Enable parameter determines whether the XNS router is automatically enabled.
	Default: Yes
	No Disables XNS routing.
Yes	Enables XNS routing if the global Auto Enable parameter is also enabled.
Circuit Group	Identifies the circuit group providing an interface between the router and the XNS network.
Checksums On	Enables or disables checksum processing. When check summing is enabled, the router verifies the Internet packet checksum when the packet arrives at the router, and generates a new checksum when relaying the packet to its destination. Check summing is ordinarily be enabled for the XNS protocol.
	Default: No

No Disables check summing.

Yes Enables check summing.

Dest Host (high) Sets the high boundary of the range for filtering an XNS packet based on the contents of its destination host field.

- Options ■ Leave this field blank if you do not want to filter XNS destination hosts.
- Leave this field blank and enter the XNS host number in the Dest Host (low) field if you are filtering a single XNS destination host,
 - Enter the highest XNS host number in the range if you are filtering a range of XNS destination hosts.
 - Leave this field blank and enter the name of the Host list in the Dest Host (low) field if you want to use a Host list to establish the upper and lower range of XNS destination host numbers.

For additional information, refer to “Dest Host (low)” later in this chapter. For more information about Host lists, refer to “Host (high)” and “Host (low)” later in this chapter.

Dest Host (low) Sets the lower boundary of the range for filtering an XNS packet based on the contents of its destination host field.

- Options ■ Leave this field blank if you do not want to filter XNS destination hosts.
- Enter the XNS host number in this field and leave the Dest Host (high) field blank if you are filtering a single XNS destination host.
 - Enter the lowest XNS host number in this field and enter the highest host number in the Dest Host (high) field if you are filtering a range of XNS destination hosts.
 - Enter the Host list name in this field and leave the Dest Host (high) field blank if you want to use a Host list to establish the upper and lower range of destination host numbers.

For additional information, refer to “Dest Host (high)” earlier in this chapter. For more information about Host lists, refer to “Host (high)” and “Host (low)” later in this chapter.

Dest Network (high) Sets the high boundary of the range for filtering an XNS packet based on the contents of its destination network field.

- Options ■ Leave this field blank if you do not want to filter XNS destination networks.

Xerox Network Systems (XNS) Router Parameters

Parameters and Options

- Leave this field blank and enter the XNS network number in the Dest Network (low) field if you are filtering a single XNS destination network numbers.
- Enter the highest XNS network number in the range if you are filtering a range of XNS destination network number.
- Leave this field blank and enter the name of the Network list in the Dest Network (low) field if you want to use a Network list to establish the upper and lower range of XNS destination network numbers.

For additional information, refer to “Dest Network (low)” later in this chapter. For more information about Network lists, refer to “Network Number (high)” and “Network Number (low)” later in this chapter.

Dest Network (low) Sets the lower boundary of the range for filtering an XNS packet based on the contents of its destination network field.

- Options
- Leave this field blank if you do not want to filter XNS destination networks.
 - Enter the XNS network number in this field and leave the Dest Network (high) field blank if you are filtering a single XNS destination network number.
 - Enter the lowest XNS network number in this field and enter the highest network number in the Dest Network (high) field if you are filtering a range of XNS destination network numbers.
 - Enter the Host list name in this field and leave the Dest Host (high) field blank if you want to use a Host list to establish the upper and lower range of destination host numbers.

For additional information, refer to “Dest Network (high)” earlier in this chapter. For more information about Network lists, refer to “Network Number (high)” and “Network Number (low)” later in this chapter.

Dest Socket (high) Sets the high boundary of the range for filtering an XNS packet based on the contents of its destination socket field.

- Options
- Leave this field blank if you do not want to filter XNS destination sockets.
 - Leave this field blank and enter the XNS socket number in the Dest Socket (low) field if you are filtering a single XNS destination socket.
 - Enter the highest XNS socket number in the range if you are filtering a range of XNS destination sockets.

- Leave this field blank and enter the name of the Socket list in the Dest Socket (low) field if you want to use a Socket list to establish the upper and lower range of XNS destination socket numbers.

For additional information, refer to “Dest Socket (low)” later in this chapter. For more information about Socket lists, refer to “Socket (high)” and “Socket (low)” later in this chapter.

Dest Socket (low) Sets the lower boundary of the range for filtering an XNS packet based on the contents of its destination socket field.

- Options
- Leave this field blank if you do not want to filter XNS destination sockets.
 - Enter the XNS socket number in this field and leave the Socket Host (high) field blank if you are filtering a single XNS destination socket.
 - Enter the lowest XNS socket number in this field and enter the highest socket number in the Socket Host (high) field if you are filtering a range of XNS destination sockets.
 - Enter the Socket list name in this field and leave the Dest Socket (high) field blank if you want to use a Socket list to establish the upper and lower range of destination socket numbers.

For additional information, refer to “Socket Host (high)” earlier in this chapter. For more information about Host lists, refer to “Socket (high)” and “Socket (low)” later in this chapter.

Effect Determines whether a packet is dropped or relayed (filtered) based on the contents of a packet field and a range established by a matching set of (low) and (high) parameters. The packet field and corresponding (low) and (high) parameters are listed in the following table:

Packet Field	XNS Parameter
Destination Host	Dest Host (low) and Dest Host (high)
Destination Network	Dest Network (low) and Dest Network (high)
Destination Socket	Dest Socket (low) and Dest Socket (high)
Packet Type	Packet Type (low) and Packet Type (high)
Source Host	Source Host (low) and Source Host (high)
Source Network	Source Network (low) and Source Network (high)
Source Socket	Source Socket (low) and Source Socket (high).

Default: Ignore

Don't Match Applies the filtering action (drop/accept/log) if the contents of the packet field do not fall within the range established by the matching set of (low) and (high) filter parameters.

Xerox Network Systems (XNS) Router Parameters

Parameters and Options

Ignore	Applies no filtering action if the contents of the packet field falls within the range established by the matching set of (low) and (high) parameters..
Match	Applies the filtering action (drop/accept/log) if the contents of the packet field falls within the range established by the matching set of (low) and (high) parameters.
Host lists	Displays parameters for setting the lower and upper boundaries of the range for a Host list. For more information, refer to "Host (low)" and "Host (high)."
Host (high)	Sets the upper boundary of the range for filtering XNS source or destination hosts when creating a Host list.
Options	<ul style="list-style-type: none">■ Leave this field blank and enter the XNS host number in the Host (low) field if you are filtering a single XNS source or destination host.■ Enter the highest XNS host number in the range if you are filtering a range of XNS source or destination hosts. <p>For additional information, refer to "Host (low)" later in this chapter. To learn how to assign a Host list to a filter, refer to "Dest Host (low)" and "Source Host (low)" later in this chapter.</p>
Host (low)	Sets the lower boundary of the range for filtering XNS source or destination hosts when creating a Host list.
Options	<ul style="list-style-type: none">■ Enter the XNS host number in this field and leave the Host (high) field blank if you are filtering a single XNS source or destination host.■ Enter the lowest XNS host number in this field and enter the highest host number in the Host (high) field if you are filtering a range of XNS source or destination hosts. <p>For additional information, refer to "Host (high)" earlier in this chapter. To learn how to assign a Host list to a filter, refer to "Dest Host (low)" and "Source Host (low)" later in this chapter.</p>
Host Number	<p>Assigns a unique XNS physical host address to the router. Your HP router was shipped with a unique, universally-administered 48-bit station address for each port stored in read-only memory (ROM).</p> <p>Default: Blank (assigns the factory-default station address).</p>
Network Number (high)	Sets the upper boundary of the range for filtering XNS source or destination networks when creating a Network list.

- Options ■ Leave this field blank and enter the XNS network number in the Network Number (low) field if you are filtering a single XNS source or destination network.
- Enter the XNS highest network number in the range if you are filtering a range of XNS source or destination networks.

For additional information, refer to “Network Number (low)” later in this chapter. To learn how to assign a Network list to a source or destination network filter, refer to “Dest Network (low)” and “Source Network (low)” later in this chapter.

Network Number (low) Sets the lower boundary of the range for filtering XNS source or destination networks when creating a Network list.

- Options ■ Enter the XNS network number in this field and leave the Network Number (high) field blank if you are filtering a single XNS source or destination network.
- Enter the lowest XNS network number in this field and enter the highest network number in the Network Number (high) field if you are filtering a range of XNS source or destination networks.

For additional information, refer to “Network Number (high)” earlier in this chapter. To learn how to assign a Network list to a source of destination network filter, refer to “Dest Network (high)” and “Dest Network (low)” later in this chapter.

Network lists Displays additional parameters for creating a Network list. For additional information about creating a Network list, refer to “Network Number (low)” and “Network Number (high)” earlier in this chapter. For information about creating a filter with a Network list, refer to “Dest Network (low)” and “Dest Network (high)” earlier in this chapter.

Network Number Identifies the XNS network for interfacing connections. All XNS networks are identified by a 32-bit network number assigned by the local network administrator.

Next Hop Host Identifies the next-hop router by its 48-bit XNS host address. You must acquire the host number—often identical to one of the station (MAC) addresses actually being used on that router which may be reset from the user-configured host number or factory-configured station address by various other options and protocols. Type the XNS host address in 12-character hexadecimal format.

Next Hop Net Assigns a network number to the next router in the hop sequence.

Packet Type (high) Sets the upper boundary of the range for filtering XNS packet type numbers when creating a Packet Type filter or Packet Type list.

- Options ■ Leave this field blank and enter the XNS packet type number in the Packet Type (low) field if you are filtering a single XNS packet type number.

Xerox Network Systems (XNS) Router Parameters

Parameters and Options

- Enter the highest XNS packet type number in the range if you are filtering a range of XNS packet type numbers.
- Enter the list name in the Packet Type (low) field and leave this field blank if you are creating an XNS Packet Type filter and want to create a range of packet type numbers with a filter list.

For additional information, refer to “Packet Type (low)” later in this chapter.

Packet Type (low) Sets the upper boundary of the range for filtering DECnet packet type numbers when creating a Packet Type filter or Packet Type list.

- Options
- Enter the XNS packet type number in this field and leave the Packet Type (high) field blank if you are filtering a single XNS packet type number.
 - Enter the lowest XNS packet type number in this field and enter the highest packet type number in the Packet Type (high) field if you are filtering a range of XNS packet type numbers.
 - Enter the list name in this field and leave the Packet Type (high) field blank. if you are creating an XNS Packet Type filter and want to establish the range of packet type numbers with a filter list.

For additional information, refer to “Packet Type (high)” earlier in this chapter.

Precedence Assigns a priority value to the filter—the higher the precedence, the greater the priority. You can construct up to 31 filters per XNS circuit group. The Precedence value is used when an incoming packet meets multiple filter rules. In such an instance, the filter with the highest priority is applied to the frame.

Default: 31
Range: 1 to 31

Note: When two filters have equal precedence, the first configured filter takes precedence over the second filter.

RIP Interface Cost Sets the cost for each router hop.

Default: 1

RIP Listen Enables or disables the RIP listen function.

Default:

No Sets the router to ignore RIP updates received from neighboring routers.

	<p>Yes Sets the router to add routes received in RIP updates from neighboring routers to its own internal routing table.</p>
RIP Supply	<p>Enables or disables the RIP supply function, determining whether the XNS router transmits periodic RIP updates to neighboring routers across the Circuit Group.</p> <p>Default: Yes</p> <p>No Prevents the router from transmitting updates. Use this setting to inactivate RIP for circuit groups configured with static routes.</p> <p>Yes Allows the router to transmit RIP updates.</p>
Socket (high)	<p>Sets the upper boundary of the range for filtering XNS source or destination sockets when creating a Socket list.</p> <p>Options</p> <ul style="list-style-type: none">■ Leave this field blank and enter the XNS socket number in the Socket (low) field if you are filtering a single XNS source or destination socket.■ Enter the highest XNS socket number in the range if you are filtering a range of XNS source or destination sockets, <p>For additional information, refer to “Socket (low)” later in this chapter. To learn how to assign a Socket list to a filter, refer to “Dest Socket (low)” and “Source Socket (low).”</p>
Socket (low)	<p>Sets the lower boundary of the range for filtering XNS source or destination sockets when creating a Socket list.</p> <p>Options</p> <ul style="list-style-type: none">■ Enter the XNS socket number in this field and leave the Socket (high) field blank if you are filtering a single XNS source or destination socket.■ Enter the lowest XNS socket number in this field and enter the highest socket number in the Socket (high) field if you are filtering a range of XNS source or destination sockets. <p>For additional information, refer to “Socket (high)” earlier in this chapter. To learn how to assign a Socket list to a filter, refer to “Dest Socket (low)” and “Source Socket (low).”</p>
Source Route (Token Ring)	<p>Enables or disables source routing over token ring media for the interface being defined. Source route functionality allows the XNS router to transmit and receive frames over a token ring network extended with source routing bridges. For the HP router TR, this option can be set to either Yes or No, depending on whether or not you want to use the token ring capability.</p> <p>Default: No</p>

Xerox Network Systems (XNS) Router Parameters
Parameters and Options

No Disables source routing over token ring media.

Yes Enables source routing over token ring media.

Note: If the router does not have a token ring port, always set this parameter to No.

Source Host (high) Sets the upper boundary of the range for filtering an XNS packet based on the contents of its source host field.

- Options ■ Leave this field blank if you do not want to filter XNS source hosts.
- Leave this field blank and enter the XNS host number in the Source Host (low) field if you are filtering a single XNS source host.
 - Enter the highest XNS host number in the range if you are filtering a range of XNS source hosts.
 - Leave this field blank and enter the name of the Host list in the Source Host (low) field if you want to use a Host list to establish the upper and lower range of XNS source host numbers.

For additional information, refer to “Source Host (low)” later in this chapter. For more information about Host lists, refer to “Host (high)” and “Host (low)” later in this chapter.

Source Host (low) Sets the lower boundary of the range for filtering an XNS packet based on the contents of its source host field.

- Options ■ Leave this field blank if you do not want to filter XNS source hosts.
- Enter the XNS host number in this field and leave the Dest Host (high) field blank if you are filtering a single XNS source host.
 - Enter the lowest XNS host number in this field and enter the highest host number in the Source Host (high) field if you are filtering a range of XNS destination hosts.
 - Enter the Host list name in this field and leave the Source Host (high) field blank if you want to use a Host list to establish the upper and lower range of source host numbers.

For additional information, refer to “Source Host (high)” earlier in this chapter. For more information about Host lists, refer to “Host (high)” and “Host (low)” later in this chapter.

Source Network (high) Sets the upper boundary of the range for filtering an XNS packet based on the contents of its source network field.

Options ■ Leave this field blank if you do not want to filter XNS source networks.

- Leave this field blank and enter the XNS network number in the Source Network (low) field if you are filtering a single XNS source network.
- Enter the highest XNS host number in the range if you are filtering a range of XNS source networks.
- Leave this field blank and enter the name of the Network list in the Source Network (low) field if you want to use a Network list to establish the upper and lower range of XNS source network numbers.

For additional information, refer to “Source Network (low)” later in this chapter. For more information about Host lists, refer to “Network Number (high)” and “Network Number (low)” earlier in this chapter.

Source Network (low) Sets the lower boundary of the range for filtering an XNS packet based on the contents of its source network field.

Options ■ Leave this field blank if you do not want to filter XNS source networks.

- Enter the XNS network number in this field and leave the Source Network (high) field blank if you are filtering a single XNS source network.
- Enter the lowest XNS network number in this field and enter the highest host number in the Source Network (high) field if you are filtering a range of XNS source networks.
- Enter the Network list name in this field and leave the Source Network (high) field blank if you want to use a Network list to establish the upper and lower range of network numbers.

For additional information, refer to “Source Network (high)” earlier in this chapter. For more information about Network lists, refer to “Network Number (high)” and “Network Number (low)” earlier in this chapter.

Source Socket (high) Sets the upper boundary of the range for filtering an XNS packet based on the contents of its source socket field.

Options ■ Leave this field blank if you do not want to filter XNS source sockets.

- Leave this field blank and enter the XNS socket number in the Source Socket (low) field if you are filtering a single XNS source socket.
- Enter the highest XNS socket number in the range if you are filtering a range of XNS source sockets.

Xerox Network Systems (XNS) Router Parameters

Parameters and Options

- Leave this field blank and enter the name of the Socket list in the Source Socket (low) field if you want to use a Socket list to establish the upper and lower range of XNS socket numbers.

For additional information, refer to “Source Socket (low)” later in this chapter. For more information about Socket lists, refer to “Socket (high)” and “Socket (low)” earlier in this chapter.

Source Socket (low) Sets the lower boundary of the range for filtering an XNS packet based on the contents of its source socket field.

Options ■ Leave this field blank if you do not want to filter XNS source sockets.

- Enter the XNS socket number in this field and leave the Source Socket (high) field blank if you are filtering a single XNS source socket.
- Enter the lowest XNS socket number in this field and enter the highest socket number in the Source Socket (high) field if you are filtering a range of XNS source sockets.
- Enter the Socket list name in this field and leave the Source Socket (high) field blank if you want to use a Socket list to establish the upper and lower range of socket numbers.

For additional information, refer to “Source Socket (high)” earlier in this chapter. For more information about Socket lists, refer to “Socket (high)” and “Socket (low)” earlier in this chapter.

Target Net Identifies a specific destination XNS network in an internet. All XNS networks are identified by a 32-bit network number assigned by the local network administrator. Type in the network number in an eight-character hexadecimal format.

IPX Protocol Parameters

Overview

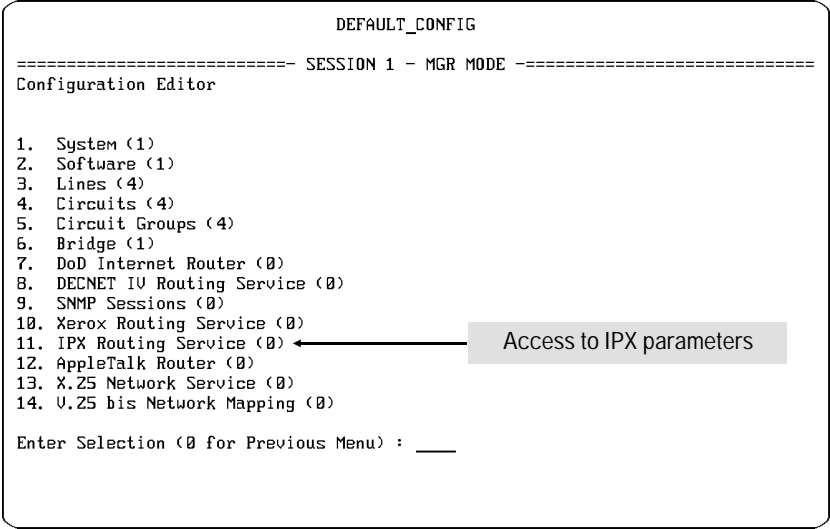


Figure 11-1. Access to IPX Parameters

IPX Parameters: Enable use of the Internet Packet Exchange Protocol (IPX) in support of a wide variety of LAN topologies and media.

Page	IPX Parameters
11-5	Accept NETBIOS Bcasts from net
11-5	Action
11-5	Auto Enable
11-6	Circuit Group
11-6	Deliver NETBIOS Bcasts to net
11-6	Dest Host (high)
11-6	Dest Host (low)
11-7	Dest Network (Hex)
11-7	Dest Network (high)
11-7	Dest Network (low)
—Continued Next Page—	

Page	IPX Parameters
<i>—Continued from previous page—</i>	
11-8	Dest Socket (high)
11-8	Dest Socket (low)
11-9	Effect
11-9	Encapsulation Type
11-10	Host lists
11-10	Host Number (high)
11-10	Host Number (low)
11-11	Internal Network Number
11-11	Internal Router Name
11-11	IPXWAN
11-11	List Name
11-11	Network lists
11-11	Network Number
11-11	Network Number (high)
11-12	Network Number (Hex)
11-12	Network Number (low)
11-12	NETBIOS Resource Name
11-12	Next Hop Host
11-12	Next Hop Net
11-12	Packet type lists specify
11-12	Packet Type (high)
11-13	Packet Type (low)
11-13	Precedence
11-13	Random load balancing
11-14	RIP Interface Cost
11-14	RIP Listen
11-14	RIP Supply
11-14	RIP Table Cost
11-14	RIP and SAP split horizon
11-15	SAP driven RIP supply
11-15	Server Name
11-15	Server Type (Hex)
11-15	Socket (high)
11-16	Socket (low)
<i>—Continued Next Page—</i>	

IPX Protocol Parameters

Overview

Page	IPX Parameters
<i>—Continued From Previous Page—</i>	
11-16	Source Host (high)
11-16	Source Host (low)
11-17	Source Network (high)
11-17	Source Network (low)
11-18	Source Route (Token Ring)
11-18	Source Socket (high)
11-18	Source Socket (low)
11-19	Target Net
11-19	WAN SAP Period

Parameters and Options

Accept NETBIOS Bcasts from net		Enables or disables “local” client access to remote NETBIOS servers. Default: Yes
	No	Disables client access to the internet and effectively restricts NETBIOS clients to those services offered by local servers.
	Yes	Enables NETBIOS client access to the internet; NETBIOS broadcasts generated by clients are broadcast across all IPX router interfaces (save those specifically configured not to accept NETBIOS broadcasts).
Action		Determines the outbound filtering action applied to a SAP (Service Advertising Protocol) filter when the contents of a packet field fall within the range established by a matching set of (low) and (high) parameters. Default: Drop (for most filters) Default: Advertise (for Network Number/Server Type filters) Action parameter options are not the same for all filters. The following options may be available depending on the type of filter you are creating.
	Drop	Discards a packet meeting the filter rule.
	Accept	Relays a packet meeting the filter rule.
	Advertise	Transmits SAP (Service Advertising Protocol) advertisements among those servers meeting the filter rule.
	Ignore	Drops those servers not meeting the filter rule for SAP advertisements and does not advertise those services out of the interface.
Auto Enable		Enables or disables the IPX router. The IPX-specific <code>Auto Enable</code> parameter works in conjunction with the global <code>Auto Enable</code> parameter to enable or disable the IPX application software when the node boots. ■ When the global <code>Auto Enable</code> parameter is set to No, the IPX router (as are all other application software modules) is unconditionally disabled. If you have set the global <code>Auto Enable</code> parameter to No. You will subsequently need to enable the IPX router manually with the NCL Interpreter after the node boots.

IPX Protocol Parameters

Parameters and Options

- When the global Auto Enable is set to Yes, the IPX router (as are all other application software modules) is conditionally enabled—the IPX router can be enabled or disabled by setting the IPX-specific Auto Enable parameter.

Default: Yes

No Disables the IPX router. You will need to re-enable the IPX router manually with the NCL Interpreter after the node boots.

Yes Enables the IPX router.

Circuit Group Identifies the circuit group providing a connection between the node and IPX network.

Deliver NETBIOS Bcasts to net Enables or disables remote access to “local” servers.

Default: Yes

No Disables broadcasting and effectively isolates local NETBIOS servers from remote clients.

Yes Enables the delivery of received NETBIOS broadcasts across the local interface, thus making local NETBIOS servers available to remote users.

Dest Host (high) Sets the upper boundary of the range for filtering an IPX packet based on the contents of its destination host field.

- Options
- Leave this field blank if you do not want to filter IPX destination hosts.
 - Leave this field blank and enter the IPX host number in the Dest Host (low) field if you are filtering a single IPX destination host.
 - Enter the highest IPX host number in the range if you are filtering a range of IPX destination hosts.
 - Leave this field blank and enter the name of the Host list in the Dest Host (low) field if you want to use a Host list to establish the upper and lower range of IPX destination host numbers.

For additional information, refer to “Dest Host (low)” later in this chapter. For more information about Host lists, refer to “Host Number (high)” and “Host Number (low)” later in this chapter.

Dest Host (low) Sets the lower boundary of the range for filtering an IPX packet based on the contents of its destination host field.

- Options
- Leave this field blank if you do not want to filter IPX destination hosts.
 - Enter the IPX host number in this field and leave the Dest Host (high) field blank if you are filtering a single IPX destination host.
 - Enter the lowest IPX host number in this field and enter the highest host number in the Dest Host (high) field if you are filtering a range of IPX destination hosts.
 - Enter the Host list name in this field and leave the Dest Host (high) field blank if you want to use a Host list to establish the upper and lower range of destination host numbers.

For additional information, refer to “Dest Host (high)” earlier in this chapter. For more information about Host lists, refer to “Host Number (high)” and “Host Number (low)” later in this chapter.

Dest Network (Hex) Identifies the network where the NETBIOS target resides. Enter the network number in 8-digit hexadecimal format (use leading 0's if necessary).

Dest Network (high) Sets the upper boundary of the range for filtering an IPX packet based on the contents of its destination network field.

- Options
- Leave this field blank if you do not want to filter IPX destination networks.
 - Leave this field blank and enter the IPX network number in the Dest Network (low) field if you are filtering a single IPX destination network.
 - Enter the highest IPX network number in the range if you are filtering a range of IPX destination networks.
 - Leave this field blank and enter the name of the Network list in the Dest Network (low) field if you want to use a Network list to establish the upper and lower range of IPX destination network numbers.

For additional information, refer to “Dest Network (low)” later in this chapter. For more information about Network lists, refer to “Network Number (high)” and “Network Number (low)” later in this chapter.

Dest Network (low) Sets the lower boundary of the range for filtering an IPX packet based on the contents of its destination network field.

- Options
- Leave this field blank if you do not want to filter IPX destination networks.
 - Enter the IPX network number in this field and leave the Dest Network (high) field blank if you are filtering a single IPX destination network.

IPX Protocol Parameters

Parameters and Options

- Enter the lowest IPX network number in this field and enter the highest network number in the Dest Network (high) field if you are filtering a range of IPX destination networks.
- Enter the Network list name in this field and leave the Dest Network (high) field blank if you want to use a Network list to establish the upper and lower range of destination network numbers.

For additional information, refer to “Dest Network (high)” earlier in this chapter. For more information about Network lists, refer to “Network Number (high)” and “Network Number (low)” later in this chapter.

Dest Socket (high) Sets the upper boundary of the range for filtering an IPX packet based on the contents of its destination socket field.

- Options
- Leave this field blank if you do not want to filter IPX destination sockets.
 - Leave this field blank and enter the IPX socket number in the Dest Socket (low) field if you are filtering a single IPX destination socket.
 - Enter the highest IPX socket number in the range if you are filtering a range of IPX destination sockets.
 - Leave this field blank and enter the name of the Socket list in the Dest Socket (low) field if you want to use a Socket list to establish the upper and lower range of IPX destination socket numbers.

For additional information, refer to “Dest Socket (low)” later in this chapter. For more information about Socket lists, refer to “Socket (high)” and “Socket (low)” later in this chapter.

Dest Socket (low) Sets the lower boundary of the range for filtering an IPX packet based on the contents of its destination socket field.

- Options
- Leave this field blank if you do not want to filter IPX destination sockets.
 - Enter the IPX socket number in this field and leave the Dest Socket (high) field blank if you are filtering a single IPX destination socket.
 - Enter the lowest IPX socket number in this field and enter the highest socket number in the Dest Socket (high) field if you are filtering a range of IPX destination sockets.
 - Enter the Socket list name in this field and leave the Dest Socket (high) field blank if you want to use a Socket list to establish the upper and lower range of destination socket numbers.

For additional information, refer to “Dest Socket (high)” earlier in this chapter. For more information about Socket lists, refer to “Socket (high)” and “Socket (low)” later in this chapter.

Effect	Determines whether packets are dropped or relayed (filtered) based on the contents of packet fields and a range established by a matching set of (low) and (high) filter parameters. The matching (high) and (low) router parameters and corresponding packet fields are listed in the following table:																
	<table><tr><th>Packet Field</th><th>IPX Parameters</th></tr><tr><td>Destination Host</td><td>Dest Host (low) and Dest Host (high)</td></tr><tr><td>Destination Network</td><td>Dest Network (low) and Dest Network (high)</td></tr><tr><td>Destination Socket</td><td>Dest Socket (low) and Dest Socket (high)</td></tr><tr><td>Source Host</td><td>Source Host (low) and Source Host (high)</td></tr><tr><td>Source Network</td><td>Source Network (low) and Source Network (high)</td></tr><tr><td>Source Socket</td><td>Source Socket (low) and Source Socket (high)</td></tr><tr><td>Packet Type</td><td>Packet Type (low) and Packet Type (high)</td></tr></table>	Packet Field	IPX Parameters	Destination Host	Dest Host (low) and Dest Host (high)	Destination Network	Dest Network (low) and Dest Network (high)	Destination Socket	Dest Socket (low) and Dest Socket (high)	Source Host	Source Host (low) and Source Host (high)	Source Network	Source Network (low) and Source Network (high)	Source Socket	Source Socket (low) and Source Socket (high)	Packet Type	Packet Type (low) and Packet Type (high)
Packet Field	IPX Parameters																
Destination Host	Dest Host (low) and Dest Host (high)																
Destination Network	Dest Network (low) and Dest Network (high)																
Destination Socket	Dest Socket (low) and Dest Socket (high)																
Source Host	Source Host (low) and Source Host (high)																
Source Network	Source Network (low) and Source Network (high)																
Source Socket	Source Socket (low) and Source Socket (high)																
Packet Type	Packet Type (low) and Packet Type (high)																
	Default: Ignore																
Don't Match	Applies the filtering action (drop/accept/log) if the contents of the applicable packet field do not fall within the range established by the matching (low) and (high) filter parameter.																
Ignore	Applies no filtering action if the contents of the applicable packet field fall within the range established by the matching (low) and (high) filter parameters.																
Match	Applies the filtering action (drop/accept/log) if the contents of the applicable packet field fall within the range established by the matching (low) and (high) filter parameters.																
Encapsulation Type	Selects from three available encapsulation methods that can be used on the IEEE 802.3 cable type (media); this parameter has no effect on other media types (token ring, WAN, etc.). Default: Novell Note: “Encapsulation Type” is also referred to as “Frame Type”.																

IPX Protocol Parameters

Parameters and Options

802.2	Enables IEEE 802.2 logical link control encapsulation. The 802.2 encapsulation method prefixes one octet of destination service access point identification, one octet of source service access point identification, and one octet of control information to the IPX packet. The 802.2 packet, in turn, will be encapsulated within a packet specific to the cable type. For media other than 802.3 (ThinLAN, ThickLAN, and EtherTwist), an encapsulation method is implicitly chosen.
Ethernet	Enables Ethernet 2.0 encapsulation. Ethernet encapsulation prefixes an eight-octet preamble, six octets of destination-address information, and two octets of protocol type information (hexadecimal 8137) to the IPX packet. It appends a four-octet frame check sequence to the packet.
Novell	Enables Novell proprietary encapsulation. Novell encapsulation prefixes an eight-octet preamble, six octets of destination-address information, six octets of source-address information, and two octets of packet-length information to the unchecksummed IPX packet. It appends a four-octet frame check sequence to the packet.
Host lists	Displays a screen with parameters for creating a Host list. For information about creating a Host list, refer to "Host Number (low)" and "Host Number (high)" later in this chapter. For information about assigning the Host list to a filter, refer to "Dest Host (low)" and "Source Host (low)."
Host Number (high)	Sets the upper boundary of the range for filtering IPX source or destination hosts when creating a Host list.
Options	<ul style="list-style-type: none">■ Leave this field blank and enter the IPX host number in the Host Number (low) field if you are filtering a single IPX source or destination host.■ Enter the highest IPX host number in the range if you are filtering a range of IPX source or destination hosts. <p>For additional information, refer to "Host Number (low)" later in this chapter. To learn how to assign a Host list to a filter, refer to "Dest Host (low)" and "Source Host (low)."</p>
Host Number (low)	Sets the lower boundary of the range for filtering IPX source or destination hosts when creating a Host list.
Options	<ul style="list-style-type: none">■ Enter the IPX host number in this field and leave the Host Number (high) field blank if you are filtering a single IPX source or destination host.■ Enter the lowest IPX host number in this field and enter the highest host number in the Host Number (high) field if you are filtering a range of IPX source or destination hosts.

For additional information, refer to "Host Number (high)" earlier in this chapter. To learn how to assign a Host list to a filter, refer to "Dest Host (low)" and "Source Host (low)."

Internal Network Number	Required if IPXWAN is set to "Yes". Must be unique within the relevant routing area, and is distinct from the network numbers of the physical network segments in a routing area. The internal network number is an 8-digit hexadecimal value (padded with zeroes if necessary).
Internal Router Name	Required if IPXWAN is set to "Yes". Provides an easily-identifiable name, especially for network management purposes to identify systems by user-defined mnemonic names. Can be from 1 to 47 uppercase English characters, plus the underscore (_), hyphen (-) and @ sign. Blank spaces are not allowed. Note: Blank spaces are not supported.
IPXWAN	Enables or disables IPX operation over a WAN link. If enabled, <i>requires</i> values for the Internal Network Number and the Internal Router Name parameters (accessed through the "4. Internal Network Number and Router Name" IPX menu item). Currently supported over the following WAN protocols: PPP, Frame Relay, X.25, Point-to-Point, and HP Point-to-Point. Default: No No Disables IPX operation over a WAN link. Yes Enables IPX operation over a WAN link.
List Name	Accepts the name of a Host list, Network list, Packet Type list, or Socket list.
Network lists	Displays a screen with parameters for defining a Network list. For information about creating a Network list, refer to "Network Number (low)" and "Network Number (high)" later in this chapter. For information about assigning the Network list to a filter, refer to "Dest Network (low)" and "Source Network (low)."
Network Number	Accepts the IPX network number for the IPX network connected to the router interface. All IPX networks are identified by a locally-assigned network number. IPX network numbers consist of an 8-digit hexadecimal value (pad with leading zeros if necessary). Note: HP routers support one IPX network number per interface.
Network Number (high)	Sets the upper boundary of the range for filtering IPX source or destination networks when creating a Network list.

IPX Protocol Parameters

Parameters and Options

- Options
- Leave this field blank and enter the IPX network number in the Network Number (low) field if you are filtering a single IPX source or destination network.
 - Enter the highest IPX network number in the range if you are filtering a range of IPX source or destination networks.

For additional information, refer to “Network Number (low)” later in this chapter. To learn how to assign a Network list to a filter, refer to “Dest Network (low)” and “Source Network (low).”

Network Number (Hex)

Specifies the network portion of the SAP (Service Advertising Protocol) filter pattern.

Network Number (low)

Sets the lower boundary of the range for filtering IPX source or destination networks when creating a Network list.

- Options
- Enter the IPX network number in this field and leave the Network Number (high) field blank if you are filtering a single IPX source or destination network.
 - Enter the lowest IPX network number in this field and enter the highest network number in the Network Number (high) field if you are filtering a range of IPX source or destination networks.

For additional information, refer to “Network Number (high)” earlier in this chapter. To learn how to assign a Network list to a filter, refer to “Dest Network (low)” and “Source Network (low).”

NETBIOS Resource Name

The name of the NETBIOS target. NETBIOS names consist of up to 16 characters and can include any keyboard character except the tilde (~). The backslash (\) can be entered only as “\\”. If a character cannot be entered from the keyboard it can be entered in two-digit hexadecimal form as “\hh” (where hh is a two-digit hexadecimal value).

Note: Matching is case sensitive—“JOE’s” Server is not equivalent to “joe’s” server.

Next Hop Host

Identifies the host address of the next-hop router used to reach Target Net.

Next Hop Net

Identifies the network address of the next router in the hop sequence.

Packet type lists specify

Displays a screen with parameters for creating Packet Type lists. For information about creating a Packet Type list and associating the list with a Packet Type filter, refer to “Packet Type (low)” and “Packet Type (high)” later in this chapter.

Packet Type (high)

Sets the upper boundary of the range for filtering IPX packet type numbers when creating a Packet Type filter or Packet Type list.

- Options
- Leave this field blank and enter the IPX packet type number in the Packet Type (low) field if you are filtering a single IPX packet type number.
 - Enter the highest IPX packet type number in the range if you are filtering a range of IPX packet type numbers.
 - Enter the list name in the Packet Type (low) field and leave this field blank if you are creating an IPX Packet Type filter and want to create a range of packet type numbers with a filter list.

For additional information, refer to “Packet Type (low)” later in this chapter.

Packet Type (low) Sets the lower boundary of the range for filtering IPX packet type numbers when creating a Packet Type filter or Packet Type list.

- Options
- Enter the IPX packet type number in this field and leave the Packet Type (high) field blank if you are filtering a single IPX packet type number.
 - Enter the lowest IPX packet type number in this field and enter the highest packet type number in the Packet Type (high) field if you are filtering a range of IPX packet type numbers.
 - Enter the list name in this field and leave the Packet Type (high) field blank if you are creating an IPX Packet Type filter and want to establish the range of packet type numbers with a filter list.

For additional information, refer to “Packet Type (high)” earlier in this chapter.

Precedence Assigns a priority value to the filter—the higher the precedence, the greater the priority. You can construct up to 31 filters per interface. The Precedence value is used when an in-coming packet meets several filter rules. In such an instance, the filter rule with the highest priority (precedence) is applied to filter the packet.

Default: 1
Range: 1 to 31

Note: When two filters have equal precedence, the first configured filter takes precedence over the second filter.

Random load balancing Provides two methods for managing IPX network traffic across circuits in a circuit group: Random load balancing, Host ID load balancing.

Default: No

- No
- Enables Host ID load balancing—the router selects a circuit to carry all network traffic (packets) between the source and destination systems.

IPX Protocol Parameters

Parameters and Options

Yes Enables random load balancing and disables Host ID load balancing—the router evenly distributes IPX network traffic among all circuits within a circuit group to carry all network traffic (packets) between the source and destination.

Note: In some cases, random load balancing can interfere with Novell burst mode NLM.

RIP Interface Cost Sets the cost for each router hop. Standard IPX RIP implementations assign a cost of 1 to each hop.

Default: 1

RIP Listen Enables or disables the RIP listen function. RIP Listen specifies whether the IPX router adds routes received in RIP updates from neighboring routers to its own internal routing table.

Default: Yes

Yes Enables the RIP listen function.

No Disables the RIP listen function.

RIP Supply Enables or disables the `RIP supply` function. RIP Supply determines whether the IPX router transmits periodic RIP updates.

Default: Yes

Yes Enables the RIP supply function.

No Disables the RIP supply function.

RIP Table Cost Sets the cost for the relay to the next-hop.

RIP and SAP split horizon Determines whether the router can exclude or include RIP and SAP updates sent to a neighbor that were already learned by the neighbor.

Default: Yes

No Include RIP and SAP updates already learned by a neighbor.

Yes Exclude RIP and SAP updates already learned by a neighbor.

SAP driven RIP supply	<p>Decreases the amount of RIP traffic advertised by the IPX router over specified interfaces. SAP driven RIP supply works in conjunction with any SAP filters that you may have enabled on an interface to determine which servers are advertised by the interface.</p> <ul style="list-style-type: none"> ■ If SAP-driven RIP supply is configured on the interface, then only networks containing at least one server are advertised by this interface. Networks that do not contain a server are not advertised. ■ If a SAP filter is also configured on the interface, then only those networks containing servers that match the SAP filter are advertised by this interface. <p>Default: No.</p> <p>No Disables the SAP-driven RIP supply function.</p> <p>Yes Enables the SAP-driven RIP supply function.</p>
Server Name	<p>Assigns the server name portion of the filter pattern. Server Name can be any valid Novell server name up to 48 characters in length. Any keyboard character with the exception of the tilde (~) character can be used.</p> <ul style="list-style-type: none"> ■ If Server Name contains 48 characters, the node sets the final character to NULL (hexadecimal 00) when matching against actual server names. ■ If Server Name contains less than 48 characters, it is left-justified and the remaining characters are NULL-filled. Name matching is performed up to the first NULL character. <p>Note: Server name matching is case sensitive—Technology Suite Router is not equivalent to Technology suite router.</p>
Server Type (Hex)	Specifies the server type portion of the filter pattern.
Socket (high)	<p>Sets the upper boundary of the range for filtering IPX source or destination sockets when creating a Socket list.</p> <p>Options</p> <ul style="list-style-type: none"> ■ Leave this field blank and enter the IPX socket number in the Socket (low) field if you are filtering a single IPX source or destination socket. ■ Enter the highest IPX socket number in the range if you are filtering a range of IPX source or destination sockets, <p>For additional information, refer to “Socket (low)” later in this chapter. To learn how to assign a Socket list to a filter, refer to “Dest Socket (low)” and “Source Socket (low).”</p>

IPX Protocol Parameters

Parameters and Options

Socket (low) Sets the lower boundary of the range for filtering IPX source or destination sockets when creating a Socket list.

- Options
- Enter the IPX socket number in this field and leave the Socket (high) field blank if you are filtering a single IPX source or destination socket.
 - Enter the lowest IPX socket number in this field and enter the highest socket number in the Socket (high) field if you are filtering a range of IPX source or destination sockets.

For additional information, refer to “Socket (high)” earlier in this chapter. To learn how to assign a Socket list to a filter, refer to “Dest Socket (low)” and “Source Socket (low).”

Source Host (high) Sets the upper boundary of the range for filtering an IPX packet based on the contents of its source host field.

- Options
- Leave this field blank if you do not want to filter IPX source hosts.
 - Leave this field blank and enter the IPX host number in the Source Host (low) field if you are filtering a single IPX source host.
 - Enter the highest IPX host number in the range if you are filtering a range of IPX source hosts.
 - Leave this field blank and enter the name of the Host list in the Source Host (low) field if you want to use a Host list to establish the upper and lower range of IPX source host numbers.

For additional information, refer to “Source Host (low)” later in this chapter. For more information about Host lists, refer to “Host Number (high)” and “Host Number (low)” earlier in this chapter.

Source Host (low) Sets the lower boundary of the range for filtering an IPX packet based on the contents of its source host field.

- Options
- Leave this field blank if you do not want to filter IPX source hosts.
 - Enter the IPX host number in this field and leave the Source Host (high) field blank if you are filtering a single IPX source host.
 - Enter the lowest IPX host number in this field and enter the highest host number in the Source Host (high) field if you are filtering a range of IPX source hosts.
 - Enter the Host list name in this field and leave the Source Host (high) field blank if you want to use a Host list to establish the upper and lower range of source host numbers.

For additional information, refer to “Source Host (high)” earlier in this chapter. For more information about Host lists, refer to “Host Number (high)” and “Host Number (low)” earlier in this chapter.

Source Network (high) Sets the upper boundary of the range for filtering an IPX packet based on the contents of its source network field.

- Options
- Leave this field blank if you do not want to filter IPX source networks.
 - Leave this field blank and enter the IPX network number in the Source Network (low) field if you are filtering a single IPX source network.
 - Enter the highest IPX network number in the range if you are filtering a range of IPX source networks.
 - Leave this field blank and enter the name of the Network list in the Source Network (low) field if you want to use a Network list to establish the upper and lower range of IPX source network numbers.

For additional information, refer to “Source Network (low)” later in this chapter. For more information about Network lists, refer to “Network Number (high)” and “Network Number (low)” earlier in this chapter.

Source Network (low) Sets the lower boundary of the range for filtering an IPX packet based on the contents of its source network field.

- Options
- Leave this field blank if you do not want to filter IPX source networks.
 - Enter the IPX source network number in this field and leave the Source Network (high) field blank if you are filtering a single IPX source network.
 - Enter the lowest IPX network number in this field and enter the highest network number in the Source Network (high) field if you are filtering a range of IPX source networks.
 - Enter the Network list name in this field and leave the Source Network (high) field blank if you want to use a Network list to establish the upper and lower range of source network numbers.

For additional information, refer to “Source Network (high)” earlier in this chapter. For more information about Network lists, refer to “Network Number (high)” and “Network Number (low)” later in this chapter.

IPX Protocol Parameters

Parameters and Options

Source Route (Token Ring) Enables or disables source routing over token ring media for the interface you are defining. Because the HP Router PR does not have a token ring port, this option should always be set to No.

Default: No

No Disables token ring source routing.

Source Socket (high) Sets the upper boundary of the range for filtering an IPX packet based on the contents of its source socket field.

- Options
- Leave this field blank if you do not want to filter IPX source sockets.
 - Leave this field blank and enter the IPX socket number in the Source Socket (low) field if you are filtering a single IPX source socket.
 - Enter the highest IPX socket number in the range if you are filtering a range of IPX source sockets.
 - Leave this field blank and enter the name of the Socket list in the Source Socket (low) field if you want to use a Socket list to establish the upper and lower range of IPX source socket numbers.

For additional information, refer to “Source Socket (low)” later in this chapter. For more information about Socket lists, refer to “Socket (high)” and “Socket (low)” earlier in this chapter.

Source Socket (low) Sets the lower boundary of the range for filtering an IPX packet based on the contents of its source socket field.

- Options
- Leave this field blank if you do not want to filter IPX source sockets.
 - Enter the IPX socket number in this field and leave the Source Socket (high) field blank if you are filtering a single IPX source socket.
 - Enter the lowest IPX socket number in this field and enter the highest socket number in the Source Socket (high) field if you are filtering a range of IPX source sockets.
 - Enter the Socket list name in this field and leave the Source Socket (high) field blank if you want to use a Socket list to establish the upper and lower range of source socket numbers.

For additional information, refer to “Source Socket (high)” earlier in this chapter. For more information about Socket lists, refer to “Socket (high)” and “Socket (low)” earlier in this chapter.

IPX Protocol Parameters
Parameters and Options

Target Net	Identifies a specific network in an internet.
WAN SAP Period	Sets the time interval elapsing when the IPX router transmits GSRs across any WAN link. Default: 1 (minute) Range: 0 to 99 (minutes)

AppleTalk Parameters

Overview

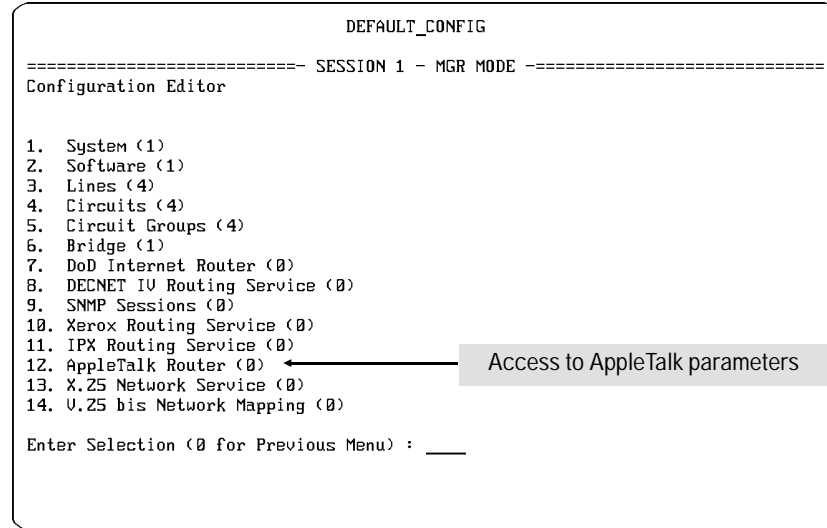


Figure 12-1. Access to AppleTalk Parameters

AppleTalk Parameters: Implement the AppleTalk Phase 2 protocol to operate with Ethernet and Token Ring networks.

Note

The AppleTalk router does not support AppleTalk Phase 1. Phase 1 traffic cannot be routed through the AppleTalk router. However, such traffic can be relayed through a bridge.

AppleTalk Parameters
Overview

Page	AppleTalk Parameters
12-6	AARP Mapping Table Size
12-6	Checksum
12-6	Circuit Group Name
12-6	Cost
12-6	DDP Type Lists
12-6	DDP Type (high)
12-7	DDP Type (low)
12-7	Default Zone Name
12-7	DDP Type (low)
12-7	Default Zone Name
12-7	Dest Net (high)
12-8	Dest Net (low)
12-8	Dest Node (high)
12-9	Dest Node (low)
12-9	Dest Sock (high)
12-9	Dest Sock (low)
12-10	Effect
12-10	List Members
12-11	List Name
12-11	Network Lists
12-11	Network
12-11	Network Max
12-12	Network Min
12-12	Network (high)
12-12	Node (high)
12-13	Node ID
12-13	Node Lists
12-13	Node (low)
12-13	Precedence
12-14	Probe
12-14	Routing Table Size
12-14	Seed Router
12-14	Socket Lists
12-15	Socket (high)
<i>—Continued on Next Page—</i>	

AppleTalk Parameters
Overview

Page	AppleTalk Parameters
<i>—Continued From Previous Page—</i>	
12-15	Socket (low)
12-15	Source Net (high)
12-15	Source Net (low)
12-16	Source Node (high)
12-16	Source Node (low)
12-17	Source Route (Token Ring)
12-17	Source Sock (high)
12-17	Source Sock (low)
12-18	Zone Filter
12-18	Zone Name
12-18	Zone Table Size

Parameters and Options

Action	Determines the filtering action taken when the contents of a AppleTalk datagram field meet the criteria established for a filter rule. Default: Drop and Log
Accept	Relays a datagram meeting the filter rule.
Accept and Log	Relays a datagram meeting the filter rule and records the action in the event log.
Drop	Discards a datagram meeting the filter rule and records the action in the event log.
Drop and Log	Discards a datagram meeting the filter rule.
	Note: The Drop and Log and Accept and Log actions should be used judiciously. The processing required to log such events in the RAM-based event log consumes CPU cycles and can result in the loss of incoming DDPs. Consequently, the log actions should generally be used only to record anomalous events.
Auto Enable	Enables or disables the AppleTalk router when the router boots. The AppleTalk-specific Auto Enable parameter works in conjunction with the global Auto Enable parameter found on the Global Parameters screen in the System configuration menu. <ul style="list-style-type: none">■ When the global Auto Enable parameter is set to No, the AppleTalk router is unconditionally disabled. (Then to enable AppleTalk routing after the router boots, you will have to use the NCL Interpreter's Enable command.)■ When the global Auto Enable parameter is set to Yes, the setting of the AppleTalk-specific Auto Enable parameter determines whether the AppleTalk router is enabled. Default: Yes
No	Disables the AppleTalk router if the global Auto Enable parameter is enabled. (Then to enable it after the router boots, you must use the NCL Interpreter's Enable command.)
Yes	Enables the AppleTalk router if the global Auto Enable parameter is also enabled.

AppleTalk Parameters

Parameters and Options

AARP Mapping Table Size Specifies the number of entries in the AppleTalk router's address-resolution mapping table. Estimate the number of end nodes on the attached local network. Then select the next highest number from one of the following toggle options:

Default: 887

Options 53, 211, 523, 887, 1327, 3327, 9551.

Checksum Enables or disables the calculation of the DDP checksum for datagrams constructed and transmitted by the AppleTalk router. AppleTalk provides the option of including a 16-bit checksum in the header of DDP datagrams. Checksum has no effect upon incoming datagrams. If the AppleTalk router receives a datagram containing a checksum, it verifies the checksum value.

Default: No

No Disables DDP check summing—the AppleTalk router does not calculate a checksum, and writes a value of 0 to the DDP datagram header.

Yes Enables DDP check summing—the AppleTalk router calculates and writes a checksum to the header of any DDP datagram originating from the AppleTalk router.

Cost6 Assigns a cost value to the AppleTalk interface.

Default: 0

Range: 0 to 9, where 0 designates the highest speed (most preferred path) and 9 designates the least preferred path.

Circuit Group Name The name of a circuit group connecting to a neighboring EtherTalk network, router, or backbone network. This is one of the circuit groups configured for the Circuit Group menu

DDP Type Lists Displays a screen with parameters for creating a DDP (Data Delivery Protocol) Type filter list. For information about creating a DDP Type filter and assigning the list to a filter, refer to “DDP Type (low)” and “DDP Type (high)” later in this chapter.

DDP Type (high) Sets the upper boundary of the range for filtering a DDP Type packet based on the contents of its DDP Type field, or sets the upper boundary for one range in a DDP Type list.

- Options
- Leave this field blank and enter the DDP Type in the DDP Type (low) field if you are filtering a single DDP Type.
 - Enter the highest DDP Type in the range if you are filtering a range of DDP Types.

- Enter the list name in the DDP Type (low) field and leave this field blank. If you are creating an DDP Type filter, and want to specify one or more ranges of DDP Types with a DDP Type list.

For additional information, refer to “DDP Type (low)” later in this chapter.

Note: The creation of DDP Type filters and DDP Type lists is similar—the DDP Type (low) and DDP Type (high) parameters are used to establish a range for filtering packets. For more information about creating a DDP Type list, refer to “DDP Type Lists” earlier in this chapter.

DDP Type (low)

Sets the lower boundary of the range for filtering a DDP Type packet based on the contents of its DDP Type field, or sets the lower boundary for a DDP Type filter list.

- Options
- Enter the DDP Type in this field and leave the DDP Type (high) field blank if you are filtering a single DDP Type.
 - Enter the lowest DDP Type in this field and enter the highest DDP Type in the DDP Type (high) field if you are filtering a range of DDP Types.
 - Enter the list name in this field and leave the DDP Type (high) field blank if you are creating a DDP Type filter and want to establish the range of DDP Types with a DDP Type list.

For additional information, refer to “DDP Type (high)” earlier in this chapter.

Default Zone Name

Functional when Seed Router set to “Yes”. Determines the default zone used by inquiring nodes. A zone is a logical grouping of networks. Such a logical grouping can be confined to a single network or span multiple networks within the AppleTalk internet. Each zone is identified by a zone name, a string of up to 32 printable characters (including the SPACE character).

Note: A 32-character limit is applied when entering a zone name. For specific information, refer to your router configuration guide.

Dest Net (high)

Sets the upper boundary of the range for filtering a datagram based on the contents of its destination network field.

- Options
- Leave this field blank if you do not want to filter AppleTalk destination networks.
 - Leave this field blank and enter the AppleTalk network number in the Dest Net (low) field if you are filtering a single AppleTalk destination network.
 - Enter the highest AppleTalk network number in the range if you are filtering a range of AppleTalk destination networks.

AppleTalk Parameters

Parameters and Options

- Leave this field blank and enter the name of the Network list in the Dest Net (low) field if you want to use a Network list to establish the upper and lower range of AppleTalk destination network numbers.

For additional information, refer to “Dest Net (low)” later in this chapter. For more information about Network lists, refer to “Network Number (high)” and “Network Number (low)” later in this chapter.

Dest Net (low) Sets the lower boundary of the range for filtering a datagram based on the contents of its destination network field.

Options ■ Leave this field blank if you do not want to filter AppleTalk destination networks.

- Enter the AppleTalk network number in this field and leave the Dest Net (high) field blank if you are filtering a single AppleTalk destination network.
- Enter the lowest AppleTalk network number in this field and enter the highest network number in the Dest Net (high) field if you are filtering a range of AppleTalk destination networks.
- Enter the Network list name in this field and leave the Dest Net (high) field blank if you want to use a Network list to establish the upper and lower range of destination network numbers.

For additional information, refer to “Dest Net (high)” earlier in this chapter. For more information about Network lists, refer to “Network Number (high)” and “Network Number (low)” later in this chapter.

Dest Node (high) Sets the upper boundary of the range for filtering a datagram based on the contents of its destination node field.

Options ■ Leave this field blank if you do not want to filter AppleTalk destination nodes.

- Leave this field blank and enter the AppleTalk node identifier in the Dest Node (low) field if you are filtering a single AppleTalk destination node.
- Enter the highest AppleTalk node identifier in the range if you are filtering a range of AppleTalk destination nodes.
- Leave this field blank and enter the name of the Node list in the Dest Node (low) field if you want to use a Node list to establish the upper and lower range of AppleTalk destination node identifiers.

For additional information, refer to “Dest Node (low)” later in this chapter. For more information about Node lists, refer to “Node (high)” and “Node (low)” later in this chapter.

Dest Node (low) Sets the lower boundary of the range for filtering a datagram based on the contents of its destination node field.

- Options ■ Leave this field blank if you do not want to filter AppleTalk destination nodes.
- Enter the AppleTalk node identifier in this field and leave the Dest Node (high) field blank if you are filtering a single AppleTalk destination node.
 - Enter the lowest AppleTalk node identifier in this field and enter the highest node identifier in the Dest Node (high) field if you are filtering a range of AppleTalk destination nodes.
 - Enter the Node list name in this field and leave the Dest Node (high) field blank if you want to use a Node list to establish the upper and lower range of destination node identifiers.

For additional information, refer to “Dest Node (high)” earlier in this chapter. For more information about Node lists, refer to “Node (high)” and “Node (low)” later in this chapter.

Dest Sock (high) Sets the upper boundary of the range for filtering a datagram based on the contents of its destination socket field.

- Options ■ Leave this field blank if you do not want to filter AppleTalk destination sockets.
- Leave this field blank and enter the AppleTalk socket number in the Dest Sock (low) field if you are filtering a single AppleTalk destination sockets.
 - Enter the highest AppleTalk socket number in the range if you are filtering a range of AppleTalk destination sockets.
 - Leave this field blank and enter the name of the Socket list in the Dest Sock (low) field if you want to use a Socket list to establish the upper and lower range of AppleTalk destination socket numbers.

For additional information, refer to “Dest Sock (low)” later in this chapter. For more information about Socket lists, refer to “Socket (high)” and “Socket (low)” later in this chapter.

Dest Sock (low) Sets the lower boundary of the range for filtering a datagram based on the contents of its destination socket field.

- Options ■ Leave this field blank if you do not want to filter AppleTalk destination sockets.
- Enter the AppleTalk socket number in this field and leave the Dest Sock (high) field blank if you are filtering a single AppleTalk destination socket.

AppleTalk Parameters

Parameters and Options

- Enter the lowest AppleTalk socket number in this field and enter the highest socket number in the Dest Sock (high) field if you are filtering a range of AppleTalk destination sockets.
- Enter the Socket list name in this field and leave the Dest Sock (high) field blank if you want to use a Socket list to establish the upper and lower range of destination socket numbers.

For additional information, refer to “Dest Sock (high)” earlier in this chapter. For more information about Socket lists, refer to “Socket (high)” and “Socket (low)” later in this chapter.

Effect

Determines whether datagrams are dropped or relayed (filtered) based on the contents of a datagram field and a range established by a matching set of (low) and (high) filter parameters. The datagram field and corresponding of (low) and (high) filter parameters are listed in the following table:

Datagram Field	AppleTalk Router Parameter
DDP type	DDP Type (low) and DDP Type (high)
destination node	Dest Node (low) and Dest Node (high)
destination socket	Dest Sock (low) and Dest Sock (high)
destination network	Dest Net (low) and Dest Net (high)
source network	Source Net (low) and Source Net (high)
source node	Source Node (low) and Source Node (high)
source socket	Source Sock (low) and Source Sock (high)

Default: Ignore

Don't Match Applies the filtering action (drop/accept/log) if the contents of the datagram field do not fall within the range established by the matching (low) and (high) filter parameters.

Ignore Applies no filtering action if the contents of the datagram field falls within the range established by the matching (low) and (high) filter parameters.

Match Applies the filtering action (drop/accept/log) if the contents of the datagram field falls within the range established by the matching (low) and (high) filter parameters.

List Members

Displays a screen with options for creating a DDP Type list, Network list, Node list, and Socket list. Each option on the screen displays a set of matching (low) and (high) parameters for creating a list. The screen options and corresponding (low) and (high) parameters are listed in the following table:

List Type	Parameters
DDP Type	DDP Type (low) and DDP Type (high)
Network	Network (low) and Network (high)
Node	Node (low) and Node (high)
Socket	Socket (low) and Socket (high)

Note: Lists can simplify the process of creating filters. For example, you could enter the name of a Node list in the Dest Node (low) field rather than creating a range of nodes to filter by entering a range of nodes in the Dest Node (low) and Dest Node (high) fields. Lists save time when you need to filter the same range of source or destination points on the AppleTalk network using different filter rules.

List Name	Accepts a list name when creating a DDP Type list, Network list, Node list, or Socket list.
Network Lists	Displays a screen with parameters for creating a Network list. For information about creating a Network list, refer to “Network Number (low)” and “Network Number (high)” later in this chapter. For information about assigning the Network list to a filter, refer to “Dest Net (low)” and “Source Net (low).”
Network	<p>Functional when Seed Router set to “yes”. Specifies the circuit-group-specific network number. The network number for each AppleTalk network must be unique. You can explicitly assign the network number, or you can allow the AppleTalk seed router to assign a random value in the range specified by Network Min and Network Max</p> <p>Default: 0 Range: 1 to 65279 (decimal)</p> <p>Note: To explicitly assign the network number, enter a decimal number equal to or greater than Network Min and equal to or less than Network Max.</p>
Network Max	<p>Functional when Seed Router set to “Yes”. Operates in conjunction with Network Min to specify the range of network numbers available to nodes on the directly-connected AppleTalk network. This Network Max parameter specifies the highest network number for the range.</p> <p>Default: 0 (port is treated as a nonseed router) Disable: 0 Range: 1 to 65279 (decimal)</p> <p>Note: When enabling this feature, you must enter a decimal number greater than or equal to the value selected for the Network Min. parameter.</p>

AppleTalk Parameters

Parameters and Options

Network Min	<p>Functional when Seed Router set to “Yes”. Operates in conjunction with Network Max to specify the range of network numbers available to nodes on the directly-connected AppleTalk network. In order to increase the number of nodes residing on a local network, AppleTalk Phase 2 mandates that the seed router provide a range of network numbers, which are then made available to network nodes. Network nodes can then randomly generate a network number within the provided range, just as they randomly generate a node identifier. This Network Min parameter specifies the lowest network number for the range.</p> <p>Default: 0 (port is treated as a nonseed router) Disable: 0 Range: 1 to 65279</p>
Network (high)	<p>Sets the upper boundary of the range for filtering AppleTalk source or destination networks when creating a Network list.</p> <p>Options</p> <ul style="list-style-type: none">■ Leave this field blank and enter the AppleTalk network number in the Network (low) field if you are filtering a single AppleTalk source or destination network.■ Enter the highest AppleTalk network number in the range if you are filtering a range of AppleTalk source or destination networks. <p>For additional information, refer to “Network (low)” later in this chapter. To learn how to assign a Network list to a filter, refer to “Dest Net (low)” and “Source Net (low).”</p>
Network (low)	<p>Sets the lower boundary of the range for filtering AppleTalk source or destination networks when creating a Network list.</p> <p>Options</p> <ul style="list-style-type: none">■ Enter the AppleTalk network number in this field and leave the Network (high) field blank if you are filtering a single AppleTalk source or destination network.■ Enter the lowest AppleTalk network number in this field and enter the highest network number in the Network (high) field if you are filtering a range of AppleTalk source or destination networks. <p>For additional information, refer to “Network (high)” earlier in this chapter. To learn how to assign a Network list to a filter, refer to “Dest Net (low)” and “Source Net (low).”</p>
Node (high)	<p>Sets the upper boundary of the range for filtering AppleTalk source or destination nodes when creating a Node list.</p> <p>Options</p> <ul style="list-style-type: none">■ Leave this field blank and enter the AppleTalk node identifier in the Node (low) field if you are filtering a single AppleTalk source or destination node.■ Enter the highest AppleTalk node identifier in the range if you are filtering a range of AppleTalk source or destination nodes.

For additional information, refer to “Node (low)” later in this chapter. To learn how to assign a Node list to a filter, refer to “Dest Node (low)” and “Source Node (low).”

Node ID Assigns the circuit-group-specific node identifier portion of the AppleTalk address. The AppleTalk router uses multiple AppleTalk addresses (one address for each port to which the router is directly connected). The AppleTalk address (that is, the network number and node identifier pair) must be unique for each node within the AppleTalk internet. You can explicitly assign a node identifier, or you can allow the AppleTalk router to assign its own node identifier. Regardless of the method used, it is strongly recommended that you enable Probe to ensure a unique node identifier.

Default: 0 (AppleTalk assigns the node identifier)
Range: 1 to 253 (decimal)

Node Lists Displays a screen with parameters for creating a Node list. For information about creating a Node list, refer to “Node (low)” and “Node (high).” For information about assigning the Node list to a filter, refer to “Dest Node (low)” and “Source Node (low).”

Node (low) Sets the lower boundary of the range for filtering AppleTalk source or destination nodes when creating a Node list.

- Options
- Enter the AppleTalk node identifier in this field and leave the Node (high) field blank if you are filtering a single AppleTalk source or destination node.
 - Enter the lowest AppleTalk node identifier in this field and enter the highest node identifier in the Node (high) field if you are filtering a range of AppleTalk source or destination nodes.

For additional information, refer to “Node (high)” earlier in this chapter. To learn how to assign a Node list to a filter, refer to “Dest Node (low)” and “Source Node (low).”

Precedence Assigns a priority value to a filter—the higher the precedence, the greater the priority. You can construct up to 31 filters per AppleTalk interface. The Precedence value is used when an in-coming packet meets several filter rules. In such an instance, the filter rule with the highest priority (precedence) is applied to filter the packet.

Default: 31
Range: 1 to 31

Note: When two filters have equal precedence, the first filter configured takes precedence the second filter.

AppleTalk Parameters

Parameters and Options

Probe	<p>Works in conjunction with the Node ID parameter and, in the case of seed routers, the Network parameter to enable or disable the generation of AARP Probe datagrams and their subsequent transmission across Circuit Group Name.</p> <p>Note: It is recommended that you enable Probe, even if you plan to assign an explicit node identifier. Enabling Probe guards against duplicate AppleTalk addresses within an internet.</p>				
Routing Table Size	<p>Determines the number of entries in the AppleTalk router's routing table.</p> <p>Default: 887</p> <p>Options 53, 211, 523, 887, 1327, 3327, 9551</p>				
Seed Router	<p>Determines whether the AppleTalk router is a seed or nonseed router for the network attached by the circuit group. A seed router is a router whose port descriptor includes a network range and default zone name (and possibly an optional zone name list). In the case of a network serviced by multiple AppleTalk routers, only a single router need be configured as the seed (with an explicitly-assigned network range). The other AppleTalk routers servicing the network can be configured as nonseed routers. Nonseed routers acquire the correct network information (network range and zone names) by receiving RTMP DATA and ZIP datagrams transmitted by the seed router. In the case of a network serviced by a single AppleTalk router, the router must be configured as a seed router.</p> <p>Default: No</p> <p>No Assigns the AppleTalk router as a nonseed router. This completes the configuration of one circuit group for AppleTalk routing. If you select this option, the console prompts for traffic filters.</p> <p>Yes Assigns the AppleTalk router as the seed router for the network. Results in the following seed-router parameters:</p> <table><tr><td>Default Zone Name</td><td>Network Max</td></tr><tr><td>Network</td><td>Network Min</td></tr></table> <p>Note: More than one router on the same network segment can be configured as seed router to create a redundant networking topology. All the seed routers must be configured with the identical network number range and zone name data.</p>	Default Zone Name	Network Max	Network	Network Min
Default Zone Name	Network Max				
Network	Network Min				
Socket Lists	<p>Displays a screen with parameters for creating a Socket list. For information about creating a Socket list, refer to "Socket (low)" and "Socket (high)" later in this chapter. For information about assigning the Socket list to a filter, refer to "Dest Sock (low)" and "Source Sock (low)."</p>				

Socket (high)	<p>Sets the upper boundary of the range for filtering AppleTalk source or destination sockets when creating a Socket list.</p> <p>Options</p> <ul style="list-style-type: none">■ Leave this field blank and enter the AppleTalk socket number in the Socket (low) field if you are filtering a single AppleTalk source or destination socket.■ Enter the highest AppleTalk socket number in the range if you are filtering a range of AppleTalk source or destination sockets. <p>For additional information, refer to “Socket (low)” later in this chapter. To learn how to assign a Socket list to a filter, refer to “Dest Sock (low)” and “Source Sock (low).”</p>
Socket (low)	<p>Sets the lower boundary of the range for filtering AppleTalk source or destination sockets when creating a Socket list.</p> <p>Options</p> <ul style="list-style-type: none">■ Enter the AppleTalk socket number in this field and leave the Socket (high) field blank if you are filtering a single AppleTalk source or destination socket.■ Enter the lowest AppleTalk socket number in this field and enter the highest socket number in the Socket (high) field if you are filtering a range of AppleTalk source or destination sockets. <p>For additional information, refer to “Socket (high)” earlier in this chapter. To learn how to assign a Socket list to a filter, refer to “Dest Sock (low)” and “Source Sock (low).”</p>
Source Net (high)	<p>Sets the upper boundary of the range for filtering a datagram based on the contents of its source network field.</p> <p>Options</p> <ul style="list-style-type: none">■ Leave this field blank if you do not want to filter AppleTalk source networks.■ Leave this field blank and enter the AppleTalk network number in the Source Net (low) field if you are filtering a single AppleTalk source network.■ Enter the highest AppleTalk network number in the range if you are filtering a range of AppleTalk source networks.■ Leave this field blank and enter the name of the Network list in the Source Net (low) field if you want to use a Network list to establish the upper and lower range of AppleTalk destination network numbers. <p>For additional information, refer to “Source Net (low)” later in this chapter. For more information about Network lists, refer to “Network Number (high)” and “Network Number (low)” later in this chapter.</p>
Source Net (low)	<p>Sets the lower boundary of the range for filtering a datagram based on the contents of its source network field.</p>

AppleTalk Parameters

Parameters and Options

Options ■ Leave this field blank if you do not want to filter AppleTalk source networks.

- Enter the AppleTalk network number in this field and leave the Source Net (high) field blank if you are filtering a single AppleTalk source network.
- Enter the lowest AppleTalk network number in this field and enter the highest network number in the Source Net (high) field if you are filtering a range of AppleTalk source networks.
- Enter the Network list name in this field and leave the Source Net (high) field blank if you want to use a Network list to establish the upper and lower range of source network numbers.

For additional information, refer to “Source Net (high)” earlier in this chapter. For more information about Network lists, refer to “Network Number (high)” and “Network Number (low)” later in this chapter.

Source Node (high) Sets the upper boundary of the range for filtering a datagram based on the contents of its source node field.

Options ■ Leave this field blank if you do not want to filter AppleTalk source nodes.

- Leave this field blank and enter the AppleTalk node identifier in the Source Node (low) field if you are filtering a single AppleTalk source node.
- Enter the highest AppleTalk node identifier in the range if you are filtering a range of AppleTalk source nodes.
- Leave this field blank and enter the name of the Node list in the Source Node (low) field if you want to use a Node list to establish the upper and lower range of AppleTalk source node identifiers.

For additional information, refer to “Source Node (low)” later in this chapter. For more information about Node lists, refer to “Node (high)” and “Node (low)” earlier in this chapter.

Source Node (low) Sets the lower boundary of the range for filtering a datagram based on the contents of its source node field.

Options ■ Leave this field blank if you do not want to filter AppleTalk source nodes.

- Enter the AppleTalk node identifier in this field and leave the Source Node (high) field blank if you are filtering a single AppleTalk source node.
- Enter the lowest AppleTalk node identifier in this field and enter the highest node identifier in the Source Node (high) field if you are filtering a range of AppleTalk source nodes.

- Enter the Node list name in this field and leave the Source Node (high) field blank if you want to use a Node list to establish the upper and lower range of source node identifiers.

For additional information, refer to “Source Node (high)” earlier in this chapter. For more information about Node lists, refer to “Node (high)” and “Node (low)” earlier in this chapter.

**Source Route
(Token Ring)**

Enables or disables source routing over token ring media for the interface being defined. Source route functionality allows the AppleTalk router to transmit and receive frames over a token ring network extended with source routing bridges. If the router you are configuring does not have a token-ring port, you should always set this option to No.

Default: No

No Disables source routing over token ring media.

Yes Enable source routing over token ring media.

Source Sock (high)

Sets the upper boundary of the range for filtering a datagram based on the contents of its source socket field.

Options ■ Leave this field blank if you do not want to filter AppleTalk source sockets.

- Leave this field blank and enter the AppleTalk socket number in the Source Sock (low) field if you are filtering a single AppleTalk source socket.
- Enter the highest AppleTalk socket number in the range if you are filtering a range of AppleTalk source sockets.
- Leave this field blank and enter the name of the Socket list in the Source Sock (low) field if you want to use a Socket list to establish the upper and lower range of AppleTalk source socket numbers.

For additional information, refer to “Source Sock (low)” later in this chapter. For more information about Socket lists, refer to “Socket (high)” and “Socket (low)” earlier in this chapter.

Source Sock (low)

Sets the lower boundary of the range for filtering a datagram based on the contents of its source socket field.

Options ■ Leave this field blank if you do not want to filter AppleTalk source sockets.

- Enter the AppleTalk socket number in this field and leave the Source Sock (high) field blank if you are filtering a single AppleTalk source socket.

AppleTalk Parameters

Parameters and Options

- Enter the lowest AppleTalk socket number in this field and enter the highest socket number in the Source Sock (high) field if you are filtering a range of AppleTalk source sockets.
- Enter the Socket list name in this field and leave the Source Sock (high) field blank if you want to use a Socket list to establish the upper and lower range of source socket numbers.

For additional information, refer to “Source Sock (high)” earlier in this chapter. For more information about Socket lists, refer to “Socket (high)” and “Socket (low)” earlier in this chapter.

Zone Filter

Enables control of the AppleTalk zone names that a router advertises onto a local network. (Zone filters help to reduce the number of zones that appear on a user’s “Chooser” menu by filtering out all but those zone names that match the local list.” They also act as a security measure by restricting the AppleTalk zones to which users have access.

Default: No

Yes Enables Zone Filter operation.

No Disables Zone Filter operation.

Zone Name)

Identifies a zone that nodes on this port may choose for this circuit group. Note that zones are logical groupings, and that a zone can encompass more than one network. Zone name is optional. You can configure up to 36 zone names (in addition to the mandatory default zone—refer to “Default Zone Name” on page 12-7).

Zone Table Size

Default: 512

X.25 Service Parameters

Overview

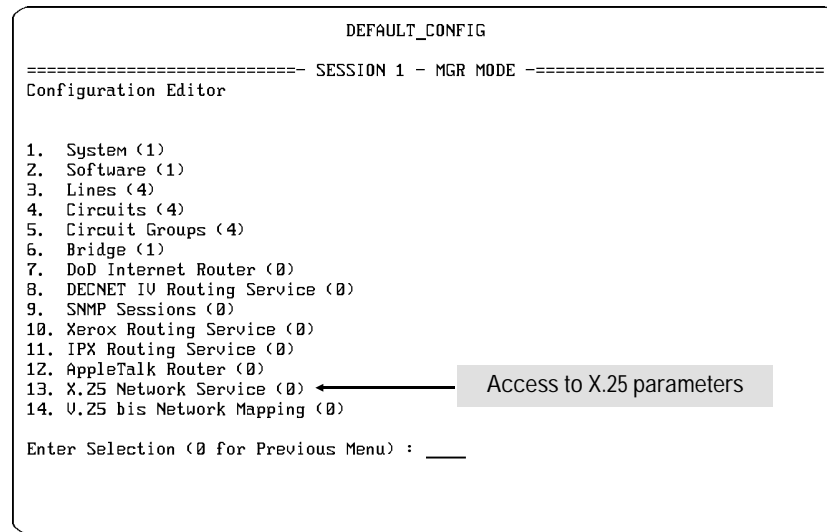


Figure 13-1. Access to X.25 Parameters

X.25 Parameters: Use LAPB circuits to operate X.25 DDN, X.25 PDN, and X.25 Point to Point services.

X.25 Service Parameters

Overview

13

X.25 Service Parameters

Page	X.25 Parameters
13-4	Auto Enable
13-4	Broadcast
13-4	Call Retry Timer (secs)
13-5	Circuit Name
13-5	Circuit Type
13-5	Closed User Group
13-5	Connection ID
13-6	Flow Control
13-6	Group Number
13-6	High PVC LCN
13-6	High SVC LCN
13-7	Internet Address
13-7	IP Address
13-8	Local DTE Address
13-8	Lower Circuit Name
13-8	Low PVC LCN
13-8	Low SVC LCN
13-8	Max Conns
13-8	Max Idle Time (secs)
13-9	Max Link Latency (ms)
13-9	Max Queue Size
13-9	Min Frame Spacing
13-9	Min Idle Time (secs)
13-9	MTU Size
13-10	Outgoing Access
13-10	PDN
13-11	Pkt Size
13-11	Pkt Window
13-11	Precedence
13-11	PVC
13-11	Quality of Service
13-11	Remote DTE Address
13-12	SVC
13-12	T1
13-12	Upper Circuit Name
13-12	X.121 Address

Parameters and Options

Auto Enable	<p>Determines the initial state of the LAPB circuit.</p> <p>The LAPB-specific Auto Enable parameter works in conjunction with the global Auto Enable parameter based on the following criteria:</p> <ul style="list-style-type: none">■ When global Auto Enable is No, the LAPB circuit identified by Circuit Name is unconditionally disabled—the LAPB-specific Auto Enable parameter is disabled when the global Auto Enable parameter is disabled.■ When global Auto Enable is Yes, the LAPB circuit is conditionally enabled—the LAPB-specific Auto Enable parameter can be enabled or disabled when global Auto Enable is enabled. <p>Default: Yes</p> <p>Yes Automatically enables the LAPB circuit when the global Auto Enable parameter is enabled.</p> <p>No Automatically disables the LAPB circuit when the global Auto Enable parameter is enabled. (Then, to enable the circuit after the router boots, use the NCL Interpreter's Enable command.)</p> <p>Note: The LAPB-specific Auto Enable parameter should be set to an applicable setting regardless if the global Auto Enable parameter is enabled. If the global Auto Enable parameter is later enabled, the current setting for the LAPB-specific Auto Enable parameter takes effect.</p>
Broadcast	<p>Identifies IP Address as a possible recipient of broadcast messages.</p> <p>Yes ■ X.25 forwards broadcast messages to IP Address.</p> <p>No ■ X.25 does not forward broadcast messages.</p>
Call Retry Timer (secs)	<p>Sets the interval between call request packets to a specific destination. In the event of an unsuccessful call attempt (for example, the call request is cleared), the router waits Call Retry Timer (secs) before sending another call request to the destination. Any IP datagrams received for the destination during this period are dropped by the router.</p>

Call Retry Timer (secs) is activated in the event of an failed call attempt and prevents a potential “thrashing” situation that may occur when the IP router directs a stream of datagrams to a busy or unreachable destination. With the timer enabled (set at a non-zero value), the X.25 PDN service drops received datagrams and transmits another call request at the expiration of the timer. With the timer disabled (set to 0), the X.25 PDN service sends call request packets for every datagram received from the IP router until the call is accepted.

Default: 60
Range: 0 to 9999

Circuit Name	Accepts an ASCII character string identifying the LAPB circuit name.
Circuit Type	Determines the circuit type.
	LAPB Always set to LAPB—ignore all other protocol options when configuring LAPB circuits.
Closed User Group	Determines whether the lower circuit is connected to a port subscribing to CUG (Closed User Group). For additional information, refer to Table 13-2.
	Default: No
	No Disables CUG security, and access into or out of the router is controlled only by the X.25 features supported by the PDN subscription service.
	Yes Enables CUG security. CUG provides various classes of security, depending on the particular X.25 features purchased from the PDN subscription service. When Closed User Group is set to Yes, the Outgoing Access and Group Number parameters appear on the configuration screen.
Connection ID	Enables the establishment of multiple, parallel dedicated virtual circuits between two routers. Such parallel circuits may result in higher throughput, because of the increased window size afforded by multiple virtual circuits.
	Default: None Range: 1 to 99
Options	<ul style="list-style-type: none"> ■ If you are establishing only one dedicated virtual circuit between the local router and the remote peer designated by Remote DTE Address, enter 1. When configuring the remote peer, you must ensure that you also assign a Connection ID of 1. ■ If you are establishing multiple dedicated virtual circuits between the local and remote peers, you must assign a unique Connection ID to each virtual circuit. When configuring the remote peer, you must ensure that you assign identical Connection ID values.

X.25 Service Parameters

Parameters and Options

Flow Ctrl	Enables or disables Flow Control Parameter Negotiation. Flow Control Parameter Negotiation is available as a subscription option from most service providers. Default: Negot
Deflt	Disables flow control negotiation. With negotiation disabled, the configured values for Pkt Window and Pkt Size serve as the defaults across the circuit. Note: If you disable flow control, assure that the X.25 DCE has also disabled flow control. Additionally, assure that the values selected for Pkt Window and Pkt Size match those of the DCE.
Negot	Enables flow control negotiation. With flow control enabled, the window and packet size are negotiated on a physical circuit basis. Results in the following two parameters: Negotiated Pkt Window Negotiated Pkt Size
Group Number	Accepts the group number of the port assigned to the PDN subscription service. Appears only when the Closed User Group parameter is set to Yes. The Group Number must be the group number associated with the port used to connect with the PDN subscription service. Default: 0 Range: 0 to 99
High PVC LCN	Sets the maximum LCN for a permanent virtual circuit (PVC). The calculation of High PVC LCN is identical to High SVC LCN. For additional information, refer to the High SVC LCN parameter. Note: PVC LCN ranges and SVC LCN ranges must not overlap.
High SVC LCN	Sets the maximum LCN for a switched virtual circuit (SVC). The router supports up to 32 dedicated SVCs (used for X.25 Point-to-Point service) for each LAPB connection and up to 254 VCs per slot (SVCs and PVCs). Upon initialization, the router first allocates dedicated SVCs and PVCs to X.25 Point-to-Point service; it then makes the remaining LCNs available (on an equal basis) to X.25 PDN, X.25 DDN, or X.25 Switch services.
Options	<ul style="list-style-type: none">▪ If the LAPB circuit supports only X.25 Point-to-Point service, add the number of dedicated switched two-way virtual circuits provided for by your X.25 subscription agreement to the value assigned to Low SVC LCN and then decrease the result by 1.▪ If you are configuring only X.25 DDN, X.25 PDN, and/or X.25 Switch service on the current slot, use the following formula to calculate High SVC LCN:

$$\text{High SVC LCN} = [254 / N] + \text{Low SVC LCN} - 1$$

where:

N is the number of LAPB circuits on the slot.

$[254 / N]$ is the integer quotient of 254 divided by *N*.

Low SVC LCN is the value assigned to the Low SVC LCN parameter.

- If you are configuring a combination of X.25 DDN, X.25 PDN or X.25 Switch service in conjunction with X.25 Point-to-Point service, use the following formula to calculate High SVC LCN:

$$\text{High SVC LCN} = [(254 - V) / N] + \text{Low SVC LCN} - 1$$

where:

V is the number of X.25 Point-to-Point service dedicated virtual circuits and PVCs on the slot.

N is the number of LAPB B circuits on the slot.

$[(254 - V) / N]$ is the integer quotient of (254 - *V*) divided by *N*.

Low SVC LCN is the value assigned to the Low SVC LCN parameter.

Enter the value of High SVC LCN (within the range 0 to 4095) as calculated above, then press **Return**.

Note: Because the LCN range for the physical link determines the number of virtual connections that can be established, the values assigned to Low SVC LCN and High SVC LCN must be identical on both sides of the X.25 physical link.

Note: PVC LCN ranges and SVC LCN ranges must not overlap.

Internet Address	Specifies the 32-bit IP address of Upper Circuit Name. Enter this address in dotted-decimal notation. The DDN algorithm maps the IP address to an X.121 address. For more information about entering addresses in dotted-decimal notation, refer to Appendix D, "Network Addresses".
IP Address	Accepts the IP address of a recipient of IP datagrams transmitted by an X.25 PDN service. Enter the 32-bit IP address in dotted-decimal notation. For more information about entering addresses in dotted-decimal notation, refer to Appendix D, "Network Addresses".

X.25 Service Parameters

Parameters and Options

Local DTE Address	Sets the network-supplied decimal number (X.121 Address) identifying the interface between the router and the X.25 network. After assigning the local DTE address, the screen prompts for X.25 address map data.
Lowexxr Circuit Name	Assigns the circuit providing the LAPB service. Enter the name of the previously configured LAPB circuit.
Low PVC LCN	<p>Sets the minimum LCN for a permanent virtual circuit (PVC). The LCN is a decimal number that identifies the PVC.</p> <p>Default: 33 Range: 0 to 4095</p> <p>Note: PVC LCN ranges and SVC LCN ranges must not overlap.</p>
Low SVC LCN	<p>Sets the minimum LCN for a switched virtual circuit (SVC). The LCN is a decimal number identifying the switched virtual circuit.</p> <p>Default: 1 Range: 0 to 4095</p> <p>Note: PVC LCN ranges and SVC LCN ranges must not overlap.</p>
Max Conns	<p>Specifies the maximum number of connections simultaneously established with IP Address. The X.25 PDN service clears any incoming calls exceeding this limit. Similarly, the X.25 PDN service makes no attempt to place out going calls that would exceed this limit. The establishment of multiple connections with a single destination may improve throughput by increasing the window size.</p> <p>Default: 2</p>
Options 1, 2, 3, 4	
Max Idle Time (secs)	<p>Specifies the maximum period that a call can remain idle. After the expiration of max idle timer, the router clears the call. This parameter is intended to minimize CPU and network overhead during periods of low datagram traffic. If Min Idle Time (secs) is set to 0, this parameter is ignored.</p> <p>Default: 120 Range: 0 to 9999</p> <p>Note: If the IP router uses the Routing Information Protocol (RIP), you should set the Max Idle Time parameter to a value greater than 30 seconds (the RIP update period) to prevent call/clear thrashing.</p>

Max Link Latency (ms) (0=none)	Determines how many bytes can be queued on a WAN link (expressed in milliseconds). For a detailed description, refer to “Max Link Latency (ms) (0=none)” on page -.
Max Queue Size	<p>Sets the maximum size (in packets) of the transmit queue of each individual X.25 virtual circuit. If the value specified by Max Queue Size is exceeded, the router drops the oldest packet(s) in the transmit queue.</p> <p>Default: 10 Range: 1 to 999</p>
Min Frame Spacing	<p>Sets the minimum number of flag sequences prefixed to an X.25 packet.</p> <p>As is the HDLC packet, an X.25 frame is prefixed by a variable number of 8-bit flag sequences, and is terminated by a single instance of the same flag. Therefore, the number of flags transmitted between sequential frames is equal to the constant 1 (the trailing flag) plus the (variable) number of leading flags.</p> <p>After determining the minimum number of flags to prefix to each frame, reduce this number by 1 (to account for the terminating flag).</p> <p>Default: 2 Range: 2 to 62 (even values only)</p>
Min Idle Time (secs)	<p>Sets the minimum period of circuit inactivity (no IP datagrams sent to or received from IP Address) before a circuit can be cleared and reused for a call to another destination. A value of 0 (implying an infinite idle time) prevents a connection to IP Address from ever being cleared once such a connection is established.</p> <p>Default: 10 (seconds) Range: 0 to 9999</p>
MTU Size	<p>Sets the maximum number of bytes in a packet delivered to the X.25 PDN service from an upper level redirecting protocol. It facilitates X.25 PDN service if the remote end of the virtual circuit requires a specific data packet length.</p> <p>Allowable values are in the range up to 1600 bytes (the largest packet sent by an upper level redirecting protocol to X.25 PDN). Should you enter a value greater the 1600, X.25 enforces the upper boundary limit.</p> <p>Default: 590 Range: 0 to 1600</p> <p>Note: Ensure that the value you enter at MTU Size is equal to or greater than the value specified at Pkt Size.</p>

X.25 Service Parameters

Parameters and Options

N2	<p>Determines the number of times a frame is retransmitted before the circuit is reset. If a frame remains unacknowledged at the expiration of the T1 timer, X.25 retransmits the outstanding frame up to N2 times, with each retransmittal requesting an immediate acknowledgment. If the frame remains unacknowledged after N2 retries, the router resets the LAPB circuit.</p> <p>Default: 20 Range: 1 to 255.</p>										
Negotiated Pkt Size	<p>Appears when Flow Control is set to Negot. Specifies the packet size that appears in the facilities field of Call Request packets originated on Circuit Name.</p> <p>Default: 128 Range: 128 through 2048</p>										
Negotiated Pkt Window	<p>Appears when Flow Control is set to Negot. Specifies the packet size that appears in the facilities field of Call Request packets originated on Circuit Name.</p> <p>Default: 2 Range: 1 through 7</p>										
Outgoing Access	<p>Determines whether the router can initiate calls to other routers or data terminal devices that are not in CUG. Appears and operates only when the Closed User Group parameter is set to Yes.</p> <p>Default: No</p> <table><tr><td>No</td><td>Prevents the router from initiating calls to other routers and remote terminal devices.</td></tr><tr><td>Yes</td><td>Allows the router to initiate calls to other routers and remote terminal devices.</td></tr></table>	No	Prevents the router from initiating calls to other routers and remote terminal devices.	Yes	Allows the router to initiate calls to other routers and remote terminal devices.						
No	Prevents the router from initiating calls to other routers and remote terminal devices.										
Yes	Allows the router to initiate calls to other routers and remote terminal devices.										
PDN	<p>Identifies the supplier of X.25 services.</p> <p>Default: TELENET</p> <table><tr><td>DDN</td><td>The Defense Data Network (DDN) provides end-to-end connectivity between the router and a remote host or gateway equipped to support DDN Standard Service. DDN service is used only by TCP/IP to transmit IP datagrams over the DDN.</td></tr><tr><td>TELENET</td><td>PDN subscription service.</td></tr><tr><td>UK-PSS</td><td>PDN subscription service.</td></tr><tr><td>NET2</td><td>PDN subscription service.</td></tr><tr><td>Other</td><td>Same as TELENET</td></tr></table>	DDN	The Defense Data Network (DDN) provides end-to-end connectivity between the router and a remote host or gateway equipped to support DDN Standard Service. DDN service is used only by TCP/IP to transmit IP datagrams over the DDN.	TELENET	PDN subscription service.	UK-PSS	PDN subscription service.	NET2	PDN subscription service.	Other	Same as TELENET
DDN	The Defense Data Network (DDN) provides end-to-end connectivity between the router and a remote host or gateway equipped to support DDN Standard Service. DDN service is used only by TCP/IP to transmit IP datagrams over the DDN.										
TELENET	PDN subscription service.										
UK-PSS	PDN subscription service.										
NET2	PDN subscription service.										
Other	Same as TELENET										

TRANSPAC	PDN subscription service.
Use Bitmap	Displays the Bitmap (hex) field and allows you to construct a 32-bit status word for specifying certain low-level attributes of the interface between the router and the X.25 service provider. Table 13-1 (page 13-13), "X.25 PDN Parameter Bitmap Argument Values", shows you how to construct the status word. Enter the status word in eight-digit hexadecimal format.
Pkt Size	<p>Determines the maximum number of bytes in the information field of an X.25 level-3 packet.</p> <p>Default: 128 Range: 1 to 2048</p> <p>Note: Current buffer size limitations prevent upper level redirecting protocols from presenting packets larger than 1600 bytes to X.25. Consequently, the actual maximum size of the information field that will actually be transmitted by X.25 (even if Pkt Size is set to 2048) is 1600 bytes.</p>
Pkt Window	<p>Determines the maximum number of outstanding (unacknowledged) packets.</p> <p>Default: 2 Range: 1 to 127</p>
Precedence	<p>Enables or disables a request for "Level 0" precedence.</p> <p>Default: Deflt</p>
	<p>Deflt Disables precedence requests.</p>
	<p>Negot Enables a request for "Level 0" precedence in all outgoing calls.</p>
PVC	<p>Enables or disables permanent virtual circuits (PVCs).</p> <p>Default: No</p>
	<p>No Disables permanent virtual circuits.</p>
	<p>Yes Enables permanent virtual circuits. When PVC is enabled, the Low PVC LCN and High PVC LCN parameters take effect.</p>
Quality of Service	Determines the quality of service. You must set this parameter to X.25 for LAPB circuits.
Remote DTE Address	Specifies the network-supplied decimal number (X.121 address) identifying the interface between the remote peer and the X.25 network.

X.25 Service Parameters

Parameters and Options

SVC	<p>Enables or disables switched virtual circuits (SVCs).</p> <p>Default: Yes</p> <p>No Disables switched virtual circuits.</p> <p>Yes Enables switched virtual circuits. When SVC is enabled, the Low SVC LCN and High SVC LCN parameters take effect.</p>
T1	<p>Sets the T1 time interval, in tenths of a second, determining how long a frame can remain unacknowledged.</p> <p>Default: 30 Range: 1 to 9999</p> <p>Typically, a T1 value in excess of three seconds is required only if your network connection has a substantial path delay (for instance, if the connection is accomplished with a satellite link). Under these conditions, T1 must have a value greater than the round-trip frame-transmission time, plus the time required to process the frame at the receiving end.</p> <p>Note: If the T1 value is too small, throughput is reduced because of needless retransmittal of frames. If T1 is too large, X.25 takes an excessive length of time to detect lost frames.</p> <p>Enter the T1 timer value, taking note that the timer is expressed in tenths of seconds (for example, a value of 30 sets the timer to 3 seconds). The value of T1 must be the same for both ends of the link.</p>
Upper Circuit Name	<p>Identifies a “software circuit” or “pipe” providing the interface between a protocol suite (for PDN, this is TCP/IP) and X.25 packet-level services. The upper circuit provides an interface between the upper layer protocol and X.25 network services. The lower (LAPB) circuit, in contrast, provides an interface (via a device driver) between X.25 network services and the X.25 service provider.</p>
X.121 Address	<p>Accepts the X.121 address corresponding to IP Address.</p>

Table 13-1. X.25 PDN Parameter Bitmap Argument Values

Bit Number	Function	ON (logical 1)	OFF (logical 0)
20 to 31	Reserved for future use	n/a	n/a
19	LINE_MODE	X.25 line behaves as a DCE at network and data-link layers, but remains DTE at physical layer.	X.25 line behaves as a DTE at network, data-link, and physical layers.
18	FRAME LEVEL KEEP_ALIVE	An RR with Poll Bit set is generated when the link has been idle for 2 seconds. In the absence of DCE response, normal retry and link recovery procedures will be initiated.	The link is not polled when it has been idle.
17	X.25	The 1984 version of X.25 is supported.	The 1980 version of X.25 is supported.
16	ADDRESS SUPPRESSION	The local X.121 address is not included in any call packet sent from the device.	The local X.121 address is included in all locally originated call packets.
15	LINE RESTART	A RESTART packet is transmitted whenever Frame Level is established.	Frame Level establishment does not generate a RESTART packet.
14	DATAPAC FACILITIES	Enables special DATAPAC facilities checking.	Disables special DATAPAC facilities checking.
13	UNASSIGNED LCN	X.25 clears calls received on an invalid LCN.	X.25 ignores calls received on an invalid LCN.
12	CLEAR LENGTH	X.25 rejects CLEAR INDICATION and CLEAR CONFIRMATION packets if they contain facilities or user data.	X.25 accepts CLEAR INDICATION and CLEAR CONFIRMATION packets even if they contain facilities or user data.
11	TIMER DIAG	If a T20 (3 minutes) timeout occurs, a RESTART packet is retransmitted with the original diagnostic code.	If a T20 timeout occurs, a RESTART packet is retransmitted with a "T20 Expired" diagnostic code.

X.25 Service Parameters
Parameters and Options

Table 13-1. X.25 PDN Parameter Bitmap Argument Values *(Continued)*

Bit Number	Function	ON (logical 1)	OFF (logical 0)
10	COLLISION REJECT	If a Clear Collision occurs, and the received CLEAR packet has a bad length, a new CLEAR packet is sent with a diagnostic code.	If a Clear Collision occurs, and the received CLEAR packet has a bad length, a new CLEAR packet is dropped.
9	D BIT CONFIRMATION	Disables the D bit in CALL CONFIRM packets.	Enables the D bit in CALL CONFIRM packets.
8	CALL DATA	X.25 will accept a CALL ACCEPT packet containing a User Data field, even if Fast Select was not specified in the call request.	X.25 will not accept a CALL ACCEPT packet containing a User Data field, unless Fast Select was specified in the call request.
7	ACTIVE CONNECTION	X.25 begins sending SABMs as soon as the physical connection is established.	X.25 waits for an SABM from the remote end to initiate establishment of Frame Level.
6	N2 ACTION	If X.25 is waiting for a UA, and receives either a T1 timeout or a DM, it retries the SABM up to N2 times. If after N2 retries, it has still not received a UA, it goes to disconnect mode and ceases to transmit SABMs.	If X.25 is waiting for a UA, and receives either a T1 timeout or a DM, it retries the SABM up to N2 times. If after N2 retries, it has still not received a UA, it goes to disconnect mode and continues sending SABMs at intervals of T3 (20) seconds.
5	INFO COUNT	If the X.25 (1) enters the T1 timeout state, (2) sends an RR, (3) obtains an RR response, and (4) then retransmits the unacknowledged INFO frame—the retry counter is not cleared until the retransmitted INFO frame is acknowledged. This procedure avoids an endless loop that would occur if the DCE were processing RR frames, but not INFO frames.	If the X.25 (1) enters the T1 timeout state, (2) sends an RR, (3) obtains an RR response, and (4) retransmits the unacknowledged INFO frame—the retry counter clears immediately per the CCCIT definition. This procedure leaves open the possibility of an endless loop if the DCE were processing RR frames, but not INFO frames.
4	DISC ACTION	If X.25 sends an SABM (or is waiting for one), and receives a DISC, it sends an SABM immediately after responding to the previous flag.	If X.25 sends an SABM (or is waiting for one), and receives a DISC, it disconnects the link after responding to the previous flag.

Table 13-1. X.25 PDN Parameter Bitmap Argument Values *(Continued)*

Bit Number	Function	ON (logical 1)	OFF (logical 0)
3	DISC ANSWER	If X.25 sends an SABM (or is waiting for one), and receives a DISC, it responds with a UA.	If X.25 sends an SABM (or is waiting for one), and receives a DISC, it responds with a DM.
2	CLEAR P/F	Receiving an unknown frame causes an FRMR frame to be sent with its P/F bit set to zero (0), regardless of the P/F setting in the received frame.	Receiving an unknown frame causes an FRMR frame to be sent with its P/F bit set to the same value as the P/F bit in the received frame.
1	FRMR ON RR	If X.25 sends an FRMR on the line, the reception of an RR frame causes another FRMR to be sent. All other frames (except SABM, DISC, and FRMR) are ignored.	If X.25 sends an FRMR on the line, the reception of any frame other than an SABM, DISC, or FRMR (to clear the condition) is ignored.
0	FORCE FRMR	If X.25 sends an FRMR on the line, the reception of any frame other than an SABM, DISC, or FRMR causes another FRMR to be sent.	If X.25 sends an FRMR on the line, the reception of any frame other than an SABM, DISC, or FRMR is ignored.

Table 13-2. CUG Communication with Devices Outside of the Closed User Group

Type of Subscription Service	Operation Permitted
Incoming and outgoing services	Calls to and from device outside of the group
Outgoing service only (Outgoing Access set to Yes)	Calls to device outside the group
Incoming service only	Calls from devices outside the group
Outgoing service only (Outgoing Access set to No)	No calls to or from devices outside the group

V.25 bis Network Mapping

Overview

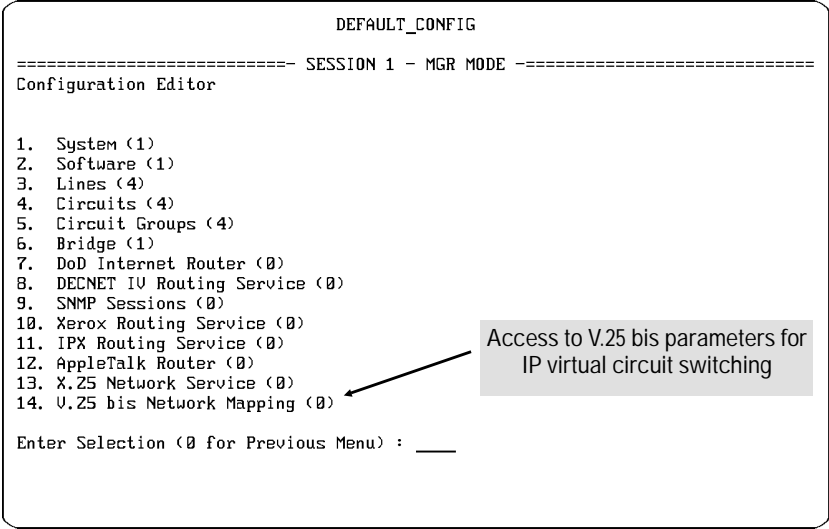


Figure 14-1. Access to Lines, Circuits, and Circuit Group Parameters

V.25 bis Network Mapping Parameters: Enable the router to choose an available port for establishing a v.25 bis connection with a remote router. Used when you want the router to be able to contact more than one next-hop router.

Page	Circuits Parameters
14-3	Connect Retry
14-3	Connect wait time
14-3	Hold down time
14-4	IP Next Hop
14-4	Remote station number
14-4	Subaddress
14-4	VC inactivity time

Parameters and Options

Connect retry count	<p>Sets the number of times per phone number that the router tries to establish a connection if the initial call attempt fails. The range is 1 (try only once) to 30. Where multiple phone numbers are specified, they will be used in a circular fashion. For example, if you set Connect retry count to 3, the router makes up to three call attempts for each outbound phone number you provide. If the router is unsuccessful in establishing a connection, the internal record of connect attempts is reset to zero and an error log message is sent to the error log file. This value overrides the Connect retry count parameter configured for v.25 bis under the Circuits menu.</p> <p>Options Default: Use Circuit defined count Range: 1 to 30</p>
Connect wait time (sec)	<p>Sets how long to wait after trying to make a call for the actual connection to be established. If the connection is not established within the specified time, the router drops DTR and retries the call. ("Retry" means to bring the DTR line back up.) This pattern repeats until either the router makes the connection or the specified number of retries is reached. This value overrides the Connect wait time parameter configured for v.25 bis under the Circuits menu.</p> <p>Options Default: Use Circuit defined time Range: 1, 5, 10, 15, 20, 30, 60, 120, 255, Infinity</p>
Hold down time	<p>Hold down time (sec) is used when there is a failure to establish a v.25 bis connection for this virtual circuit. After a connection failure (retrys have been exhausted), the IP map cannot be re-used until the hold down time has passed. This prevents a circuit from continuously retrying on a remote that it cannot reach at present. The resolution of this parameter is in seconds (between 0 and 720 seconds), or you can select Leave map down on failure. In this case, the map cannot be used until you execute the NCL Enipmap command.</p> <p>Default: 10 Range: 0 – 720; Leave map down on failure</p>

V.25 bis Network Mapping
Parameters and Options

IP Next Hop	Designates the router through which to access the target network. This is the next hop router address configured under IP static routes. Enter the IP address of the next hop router in dotted decimal notation.
Remote Station Number	<p>Is the phone number to the next-hop router. You can assign up to 15 numbers to the same router. If the first number fails, the remaining numbers will be retried in sequence until a connection is made. The last successful number used will be the first tried when the next call is attempted.</p> <p>Each number will be tried as many times as specified in the Connect retry count parameter. Thus, with three phone numbers entered and a Connect retry count set to 3, the router will try up to nine times to establish a connection.</p>
Subaddress	Is any additional phone number, such as an internal extension, required to reach the next-hop router identified by the Remote station number parameter.
VC inactivity time (sec)	Sets the minimum time to leave the v.25 bis circuit up if other virtual circuits are queued waiting for a v.25 bis port to become available. If no other virtual circuits are waiting, then the v.25 bis Minimum connect duration and Connect inactivity time parameters are used.
Options	Default: 10 Range: 1 through 60

Part II

Part II

General Operating Reference

Part II

Using the Statistic Screens

Using the Statistic Screens

This chapter provides a reference to the statistics screen outputs available in Hewlett-Packard routers. For information on how to operate the statistics screens, refer to the *User's Guide*.

The range of statistics available in most Hewlett-Packard routers includes:

AppleTalk Router statistics (page 15-4) Summarizes for each AppleTalk router circuit group how many packets received, forwarded, and dropped.

Bridge statistics (page 15-6) Summarizes for each bridging circuit group how many frames received, forwarded, flooded, and dropped.

Buffers Usage statistics (page 15-8) Provides information on buffer allocation and use.

Circuit statistics (page 15-10) Summarizes for each individual circuit how many bytes and frames were received and transmitted and how many frames contained errors.

DECnet Router statistics (page 15-12) Summarizes for each DECnet router circuit group how many frames received, forwarded, and dropped.

DoD IP Router statistics (page 15-14) Summarizes for each IP router network interface how many datagrams received, forwarded, handled within the router, and dropped.

IPX Router statistics (page 15-16) Summarizes for each IPX network interface how many datagrams received, forwarded, handled within the router, and dropped.

Per Second statistics (page 15-18) Summarizes for each circuit the number of bytes and frames transmitted and received per second.

XNS Router statistics (page 15-20) Summarizes for each XNS network interface: how many datagrams received, forwarded, handled within the router, and dropped.

In the factory default state, the Circuit, Per Second, Bridge, and Buffers Usage statistics are available. The individual routing service statistics are available when the corresponding routing services are enabled by the Protocol parameter in the Software menu in your router's configuration.

Note

All of the above-listed statistics are available in all Hewlett-Packard routers that have the corresponding routing services. To verify the routing services available in your router, refer to the release notes you received with the router or the most recent software update.

AppleTalk Router Statistics Screen

The AppleTalk Router Statistics screen is available if the AppleTalk routing service is enabled in your configuration. This screen summarizes AppleTalk traffic volume for each circuit group. To see more detailed AppleTalk statistics maintained by the router, you can use the NCL Get command.

SAMPLE_CONFIG6-Jan-1991 21:31:46

----- SESSION 1 - MGR MODE -----
Appletalk Router Statistics

NAME	FRAMES:	Receive	Forward	Drop
1. ether1g		0	0	0
2. token1g		0	0	0
3. wan1g		0	0	0
4. wan2g		0	0	0
TOTAL		0	0	0

PRESS: 'r' for reset, Down, Up, <- to exit

Figure 15-1. AppleTalk Router Statistics Screen

Using the Statistic Screens
AppleTalk Router Statistics Screen

Categories on the AppleTalk Router Statistics screen are the following:

NAME	Lists each AppleTalk circuit group by name.
Receive	Lists the number of AppleTalk packets received on the circuit group.
Forward	Lists the number of AppleTalk packets transmitted.
Drop	Lists the number of received AppleTalk packets dropped by the AppleTalk Router.
TOTAL	Lists the total for each of the above counts for all AppleTalk circuit groups.

Bridge Statistics Screen

The Bridge Statistics screen is available if the bridge service is enabled in your configuration. This screen summarizes bridge traffic volume for each circuit group.

```

SAMPLE_CONFIG
6-Jan-1991 20:44:33
----- SESSION 1 - MGR MODE -----
Bridge Statistics

```

NAME	FRAMES:	Receive	Forward	Flood	Drop
1. ether1g		419	0	0	419
2. token1g		0	0	0	0
3. wan1g		0	0	0	0
4. wan2g		0	0	0	0
TOTAL		419	0	0	419

```

PRESS: 'r' for reset, Down, Up, <- to exit

```

Figure 15-2. Bridge Statistics Screen

Categories on the Bridge Statistics screen are the following:

NAME	Lists each individual circuit group by name.
Receive	Lists the number of frames received by the circuit group.
Forward	Lists the number of received frames that were forwarded by the bridge. Forwarding requires that the bridge “learned” the destination address.
Flood	Lists the number of received frames that were flooded by the bridge. Flooding indicates: (1) that the bridge had not “learned” the destination address at the time of packet reception, or (2) the packet contained a multicast address.
Drop	Lists the number of received frames that were dropped by the bridge. Reasons for dropping packets include (but are not limited to): (1) the packet is local to the circuit, (2) the packet was directed to a blocked port, and (3) protocol/source address filtering.
TOTAL	Lists the total for each of the above counts for all circuit groups.

Buffers Usage Statistics Screen

The Buffers Usage Statistics screen, always available, summarizes the allocation, usage, and availability of global memory buffers within the router. Global memory contains two types of buffers: message and packet. Message buffers are used for inter-process communications internal to the router. Packet buffers are used for external network communications by temporarily storing incoming or outgoing data packets.

SAMPLE_CONFIG6-Jan-1991 23:10:17

----- SESSION 1 - MGR MODE -----

Buffers Usage Statistics

NAME	MSG: miss	init	free	min	PKT: miss	init	free	min
--> TOTAL	0	198	184	161	0	376	277	178

PRESS: 'r' for reset, Down, Up, <- to exit

Figure 15-3. Buffers Usage Statistics Screen

Categories on the Buffers Usage Statistics screen are the following:

MSG: miss	Lists the number of times the router was unable to obtain a message buffer (that is, all buffers were in use).
MSG: init	Lists the number of message buffers allocated when the router booted.
MSG: free	Lists the number of message buffers available for use. Due to overhead, the number of buffers available is somewhat less than the number allocated.
MSG: min	Lists the lowest number of message buffers that were available since the router booted. This count corresponds to the MSG: miss count; if message buffers were always available (MSG: min > 0), then MSG: miss = 0.
PKT: miss	Lists the number of times the router was unable to obtain a packet buffer (that is, all buffers were in use).
PKT: init	Lists the number of packet buffers allocated when the router booted.
PKT: free	Lists the number of packet buffers available for use. Due to overhead, the number of buffers available is somewhat less than the number allocated.
PKT: min	Lists the lowest number of packet buffers that were available since the router booted. This count corresponds to the PKT: miss count; if packet buffers were always available (PKT: min > 0), then PKT: miss = 0.

Circuit Statistics Screen

The Circuit Statistics screen summarizes traffic volume for each circuit on the router. For more detailed circuit statistics maintained by the router, use the NCL Get command.

```

-
                                SAMPLE_CONFIG                                6-Jan-1991  20:40:16
-----
--> 1. ether1                    225358                    2586                    861                    4718                    75                    0
    2. token1                     0                      0                      0                      0                      0                    0
    3. wan1                       0                      0                      0                      0                      0                    0
    4. wan2                       0                      0                      0                      0                      0                    0
-----
      TOTAL                    225358                    2586                    861                    4718                    75                    0
-----
PRESS: 'r' for reset, Down, Up, <- to exit

```

Figure 15-4. Circuit Statistics Screens

Categories on the Circuit Statistics screen are the following:

NAME	Lists each individual configured circuit by name.
Rx: Bytes	Lists the number of bytes of data received by the circuit.
Rx: Frames	Lists the number of frames received by the circuit.
Rx: Err	Lists the number of faulty frames (frames that contained an error) received by the circuit.
Tx: Bytes	Lists the number of bytes of data transmitted by the circuit.
Tx: Frames	Lists the number of frames transmitted by the circuit.
Tx: Err	Lists the number of frames that were not transmitted because of errors.
TOTAL	Lists the total for each of the above counts for all circuits.

DECnet Router Statistics Screen

The DECnet Router Statistics screen is available if the DECnet routing service is enabled in your configuration. This screen summarizes DECnet traffic volume for each circuit group. To see more detailed DECnet statistics maintained by the router, you can use the NCL Get command.

```

SAMPLE_CONFIG
6-Jan-1991 20:53:00

===== SESSION 1 - MGR MODE =====
DECnet Router Statistics

      NAME          FRAMES:  Receive    Forward      Drop
-----
--> 1. ether1g             0           0           0
2. token1g                0           0           0
3. wan1g                   0           0           0
4. wan2g                   0           0           0
-----
      TOTAL                0           0           0

PRESS: 'r' for reset, Down, Up, <- to exit

```

Figure 15-5. DECnet Router Statistics Screen

Categories on the DECnet Router Statistics screen are the following:

NAME	Lists each DECnet circuit group by name.
Receive	Lists the number of data frames received on the circuit group.
Forward	Lists the number of data frames transmitted on the circuit group.
Drop	Lists the number of data frames dropped by the router.
TOTAL	Lists the total for each of the above counts for all DECnet circuit groups.

DoD IP Router Statistics Screen

The DoD IP Router Statistics screen is available if DoD Internet (IP) routing is enabled in your configuration. This screen summarizes traffic volume for each IP network interface.

```

SAMPLE_CONFIG
6-Jan-1991 21:01:52
----- SESSION 1 - MGR MODE -----
DoD IP Router Statistics

```

	NAME	PACKETS:	Receive	Transmit	Deliver	Dropped
--> 1.	15.8.129.97		489	107	316	157
2.	15.9.129.97		0	0	0	0
3.	15.10.129.97		0	0	0	0
4.	15.11.129.97		0	0	0	0
	TOTAL		489	107	316	157

```

PRESS: 'r' for reset, Down, Up, <- to exit

```

Figure 15-6. DoD IP Router Statistics Screen

Categories on the DoD IP Router Statistics screen are the following:

NAME	Lists each network interface address in dotted decimal notation.
Receive	Lists the number of IP datagrams received by the network interface.
Transmit	Lists the number of IP datagrams transmitted by the network interface.
Deliver	Lists the number of IP datagrams addressed to the IP router and delivered by the router to one of three upper-layer protocols for processing. The three protocols are ICMP (Internet Control Message Protocol), TCP (Transmission Control Protocol), and UDP (User Datagram Protocol). To see the counts of received and transmitted ICMP datagrams detailed by message type, you can use NCL's Get command.
Dropped	Lists the number of IP datagrams dropped by the network interface. Dropped datagrams include (but are not limited to) datagrams with faulty checksums and datagrams requiring absent protocols. The interface also drops datagrams as directed by source-address filters and destination-address filters that were established during the configuration process.
TOTAL	Lists the total for each of the above counts for all IP network interfaces.

IPX Router Statistics Screen

The IPX Router Statistics screen is available if IPX routing is enabled in your configuration. This screen summarizes traffic volume for each IPX network interface.

```

SAMPLE_CONFIG
6-Jan-1991 21:26:07

----- SESSION 1 - MGR MODE -----
IPX Router Statistics

NAME          PACKETS:  Receive  Transmit  Deliver  Dropped
-----
--> 1. 00000003          0         0         0         0
2. 00000005          0         0         0         0
3. 00000007          0         0         0         0
4. 00000009          0         0         0         0
-----
TOTAL              0         0         0         0

PRESS: 'r' for reset, Down, Up, <- to exit

```

Figure 15-7. IPX Router Statistics Screen

Categories on the IPX Router Statistics screen are the following:

NAME	Lists the network interface address in 8-digit hexadecimal format.
Receive	Lists the number of IPX datagrams received by the network interface.
Transmit	Lists the number of IPX datagrams transmitted by the network interface.
Deliver	Lists the number of IPX datagrams delivered by the router to an upper-layer protocol for processing.
Dropped	Lists the number of IPX datagrams dropped by the network interface. Dropped datagrams include (but are not limited to) datagrams with faulty checksums and datagrams with faulty header information.
TOTAL	Lists the total for each of the above counts for all IPX network interfaces.

Per Second Statistics Screen

The Per Second Statistics screen summarizes traffic volume per second for each circuit on the router.

DEFAULT_CONFIG						
----- SESSION Z - MGR MODE -----						
Per Second Statistics						
NAME	RX:	Bytes	Frames	TX:	Bytes	Frames
-----		-----	-----		-----	-----
--> 1. wanZ1		0	0		0	0
2. ether41		256	4		355	4
-----		-----	-----		-----	-----
TOTAL		256	4		355	4
PRESS: 'r' for reset, Down, Up, <- to exit						

Figure 15-8. Per Second Statistics Screen

Using the Statistic Screens
Per Second Statistics Screen

Categories on the Per Second Statistics screen are the following:

NAME	Lists the circuit name(s).
RX: Bytes	Lists the number of bytes per second of data received by the circuit.
RX: Frames	Lists the number of frames per second received by the circuit.
TX: Bytes	Lists the number of bytes per second of data transmitted by the circuit.
TX: Frames	Lists the number of frames per second transmitted by the circuit.
TOTAL	Lists the total for each of the above counts for all circuits.

XNS Router Statistics Screen

The XNS Router Statistics screen is available if the XNS routing service is enabled in your configuration. This screen summarizes traffic volume for each XNS network interface.

```

_
                                SAMPLE_CONFIG                                7-Jan-1991 19:56:09
=====-- SESSION 1 - MGR MODE -----
                                Xerox Router Statistics

```

	NAME	PACKETS:	Receive	Transmit	Deliver	Dropped
	-----		-----	-----	-----	-----
--> 1.	00000001		0	1	0	0
2.	00000002		0	0	0	0
	-----		-----	-----	-----	-----
	TOTAL		0	1	0	0

```

PRESS: 'r' for reset, Down, Up, <- to exit

```

Figure 15-9. XNS Router Statistics Screen


Categories on the XNS Router Statistics screen are the following:

NAME	Lists the network interface address in 8-digit hexadecimal format.
Receive	Lists the number of XNS datagrams received by the network interface.
Transmit	Lists the number of XNS datagrams transmitted by the network interface.
Deliver	Lists the number of XNS datagrams delivered by the router to an upper-layer protocol for processing.
Dropped	Lists the number of XNS datagrams dropped by the network interface. Dropped datagrams include (but are not limited to) datagrams with faulty checksums and datagrams with faulty header information.
TOTAL	Lists the total for each of the above counts for all XNS network interfaces.

Using the Network Control Language

Managing Router Operations and Resources

The commands available in this category are the following.

Command	Function
 <i>[repetitions]</i>	Repeat the last NCL command (page 16-4).
Atping <i>x.x [wait]</i>	Send an AppleTalk Echo Protocol request to another AppleTalk node (page 16-4).
Boot	Reboot the router (page 16-5).
Browse	Display the entire current configuration, in Configuration Editor format (page 16-6).
Config	Display the entire current configuration, in machine-readable format (page 16-6).
Crash	Display the router's shutdown history (page 16-7).
Date <i>[mm/dd/yy] [hh:mm:ss]</i>	Set or display the router's current date and time (page 16-7).
Disable <i>identifier</i>	Disable a protocol, service, slot, or other configuration entity (page 16-8).
Edit	Invoke the Configuration Editor without leaving NCL (page 16-8).
Enable <i>identifier</i>	Enable a protocol, service, slot, or other configuration entity (page 16-9).
Exit	Leave NCL and return to the Main menu (page 16-10).
Help <i>[type]</i>	Get help for NCL commands (page 16-10).
Log <i>[specifier]</i>	Lists the following:(page 16-11): <ul style="list-style-type: none">■ The event log messages generated since the last boot.■ Warning, Performance, and Major event log messages only.■ All messages in the current event log. (Lists up to 1000 lines.)■ Only messages that contain the specified text string.
Logi	Invoke the automatically updating Event Log without leaving NCL (page 16-13).
page	Disable and re-enable display-paging mode for the console (page 16-14).
Password	Assign, change, or remove password protection on the router (page 16-15).
Ping <i>X.X.X.X [count] [wait]</i>	Send an Internet Control Message Protocol echo request to another node (page 16-18).
Print <i>output command [type]</i>	Direct NCL display command output to a printer or file (page 16-19).
Quick	Invoke Quick Configuration without leaving NCL (page 16-20).
Rboot <i>X.X.X.X [community]</i>	Reboot the remote router at the indicated IP address (page 16-21)

Using the Network Control Language
Managing Router Operations and Resources

Command	Function
Repeat	Continually repeat the last NCL command until another key is pressed (page 16-22).
Stamp	Display software version information (page 16-23).
Stats	Invoke the Statistics Screens menu without leaving NCL (page 16-24).
Summary	Display the Quick Configuration summary without leaving NCL (page 16-25).
Telnet <i>X.X.X.X</i>	Establish an IP virtual terminal connection to another node (page 16-27).
Test <i>mac_addr [count] [delay]</i>	Send an 802.2 Test packet to another node (page 16-28).
Time <i>[mm/dd/yy] [hh:mm:ss]</i>	Set or display the router's current date and time (page 16-29).

! Repeating the Previous NCL Command

Use the exclamation mark (the **!** key) to repeat the previous NCL command once or a number of times.

Syntax

`![repetitions]`

[repetitions] (optional) specifies how many times to repeat the previous command. If you do not specify a number, it is repeated only once.

Example

<code>get lb.ether1g.recv !</code>	Repeats the Get command for an updated bridge packet count.
------------------------------------	---

Atping: Sending an AppleTalk Echo Protocol Request Message

Use NCL's Atping command to send an AppleTalk Echo Protocol (AEP) request message to a specific AppleTalk node address, as a network-layer test of the reachability of the node.

Syntax

`atping X.X [wait]`

X.X is the AppleTalk address (network number and node identifier) of the target.

[wait](optional) is how many seconds to wait for a response. If an integer is not included, the response must be received in five seconds to be successful.

Examples

<code>atping 178.46 5</code>	Sends AEP request and waits 5 seconds for reply.
<code>atping 178.46 1</code>	Sends AEP request and waits 1 second for reply.

Boot: Rebooting the Router

Use NCL's Boot command to reboot the router. Any changes in configuration or password will take effect, and the console session is restarted.

Note

If you see "NCL ERR—invalid command (ignored)" in response to the Boot command, it is possible you did not use the manager password when starting this console session or did not enter the manager password when prompted in this command.

Syntax

boot	The console displays "Enter current manager password" if a manager password exists.
mgr	mgr is the current manager password, required if assigned. The console displays "Do you want to reboot the system? [y/n]".
y	(Answer yes to go ahead and boot.)

Browse: Displaying the Formatted Configuration

Use NCL's Browse command to display all of the configuration screens that the Configuration Editor presents, as if you had chosen the Browse action for each screen. The configuration is displayed in its entirety on the console screen, not divided into the same interactive screens as the Configuration Editor. You remain in NCL; you do not actually go into the Configuration Editor as selected from the Main menu. The output is divided into screens to fit the console screen, with a prompt for “—MORE—” at the end of each screen, as long as page mode is enabled (as it is by default). Page mode and how to get “more” screens are described on page 16-14.

(To output the configuration display to a printer or file instead of your console screen, see the Print command on page 16-19.)

Syntax

```
browse
```

Config: Displaying the Unformatted Configuration

Use NCL's Config command to display the configuration as stored in nonvolatile memory and read by the router whenever it is booted. This configuration is an ASCII text file and contains all configuration parameter settings. It is not formatted into menus and tables and labeled with field names as presented by the Configuration Editor or by Quick Configuration or by the Browse command. Its lines are arranged for display on the screen.

Before using Config, make sure that page mode is enabled (as it is by default) so that the configuration is displayed one screen at a time with a prompt for “—MORE—”. Page mode and how to get “more” screens are described on page 16-14.

(To output the display of the configuration file to a printer or file instead of your console screen, see the Print command on page 16-19.)

Syntax

```
config
```

Crash: Displaying the Crash and Reboot History

Use NCL's Crash command to display the times and reasons for the last four occasions the router was rebooted or restarted. For the HP Router 650, Crash also displays this information for each of the interface modules. (To output the display to a printer or file instead of your console screen, see the Print command on page 16-19.)

Syntax

```
crash
```

Date: Setting or Displaying the Date and Time

Same as Time Command

Disable: Disabling Configured Entities

Use NCL's Disable command to remove a routing service, a circuit, an X.25 point-to-point virtual circuit, or another configured software object from service. (You cannot use Disable to disable a line.) On the HP Router 650, you can also enable a previously disabled interface module slot. You need to identify the object by its management information base (MIB) variable name or object identification code. See "Managed Objects Table" on page 16-32 and the List command on page 16-35 for object names, codes, and pathnames.

Syntax

```
disable identifier
```

identifier is the pathname identifying the software object. You can use object identification codes and/or object names.

Examples

<code>disable ip</code>	Disables the IP router.
<code>disable 5</code>	(5 is the equivalent object identification code for ip.)
<code>disable cct.ether1 cct.wan1</code>	Disables the circuits named "Ether1" and "WAN1".
<code>disable echo</code>	Disables TCP echo service.
<code>disable pm.2</code>	Disables the interface module in slot 2 (HP Router 650 only).

Edit: Invoking the Configuration Editor

Use NCL's Edit command to switch to the Configuration Editor menu, as if you had chosen "Configuration Editor" from the Main menu, but without leaving NCL. Refer to the *User's Guide* for information on how to use the Configuration Editor. When you choose "Exit without Saving" or "Save and Exit", you will return to the NCL prompt rather than to the Main menu.

Syntax

```
edit
```

Enable: Enabling Configured Entities

Use NCL's Enable command to place a configured protocol application, circuit, an X.25 point-to-point virtual circuit, or other configured software object into service. You would do this for:

- Entities previously disabled using the Disable command
- Entities configured not to be auto-enabled when the router boots
- Configuration conflicts and errors

(On the HP Router 650, you can also enable a previously disabled interface module slot.) You need to identify the object by its management information base variable name or object identification code. See the "Managed Objects Table" on page 16-32 and the List command on page 16-35 for object names, codes, and pathnames.

Syntax

```
enable identifier
```

identifier is the pathname identifying the software object. You can use object identification codes and/or object names.

Examples

<code>enable ip</code>	Both enable the IP router.
<code>enable 5</code>	(5 is the equivalent object identification code for ip.)
<code>enable cct.ether1 cct.wan1</code>	Enables the circuits named "Ether1" and "WAN1".
<code>enable echo</code>	Enables TCP echo service.
<code>enable pm.2</code>	Enables the interface module in slot 2 (HP Router 650 only).

Exit: Leaving NCL, Back to the Main Menu

Use NCL's Exit command to exit NCL and return to the Main menu (see figure 1-2 in chapter 1).

Syntax

```
exit
```

Help: Listing the NCL Commands

Use NCL's Help command to display a summary of syntax and functions of NCL commands. (To output the display to a printer or file instead, see the Print command on page 16-19.)

Syntax

```
help [type]
```

[*type*] (optional) specifies a portion (as shown below) of all the NCL commands to list. If you do not specify the portion, the most commonly used commands are listed.

rget	For the commands beginning with "rget". (See pages 16-40 through 16-69.)
zmodem	For Zmodem commands. (See page 16-98.)
ospf	For the commands beginning with ospf. (See page 16-72.)
other	For the remaining commands not listed for any of the above.
all	For the entire set of NCL commands.

Examples

```
help
help rget
help zmodem
help all
```

Log: Viewing the Entire Event Log or Selected Message Categories

Use NCL's Log command to display any of the following:

- The event log messages generated since the last boot.
- The entire event log that is stored in RAM (up to 1000 lines)
- The events whose severity is Warning, Performance, or Major
- The events that contain a search string that you specify

This command displays the current log events once and then returns you to the NCL prompt.

Log Lists the contents of the event log generated since the last boot.

Log Filter Lists only the log events whose severity is Warning, Performance, and Major that have occurred since the last boot.

Log 'string': Lists only those log messages having the text string that you designate and which have occurred since the last boot.

Log -a [specifier]: Lists the specified message types contained in the entire event log.

The maximum number of events that can be stored in RAM is 1000. To output the display of a Log command to a printer or file instead of the screen, place the command within the Print command (see page 16-19). For an automatically updating view of the event log, use the Logi command (see page 16-13).

Before using one of the Log commands, make sure that page mode is enabled (as it is by default) so that the events are displayed one screen at a time with a prompt for "—MORE—". Page mode and how to get "more" screens are described on page 16-14.

Refer to chapter 17 for how to interpret the events listed. You will not use the accessing commands described in that chapter, however; you will use NCL's accessing commands described in the "More" section on page 16-14.

Syntax

```
log
log filter
```

```
log 'string'  
log -a  
log -a filter  
log -a 'string'
```

Examples of Log “string”


log 'mgr'	Displays all messages in the event log (since the last boot) that have the string “mgr”.
log 'rok'	Displays all messages in the event log (since the last boot) that have the string “rok”.
log -a 'mgr'	Displays all messages in the event log that have the string ‘mgr’.
log -a 'rok'	Displays all messages in the event log that have the string “rok”.

Note

The *string* used with Log is not case-sensitive.

In a log 'string' command, you can use a double quote (") instead of a single quote (') if you prefer, and can omit the closing quote mark if it is convenient. For example, all of the following commands produce the same result: log 'cct', log "cct", log 'cct.

Logi: Invoking the Automatically Updating Event Log

Use NCL's Logi command to switch to the event log view, as if you had chosen "Event Log" from the Main menu. The function of Logi is to allow you to go to the event log without leaving NCL. Refer to chapter 17 for information on interpreting the contents of the event log. (If you need to learn how to use the event log, refer to the *User's Guide*.) When you use the  key (left cursor) to exit Event Log, you will return to the NCL prompt rather than to the Main menu.

In contrast to the Log command, Logi allows you to stay in the event log until you exit, and automatically updates the end of the log with the new events that occur.

Syntax

```
logi
```

Page: Toggle Page Mode

Use NCL's Page command to enable or disable page mode. With page mode enabled (the default), output is displayed on the console one page (twenty lines) at a time. With page mode disabled, output is displayed continuously.

Syntax

```
page
```

More: Continuing the Display

When page mode is enabled (as it is by default), and more than twenty lines are required to display all output for an NCL command, you will see “—MORE—” at the bottom of the display area. Your choices are:

- Press a key, such as `[SPACE]`, for an additional screen of data.
- Press `[Return]` for one more line of data.
- Type a number from 1 through 9 to display that number of additional lines.
- Press `[←]` key (left cursor) or `[Ctrl]-[C]` or `[Q]` to stop the display and return to NCL's prompt.

Password: Implementing Password Protection

Use NCL's Password command to assign, change, or remove the passwords protecting console access to the router. Such access may be local, through a modem, or through Telnet. The router is shipped from the factory with no passwords set and thus no password protection. Two types of password can be set: a user password and/or a manager password. To set both passwords, use this command twice. Starting the console session with the *manager* password (if one is set) is required to change either password, change the date or time, boot the router with the Boot command, modify configuration, reset statistics or MIB variables, enable or disable services, download, use the Fget or Fput command, or use the Ping or Test command. In addition, the manager password is again required when using the Boot or Password or Fget OS command. Starting the console session with the *user* password allows monitoring of the router only—viewing statistics, event log, MIB variables, and configuration values.

For added console security with passwords, select “Logout” in the Main menu when leaving a console unattended, and/or use the Configuration Editor to set the Connection Inactivity Time parameter to automatically log out the console session when there's no console activity for the time you configure. After logging out of the session, a password must be given to use the console again. (If a modem is used, “Logout” also gives you the option of disconnecting your modem line.)

Notes

If you see “NCL ERR—invalid command (ignored)” in response to the Password command, it is possible you did not use the manager password when starting this console session or did not enter the manager password when prompted in this command.

Pressing the Clear button on the router removes both passwords, so that a console session could be started and all commands used without giving a password. Use Clear if you forget a password; then set the passwords again with this Password command.

Using the Network Control Language
Managing Router Operations and Resources

Syntax To assign an initial password:

password	The console displays “Which password is changing?”.
type	<i>type</i> is either M for manager or U for user password. The console displays “Enter current manager password”, if a manager password already exists.
mgr	<i>mgr</i> is the current manager password required, if existing, to assign the user password. The console displays “Enter new password”.
new	<i>new</i> is 1 to 14 alphanumeric characters, for the manager or user type you selected. (Passwords are case-sensitive; “INTERNET” and “internet” are not equivalent.) The console displays “Enter new password again”.
new	<i>new</i> is the same new password you typed above.

Syntax To change an existing password:

password	The console displays “Which password is changing?”.
type	<i>type</i> is either M for manager or U for user password. The console displays “Enter current manager password” if a manager password exists.
mgr	<i>mgr</i> is the current manager password required, if existing, to change either password. The console displays “Enter current password”.
current	<i>current</i> is the password currently set for the type you selected. The console displays “Enter new password”.
new	<i>new</i> is 1 to 14 alphanumeric characters, for the manager or user type you selected. (Passwords are case-sensitive; “INTERNET” and “internet” are not equivalent.) The console displays “Enter new password again”.
new	<i>new</i> is the same new password you typed above.

Syntax To remove a password from protecting the router:

password	The console displays "Which password is changing?".
type	<i>type</i> is either M for manager or U for user password. The console displays "Enter current manager password" if a manager password exists.
mgr	<i>mgr</i> is the current manager password required, if assigned, to remove either password. The console displays "Enter current password".
current	<i>current</i> is the password currently set for the type you selected. The console screen displays "Enter new password".
<input type="text" value="Return"/>	(Just press <input type="text" value="Return"/> without typing anything else. The console displays "Enter new password again".
<input type="text" value="Return"/>	(Just press <input type="text" value="Return"/> again to confirm.)

Ping: Sending an ICMP Echo Request Message

Use NCL's Ping command to send an Internet Control Message Protocol (ICMP) echo request message to a specific IP address, as a network-layer test of the reachability of the node. Ping does not support loopback (pinging this router) or broadcast addresses. This router must have IP routing configured. After transmitting the request message to the node, the router waits for a response. If it is received within the specified or default interval, the console displays a message indicating that the target is "alive". If an echo response is not received within the specified or default interval, the console displays a message indicating that the target did not respond.

Syntax

```
ping X.X.X.X [count] [wait]
```

X.X.X.X is the IP address of the target node in dotted decimal notation.

[count] (optional) is the number of times to repeat the echo request packet. If an integer is not included, the packet is sent once.

[wait] (optional) is how many seconds to wait for a response. If a second integer is not included, the response must be received in five seconds to be successful.

Examples

ping 15.3.0.99	Sends it once and waits 5 seconds.
ping 15.3.0.99 5	Sends it 5 times and waits 5 seconds.
ping 15.3.0.99 1 30	Sends it once and waits 30 seconds.

Print: Outputting a Display Command to a File or Printer

Use NCL's Print command to redirect the output of any NCL command that displays data on the console screen to a printer or a file. Each line of output is terminated with carriage return and line feed. You can use Print with the commands Help, Time and Date (with no arguments), Summary, Browse, Config, Crash, Stamp, Log, List, Get, and commands beginning with "Rget", as shown for the syntax below.

Printer output: If your console is a terminal or a PC emulating a terminal and has a printer attached, switch on your terminal/emulators function for logging output to the printer (such as `LOG BOTTOM` on HP 700 series terminals), when the command output waits before beginning. Then switch off the printer logging function when the output waits at the end.

File output: If your console is a PC, invoke your terminal emulator function for capturing output in a local file, when the command output waits before beginning. Then switch off the file logging function when the output waits at the end.

Syntax

```
print help
print help rget
print help other
print help all
print time
print date
print summary
print browse
print config
print crash
print stamp
print log
print log filter
```

```
print list [identifier]
print log 'string'
print get identifier
print rget...
print ospf...
```

(Commands beginning with `rget` and with `ospf` are described in later sections of this chapter.)

Quick: Invoking Quick Configuration

Use NCL's `Quick` command to switch to Quick Configuration, as if you had chosen "Quick Configuration" from the Main menu, but without leaving NCL. For information on Quick Configuration, refer to the *User's Guide*. When you exit Quick Configuration, you will return to the NCL prompt rather than to the Main menu.

Syntax

```
quick
```

Quickr: Invoking Quick Remote

Use NCL's `Quickr` command to switch to Quick Remote, as if you had chosen "Quick Remote" from the Main menu, but without leaving NCL. For information on Quick Remote, refer to the *User's Guide*. When you exit Quick Remote, you will return to the NCL prompt rather than to the Main menu.

Syntax

```
quickr
```

Rboot: Rebooting a Remote Router

Use the NCL Rboot command to reboot a remote router having version A.08 or later operating code. Any changes made in the configuration or password since the remote router was last booted will take effect.

Syntax

```
rboot X.X.X.X [community]
```

X.X.X.X is the IP address (in dotted decimal notation) of a port on the remote router.

[community] is the SNMP community name to which the above port is assigned.

If the remote router has no password, the router reboots immediately.

If the remote router has a manager password, you will be prompted to enter the password before the reboot begins:

```
Enter remote password:
```

When the remote router reboots, you will see the message

```
Reboot Successful
```

Note

If no message is received, the remote router may have a version of operating code that predates version A.08 and does not support the Rboot command.

If the reboot does not occur, you may see one of the following messages:

```
Password Incorrect
```

which means that the manager password for the remote router was incorrect.

```
Timeout: no SNMP response recvd
```

A community name may be required, SNMP is not configured, or an incorrect IP address may have been used.

Repeat: Continuing to Repeat the Previous NCL Command

Use NCL's Repeat command to repeat the previous NCL command over and over until you press any key to stop. The frequency interval is configurable using the Screen Refresh Rate parameter in the Configuration Editor; the default is three seconds.

Syntax

```
repeat
```

Example

```
get cct.ether1.octets_tx_ok
```

```
repeat
```

Continually repeats the Get command for an updated octet count.

```
SPACE
```

Stops repeating.

Stamp: Displaying the Operating Code Version

Use NCL's Stamp command to display the router's operating code version and date. (To output the display to a printer or file instead of your console screen, see the Print command on page 16-19.) For example, "A.08.01" is a full version number, which has three fields.

- The character in the first field ("A") identifies the function set included in your router:
 - B: Basic functionality (IP and IPX routing services)
 - A: Advanced functionality (Basic functionality plus AppleTalk, XNS, DECnet, and other features)

(For a more comprehensive listing of features available in your router, refer to the release notes you received with the router or with your most recent software upgrade.)

- The number in the second field ("08", in this case) identifies the release number, common to all HP routers.
- The number in the third field ("01", in this case) identifies the level of update to the release indicated in the second field.

On an HP Series 650 router, Stamp also produces a version and date for each installed interface module.

Syntax

stamp

Stats: Invoking the Statistics Screens

Use NCL's Stats command to switch to the Statistics Screen menu, as if you had chosen "Statistics Screen Menu "from the Main menu, as described in chapter 1. The function of Stats is to allow you to view the statistics screens without leaving NCL. Refer to chapter 15 for information on how to interpret the contents of statistics menus. For information on how to operate the statistics screens, refer to the *User's Guide*. When you choose the Statistics Screens menu item "Return to Previous Menu", you will return to the NCL prompt rather than to the Main menu.

Syntax

```
stats
```

Summary: Displaying the Quick Configuration Summary

Use NCL's Summary command to display the summary table that Quick Configuration presents at the top of the screen. You remain in NCL; you do *not* actually go into Quick Configuration as selected from the Main menu. (To output the display to a printer or file instead of your console screen, see the Print command on page 16-19.)

Syntax

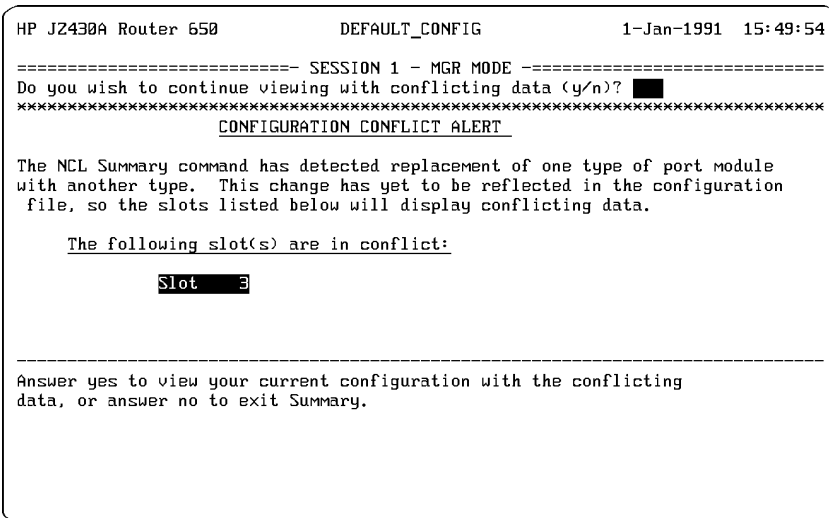
summary

For control of the Summary screen:

- Use the `←`, `→`, `↑`, and `↓` to move in the Summary screen.
- Use the Space bar or `Return` to sequence through the screen and return to the NCL prompt.
- Use the `Ctrl` `C` key combination to exit from any part of the Summary screen and return to the NCL prompt.

Hotswapping in the HP Router 650 If there is a conflict between a slot configuration in the configuration file and the hardware installed in that slot when Summary is invoked (such as when you have hotswapped an interface module but have not yet reconfigured the router), you will see a screen similar to the one shown on the next page.

Using the Network Control Language
Managing Router Operations and Resources



```
HP J2430A Router 650          DEFAULT_CONFIG          1-Jan-1991  15:49:54
=====
----- SESSION 1 - MGR MODE -----
Do you wish to continue viewing with conflicting data (y/n)? 
*****
          CONFIGURATION CONFLICT ALERT
*****

The NCL Summary command has detected replacement of one type of port module
with another type.  This change has yet to be reflected in the configuration
file, so the slots listed below will display conflicting data.

    The following slot(s) are in conflict:

        Slot 3

-----
Answer yes to view your current configuration with the conflicting
data, or answer no to exit Summary.
```

Figure 16-1. The "Conflict Alert" Screen for Summary in the HP Router 650

- If you enter “y” (for “Yes”) you will then see the configuration with the conflicting information.
- If you enter “n” (for “No”) the router exits from Summary and displays the NCL prompt.

Note The above hotswap operation applies only to the HP Router 650.

Telnet: Establishing a Virtual Terminal Connection

Use NCL's Telnet command to establish a Transmission Control Protocol (TCP) virtual terminal connection to a remote node, allowing you to interact with the remote nodes interface. This router must have IP routing and a Telnet session configured. This router supports a maximum of four simultaneous TCP connections. The remote node must have Telnet service.

Syntax

```
telnet X.X.X.X
```

X.X.X.X is the IP address of the remote node in dotted decimal notation.

Example

```
telnet 15.3.0.97
```

Once a connection is established, Telnet passes keystrokes from your router to the remote node.

- If the remote system is another HP router, you will see the system name of the remote node as the NCL prompt at the bottom of the display. You can use the same commands that you use on your own router. You can use NCL's Exit command to exit NCL and access the Main menu on the remote router.

To disconnect, select "Logout" from the Main menu. At:

Do you want to disconnect? [Y/N:]

answer ☒ for yes. The remote node and Telnet are disconnected, and you will see your own system name on the the display.

- If the remote system is not another HP router, then type the appropriate commands to interact with that system. Disconnect Telnet when you are finished. When Telnet is disconnected, you will see your own system name on the display.

Test: Sending an IEEE 802.2 Test Packet

Use NCL's Test command to perform a link-layer test of a directly connected network or a bridged link. Test sends an IEEE 802.2 test packet to a specified target node on a network directly attached to a port on this router, or on a network bridged from a WAN port on this router (for example, using an HP Remote Bridge). The target node must be able to respond to the test packet for the test to work. IEEE 802.3 devices, but *not* Ethernet devices, can respond to the test packet. After transmitting the test packet to the node, the router waits for a response. If a response is received within the specified or default interval, the console displays a message indicating success or response received. If a response is *not* received within the specified or default interval, the console displays a message indicating that the test timed out.

Syntax

```
test mac_addr [count] [delay]
```

mac_addr is the station address of the target node in 12-character hexadecimal format.

[count] (optional) is the number of test packets to send. The number that succeeded will be indicated on the console display. If an integer is not included, the packet is sent once.

[delay] (optional) is how many seconds to wait for a response to each packet. If a second integer is not included, the response must arrive in two seconds to be successful.

Examples

test 080009123456	Sends it once and waits 2 seconds.
test 080009123456 5	Sends it 5 times and waits 2 seconds.
test 080009123456 1 30	Sends it once and waits 30 seconds.

Time: Setting or Displaying the Date and Time

Use NCL's Time command to set the router's clock and/or calendar. Using the Time command without any arguments simply displays the current date and time. (To output the date and time display to a printer or file instead, see the Print command on page 16-19.) The current date and time also are continuously displayed in the upper right corner of the console display. The date and time are always reset when the router's power is switched on.

An alternative to setting the date and time every time power is switched on is to configure the IP Internet's Time protocol and set this router to be a client of a time server elsewhere on the network. However, if this router is configured to be a time server, then you must set its date and time with this command.

Syntax

```
time [mm/dd/yy] [hh:mm:ss]
```

[mm/dd/yy] (optional) is the date in month/day/year format. You can omit /yy to specify the year that is currently set. If you omit the date entirely, it is not changed.

[hh:mm:ss] (optional) is the time specified as hours:minutes:seconds in 24-hour format. You can omit :ss to specify the seconds that are currently set. If you omit the time entirely, the time is not changed.

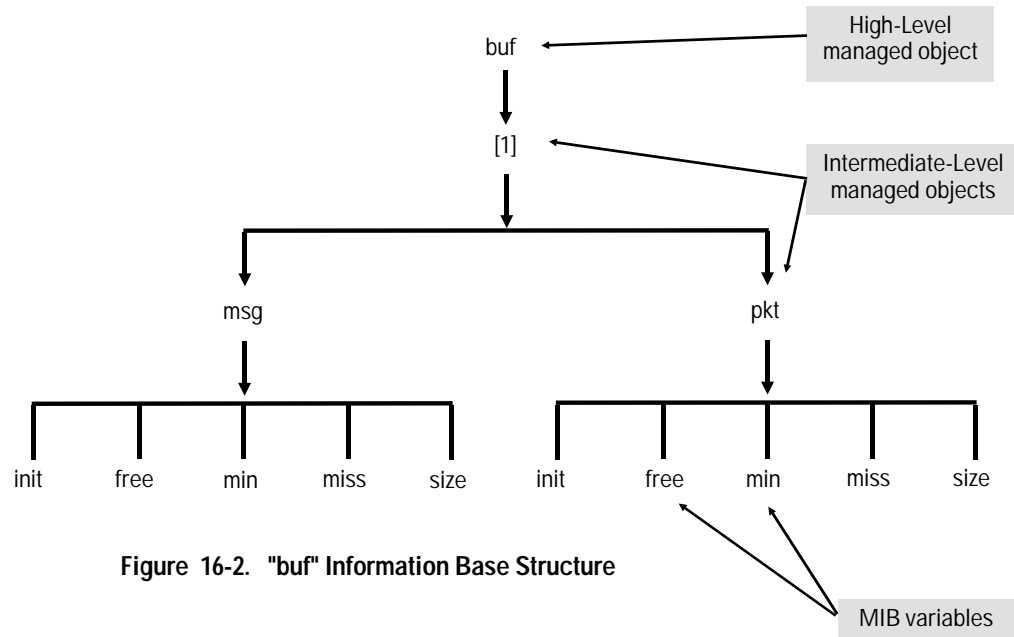
If you omit both arguments, the current date and time are displayed and not changed.

Examples

time 10/29/93 14:15:00	Sets the time and date to 2:15 PM on October 29, 1993.
time 11/20/92	Sets the date to November 20, 1992.
time 23:00:00	Sets the time to 11 PM.
time	Displays current date and time.

Accessing the Management Information Base

The management information base (the MIB) is the repository of all variables gathered and used by the router, as well as accessible to the router's console and to other devices in the network using SNMP. The MIB's hierarchical structure can be represented as an inverted tree, such as the one shown on the next page for the buffers ("buf") object.



The Get, List, and Reset commands use MIB pathnames for access to the MIB structure. For more details on the MIB structure itself and how to specify a pathname to a MIB variable, refer to "Accessing the Management Information Base" in chapter 7 of the *User's Guide*.

The router's "managed objects" define the major MIB categories and are the software resources that enable network services. Which managed objects are currently resident within the router depends on which protocols and services are enabled. (For example, if X.25 service is not configured, the X.25 object is not resident in the router.) The table on page 16-32 lists the managed objects. These managed objects are the heads of objects, leading in some number of levels, or intermediate objects, to single MIB variables. The names of the objects at each level make up pathnames for the variables. Chapter 18, "Management Information Base Variables" lists and defines the MIB variables that are accessed through the managed objects.

Note

Certain managed objects include a slot number in their pathnames. On the HP Router 650, the slot number corresponds to the slot containing the desired MIB activity (slots 2 through 5). On HP series 200 and 400 routers, the slot number is always "1".

Using the Network Control Language

Accessing the Management Information Base

Managed Objects Table

Managed Objects Table (continued)	Name
Alarms (uses slot #)	alarm
AppleTalk router	at
AppleTalk router MIB	atmib
Bridge	lb
Bridge address table	lbmib
Buffers (uses slot #)	buf
Chassis information base	chassis
Circuits	cct
Configuration	config
Data link services	dls
DECnet router	drs
DECnet routing table	decnet
Device drivers (uses slot #)	driver
Event log information base	log
Experimental MIB (for future use)	exmib
Exterior Gateway Protocol	egp
Hardware (uses slot #)	hw
HP network management	hpnm
IP router	ip
IP (Internet) standard MIB	mib
IPX router	ipx
Key	key
Memory (uses slot #)	mem
Name server (uses slot #)	name
OSPF	ospf
Port module manager	pm
Router operating kernel	rok
Simple Network Management Protocol	snmp
System Manager	mgr
System services (SVC) (uses slot #)	svc
Telnet	telnet
Time Protocol	timep
Timers (use slot #)	timer
Transmission Control Protocol	tcp

(Continued on Next Page)

Managed Objects Table (continued)	Name
TCP echo service	echo
Trivial File Transfer Protocol	tftp
V.25 bis	isdn
XNS router	xrx
X.25	x25

Command	The MIB commands are: Function
Get <i>identifier</i>	Display on the console the value of a MIB variable (page 16-34).
List [<i>identifier</i>]	Display on the console a variable or part of the MIB structure (page 16-35).
Reset <i>identifier</i>	Reset the value of a MIB variable to 0 (page 16-39).

Get: Displaying the Value of a MIB Variable

Use NCL's Get command to display the value of a MIB variable on the router. You need to specify the path to the variable. You can obtain the pathname using the List command (see page 16-35). To output the display to a printer or file instead of the screen, place the get command within the Print command (described on page 16-19).

Syntax

```
get identifier
```

identifier is the pathname identifying a specific variable. You must provide the pathname from the router's highest-level objects, using object identification codes and/or object names. You can use the asterisk (*) as a wild card at the end of your identifier. It specifies all variables in the branch descending from the object specified in front of it.

Examples

<code>get telnet.tx_bytes</code>	Displays the value of the Telnet variable "tx_bytes".
<code>get svc.*</code>	Displays values of all system service variables.
<code>get svc[3].*</code>	Displays values of all system-service variables for slot 3 in the router 650.
<code>get config.version[0]</code>	Displays version number of the operating code.

List: Displaying the MIB

Use NCL's List command to display all or any part of the structure of the router's management information base. List tells you what specific variables that part of the MIB contains, showing their pathnames. To output the display to a printer or file instead of the screen, place the List command within the Print command (described on page 16-19). After obtaining the pathname using List, you can use the Get command to see the actual values of the variables (described on page 16-34).

Syntax

```
list [identifier]
```

[identifier] (optional) is the pathname identifying any MIB branch, from the router's highest-level objects to a specific variable. (See the "Managed Objects Table" on page 16-32--and in chapter 7 of the User's Guide--for a list of those objects.) You can use the asterisk (*) as a wild card at the end of your identifier. It specifies the entire branch from the object specified in front of the asterisk. List displays all the MIB branches that descend from the branch you identify (as shown in figure 16-31). If you omit the identifier entirely, List displays all of the router's highest-level objects.

A pathname can be a sequence of names for objects on contiguous levels of the hierarchy, which mirrors the hierarchical structure of the information base. The component names are separated by periods. Some components (such as slot number) are enclosed by square brackets, such as the level below "buf" in figure 16-31; in this case the period in front of the left bracket is omitted. An example is "buf[1].pkt.size".

A pathname can also be specified by equivalent numbers, called object identification codes, in place of each name in the path. The "Examples" section of the List command (below) describes how to discover and use object identification codes for MIB identifiers.

Using the Network Control Language
Accessing the Management Information Base

Examples

<code>list</code>	Displays a list of router-resident managed objects (the items in the “Managed Objects Table”, page 16-32).
<code>list ip.*</code>	Displays the “ip” (IP router) MIB branch. (See the “Managed Objects Table”, page 16-32, for others.)
<code>list buf[2]</code>	Displays a list of the MIB variables for buffers for slot 2 of a Router 650.
<code>list 11.2</code>	Same as preceeding example, except uses object identification codes.

```

                                DEFAULT_CONFIG                                30-Jun-1994  15:54:55
===== SESSION 1 - MGR MODE =====
mgr                                map=0002  code=0
dev                                map=0002  code=1
cct                                map=0002  code=2
lb                                 map=0002  code=3
svc                                map=0002  code=9
buf                                map=0002  code=11
MEM                                map=0002  code=13
name                               map=0002  code=14
timer                              map=0002  code=15
alarm                              map=0002  code=16
hw                                 map=0002  code=30
lbmib                              map=0002  code=31
config                             map=0002  code=35
bootp                              map=0002  code=37
key                                map=0002  code=38
rok                                map=0002  code=51
dls                                map=0002  code=55
testmode                           map=0002  code=56
log                                map=0002  code=57

DEFAULT_CONFIG:
```

Figure 16-3. Example of a List Display

The first column in figure 16-3 names the higher-level objects within the router. The second column (“map=”) contains a hexadecimal number 2 that corresponds to the decimal number 1 in the “[1]” field of some of the variables. (Different values appear for the HP Router 650.) The third column (“code=”) contains the object identification code that corresponds to the object name in the first column.

If you wish to see branches descending from an object in the MIB, use the List command again, with either the name (from the first column of figure 16-3) or the object identification code (from the third column of figure 16-3) for one of the fields in *[identifier]*.

The following paragraphs describe how to use the List command to step through branches of the MIB, using the “buf” information base as an example (see figure 16-2 above).

To begin with “buf” after displaying the objects shown in figure 16-3, you would enter at the NCL prompt:

```
list buf
```

or

```
list 11
```

Note in figure 16-3 that 11 is the object identification code for buffers. It can be substituted for the name “buf”.

In response, the console displays formatted data like the following:

```
[1]                                map=0002code=1
```

(There is only a single branch descending from “buf”).

To see branches descending from “[1]”, you would enter:

```
list buf[1]
```

or

```
list 11.1 (from the code shown in the last response)
```

In response, the console displays formatted data like the following:

```
msg                                map=0002code=0
pkt                                map=0002code= 1
```

To see branches descending from “pkt”, you would enter:

```
list buf[1].pkt
```

or

```
list 11.1.1
```

In response, the console displays formatted data like the following:

```
init                                map=0004code=1
free                                map=0004code=2
min                                 map=0004code=3
miss                                map=0004code=4
size                                map=0004code=5
corrupted                           map=0004code=6
```

Using the Network Control Language

Accessing the Management Information Base

As shown in figure 16-2, those six items are the lowest-level variables in the buffers MIB. If you attempted to use List to display more variables, for example, by entering the following:

```
list 11.1.1.1
```

In response, the console would display no data and simply return you to the NCL prompt. To see the contents of variable 11.1.1.1 ("init"), specify it in the Get command (described on page 16-34).

As defined above for *[identifier]*, you can use the asterisk (*) as a wild card to display the entire buffers information base. Thus, as a short cut for the above procedure, you would enter:

```
list buf.*
```

or

```
list 11.*
```

In response, the console displays the same formatted data seen in the last step of the above procedure:

init	map=0002code=1
free	map=0002code=2
min	map=0002code=3
miss	map=0002code=4
size	map=0002code=5
corrupted	map=0002code=6

Reset: Setting the Value of a MIB Variable to Zero

Use NCL's Reset command to set the value of one or more MIB variables to zero. You can obtain the pathname using the List command (see page 16-35).

Syntax

```
reset identifier
```

identifier is the pathname identifying a specific variable. You must provide the pathname from the router's highest-level objects, using object identification codes and/or object names. You can use the asterisk (*) as a wild card at the end of your identifier. It specifies all variables in the branch descending from the object specified in front of it.

Examples

<code>reset telnet.tx_bytes</code>	Resets the value of the Telnet variable "tx_bytes".
<code>reset lb.lab_net.xmit</code>	Resets the value of the variable containing the number of bridge frames transmitted across circuit group "lab_net".
<code>reset cct.jrb.*</code>	Resets all variables associated with the circuit "jrb".

Accessing the Internet Management Information Base

Internet Request for Comments 1156 defines the variable set required for monitoring and controlling various components of the IP Internet. The router's MIB implementation is fully compliant with all requirements of RFC 1156. Some of the NCL commands work in conjunction with the Simple Network Management Protocol (SNMP) agent and the IP routing application to provide access to the Internet standard MIB. Use these commands to examine the MIB of any local or remote network node that provides a standard SNMP/MIB implementation.

The commands available in this category are the following.

Command	Function
Rgeta	Display the MIB IP address translation table (page 16-41).
Rgeti	Display the MIB IP address table (page 16-42).
Rgetms	Display the value of a branch of Internet standard MIB variables. (page 16-43).
Rgetr	Display the MIB IP routing table. (page 16-45).
Rgets	Display the value of an individual Internet standard MIB variable. (page 16-47).

These commands are described below. They display their output on the console screen. To output the display to a printer or file instead of the console screen, place the command syntax, as shown below for each command, within the Print command (described on page 16-19).

Rgeta: Displaying the MIB IP Address Translation Table

Use NCL's Rgeta command to format and display the Internet MIB IP address translation (ARP) table (also termed the "ARP cache table") for a local or a remote network node.

Syntax

```
rgeta [X.X.X.X] [community]
```

[X.X.X.X] (optional) is the IP address of the local or remote node in dotted decimal notation. If you omit this field, an IP address on the *local*/router will be used.

[community] (optional) is the name of the SNMP community that grants access to that node. If you omit the name, "public" is used. If you include a name, the IP address must also be included.

Example

```
rgeta
```

Displays the Internet MIB IP address translation (ARP) table for this router:

IP Addr	Physical Addr	IF
192.32.1.68	080009297080	1
192.32.1.69	0800090b8ce5	1
192.32.2.74	0800094478a4	2
192.32.3.01	080009a4005e	3

The fields in the table are as follows:

- IP Addr lists the network address (in dotted decimal notation).
- Physical Addr lists the station (also called physical or MAC) address that matches the IP address.
- IF lists the sequential number the router assigned to the network interface.

Rgeti: Displaying the MIB IP Address Table

Use NCL's Rgeti command to format and display the Internet MIB IP address table for a local or remote network node.

Syntax

```
rgeti [X.X.X.X] [community]
```

[X.X.X.X] (optional) is the IP address of the local or remote node in dotted decimal notation. If you omit this field, an IP address on the *local*/router will be used.

[community] (optional) is the name of the SNMP community that grants access to that node. If you omit the name, "public" is used. If you include a name, the IP address must also be included.

Example

```
rgeti 192.32.1.94
```

Displays the MIB IP address table for the node whose IP address is 192.32.1.94:

IP Address	Net Mask	Bcast	IF
192.32.1.94	255.255.255.224	1	1
192.32.1.194	255.255.255.224	1	2

The fields in the table are as follows:

- **IP Address** lists the network address (in dotted decimal notation).
- **Net Mask** lists the subnet mask (in dotted decimal notation) associated with that IP address. The subnet mask is an IP address with all the network bits set to 1 and all the host bits set to 0.
- **Bcast** lists the value of the least-significant bit in the IP broadcast address for that IP address. In most cases the broadcast address type (all 0s or all 1s) can be determined by examining a single bit. In the event of an explicitly assigned broadcast address, however, this single bit is not significant.
- **IF** lists the sequential number the router assigned to the network interface.

Rgetms: Displaying the Values of a MIB Variable Class

Use NCL's Rgetms command to display the values of the variables in a branch of the standard Internet MIB, for either a local or remote network node. You can also use Rgetms to display the values of Internet standard MIB variables on this (local) router. Rgetms defaults the standard Internet MIB portion of the complete pathname, "iso.org.dod.internet.mgmt.mib" or "1.3.6.1.2.1".

Syntax

```
rgetms identifier [X.X.X.X] [community]
```

identifier is the object identification path identifying a branch of Internet MIB variables defined in RFC 1156. Do not include the path to the Internet MIB, 1.3.6.1.2.1, since it is assumed.

[*X.X.X.X*] (optional) is the IP address of the local or remote node in dotted decimal notation. If you omit this field, an IP address on the *local*/router will be used.

[*community*] (optional) is the name of the SNMP community that grants access to that node. If you omit the name, "public" is used. If you include a name, the IP address must also be included.

Examples

```
rgetms 7
```

Displays the values of the Internet MIB User Datagram Protocol (UDP) branch on this router:

1.3.6.1.2.1.7.1.0 =	(number of UDP datagrams delivered to UDP users)
1.3.6.1.2.1.7.2.0 =	(number of received UDP datagrams for which there was no application at the destination port)
1.3.6.1.2.1.7.3.0 =	(number of undeliverable UDP datagrams)
1.3.6.1.2.1.7.4.0 =	(number of transmitted UDP datagrams)

Using the Network Control Language

Accessing the Internet Management Information Base

```
rgetms 6.13 192.32.2.194
```

Displays the Internet MIB Transmission Control Protocol (TCP)
connection table from the node whose IP address is 192.32.2.194:

```
1.3.6.1.2.1.6.13.1.1.192.32.2.194.23.192.32.1.167.1665 =  
(TCP connection state)
```

```
1.3.6.1.2.1.6.13.1.2.192.32.2.194.23.192.32.1.167.1665 =  
(local IP address for the TCP connection)
```

```
1.3.6.1.2.1.6.13.1.3.192.32.2.194.23.192.32.1.167.1665 =  
(local port number for the TCP connection)
```

```
1.3.6.1.2.1.6.13.1.4.192.32.2.194.23.192.32.1.167.1665 =  
(remote IP address for the TCP connection)
```

```
1.3.6.1.2.1.6.13.1.5.192.32.2.194.23.192.32.1.167.1665 =  
(remote port number for the TCP connection)
```

Rgetr: Displaying the MIB IP Routing Table

Use NCL's Rgetr command to format and display the Internet MIB IP routing table for a local or remote network node.

Syntax

```
rgetr [X.X.X.X] [community]
```

[X.X.X.X] (optional) is the IP address of the local or remote node in dotted decimal notation. If you omit this field, an IP address on the *local*/router will be used.

[community] (optional) is the name of the SNMP community that grants access to that node. If you omit the name, "public" is used. If you include a name, the IP address must also be included.

Example

```
rgetr 192.32.1.94
```

Displays the MIB IP routing table for the node whose IP address is 192.32.1.94 (with subnet mask 255.255.255.224):

Destination	Mtr	Next Hop	T/P	Age	IF
192.32.1.32	1	192.32.1.193	R/R	23	2
192.32.1.64	1	192.32.1.94	D/L	12846	1
192.32.1.160	1	192.32.1.193	R/L	12850	2
192.32.10.0	2	192.32.1.193	R/R	25	2
192.32.1.0	2	192.32.1.193	R/R	26	2

Using the Network Control Language

Accessing the Internet Management Information Base

The fields in the table are as follows:

- **Destination** lists the destination subnetwork address (in dotted decimal notation).
- **Mtr** lists the hop count plus cost to **Destination**.
- **Next Hop** lists the address (in dotted decimal notation) of the next hop.
- **T** lists the route type as follows:
 - D a (local) route to a directly connected subnetwork
 - I an invalid route
 - R a (remote) route to a subnetwork not directly connected
- **P** lists how the route type was learned, as follows:
 - E Exterior Gateway Protocol
 - L a statically configured route
 - R Routing Information Protocol
- **Age** lists the number of seconds since the route was learned.
- **IF** lists the sequential number the router assigned to the network interface over which **Next Hop** is reached.

Rgets: Displaying the Value of an Internet MIB Variable

Use NCL's Rgets command to display the value of an individual Internet MIB variable for a remote network node (not this router). You can also use Rgets to display the value of an individual Internet standard MIB variable on this (local) router. Rgets defaults the standard Internet MIB portion of the complete pathname, "iso.org.dod.internet.mgmt.mib" or "1.3.6.1.2.1".

Syntax

```
rgets identifier [X.X.X.X] [community]
```

identifier is the object identification path identifying a specific Internet MIB variable as defined in RFC 1156. Do not include the path to the Internet MIB, 1.3.6.1.2.1, since it is assumed.

[*X.X.X.X*] (optional) is the IP address of the remote target node in dotted decimal notation. If you omit this field, an IP address on the *local*/router would be used.

[*community*] (optional) is the name of the SNMP community that grants access to that node. If you omit the name, "public" is used. If you include a name, the IP address must also be included.

Examples

```
rgets 6.4.0 192.32.1.94
```

Displays the value of the Internet MIB variable 1.3.6.1.2.1.6.4.0 (maximum number of TCP connections) from the node whose IP address is 192.32.1.94:

```
1.3.6.1.2.1.6.4.0 = (the maximum number of TCP connections)
```

```
rgets 7.1.0 192.32.2.194
```

Displays the value of the Internet MIB variable 1.3.6.1.2.1.7.1.0 (number of UDP datagrams delivered to UDP users) from the node whose IP address is 192.32.2.194:

```
1.3.6.1.2.1.7.1.0 = (the number of UDP datagrams)
```

Accessing a Remote Management Information Base

Two NCL commands work with the Simple Network Management Protocol (SNMP) agent and the IP routing application to provide access to the Wellfleet enterprise-specific section of the MIB of a remote HP or Wellfleet router. Hewlett-Packard Company and Wellfleet Communications, Inc., share this definition for their routers. The structure and the variables in this MIB are described in chapter 18. NCL's highest-level branches, listed in the "Managed Objects Table" on page 16-32, are branches in this section of the MIB. These commands default a portion of the complete pathname, "iso.org.dod.internet.private.enterprises.wellfleet.commServer.wfmib" or "1.3.6.1.4.1.18.1.1".

The commands available in this category are the following.

Command	Function
Rgetmw	Display the value of a branch of MIB variables from a remote HP router. (page 16-49).
Rgetw	Display the value of an individual MIB variable from a remote HP router. (page 16-50).

These commands are described below. They display their output on the console screen. To output the display to a printer or file instead of the console screen, place the command syntax, as shown below for each command, within the Print command (described on page 16-19).

Rgetmw: Displaying the Values of a Remote Variable Class

Use NCL's Rgetmw command to display the values of the variables in a branch of the enterprise-specific section of the MIB of a remote HP or Wellfleet router.

Syntax

```
rgetmw identifier [X.X.X.X] [community]
```

identifier is the object identification path identifying a branch of MIB variables. Do not include the path for the private enterprise, 1.3.6.1.4.1.18.1.1, since it is assumed.

[*X.X.X.X*] (optional) is the IP address of the remote router in dotted decimal notation. If you omit this field, an IP address on the *local* router would be used.

[*community*] (optional) is the name of the SNMP community that grants access to that node. If you omit the name, "public" is used. If you include a name, the IP address must also be included.

Rgetw: Displaying the Value of a Remote Variable

Use NCL's Rgetw command to display the value of an individual variable from the enterprise-specific section of the MIB of a remote HP or Wellfleet router.

Syntax

```
rgetw identifier [X.X.X.X] [community]
```

identifier is the object identification path identifying a specific MIB variable. Do not include the path for the private enterprise, 1.3.6.1.4.1.18.1.1, since it is assumed.

[*X.X.X.X*] (optional) is the IP address of the remote router in dotted decimal notation. If you omit this field, an IP address on the *local* router would be used.

[*community*] (optional) is the name of the SNMP community that grants access to that node. If you omit the name, "public" is used. If you include a name, the IP address must also be included.

Examples

```
rgetw 11.2.1.1 15.8.3.94
```

Displays the value of the enterprise-specific MIB variable 11.2.1.1 (the number of packet buffers allocated at router initialization) from the HP or Wellfleet router whose IP address is 15.8.3.94:

```
1.3.6.1.4.1.18.1.1.11.2.1.1 = (number of allocated  
                             packet buffers)
```

```
rgetw 2.1.1 15.8.2.194
```

Displays the value of the enterprise-specific MIB variable 2.1.1 (octets received without error on circuit #1) from the HP or Wellfleet router whose IP address is 15.8.2.194:

```
1.3.6.1.4.1.18.1.1.2.1.1 = (octets received without  
                             error)
```

Accessing a Foreign Management Information Base

Two NCL commands work in conjunction with the SNMP agent and the IP routing application to provide access to the enterprise-specific section of the MIB of any remote node—other than an HP or Wellfleet router—that provides a standard SNMP/MIB implementation. You must use a complete MIB pathname with these commands.

The commands available in this category are the following.

Command	Function
Rget	Display the value of an individual MIB variable from a remote foreign node. (page 16-52)
Rgetm	Display the value of a branch of MIB variables from a remote foreign node. (page 16-53)

These commands are detailed below. They display their output on the console screen. To output the display to a printer or file instead of the console screen, place the command syntax, as shown below for each command, within the Print command.

Rget: Displaying the Value of a Foreign Variable

Use NCL's Rget command to display the value of an individual variable from a foreign enterprise-specific section of the MIB of a remote node.

Syntax

```
rget identifier [X.X.X.X] [community]
```

identifier is the complete object identification path identifying a specific MIB variable.

[*X.X.X.X*] (optional) is the IP address of the remote foreign node in dotted decimal notation. If you omit this field, an IP address on the *local*/router would be used.

[*community*] (optional) is the name of the SNMP community that grants access to that node. If you omit the name, "public" is used. If you include a name, the IP address must also be included.

Example

```
rget 1.3.6.1.4.1.N.n.n.n 15.8.2.2
```

Displays the value of the enterprise-specific MIB variable from the foreign node 15.8.2.2.

1.3.6.1.4.1 is the path to the private enterprise MIB branch.

N is the corporate identifier provided by the Internet Assigned Number authority.

n.n.n is the object identification path assigned by the equipment manufacturer.

Rgetm: Displaying the Values of a Foreign Variable Class

Use NCL's Rgetm command to display the values of the variables in a branch of a foreign enterprise-specific section of the MIB of a remote node.

Syntax

```
rgetm identifier [X.X.X.X] [community]
```

identifier is the complete object identification path identifying a branch of foreign MIB variables.

[*X.X.X.X*] (optional) is the IP address of the remote foreign node in dotted decimal notation. If you omit this field, an IP address on the *local*/router would be used.

[*community*] (optional) is the name of the SNMP community that grants access to that node. If you omit the name, "public" is used. If you include a name, the IP address must also be included.

Example

```
rgetm 1.3.6.1.4.1.N.n.n.n 15.8.2.2
```

Displays the values of the enterprise-specific MIB variable branch from the foreign node 15.8.2.2.

1.3.6.1.4.1 is the path to the private enterprise MIB branch.

N is the corporate identifier provided by the Internet Assigned Number authority.

n.n.n is the object identification path assigned by the equipment manufacturer.

Accessing Bridging and Routing Tables

Some NCL commands work with the SNMP agent and the IP routing application to provide access to application- specific bridging, routing, and configuration tables maintained by local or remote HP routers.

The commands available in this category are the following.

Command	Function
Ospf Rtab*	Display IP's OSPF routing table. (Covered in a later section; page 16-80.**).
Rgeta*	Display the IP address translation table (page 16-41).
Rgetat	Display the AppleTalk configuration table (page 16-55).
Rgetata	Display the AppleTalk Address Resolution Protocol (ARP) table (page 16-57).
Rgetatr	Display the AppleTalk routing table (page 16-58).
Rgetb	Display the bridge forwarding and filtering table. (page 16-59).
Rgetd	Display DECnet configuration table (page 16-60).
Rgetda	Display the DECnet Level 2 routing table (area routes) (page 16-61).
Rgetdn	Display the DECnet Level 1 routing table (node routes) (page 16-63).
Rgeti*	Display the IP address table (page 16-42).
Rgetir	Display the IPX routing table (page 16-64).
Rgetis	Display the IPX Service Advertising Protocol (SAP) table (page 16-45).
Rgetr*	Display the IP routing table (page 16-45).
Rgetrif	Display the source routing Routing Information Field (RIF) cache (page 16-68).
Rgetrxr	Display the source routing Routing Information Field (RIF) cache (page 16-70).

All of the above commands display their output on the console screen. To output the display to a printer or file instead, place the command syntax within the Print command (described on page 16-19).

* The commands for IP tables (marked with an asterisk above) are described in an earlier section, "Accessing the Internet Management Information Base" starting on page 16-40, but are listed here for completeness.

** The command for the OSPF routing table (marked with two asterisks above) is described in a later section of this chapter, "Managing the Open Shortest Path First Protocol", but are listed here for completeness.

Rgetat: Displaying the AppleTalk Configuration Table

Use NCL's Rgetat command to format and display the AppleTalk router configuration table for a local or remote HP router.

Syntax

```
rgetat [X.X.X.X] [community]
```

[X.X.X.X] (optional) is the IP address of the local or remote router in dotted decimal notation. If you omit this field, an IP address on the local router will be used.

[community] (optional) is the name of the SNMPcommunity that grants access to that node. If you omit the name, public is used. If you include a name, the IP address must also be included.

Example

```
rgetat 15.2.1.94
```

Displays the AppleTalk router configuration table for the node with IP address 15.2.1.94:

IF	Net.Node	Net Range	Seed	Default Zone
1	133.45	130-135	N	Printer zone
2	160.37	160-160	N	Sales Dept
3	100.38	100-109	S	Bldg 12

Using the Network Control Language
Accessing Bridging and Routing Tables

Local Zone Table

IF	Zone Name
3	Bldg 12
3	Administration
3	Corporate
2	Sales Dept
1	Printer zone
1	Laser World

The fields in the table are as follows:

- **IF** lists the number the router assigned to the network interface for Net.Node.
- **Net.Node** lists the AppleTalk node address (the network number and node identifier pair) of each AppleTalk router port.
- **Net Range** lists the range of network numbers available to nodes on the directly-connected medium.
- **Seed** lists the configuration source (seed or nonseed). A seed port is configured with the network-identifying information, but a non-seed port obtains it from the network.
- **Default Zone** lists the default zone name for Net Range.
- **Local Zone Table** lists a list of zone names serviced by each of the AppleTalk router ports. This list includes the port's default zone name.

Rgetata: Displaying the AARP Table

Use NCL's Rgetata command to format and display the AppleTalk Address Resolution Protocol (AARP) table for a local or remote HP router.

Syntax

```
rgetata [X.X.X.X] [community]
```

[X.X.X.X] (optional) is the IP address of the local or remote router in dotted decimal notation. If you omit this field, an IP address on the local router will be used.

[community] (optional) is the name of the SNMP community that grants access to that node. If you omit the name, public is used. If you include a name, the IP address must also be included.

Example

```
rgetata 15.2.1.94
```

Displays the AARP table for the node whose IP address is 15.2.1.94:

Net.Node	Phys Address	IF
102.3	080009000411	3
160.147	0800098333ab	12

The fields in the table are as follows:

- **Net.Node** lists the AppleTalk node address (network number and node identifier).
- **Phys Address** lists the station (or physical or MAC) address of Net.Node.
- **IF** lists the sequential number the router assigned to the network interface for Net.Node.

Rgetatr: Displaying the AppleTalk Routing Table

Use NCL's Rgetatr command to format and display the AppleTalk routing table for a local or remote HP or Wellfleet router.

Syntax

```
rgetatr [X.X.X.X] [community]
```

[X.X.X.X] (optional) is the IP address of the local or remote router in dotted decimal notation. If you omit this field, an IP address on the local router will be used.

[community] (optional) is the name of the SNMP community that grants access to that node. If you omit the name, public is used. If you include a name, the IP address must also be included.

Example

```
rgetatr 15.2.1.94
```

Displays the AppleTalk router configuration table for the node with IP address 15.2.1.94:

Destination	Next Hop	Hop	IF
100-109	100.38	0	3
120-129	129.47	2	2
160-160	160.37	0	2
180-180	180.232	2	2
200-200	200.147	2	2
600-600	600.83	1	2

The fields in the table are as follows:

- **Destination** lists the destination network range.
- **Next Hop** lists the AppleTalk node address (the network number and node identifier pair) of the next hop router.
- **Hop** lists the hop count to Destination.
- **IF** lists the number the router assigned to the network interface for Next Hop.

Rgetb: Displaying the Bridge Forwarding/Filtering Table

Use NCL's Rgetb command to format and display the bridge forwarding/filtering table for a local or remote HP or Wellfleet router.

Syntax

```
rgetb [X.X.X.X] [community]
```

[X.X.X.X] (optional) is the IP address of the local or remote router in dotted decimal notation. If you omit this field, an IP address on the *local* router will be used.

[community] (optional) is the name of the SNMP community that grants access to that node. If you omit the name, "public" is used. If you include a name, the IP address must also be included.

Example

```
rgetb 15.2.1.94
```

Displays the bridge forwarding/filtering table for the node whose IP address is 15.2.1.94:

Physical Addr	Src	Dst	CctGrp	IF
080009000411	F	F	Ether1G	1
0800098333ab	F	F	WAN1G	1

The fields in the table are as follows:

- **Physical Addr** lists the station (also called physical or MAC) addresses learned by the bridge.
- **Src** lists the disposition of frames containing **Physical Addr** in the source address field of the Ethernet frame, as follows:
 - F forwarded
 - D dropped
- **Dst** lists the disposition of frames whose destination is **Physical Addr**.
 - F forwarded
 - D dropped
- **CctGrp** lists the circuit group connected to **Physical Addr**.
- **IF** lists the sequential number the router assigned to the network interface that corresponds to **CctGrp**.

Rgetd: Displaying the DECnet Router Configuration Table

Use NCL's Rgetd command to format and display the DECnet router configuration table for a local or remote HP router.

Syntax

```
rgetd [X.X.X.X] [community]
```

[X.X.X.X] (optional) is the IP address of the local or remote router in dotted decimal notation. If you omit this field, an IP address on the local router will be used.

[community] (optional) is the name of the SNMP community that grants access to that node. If you omit the name, public is used. If you include a name, the address must also be included.

Example

```
rgetd 15.2.1.94
```

Displays the DECnet router configuration table for the node with IP address 15.2.1.94:

Name	Stat	Cost	Hello	Prior	I/F
Ether1G	up	4	15	127	1
Token1G	up	3	15	64	2

The fields in the table are as follows:

- **Name** lists the DEC net circuit groups.
- **Stat** contains the current status, up or down, of Name.
- **Cost** contains the cost associated with Name. Costs are set by the circuit group's Cost configuration parameter.
- **Hello** contains the interval (in seconds) between DEC net Hello messages. This interval is set by the circuit group's Hello Timer configuration parameter.
- **Prior** contains the relative priority of the router. Priority is set by the circuit group's Router Priority configuration parameter.
- **IF** lists the sequential number the router assigned to the network interface that corresponds to the circuit group for Name.

Rgetda: Displaying the DECnet Router Level 2 Routing Table

Use NCL's Rgetda command to format and display the DECnet router level 2 (inter-area) routing table for a local or remote HP router.

Syntax

```
rgetda [X.X.X.X] [community]
```

[X.X.X.X] (optional) is the IP address of the local or remote router in dotted decimal notation. If you omit this field, an IP address on the local router will be used.

[community] (optional) is the name of the SNMP community that grants access to that node. If you omit the name, public is used. If you include a name, the address must also be included.

Example

```
rgetda 15.2.1.94
```

Displays the DECnet router inter-area routing table for the node whose IP address is 15.2.1.94:

Area routes for 1.1

Dst	Cst	Hop	Next Hop	IF
1	0	0	0.0	0
10	15	3	2.2	3
7	7	1	1.5	2
60	6	2	3.1	4

The fields in the table are as follows:

- **Dst** lists the destination DEC net area.
- **Cst** contains the circuit cost to Dst.
- **Hop** lists the number of router hops to Dst.
- **Next Hop** lists the DEC net area and node number of the next hop router.
- **IF** lists the number the router assigned to the network interface for Next Hop.

Rgetdn: Displaying the DECnet Router Level 1 Routing Table

Use NCL's Rgetdn command to format and display the DEC net router level 1 (node or intra-area) routing table for a local or remote HP router.

Syntax

```
rgetdn [X.X.X.X] [community]
```

[X.X.X.X] (optional) is the IP address of the local or remote router in dotted decimal notation. If you omit this field, an IP address on the local router will be used.

[community] (optional) is the name of the community that grants access to that node. If you omit the name, public is used. If you include a name, the IP address must also be included.

Example

```
rgetdn 15.2.1.94
```

Displays the DEC net router intra-area routing table for the node 15.2.1.94:

Dst	Cst	Hop	Next Hop	IF
1	0	0	0	0
2	15	1	2	2
4	4	1	4	1

The fields in the table are as follows:

- **Dst** lists the destination node number.
- **Cst** contains the circuit cost to Dst.
- **Hop** lists the number of router hops to Dst.
- **Next Hop** lists the DECnet node number of the next hop router.
- **IF** lists the number the router assigned to the network interface for Next Hop.

Rgetir: Displaying the IPX Routing Table

Use NCL's Rgetir command to format and display the IPX routing table for a local or remote HP or Wellfleet router.

Syntax

```
rgetir [X.X.X.X] [community]
```

[X.X.X.X] (optional) is the IP address of the local or remote router in dotted decimal notation. If you omit this field, an IP address on the *local* router will be used.

[community] (optional) is the name of the SNMP community that grants access to that node. If you omit the name, "public" is used. If you include a name, the IP address must also be included.

Example

```
rgetir 15.2.1.94
```

Displays the IPX routing table for the node whose IP address is 15.2.1.94:

Dst	Next Hop	Mtr	T/P	Age	IF
000b1021	080009000411	0	D/L	101	2
000b1022	0800090333ab	0	D/L	9	3
000b2022	080009000882	1	R/R	4	1

The fields in the table are as follows:

- **Dst** lists the IPX network number of the destination, in 8-digit hexadecimal format.
- **Next Hop** lists the station address of the next hop router.
- **Mtr** (Metric) lists the hop count to **Dst**.
- **T** lists the route type as follows:
 - D a direct (local) route
 - I an invalid route
 - R a remote route
- **P** lists how the route type was learned, as follows:
 - L a static route
 - R Routing Information Protocol

Using the Network Control Language

Accessing Bridging and Routing Tables

- **Age** lists the number of seconds since the route was learned.
- **IF** lists the number the router assigned to the network interface for **Next Hop**.

Rgetis: Displaying the IPX Servers (SAP) Table

Use NCL's Rgetis command to format and display the IPX Service Advertising Protocol (SAP) table for either this router or a remote HP or Wellfleet router that is running IPX.

Syntax

```
rgetis [X.X.X.X] [community]
```

[X.X.X.X] (optional) is the IP address of the local or remote router in dotted decimal notation. If you omit this field, an IP address on the *local* router will be used.

[community] (optional) is the name of the SNMP community that grants access to that node. If you omit the name, "public" is used. If you include a name, the IP address must also be included.

Example

```
rgetis 15.2.1.94
```

Displays the IPX servers that the router whose IP address is 15.2.1.94, discovered by listening to the SAP protocol:

Net Address	Sock	Idx	Name	Age	Hop	Type	IF
00010000.02608c1bbfc3	0451	01	Larry	130	1	24	2

The fields in the table are as follows:

- **Net Address** lists the server IPX network and station address in hexadecimal format.
- **Sock** lists the IPX socket for the server in hexadecimal format.
- **Idx** lists the small index integer that distinguishes multiple servers with the same **Net Address** and **Sock**.
- **Name** lists the IPX servers name (abbreviated to the first 15 characters and *)
- **Age** lists how many seconds since a SAP advertisement of this server was received.
- **Hop** lists the number of hops to the destination specified in **Net Address**.

Using the Network Control Language

Accessing Bridging and Routing Tables

- **Type** lists the service type supplied by the named server, as follows:
 - 0 Unknown
 - 3 Print Server
 - 4 File Server
 - 5 Job Server
 - 9 Archive Server
 - 24 Remote Bridge Server
 - 47 Advertising Print Server
- **IF** lists the number the router assigned to the circuit group used to reach the server.

Rgetrif: Displaying the Source Routing RIF Cache

Use NCL's Rgetrif command to format and display the source routing Routing Information Field (RIF) cache.

Syntax

```
rgetrif X.X.X.X
```

X.X.X.X is the IP address of the local or remote router in dotted decimal notation.

Example

```
rgetrif 15.2.1.94
```

Displays the source routing RIF cache for the node whose IP address is 15.2.1.94:

MAC Src Addr	MAC Dst Addr	Cct Grp	RIF
10005a9631e7	10005a95fb1a	G_T31	0820001120011001
10005a95fb1a	10005a9631e7	WAN1G	0820001170010021

The fields in the table are as follows:

- **MAC Src Addr** lists the station address of the source interface.
- **MAC Dst Addr** lists the station address of the destination interface.
- **Cct Grp** lists the circuit group that connects the source interface to the token ring.
- **RIF** describes the path used to source route packets between the source and destination nodes, in hexadecimal format.

The first two bytes are the routing control (RC) field. These 16 bits (such as 0000 1000 0010 0000 for the first example of 0820h above), from most to least significant, have the following functions:

- 2 bits for RIF type:
 - 00=Specifically Routed Frame

Using the Network Control Language

Accessing Bridging and Routing Tables

10=Spanning Tree Explorer

11=All Routes Explorer

1 bit reserved.

5 bits for the length in bytes (up to 18) of the RIF field.

1 direction bit:

0=frame moves forward

1=frame moves in reverse

4 bits for largest frame size in bytes handled (up to 4472).

3 bits reserved.

Each subsequent series of two bytes (such as 0011h and 7001h in the example above) describe the LAN ID, in the 12 most significant bits, and the bridge ID number, in the 4 least significant bits, of the next hop to the destination.

Rgetxr: Displaying the XNS Routing Table

Use NCL's Rgetxr command to format and display the Xerox XNS routing table for a local or remote HP router.

Syntax

```
rgetxr [X.X.X.X] [community]
```

[X.X.X.X] (optional) is the IP address of the local or remote router in dotted decimal notation. If you omit this field, an address on the local router will be used.

[community] (optional) is the name of the SNMP community that grants access to that node. If you omit the name, public is used. If you include a name, the IP address must also be included.

Example

```
rgetxr 15.2.1.94
```

Displays the XNS routing table for the node whose address is 15.2.1.94:

Dst	Next Hop	Hop	T/P	Age	IF
000b1021	080009000411	0	D/L	101	2
000b1022	0800090333ab	0	D/L	9	3
000b2022	080009000882	1	R/R	4	1

Using the Network Control Language
Accessing Bridging and Routing Tables

The fields in the table are as follows:

Dst lists the XNS network number at the destination, in 8-digit hexadecimal format.

- **Next Hop** lists the station address of the next hop router.
- **Hop** lists the hop count to Dst.
- **T** lists the route type as follows:
 - D direct (local) route
 - I an invalid route
 - R a remote route
- **P** lists how the route type was learned, as follows:
 - L a static route
 - R Routing Information Protocol
- **Age** lists the number of seconds since the route was learned.
- **IF** lists the number the router assigned to the network interface for Next Hop.

Managing the Open Shortest Path First Protocol

OSPF, an IP internal gateway routing protocol, has an openly available protocol specification that is not proprietary to any single vendor. You can display the status of various OSPF elements on this router using the NCL commands listed below. You must use a complete MIB pathname with each of these commands.

The commands available in this category are the following:

Command	Function
Ospf Errs	Display OSPF error counts (page 16-73).
Ospf Intf	Display the status of the OSPF interfaces (page 16-74).
Ospf Lsdb	Display the OSPF link state database (page 16-76).
Ospf Nbrs	Display the status of the OSPF neighbors (page 16-78).
Ospf Rtab	Display IP's OSPF routing table (page 16-80).
Ospf Tq	Display the OSPF timer queue (page 16-82).

These commands display their output on the console screen. To output the display to a printer or file instead of the console screen, place the command syntax, as shown below for each command, within the Print command (described in an earlier section of this chapter).

Ospf Errs: Displaying OSPF Error Counts

Use NCL's Ospf Errs command to format and display the number of errors accrued by OSPF.

Syntax

```
ospf errs
```

Example

```
ospf errs
```

Displays the number of errors, a colon, and the type and name of each error, in two columns. Some of the possible OSPF errors in this table may also appear as event messages in the event log. (For a complete listing of OSPF messages, see “ospf: OSPF Event Messages” in chapter 17).

ERRORS from 4-Oct-94 13:29:03 The time is now 4-Oct-94 18:05:26

0: IP: Bad OSPF pkt type	0: IP: Bad IP Dest
0: IP: Bad IP proto id	0: IP: Pkt svc = my IP addr
0: OSPF: Bad OSPF version	0: OSPF: Bad OSPF checksum
0: OSPF: Bad Intf area id	0: OSPF: Area mismatch
0: OSPF: Bad virt link info	0: OSPF: Auth type != area type
0: OSPF: Auth key != area key	0: OSPF: Packet is too small

Ospf Intf: Displaying the Status of the OSPF Interfaces

Use NCL's Ospf Intf command to format and display the status of the interfaces on this router over which OSPF is running.

Syntax

```
ospf intf
```

Example

Area: 0.0.0.0

IP Address	Type	State	Cost	Pri	DR	BDR
190.190.190.10	Bcast	DR	1	5	190.190.190.10	190.190.190.13

The fields in the table are as follows:

- **Area** lists the area ID for the attached network interface.
- **IP Address** lists the IP address of this interface (in dotted decimal notation).
- **Type** is the kind of network to which the interface attaches, as follows:

Bcast	Broadcast
PtoP	Point-to-Point
Virt	Virtual link

Managing the Open Shortest Path First Protocol

- **State** is the functional level of the interface between adjacent neighbors, as follows:

Down	Inoperable interface.
Loopback	Self-referential interface: not attached to a network.
Waiting	An initial packet has been sent, and the interface is waiting to hear from other routers before selecting the designated router.
Point-to-Point	A point-to-point interface does not select a designated router.
DR	The designated router on this interface.
DR Other	Neither the designated nor backup designated router on this interface.
Backup	The backup designated router on this interface.

- **Cost** lists the cost of sending a packet on the interface, expressed with the link state metric.
- **DR** lists the designated router selected for the attached network.
- **BDR** lists the backup designated router selected for the attached network.

Ospf Lsdb: Displaying the OSPF Link State Database

Use NCL's Ospf Lsdb command to format and display the database OSPF of link state advertisements.

Syntax

```
ospf lsdb
```

Example

LS Database:
Area: 0.0.0.0

Type	Link ID	Adv Rtr	Age	Len	Seq #	Metric
LS_STUB	10.0.0.0	10.0.0.0	236	24	0	0

The fields in the table are as follows:

- **Area** lists the area ID of the link state database.
- **Type** is the type of entry in this database, as follows:

LS_ASE	Describes a route to a destination network external to the AS. Originated by the AS border router.
LS_NET	Describes all routers attached to the network, including the designated router itself. Originated by the network's designated router.
LS_RTR	Describes state and cost of the router's links to the area. Originated by each router in an area.
LS_SUM_ASB	Describes a route to an AS boundary router. Originated by the area border router.
LS_SUM_NET	Describes a route to a destination network belonging to the AS but outside the area. Originated by the area border router.
LS_STUB	Describes a default route for a stub area. Each area border router originates a default summary link into the area).

Managing the Open Shortest Path First Protocol

- **Link ID** is the object attached to the router's link. The value depends on the Type, as follows:

LS_ASE	The destination IP network number.
LS_NET	The designated router's IP interface address.
LS_RTR	The neighbor's OSPF router ID.
LS_SUM_ASB	The AS boundary router's OSPF router ID.
LS_SUM_NET	The destination IP network number.
LS_STUB	The default destination (0.0.0.0).
- **Advrtr** lists the OSPF router ID of the advertisement's originator, which is given for the Type fields above.
- **Age** lists the time in seconds since this link state advertisement was originated.
- **Len** lists the length in bytes of this link state advertisement.
- **Seq #** is a sequential number identifying each successive instance of a link state advertisement, indicating old and duplicate entries.
- **Metric** is the cost of this route.

Ospf Nbrs: Displaying the Status of the OSPF Neighbors

Use NCL's Ospf Nbrs command to format and display the status of the OSPF neighbors.

Syntax

```
ospf nbrs
```

Example

Area: 0 . 0 . 0 . 0

Interface	Router ID	Nbr IP Addr	State	Mode	Priority
190.190.190.10	13.13.13.13	190.190.190.13	Full	Slave	5
190.190.190.10	12.12.12.12	190.190.190.12	Full	Slave	5

The fields in the table are as follows:

- **Area** lists the area ID for the neighbor. (Area ID 0 is reserved for the backbone.)
- **Interface** lists the interface number of the network to which the neighbor is attached.
- **Router ID** lists the 32-bit router ID number of the router in the autonomous system.
- **Nbr IP Addr** lists the IP address of the neighbor (in dotted decimal notation).

Managing the Open Shortest Path First Protocol

- **State** is the functional level of the interface with the neighbor, as follows:

Down	No recent information received from the neighbor, or the initial state of a neighbor conversation.
Attempt	No recent information received from the neighbor, but keep trying. (For neighbors attached to nonbroadcast networks.)
Init	A Hello packet recently seen from the neighbor, but bidirectional communication not yet established.
2-way	Bidirectional communication with the neighbor.
ExStart	First step in creating an adjacency with the neighbor, to decide which is the master router.
Exchange	Neighbors starting database synchronization.
Loading	Link state request packets being sent to the neighbor.
Full	Adjacent neighbors established and databases synchronized.
- **Mode** lists the mode of the neighbor, as follows:

Master	Sends the first database description packet, and allowed to retransmit.
Slave	Responds to the master's database description packet.
- **Priority** lists the router priority of the neighbor, used when selecting the designated router for the attached network.

Ospf Rtab: Displaying the OSPF Routing Table

Use NCL's Ospf Rtab command to format and display the OSPF routing table.

Syntax

```
ospf rtab
```

Example

Dest	D Mask	Area	Cost	E	Path	Nexthop	Advrtr
AS Border Routes:							
14.14.14.14	0.0.0.0	0.0.0.0	2		EXT	190.190.190.13	14.14.14.14
13.13.13.13	0.0.0.0	0.0.0.0	1		EXT	190.190.190.13	14.14.14.14
Area Border Routes:							
14.14.14.14	0.0.0.0	0.0.0.0	2		SUM	190.190.190.13	14.14.14.14
Nets:							
10.0.0.0							
10.0.0.1	255.0.0.0	0.0.0.0	1	0	INTER	10.0.0.1	10.0.0.1

The fields in the table are as follows:

- **Dest** lists the IP network number of the destination.
- **D Mask** lists the IP network mask of the destination.
- **Area** lists the ID of the area whose link state information has led to the routing table entry's collection of paths.
- **Cost** lists, for type 2 external paths, the link state cost of the portion of the path internal to the autonomous system, or the link state cost of the entire path for other types.
- **E** lists, for type 2 external paths, the cost of the path's external portion.

Using the Network Control Language

Managing the Open Shortest Path First Protocol

- **Path** is the type of path, as follows:
 - EXT1 Autonomous system (AS) external path, of type 1.
 - EXT2 Autonomous system (AS) external path, of type 2.
 - INTER Inter-area path, to destinations in other areas.
 - INTRA Intra-area path, to destinations on one of the router's attached areas.
- **Next hop** lists the next hop to the destination.
- **Advrtr** lists, for inter-area and autonomous system external paths, the router ID of the router advertising the summary link or AS external link leading to this path.

Ospf Tq: Displaying the OSPF Timer

Use NCL's Ospf Tq command to format and display the top ten times on OSPF's timer queue.

Syntax

```
ospf tq
```

Example

Type	Minutes	Seconds	USeconds
TQLsaLock	0	5	0
TQAck	0	5	0
TQHelloTimer	0	10	0
TQRetrans	0	10	0
TQSumLsdbAge	7	37	0
TQAselSdbAge	9	11	0
TQIntLsa	10	19	0
TQLsa	12	27	0

Using the Network Control Language
Managing the Open Shortest Path First Protocol

The fields in the table are as follows:

- Type is the type of timer, as follows:

TQAck	Used to send delayed acknowledge messages.
TQAselSa	When the Dijkstra algorithm will be run on external link state advertisements (recalculating the shortest path first tree using the external link information).
TQAselSdbAge	When the external link state database entries will be aged (recalculating the database checksum and checking the age of the entries).
TQHelloTimer	When a Hello packet will be sent.
TQIntLsa	When the Dijkstra algorithm will be run on internal link state advertisements (recalculating the shortest path first tree with respect to the internal areas and nets).
TQIntLsdbAge	When the internal link state database entries will be aged (recalculating the database checksum and checking the age of the entries).
TQLsaLock	When a link state advertisement could be sent (after the minimum allowable time between successive advertisements).
TQRetrans	Used to send pending retransmissions of unanswered OSPF packets.
TQSumLsa	When the Dijkstra algorithm will be run on summary link state advertisements (recalculating the shortest path first tree using summary link information).
TQSumLsdbAge	When the summary link state database entries will be aged (recalculating the database checksum and checking the age of the entries).

- **Minutes, Seconds, m Seconds** specify when the timer was issued.

Blocking and Unblocking Spanning Tree Explorer Frames

Because the spanning tree does not operate automatically on source-routing bridging circuits, it is necessary to “manually” build the spanning tree in these circuits. Two NCL commands allow you to block and unblock forwarding of spanning tree explorer frames on source-routing bridging circuit groups. This is an alternative to changing the Block STE configuration parameter in the Configuration Editor and booting the router to put the change into effect. These commands override the current setting of the Block STE parameter.

The commands available in this category are the following.

Command	Function
Blockste	Block spanning tree explorer frames on a circuit group (page 16-85).
Unblockste	Unblock spanning tree explorer frames on a circuit group (page 16-86).

These commands are described below.

Using the Network Control Language

Blocking and Unblocking Spanning Tree Explorer Frames

Blockste: Block Spanning Tree Explorer Frames

Use NCL's `Blockste` command to block forwarding of spanning tree explorer frames on source-routing bridging circuit groups, overriding the current setting of the Block STE configuration parameter.

Syntax

```
blockste all
```

```
blockste circuit-group
```

circuit-group is the name of a source-routing bridging circuit group.

Examples

```
blockste WAN1G
```

Blocks forwarding of STE frames on circuit group WAN1G.

```
blockste all
```

Blocks forwarding of STE frames on all circuits on this router.

Unblockste: Unblock Spanning Tree Explorer Frames

Use NCL's Unblockste command to restore forwarding of spanning tree explorer frames on source-routing bridging circuit groups, overriding the current setting of the Block STE configuration parameter.

Syntax

```
unblockste all
```

```
unblockste circuit-group
```

circuit-group is the name of a source-routing bridging circuit group.

Examples

```
unblockste WAN1G
```

Unblocks forwarding of STE frames on circuit group WAN1G.

```
unblockste all
```

Unblocks forwarding of STE frames on all circuits on this router.

Controlling IP-Mapped Circuits for V.25 bis

Mapped data is IP data from an IP switched virtual circuit, which is configured by defining an IP static route and a phone number to IP to V.25 bis map entry. Individual map entries can be disabled while leaving others enabled. Three NCL commands are provided for disabling, enabling, and checking the status of virtual IP maps.

The commands available in this category are the following.

Command	Function
Disipmap	Disable an IP map. (page 16-88).
Enipmap	Enable an IP map that was disabled earlier by Disipmap. (page 16-89).
Ipmap	Show the current state of an IP map. (page 16-90).

These commands are described below.

Disipmap: Disabling an IP Map for V.25 bis Switched Virtual Circuits

Use NCL's Disipmap command to disable an IP map entry—a specific location—while leaving the other mappings enabled. Then the IP next hop address configured with this map will remain unreachable as will all of the static routes with which it is associated.

Syntax

```
disipmap X.X.X.X
```

X.X.X.X is the next hop IP address, in dotted decimal notation, of the map to disable.

Using the Network Control Language
Controlling IP-Mapped Circuits for V.25 bis

Enipmap: Re-enabling an IP Map for V.25 bis Switched Virtual Circuits

Use NCL's Enipmap command to enable an IP map that was disabled earlier by using Disipmap.

Syntax

```
enipmap X.X.X.X
```

X.X.X.X is the next hop IP address, in dotted decimal notation, of the map to enable.

Ipmap: Displaying an IP Map for V.25 bis Switched Virtual Circuits

Use NCL's Ipmmap command to display the status of an IP map.

Syntax

`ipmap [X.X.X.X]`

`[X.X.X.X]` (optional) is the next hop IP address, in dotted decimal notation, of the map to show. If you omit this field, all currently configured IP maps are shown. Before using the command this way, make sure that page mode is enabled (as it is by default) so that the resulting display will scroll one screen at a time with a prompt for “—MORE—”. Page mode and how to get “more” are described on page 16-14.

Figure 16-4 shows an example of an Ipmmap display.

```

                                DEFAULT_CONFIG          6-Jun-1993   2:25:26

===== SESSION 1 - MGR MODE =====

IP map information for next hop X.X.X.X
Map state = connected : Queued packets = 0 : Circuit = WAN1
Connect time this connection instance = 36 (seconds)
Non-Mapped data DISALLOWED over this mapped connection
Outbound phone number used 4/4
Total Connect time for this map = 1:36 (minutes:seconds)
Total number of times connections have been made = 2
Packet Totals : Transmitted = 4 : Received = 4 : Dropped = 2

IP Networks accessible using next hop X.X.X.X :
Y.Y.Y.Y Z.Z.Z.Z
*****

DEFAULT_CONFIG:
```

Figure 16-4. Sample IP Map Display

Using the Network Control Language
Controlling IP-Mapped Circuits for V.25 bis

The display of Ipmap information will vary, based on the state of the map when you execute Ipmap. In all cases, the map will show the following data:

- **Next hop** address of the map.
- **Map state** lists one of the following:

disconnected	The map is disconnected; the circuit is available.
disabled	The circuit has been disabled by the Disipmap command.
connecting	The map is in the process of making a V.25 bis connection.
connected	The map is connected and the circuit is in use.
queue wait	The map has data to send, but no pool circuits are currently available. When a circuit becomes available, the map will go into the connecting state. (Refer to the VC inactivity time parameter in chapter 14 of this manual.)
hold down	A map goes into this state if it fails to connect. It cannot be used until the Hold down time expires. The IP address will again be accessible and the map will go into the disconnected state. (Refer to the Hold down time and VC inactivity time parameters in chapter 14 of this manual.)
- **Total** connect time for this map.
- **x** shows the number of separate times this map has succeeded in making a connection.
- **Packet totals** shows the total number of packets successfully transmitted and received, and the number of outbound packets dropped.
- **IP networks accessible** shows all statically configured networks reachable by the given next hop.

In some map states, the following additional information is displayed:

- **Queued packets** shows the number of packets queued to be sent.
- **Circuit** shows the name of the circuit allocated to this map.
- **Inbound or Outbound phone number** shows the phone number for a line connection on this map.

- **Connection time** this connection instance shows the amount of time the map has been connected for the currently alive connection.
- **Non-mapped data** shows whether such data is ALLOWED or DISALLOWED for the currently alive connection (refer to the discussion above on page 16-87).
- **Hold down time left** shows the amount of time this map will remain in the hold-down state.

Using TFTP To Transfer Operating Code, Configuration, and NCL Display

Two NCL commands work in conjunction with the Trivial File Transfer Protocol (TFTP) and IP routing to provide TFTP *server* and *client* capability. Using the commands on this router, you can download the router's operating code or configuration from another router or host on the network, and can copy its operating code or configuration to a host or server for storage and later downloading. You can also redirect the output of any NCL command that displays data on the console screen to a file on another host or server. These network transfers operate over any of the router's network interfaces: LAN or point-to-point.

The commands available in this category are the following.

Command	Function
Fget	Initiate a TFTP read request from a specific host or router for the configuration or operating system (page 16-95).
Fput	Initiate a TFTP write request to a specific host or to an HP Router CR for the configuration or operating system or display command output (page 16-96).

These commands are described beginning on page 16-95.

TFTP Security Features

The router provides some security measures to control access to and use of the TFTP facility. Initial TFTP connection requests are made on the well-known User Datagram Protocol (UDP) port 69. Access to TFTP on a specific network interface can be blocked, therefore, by constructing a TCP/UDP port filter to drop incoming datagrams destined for port 69.

In addition, TFTP does not auto-enable in the default state. While you can configure the TFTP Auto Enable parameter to be “Yes”, this option may not be desirable in environments where security is a concern. Use the following procedure to transfer objects (operating code, configurations, or NCL displays) to or from a system on which TFTP is not auto-enabled.

1. Telnet to the system.
2. Log in.
3. Access the “Network Control Language Interpreter” from the Main menu.
4. Use NCL's Enable command to enable TFTP (`en tftp` on this router).
5. Do the transfer using the Fget or Fput command (or other TFTP command on the remote system).
6. Disable TFTP after completing the transfer (`dis tftp` on this router).

Fget: Loading the Operating Code or Configuration

Use NCL's Fget command with TFTP to download router operating code or a configuration from another HP router on an attached network, using TFTP. The routers must have IP routing and TFTP configured and enabled. See the TFTP security notes on page 16-94.

Note The following limitations apply to the source of operating code downloaded from one router to another using Fget:

Destination Router	Version	Source Router
J2540A or J2540B	B	J2540A or J2540B only
27289B or J2543A	A	27289B or J2543A only
27285/86/87/88/89/90A	A	27285/86/87/88/89/90A only
J2530A	A	J2530A only

Syntax

fget *X.X.X.X* *os file* download router operating code

fget *X.X.X.X* *config file* download router configuration

X.X.X.X is the IP address of the remote router or host in dotted decimal notation.

file is one of the following on the remote node:

os operating code on the router.

config configuration on the router.

filename is the name of the configuration or operating code file on the remote host.

Examples

```
fget 15.3.0.97 os os
```

```
fget 15.3.0.97 config config
```

In response, you will be informed of the progress and successful or unsuccessful completion of the transfer.

Before operating code is downloaded, you will be asked to enter the current manager password if one exists, and to verify that you want the operating system changed (see page 16-15). If downloading operating code fails, the router will be operating but most of the protocols and circuits will be disabled; only the circuit used for TFTP will remain enabled. After the operating code is successfully downloaded, the router burns the new code into ROM (which may take five minutes) and then automatically reboots.

After downloading a new configuration is completed, you may modify it. You must reboot the router for the new configuration to take effect.

Fput: Storing the Configuration, Operating Code, or Display Command Output

Use NCL's Fput command to copy router operating code, the router's configuration, or the output of an NCL display command (Help, Time and Date with no arguments, Summary, Browse, Config, Crash, Stamp, Log, List, Get, or a command beginning with "Rget") to a file on a remote host or HP Router CR on an attached network, using TFTP. You cannot use Fput to put the operating code or configuration on another router; Fget must be used from the other router. The local router must have IP routing and TFTP configured. See the TFTP security notes on page 16-94.

Syntax

```
fput X.X.X.X os filename      transfer router operating
                              system code

fput X.X.X.X config filename  transfer router configuration

fput X.X.X.X NCL-command filename
                              store display command output
```

X.X.X.X is the IP address of the remote node in dotted decimal notation.

filename is the name of a file on the remote node to store the output from this router. Some TFTP servers on remote nodes require that the file already exist.

Using the Network Control Language

Using TFTP To Transfer Operating Code, Configuration, and NCL Display

NCL-command is an NCL display command string on this router. Possible commands are listed above and described earlier in this chapter. If the command has parameters and thus includes a space, then enclose the command string in double quotes.

Examples

```
fput 15.3.0.97 os rok  
fput 15.3.0.97 config account.cfg  
fput 15.3.0.97 "browse" prlcfg.txt  
fput 15.3.0.97 "rgetr 10.1.2.1 public" prltable.txt
```

In response, you will be informed of the progress and successful or unsuccessful completion of the transfer. All protocols and links on the router remain enabled.

Using ZModem to Transfer Configuration and NCL Display

With an IBM-compatible personal computer (PC host) connected to the router's console port, two NCL commands use the Zmodem protocol to do the following:

- Copy a router configuration to the PC host for storage.
- Copy a router configuration from the PC host to the original router or to other routers.
- Copy the displayed output of certain NCL commands into a PC host file.

The PC must be emulating a VT100 or ANSI terminal, and can be connected either directly or using a modem to the router's console port. Also, the PC must be running a Zmodem-compatible terminal emulation program such as PROCOMM PLUS*. This section describes the use of NCL commands with the PROCOMM PLUS terminal emulation program (version 2.01).

Note You can use other PC host versions of Zmodem. However, the exact procedure for invoking them depends on how each is implemented, and is likely to differ from the procedures shown on the following pages.

Command	Function
Zget	Copies a router configuration from a file on the console PC to the router. (page 16-99)
Zput	Copies NCL command output or the router configuration from the router to a file on the console PC. (page 16-100)

These commands are detailed below.

Note Recommended Hardware Connections: For the correct cable for either a direct or a modem connection between the PC host and the router, refer to the information on console cables in the installation guide for your router.

* PROCOMM PLUS is a product of Datastorm Technologies, Inc.

Using the Network Control Language

Using ZModem to Transfer Configuration and NCL Display

Zget: Loading the Configuration to a Router

Use NCL's Zget command to upload the router configuration previously stored as a file on the PC connected to the router as a console.

Note

Zget overwrites the router's current configuration with the uploaded configuration.

Preparation:

You must have previously used Zput to download the configuration to the PC host (see page 16-100 above). Run the PROCOMM PLUS terminal emulation program. Start a router console session with the manager password.

Procedure to upload the configuration to the router:

1. Enter the Zget command:
zget
2. Press the key to display the "Upload Protocols" window.
3. Type z to select the "ZMODEM" option and to display the "Send ZMODEM" window.
4. Enter the name of the file containing the configuration you want to upload. End with to begin uploading.

If the PC host does not respond within approximately 70 seconds after you execute step 4, the command times out and control returns to the NCL prompt.

If Zget is in use and the PC host is left in terminal emulation mode, you may see Zmodem protocol packets displayed as a series of character strings before the command times out.

You can use other host versions of Zmodem. However, the exact procedure for invoking them depends on how each is implemented.

Zput: Storing the Configuration or NCL Command Output to a PC Host File

Use NCL's Zput command to download the router configuration or NCL command output to a file on a PC connected to the router as a console.

Preparation:

1. Start PROCOMM PLUS .
2. Ensure that the PROCOMM PLUS “Auto downloading” feature for the Zmodem protocol is set to “on”.
3. Press the **[Alt] [S]** key combination to display the “PROCOMM PLUS SETUP UTILITY” screen.
4. Select “PROTOCOL OPTIONS”.
5. Select “ZMODEM PROTOCOL OPTIONS”. In the resulting menu, ensure that item C, “Auto downloading”, is set to “on”. (If it is set to “off”, follow the instructions on the screen to change the setting.)
6. Press **[Esc]** to return to “PROTOCOL OPTIONS”.
7. HP Router 650 applications only: Do this step if the router uses an F1047-80002 cable to directly connect the router console port to a 9-pin port on a PC (with no modem or adapter involved). Otherwise, skip this step and go to step 8.)
 - a. Select GENERAL OPTIONS.
 - b. In the resulting menu set item C, “Abort Xfer if CD lost” to “No”. (Follow the instructions on the screen to change the setting.) Press **[Esc]** to return to “PROTOCOL OPTIONS”.

(The PROCOMM PLUS Zmodem file transfer utility default expects the Carrier Detect line to be “on” (high) before starting the file transfer. The cabling described here—and *only* this cabling arrangement—does not supply Carrier Detect (CD) to the PC. This is the reason for configuring PROCOMM PLUS to not look for CD to be “on”—high. If you do not change the setting as described above, PROCOMM PLUS generates a “No Carrier” error message.)

Using the Network Control Language

Using ZModem to Transfer Configuration and NCL Display

8. Press **Esc** three times to return to the router's Main menu (see figure 1-2).
9. Select the "Network Control Language Interpreter" in the router's Main menu.

The procedure to download the configuration or NCL command display to a PC host file (at the NCL prompt) is shown by the syntax and examples on the following pages.

Syntax

```
zput config filename [overwrite] [format]
                                transfer router configuration
```

```
zput NCL-command filename [overwrite] [format]
                                store display command output
```

filename is the name of a file on the remote PC host to store the output from this router.

NCL-command is an NCL display command string on this router. Possible commands are listed above and described earlier in this chapter. If the command has parameters and thus includes a space, then enclose the command string in double quotes.

[overwrite] (optional) specifies whether to overwrite any existing file of the same name as *filename*, either of the following:

0 (the default) prevents overwriting.

1 allows overwriting.

[format] (optional) selects the file formatting required by the host, either:

0 (the default) ends lines with carriage returns and line feeds (CR LF), as needed by most PCs.

1 ends lines with line feeds only (LF).

Examples

```
zput config inter1.cfg
```

```
zput "rgetr 10.1.2.1 public" prtable.txt
```

In response, a status window temporarily appears to monitor transfer data and progress.

Using the Network Control Language

Using ZModem to Transfer Configuration and NCL Display

When the download is completed, a flashing “COMPLETED” message appears briefly in the status window. Then the window closes and control returns to the NCL prompt.

If the PC host does not respond within approximately 60 seconds after you execute Zput, the command times out and control returns to the NCL prompt.

Note

If the “Auto downloading” parameter described under “Preparation” above has not been set to “on”, then to complete the download you must press the **[Pg Dn]** key and follow the instructions in the resulting window. For more information, refer to the *PROCOMM PLUS User Manual*.

For information on Zput event messages, refer to the Zmodem event messages on page 17-149.

Event Log Messages

How To Use This Chapter

The event log is a first-in, first-out buffer in RAM. Each entry is a single line composed of five fields:

<i>severity</i>	<i>date</i>	<i>time</i>	<i>object</i>	<i>event message</i>
I	08/05/94	10:52:13	cct.wan1:	'WAN1 - carrier lost'

The event log messages listed in this chapter are organized alphabetically within subsections corresponding to the objects from which the messages are generated. The object name for each message appears immediately after the time stamp included in the message. For example, the object generating the above message is cct. (The “.wan1” is further information describing, in this case, the specific circuit being reported in this message.)

severity is one of the following codes:

- D (debug) indicates installation and diagnostic information.
- I (information) indicates routine events.
- W (warning) indicates that a service has behaved unexpectedly.
- P (performance) indicates that a current service has degraded or upgraded.
- M (major) indicates a service appearance/disappearance.

For information on how to operate the event log, refer to “Log: Viewing the Entire Event Log or Selected Message Categories” on page 16-16 and to chapter 5, “How To Use the Event Log To Analyze Router Operation” in the *User's Guide*.

To Locate Event Messages by Managed Object Name

Subsection	Page
at: AppleTalk Event Messages	17-4
boot: Boot Event Messages	17-15
bootp: Network Boot Protocol Event Messages	17-16
cct: Circuit Event Messages	17-18
dev: Device Event Messages	17-60
dls: Data Link Services Event Messages	17-69
drs: DECnet Event Messages	17-74
egp: Exterior Gateway Protocol Event Messages	17-79
ip: IP Event Messages	17-86
ipx: IPX Router Event Messages	17-92
lb: Bridge Event Messages	17-96
line: Lines Event Messages	17-101
mgr: Manager Event Messages	17-103
ospf: OSPF Event Messages	17-105
pm: Port Module Manager Event Messages	17-112
ppp: Point-to-Point Protocol	17-117
rok: Router Operating Kernel Event Messages	17-120
SMDS Event Messages	17-122
tcp: Transmission Control Protocol Event Messages	17-124
telnet: Telnet Event Messages	17-125
tftp: TFTP and Fget Event Messages	17-126
timep: Time Protocol Event Messages	17-133
X.25 Event Messages	17-135
xrx: XNS Router Event Messages	17-147
zmodem: Zmodem Event Messages	17-149

at: AppleTalk Event Messages

These event messages are generated by the system variable “at”, the AppleTalk router.

AARP mapping table is full

- Meaning:** The AppleTalk router cannot add an address resolution pair (AppleTalk node address and an associated station address) to its address mapping table; the table contains its maximum number of entries.
- Action:** Increase the value of the AARP mapping table parameter to expand the size of the table.

AARP PROBE/RSP: node address *X.Y*

- Meaning:** The AppleTalk router (after having issued a Probe packet to test the uniqueness of the network number and node identifier pair specified by *X.Y*) has received a Response packet indicating that the network number and node identifier pair is in use by another network node. Consequently, the AppleTalk router will generate a new address pair and issue another Probe.

AARP probing terminated for *ccg*

- Meaning:** The AppleTalk router cannot obtain a unique network number and node identifier pair for the circuit group specified by *ccg*. The directly connected medium is supporting the maximum number of nodes.
- Action:** Reconfigure the AppleTalk network with a larger network range, using the Network Min and Network Max parameters.

AARP REQ/RSP: node address *X.Y*

- Meaning:** The AppleTalk router resolved the station address for the AppleTalk node address *X.Y*, where *X* is the network number and *Y* is the node identifier.

at_amt_alloc: out of memory

- Meaning:** The AppleTalk router cannot obtain sufficient memory to allocate the AARP address mapping table.
- Action:** Reduce the AARP Mapping Table parameter to place a lesser demand on memory.

at_cg_cb_alloc: out of memory

- Meaning:** The AppleTalk router cannot obtain sufficient memory to allocate a circuit group control block.
- Action:** Reduce the Routing Table Size and/or AARP Mapping Table parameters to place a lesser demand on memory.

at_routing_tbl_alloc: out of memory

- Meaning:** The AppleTalk router cannot obtain sufficient memory to allocate the routing table.
- Action:** Reduce the Routing Table Size parameter to place a lesser demand on memory.

at_zone_name_tbl_alloc: out of memory

- Meaning:** The AppleTalk router cannot obtain sufficient memory to allocate the zone name table.
- Action:** Reduce the Routing Table Size and AARP Mapping Table parameters to place a lesser demand on memory.

Cfg: cannot get dflt zone name for *ccg*

- Meaning:** This message is generated only if the circuit group specified by *ccg* is a nonseed port. After a nonseed port establishes contact with a seed router, it issues a query to obtain the network's default zone name. This message is generated if the port fails to receive a response to its query.
- Action:** No action is required. The nonseed port repeats its query until it obtains the default zone name.

Event Log Messages
at: AppleTalk Event Messages

Cfg: cannot get zone name list for *ccg*

- Meaning:** This message is generated only if the circuit group specified by *ccg* is a nonseed port. After a nonseed port obtains the default zone name from a seed router, it issues a query to obtain a list of zone names associated with the network. This message is generated if the port fails to receive a response to its query.
- Action:** No action is required. The nonseed port repeats its query until it obtains the list of associated zone names.

Cfg: dflt zone name must be cfg'd for *ccg*

- Meaning:** The circuit group specified by *ccg* has been configured as a seed port. No response was entered, however, to the Default Zone Name parameter.
- Action:** Configure the Default Zone Name parameter for the circuit group.

Cfg: Illegal construction in Zone name

- Meaning:** The zone name has a bad \xx hex construction. An "illegal default zone..." event or an "illegal zone name..." event will follow in the Event Log to show the invalid zone name.
- Action:** Use Quick Configuration or the Configuration Editor to correct the zone name.

Cfg: illegal zone name *zone name*

- Meaning:** The zone name that you entered uses an incorrect format of the escaped character syntax. A non-hexadecimal, non-backslash (\) character was entered as one of the two characters immediately following a backslash (\) character.
- Action:** Configure a valid zone name to replace *zone name*.

Cfg: invld dflt zone name for *ccg*

- Meaning:** The circuit group specified by *ccg* has been configured as a seed port. The directly connected network is serviced also by another seed router

already in service. The default zone names conveyed by these seed routers are inconsistent.

Action: One of the seed routers must be reconfigured to ensure the consistency of the default zone names. If you reconfigure the AppleTalk router to match the default zone name of the in-service router, no further changes are necessary. If you reconfigure the in-service router to match the default zone name of the AppleTalk router, however, you must restart all network nodes and routers.

Cfg: invld zone name cfg'd for *ccg*

Meaning: The circuit group specified by *ccg* has been configured as a seed port. The directly connected network is serviced not only by this seed, but also by another seed router already in service. The zone name lists conveyed by these seed routers are inconsistent. While each list contains the same number of zone entries, the lists are not identical.

Action: One of the seed routers must be reconfigured to ensure the consistency of the zone name lists. If you reconfigure the AppleTalk router to match the zone name list of the in-service router, no further changes are necessary. If you reconfigure the in-service router to match the zone name list of the AppleTalk router, however, you must restart all network nodes and routers.

Cfg: network range incorrect for *ccg*

Meaning: The circuit group specified by *ccg* has been configured as a seed port. The directly connected network is serviced not only by this seed, but also by another seed router already in service. The network ranges conveyed by these seed routers are inconsistent.

Action: One of the seed routers must be reconfigured to ensure the consistency of the network ranges. If you reconfigure the AppleTalk router to match the network range of the in-service router, no further changes are necessary. If you reconfigure the in-service router to match the network range of the AppleTalk router, however, you must restart all network nodes and routers.

Event Log Messages
at: AppleTalk Event Messages

Cfg: No config summary record

Meaning: There is a serious problem in the router's configuration file, affecting the system configuration and not just the AppleTalk configuration. (In this case, the "/CFG_SUMMARY" record is missing.)

Action: Ensure that the router's configuration is valid.

Cfg: No BOOTLOAD record

Meaning: There is a serious problem in the router's configuration file, affecting the system configuration and not just the AppleTalk configuration. (In this case, the "/BOOT_LOAD" records are missing.)

Action Ensure that the router's configuration is valid.

Cfg: No config summary record

Meaning: There is a serious problem in the router's configuration file, affecting the system configuration and not just the AppleTalk configuration. (In this case, the "/CFG_SUMMARY" record is missing.)

Action: Ensure that the router's configuration is valid.

Cfg: No circuits configured

Meaning: No circuits are configured for AppleTalk. The configuration may be corrupted.

Action: Use Quick Configuration or the Configuration Editor to add one or more AppleTalk circuits.

Cfg: No entity records

Meaning There is a serious problem in the router's configuration file, affecting the system configuration and not just the AppleTalk configuration. (In this case, one or more "ENTITY" records are missing.)

Action Ensure that the router's configuration is valid.

Cfg: number zone names incorrect for *ccg*

- Meaning:** The circuit group specified by *ccg* has been configured as a seed port. The directly connected network is serviced not only by this seed, but also by another seed router already in service. The zone name lists conveyed by these seed routers are inconsistent; each list contains a different number of zone entries.
- Action:** One of the seed routers must be reconfigured to ensure the consistency of the zone name lists. If you reconfigure the AppleTalk router to match the zone name list of the in-service router, no further changes are necessary. If you reconfigure the in-service router to match the zone name list of the AppleTalk router, however, you must restart all network nodes and routers.

Cfg: NULL zone name cfg'd for *ccg*

- Meaning:** The AppleTalk router has configured a null zone name for the circuit group specified by *ccg*. The value entered for the Zone Name parameter was invalid.
- Action:** Configure a valid zone name for the circuit group specified by *ccg*.

Cfg: too many zone names cfg'd for *ccg*

- Meaning:** More than ten zone names have been added to the zone name list associated with the circuit group specified by *ccg*.
- Action:** No action is required. The AppleTalk router ignores any zone names beyond the maximum value of ten.

Cfg: Zone name greater than 32 chars

- Meaning:** AppleTalk zone names must be ≤ 32 characters in length. An “illegal default zone” event or an “illegal zone name” event will follow to show the invalid zone name.
- Action:** Use Quick Configuration or the Configuration Editor to correct the zone name.

Event Log Messages
at: AppleTalk Event Messages

ccg enabled with network range *X* - *Y*

Meaning: The circuit group specified by *ccg* is enabled and connected to the attached medium whose range of network numbers is *X* to *Y*.

ccg enabled with node address *X.Y*

Meaning: The circuit group specified by *ccg* is enabled with the node address *X.Y*, where *X* is the network number and *Y* is the node identifier.

Circuit Group record not configured for *cg# X*

Meaning: The configuration does not contain a circuit group record for the circuit group identified by *X*, where *X* is the system-assigned interface number that identifies the circuit group.

Action: First, use NCL's Get command (in the form `get cct.X`) to obtain the circuit group name, with associated statistics. Then verify and/or reconfigure the circuit group.

Forcing AARP probing for *cg ccg*

Meaning: The circuit group specified by *ccg* was configured with AARP Probe disabled. In completing the configuration of this circuit group, however, you did not specify a node identifier and/or you did not select a network number (for seed routers only). Consequently, the AppleTalk router has generated a quasi-random node identifier and/or network number and is using the Probe facility to ensure the uniqueness of the network number and node identifier pair.

Illegal construction in Zone name

Meaning: The zone name has a bad \xx hex construct. An "illegal default zone" event or an "illegal zone name" event will follow, showing the invalid zone name.

Action: Use Quick Configuration or the Configuration Editor to correct the zone name.

Illegal network number for *ccg*

Meaning: The network number configured for *ccg* is outside of the range specified by the Network Min and Network Max parameters.

Action: Reconfigure the network number to within the range.

Illegal network range for *ccg*

Meaning: Either the Network Min or Network Max parameter for *ccg* is outside the range of legal AppleTalk network numbers, 1 through 65279.

Action: Reconfigure the AppleTalk network range parameters.

Incoming invalid zone len *length* - zone *aa bb cc dd*

Meaning: The HP system has detected an incorrectly formatted zone information packet. The zone length (*length*) and the first four characters of the zone name (in ASCII hexadecimal format) are *aa bb cc dd*.

Action: None. The HP router will repeat its request for zone names.

Event Log Messages
at: AppleTalk Event Messages

Invalid AARP event *X*, AARP state *Y* for cg *ccg*

Meaning: The circuit group specified by *ccg* was in AARP state *Y*, and thus unable to process AARP event *X*. Possible values for *X* and *Y*:

<i>X</i> value	Event Code
0	xmit AARP PROBE
1	xmit AARP REQUEST
2	rcv AARP PROBE
3	rcv AARP REQUEST
4	rcv AARP RESPONSE
5	timer expired/cancelled

<i>Y</i> value	AARP State Code
0	circuit group disabled
1	circuit group xmit (AARP PROBE)
2	circuit group xmit (AARP REQUEST)
3	circuit group enabled

Action: None.

No AppleTalk circuit group configured

Meaning: You have not configured an AppleTalk circuit group.

Action: Configure an AppleTalk circuit group.

No AppleTalk Record configured

Meaning: The configuration does not include an AppleTalk record.

Action: Configure the AppleTalk router.

No AppleTalk software configured

Meaning: The portion of the configuration file that contains AppleTalk configuration data is faulty. One or more of the following required records may be missing: AppleTalk record, configuration summary record, entity records, or boot-load record.

Action: Verify and reconfigure the AppleTalk router.

No circuit group recorded for cg number *X*

Meaning: The configuration does not contain a valid circuit-group record for the circuit group identified by *X*, where *X* is the system-assigned interface number that identifies the circuit group.

Action: First, use NCL's Get command (in the form `get cct.X`) to obtain the circuit group name, along with associated statistics. Then verify and/or reconfigure the circuit group.

No msg buffers for alarms: CG#

Meaning: The Appletalk router cannot obtain a message buffer to create its circuit group timer.

Action: Contact your HP support provider.

No msg buffers for RTMP background alarm

Meaning: The Appletalk router cannot obtain a message buffer to create its RTMP background timer.

Action: Contact your HP support provider.

No msg buffers for RTMP validity alarm

Meaning: The Appletalk router cannot obtain a message buffer to create its RTMP validity timer.

Action: Contact your HP support provider.

Event Log Messages
at: AppleTalk Event Messages

No msg buffers for ZIP background alarm

Meaning: The Appletalk router cannot obtain a message buffer to create its ZIP background timer.

Action: Contact your HP support provider.

Rcv'd zone name(s) on port #; cannot distribute

Meaning: A list of zone names received on port # could not be sent to the other ports running AppleTalk.

Zone name table full

Meaning: The AppleTalk router cannot add a zone name to its zone name table; the table contains its maximum of 256 entries.

Action: Check your network topology. HP's AppleTalk router implementation allows a maximum of 256 zones on an internet.

boot: Boot Event Messages

This event message is generated by the system variable "boot".

System went down: *day/month/hh:mm:ss/year*

Meaning: Identifies the last time the system went down.

bootp: Network Boot Protocol Event Messages

These event messages are generated by the system variable "bootp", the network boot protocol.

buffer for timer msg can't be allocated

Meaning: Buffer memory ran out, so the Bootp request or reply could not be serviced.

can't allocate any msg buffers

Meaning: Buffer memory ran out, so the Bootp request or reply could not be serviced.

dropped BOOTP pkt, bad hdwe addr type

Meaning: A Bootp request with a station address length not equal to 48 bits was received. Station addresses that are not 48 bits long are not supported.

dropped BOOTP pkt, bad max relay hop count

Meaning: A Bootp request packet was discarded because its hop count was decremented to zero. The hop count is not the same as IP's Time To Live field. The Bootp request may have been relayed by other relay agents such that the packet is being looped.

Action: Increase the hop count (the maximum relay hops parameter) in IP's Bootp configuration, or determine why a loop exists for Bootp requests being relayed.

dropped BOOTP reply, no matching request

Meaning: The Bootp reply received had no initial request relayed. The Bootp server could have incorrectly addressed the reply or could have retransmitted the reply.

illegal action for bootp_act

Meaning: Internal messaging error.

Action: Call your local product support provider.

received BOOTP reply from server

Meaning: Reply received from Bootp server.

received BOOTP request from client

Meaning: Request received from Bootp client.

received unknown BOOTP pkt type

Meaning: Some node is generating bad packets.

cct: Circuit Event Messages

These event messages are generated by the system variable "cct", for circuits.

ATCP is down

Meaning: For the indicated PPP circuit, Appletalk Control Protocol (ATCP) has gone down.

ATCP is up

Meaning: For the indicated PPP circuit, Appletalk Control Protocol (ATCP) is up.

Adapter accepted CIC command

Meaning: The adapter accepted the router CIC command.

Adapter accepted CRN command

Meaning: The terminal adapter accepted the router CRN command.

Adapter accepted DIC command

Meaning: The adapter accepted the router DIC command.

Adapter did not accept CIC command

Meaning: The terminal adapter has rejected the router CIC command. The router will bring down the circuit and not allow any more connections on this circuit.

Action: This error indicates either a configuration error on the router or on the terminal adapter, or an incompatibility between them. You must change the configuration. If an adapter error is sent, the router will log it. (Check for this error if available.)

Adapter did not accept CRN command

- Meaning:** The terminal adapter rejected the router CRN command. The router will bring down the circuit and not allow any more connections on this circuit.
- Action:** This error indicates either a configuration error on the router or on the terminal adapter, or an incompatibility between them. You must change the configuration. This can happen if the V.25 bis extensions are used and not accepted. If an adapter error is sent, the router will log it.

Adapter did not accept DIC command

- Meaning:** The terminal adapter rejected the router DIC command. The router will bring down the circuit and not allow any more connections on this circuit.
- Action:** This error indicates either a configuration error on the router or on the terminal adapter, or an incompatibility between them. The user must change the configuration. If an adapter error is sent, the router will log it.

Adapter error = XX

- Meaning:** This indicates the two-character error code, **XX**, issued by the terminal adapter when either a call fails or it rejects the router command.
- Action:** Refer to the terminal adapter manual for the meaning of the **XX** error code issued.

adapter not responding with CTS line

- Meaning:** The router has timed out while waiting for the adapter to set Clear To Send. When the router first enables the line, it will wait for either the connection time or 255 seconds (if the Connection Time is set to 0) for the adapter to bring up Clear To Send.
- Action:** Check the connection between the adapter and the router. Also check the adapter documentation to be sure it is configured properly. Increase the Connection Time parameter as necessary.

Event Log Messages
cct: Circuit Event Messages

Attempt to init FR on inactive cct

Meaning: The indicated frame relay circuit is not active, yet there was an attempt to initialize the circuit. This is an internal problem and cannot be corrected by the user.

Bad Address option combination

Meaning: In the indicated frame relay circuit, the selected combination of addressing encoding and address length is not compatible. Allowable combinations are:

Q921	TWO BYTE only
Q922 March 90	TWO BYTE only
Q922 November 90	TWO BYTE THREE BYTE FOUR BYTE
Q922	TWO BYTE TWO + CONTROL THREE BYTE THREE + CONTROL FOUR BYTE

Action: Modify the configuration so that the address encoding and address length are compatible.

bad configuration file

Meaning: The configuration has an inconsistency or error.

Action: Check the portion of the configuration for the type of circuit named after "cct" in the object name preceding this message. Correct the configuration and reboot the router.

Bad full polling; reset to 6

Meaning: In the indicated frame relay circuit, the chosen interval between full polling parameter is not within the proper range. The proper range is between 1 and 255 polls. The default value is to send a full status enquiry every six polling cycles.

Action: Modify the configuration so that the polling interval is within the proper range.

Bad interface discriminator found <xxx>

Meaning: For the indicated frame relay circuit, a packet was received on the management interface Data Link Connection Identifier (DLCI), but the protocol discriminator field did not contain the proper value for the selected management interface method. Proper values are 9 for LMI and 8 for ANSI Annex D. <xxx> identifies the protocol discriminator that was found.

Bad poll interval; reset to 10

Meaning: For the indicated frame relay circuit, indicates that the polling interval chosen during configuration is not within the valid range of 5 to 30 seconds.

Action: Modify the frame relay configuration so that the polling interval is within the proper range.

BNCP is down

Meaning: For the indicated PPP circuit, Bridge Network Control Protocol (BNCP) has gone down.

BNCP is up

Meaning: For the indicated PPP circuit, Bridge Network Control Protocol (BNCP) is up. Bridge packets may now be sent and received on the link.

Bridge mapping table is full

Meaning: For the indicated frame relay circuit, the bridge table mapping destination station addresses to frame relay DLCIs is full and can not accommodate a new entry. This table is related to the internal bridging tables and therefore, may be indicative of a bridging problem.

Event Log Messages
cct: Circuit Event Messages

BUD Failed, SIFSTS = XXXX

Meaning: The token ring device Bring Up Diagnostic (BUD) failed, indicating a possible hardware failure.

Action: Note the code number in the event message and contact your Hewlett-Packard representative.

Call collision will rcv inbound call

Meaning: The router received an incoming call after sending a connect request (CRN command). The connect request will be stopped and the incoming call accepted if it doesn't fail any user-specified call restrictions placed on inbound calls.

Call coll to IP next hop X.X.X.X

Meaning: We were attempting to establish an outbound call to next hop X.X.X.X when we received an inbound call from that location. The outbound call will be closed and the inbound call will be used.

Can't configure 4 Mbps token interface

Meaning: You have configured 4 Mbit/s service on a 16 Mbit/s medium.

Action: Reconfigure the Ring Interface parameter setting correctly for your medium.

Can't configure 16 Mbps token interface

Meaning: You have configured 16 Mbit/s service on a 4 Mbit/s medium.

Action: Reconfigure the Ring Interface parameter setting correctly for your medium.

Carrier Detect lost on WAN #

Meaning: Carrier Detect has been lost on the indicated WAN.

Carrier detected on WAN #

Meaning: Carrier Detect has been received, either initially or after being lost, on the indicated WAN port.

Circuit has been brought down

Meaning: This indicates that the V.25 bis circuit has been brought down.

Action: See other logged events for further information.

Circuit has been brought up

Meaning: The V.25 bis circuit has been brought up.

circuit in auto-detect mode

Meaning: Occurs whenever the device or remote device reboots and detects the WAN auto-detect parameters.

Circuit reset complete

Meaning: The circuit indicated in the ***object*** field of the event message has completed resetting.

Clock lost

Meaning: For either LLC1 or LLC2 Quality of Service, transmission progress on the chip has stopped for the idle period. See also “Clock recovered”, below.

Clock recovered

Meaning: Transmission progress is again being made. (See also “Clock lost”, above.)

Event Log Messages
cct: Circuit Event Messages

config needs phone # to connect

- Meaning:** The V.25 bis circuit has been configured to be enabled when the circuit first comes up. However no outbound phone number has been configured. Therefore this circuit will only be able to connect when a call comes in.
- Action:** No user action is required unless you did not intend to configure the circuit this way.

Connection established

- Meaning:** The connection with the remote side has been established.

Connection establishment timeout

- Meaning:** An outbound connection attempt has failed and used up its retry count, or an inbound connection has timed out. The circuit will be brought down. New inbound connections will be allowed. However, outbound connections will not be allowed until the retry delay time has expired.
- Action:** Increase the retry count and/or connection time as necessary. Also check other event messages to see if other events occurred that caused the failure.

Connection inactivity timeout

- Meaning:** A live connection has timed out due to inactivity. The connection will be closed and reopened when data is available or when an incoming call arrives.
- Action:** No action required unless you want the connection to remain active longer. If so, then increase the inactivity time or change the connection to enable on cct up.

Connection retry in progress

- Meaning:** An outbound connection attempt has failed for reasons other than a timeout. The retry count has not expired for the outbound connection, so the router will try again.

Action: Check other event messages to see why the connection failed.

Connection timeout, retry in progress

Meaning: An outbound connect attempt has timed out waiting for the terminal adapter to respond. The retry count has not expired so the router will try again.

Action: Check the connection between the adapter and the router. Also check the terminal adapter documentation to be sure it is configured properly. Increase the Connection Time parameter as necessary.

CTS has come up

Meaning: The terminal adapter has brought up the Clear To Send line.

CTS has gone down

Meaning: The terminal adapter has brought down the Clear To Send line.

Action: Check other events logged for further information, and check any terminal adapter logs if available.

DATA Available

Meaning: The data has become available, so a connection will be attempted.

Data pkt clipped for use in V.25bis

Meaning: Severe packet shortage. A queued V.25 bis packet was reused in order to establish the V.25 bis connection in hope of freeing more queued packets.

Action: This should only happen if many IP-mapped circuits are waiting to come up. If this only occurs infrequently, it may be acceptable depending on the applications. To solve this, add more V.25 bis circuits to the pool, or re-arrange traffic so that not as many circuits are queued waiting for an available line. (Higher speed ISDN lines may also help.)

Event Log Messages
cct: Circuit Event Messages

Data pkt received on downed connection

- Meaning:** The adapter sent data packets on a link that was not connected. (The DSR line was down.) This is not expected when the router is in manual adapter mode.
- Action:** Check the adapter configuration. Make sure that it raises DSR when the phone call is established.

DCE set DSR TRUE before DTE sent XXX

- Meaning:** The router was about to send a v.25 bis command (XXX0) when the terminal adapter unexpectedly pulled up DSR. This indicates that the router and adapter are out of synchronization during a V.25 bis exchange. The router will drop DTR and re-attempt the connection if the retry count permits.
- Action:** No user action required. The router will try to re-synchronize the connection. If this happens frequently, check the adapter configuration.

DCE set DSR while sending CFI

- Meaning:** While the router was waiting for the connection time to expire before retrying connection establishment, the terminal adapter unexpectedly pulled up DSR. This indicates that the router and adapter are out of synchronization during a V.25 bis exchange. The router will drop DTR and re-attempt the connection if the retry count permits.
- Action:** No user action required. The router will try to re-synchronize the connection. If this happens frequently, check the terminal adapter's configuration.

DCE set DSR while waiting for CTS

- Meaning:** While the router was waiting for the clear to send (CTS) line to come up, the terminal adapter unexpectedly pulled up DSR. This indicates that the router and terminal adapter are out of synchronization during a V.25 bis exchange. The router will drop DTR and re-attempt the connection if the retry count permits.

Action: No user action required. The router will try to re-synchronize the connection. If this happens frequently, check the terminal adapter's configuration.

DCE set DSR while waiting for IND

Meaning: While the router was waiting for an indication from the terminal adapter, the adapter unexpectedly pulled up DSR. This indicates that the router and adapter are out of synchronization during a V.25 bis exchange. The router will drop DTR and re-attempt the connection if the retry count permits.

Action: No user action required. The router will try to re-synchronize the connection. If this happens frequently, check the terminal adapter's configuration.

DEV CCT: *cct*: Ethernet circuit record missing

Meaning: Circuit is undefined.

Action: Modify the configuration to include a circuit record for *cct* #.

DEV CCT: *cct* - Ethernet line record missing

Meaning: The driver cannot associate circuit *cct* with an existing line record.

Action: Modify the configuration to include proper line and circuit records.

DEV CCT: *cct* - Invalid QOS for PPP, QOS = LLC1

Meaning: The Quality of Service parameter for circuit *cct* was not configured as LLC1 (unreliable datagram). Since LLC1 is the only appropriate Quality of Service for the driver to use for Point-to-Point protocol, the Quality of Service parameter has been automatically modified to be LLC1. Note that the PPP subsystem, not the driver, provides additional services beyond LLC1.

Action: Modify the configuration so that the Quality of Service parameter is LLC1.

Event Log Messages
cct: Circuit Event Messages

DEV CCT: *cct* - Not enough memory for compression

- Meaning:** Compression is configured on the circuit, but there is not enough free memory to allocate the compression table.
- Action:** Either remove configured functionality that is unnecessary, or replace the router with another one having more memory.

DEV CCT: *cct* - transmit congestion

- Meaning:** The router has dropped packets that were to be transmitted on this circuit. The bit rate of traffic destined for this port is larger than the media can handle. This could be due to either many circuits feeding this one circuit too much data or the ring is too busy with other traffic to allow all of the traffic the router would like to place on the ring.
- Action:** Investigate resegmenting your network to balance the flow of traffic more evenly between segments.

The delay time is *X* minutes

- Meaning:** *X* minutes is the delay time request by the terminal adapter on the DLC indication.

Disabled, LLC2 retries exhausted

- Meaning:** The circuit indicated in the *object* field of the event message has been disabled because the router was unable to obtain positive acknowledgment of an outstanding frame after a sequence of retransmission attempts. The number of such attempts is governed by the Retry Counter (N2), Retry Timer (T1), and Connect Retries LLC2 parameters.
- Action:** Verify point-to-point connectivity.

DLCI too large for interface; *XXX*

- Meaning:** DLCI values exceeding that which could be fit into the length specified during configuration. Primarily this will happen if there is no management interface selected and PVCs are hand-configured with large DLCIs. *XXX* identifies the DLCI which is too large.

DLCI XXX not within range; not added

Meaning: For the indicated frame relay circuit, a DLCI value was added that was not within the range of valid values for the specified type and length. **XXX** identifies the DLCI in error.

DRSCP is down

Meaning: For the indicated PPP circuit, DECnet Routing Service Control Protocol (DRSCP) is down.

DRSCP is up

Meaning: For the indicated PPP circuit, DECnet Routing Service Control Protocol (DRSCP) is up.

DSR lost connection closed

Meaning: A live connection has been dropped by the terminal adapter dropping DSR. The router will immediately go into a state where the connection can be re-established, either by waiting for an incoming call, making more data available for transmission, or by sending a CRN command. (The action depends on the configuration.)

Action: Check any adapter connections or logs.

Dup ph# next hop X.X.X.X & Y.Y.Y.Y

Meaning: A duplicate phone number was found between IP map records. The map records that have the same number have IP next-hop addresses of X.X.X.X and Y.Y.Y.Y.

Action: Remove the duplicate phone numbers. This is a major error, and the configuration beyond the duplicate will not be read.

Enable requested on cct cct #

Meaning: The circuit named in the **object** field of the event message is requesting to be enabled.

Event Log Messages
cct: Circuit Event Messages

entity already disabled

Meaning: An already disabled circuit, identified in the ***object*** field of the event message, has received NCL's Disable command.

entity already enabled

Meaning: An already enabled circuit, identified in the ***object*** field of the event message, has received NCL's Enable command.

entity disabled

Meaning: The circuit named in the ***object*** field of the event message has been disabled in response to NCL's Disable command.

entity enabled

Meaning: The circuit named in the ***object*** field of the event message successfully initialized, or has been enabled with the NCL's Enable command.

Error in Configuration record

Meaning: The established configuration for the frame relay circuit is in error.

Action: Modify the configuration to establish a valid frame relay circuit.

Excessive collisions

Meaning: The LAN circuit named in the ***object*** field of the event message has dropped a frame after it has detected collisions on 16 successive transmission attempts.

Action: If message occurs frequently, investigate the causes of LAN congestion.

Excessive errors; interface disabled

Meaning: For the indicated frame relay circuit, when the DTE receives a designated number of errors within a designated number of events, the

interface is considered unstable and is taken down. This message indicates that this situation has occurred.

Free pkt buffs available V.25 bis clipping disabled

Meaning: The the backlog has been relieved. Packet buffers can again be queued on V.25 bis circuits as necessary.

Free pkt buffs low V.25 bis clipping enabled

Meaning: The amount of memory used for packets is low, The router will drop some of the oldest packets queued on V.25 bis mapped circuits that are waiting to be established.

Action: This should only happen if many IP-mapped circuits are waiting to come up. If this only occurs infrequently, it may be acceptable depending on the applications. To solve this, add more V.25 bis circuits to the pool, or re-arrange traffic so that not as many circuits are queued waiting for an available line. (Higher speed V.25 bis lines may also help.)

illegal packet received

Meaning: For the indicated PPP circuit, a packet was received that did not conform to standard PPP format. The packet was dropped. No further action is necessary.

Initialization Error, SIFSTS = XXXX

Meaning: Initialization of the token ring device has failed, indicating a possible hardware or operating system failure.

Action: Note the code number in the event message and contact your Hewlett-Packard representative.

insufficient mem on cct *X* for *cct*

Meaning: There is no system memory available for the given V.25 bis circuit (*cct*) to be allocated. This circuit is not available for use.

Event Log Messages

cct: Circuit Event Messages

Action: Reduce the overall size of memory resources allocated by the configuration. (For example, reduce table sizes on other configuration parameters where possible.)

insufficient mem on cct X for phone

Meaning: There is no system memory available for the given V.25 bis circuit (**cct**) to allocate storage for phone numbers. This circuit is not available for use.

Action: Reduce the overall size of memory resources allocated by the configuration. (For example, reduce table sizes on other configuration parameters where possible.)

Internal clock being generated

Meaning: This router is providing a clock because a modem eliminator cable was detected with the clock source end attached to this router.

Action: If there are problems with the link, ensure that the router on this end of the cable is configured for internal clock source and the router on the other end of the cable is configured for external clock source.

Invalid Configuration

Meaning: A Point-to-Point configuration that does not use auto-detect is being used and is incompatible with the remote device.

Action: Use auto-detect to configure the Point-to-Point WAN circuit on either the local or the remote device.

Invalid message type XXX found

Meaning: For the indicated frame relay circuit, a management message was received with an unknown or invalid message type. Valid values are:

0x7D Status
0x75 Status Enquiry
0x7B Status Update

XXX identifies the message type that was found.

Invalid MFS, dflt=2

Meaning: The configuration record for circuit: **cct** contains a faulty value in the Minimum Frame Spacing field. The system has defaulted to a value of 2.

Action: Modify Minimum Frame Spacing in the configuration.

Invalid N2, dflt=16

Meaning: The configuration record for circuit: **cct** contains a faulty value in the Retry Counter (N2) field. The system has defaulted to a value of 16.

Action: Modify Retry Counter (N2) in the configuration.

Invalid QOS. Setting to LLC1

Meaning: The Quality of Service parameter was not configured as LLC1 (unreliable datagram). Presently LLC1 is the only quality of service supported for frame relay. Therefore, the Quality of Service parameter has been automatically modified to be LLC1.

Action: Modify the configuration so that the Quality of Service parameter is LLC1.

Invalid shift parameter XXX

Meaning: A management packet was received with an unrecognizable shifting parameter. This applies only to those interfaces running ANSI Annex D. All information elements must be encoded using locking shift 5. Any other shifting parameters will be flagged as an error and data following will be discarded.

Invalid STATUS message received

Meaning: For the indicated frame relay circuit, the status message returned from the frame relay switch is not properly formatted. That is, the report type and keep-alive sequence exchange messages were not found in the proper order.

Event Log Messages

cct: Circuit Event Messages

IPCP is down

Meaning: For the indicated PPP circuit, a packet was received which did not conform to standard PPP format. The packet was dropped. No further action is necessary.

IPCP is up

Meaning: For the indicated PPP circuit, IP Control Protocol (IPCP) is up. IP packets may now be sent and received on the link.

IP next hop X.X.X.X assoc w/ YYY

Meaning: This indicates that a virtual IP circuit (IP-mapped circuit) has been associated with an actual circuit.

IPXCP is down

Meaning: For the indicated PPP circuit, IPX Control Protocol (IPXCP) has gone down.

IPXCP is up

Meaning: For the indicated PPP circuit, IPX Control Protocol (IPXCP) is up.

Keep-alive recovery (from net)

Meaning: The router is now properly receiving the network keep-alive sequence number for the identified circuit name.

LCP is being restarted

Meaning: For the indicated PPP circuit, Link Control Protocol (LCP) went down and the system is restarting LCP because the LCP Auto-Restart option was set to Yes.

LCP is down

Meaning: For the indicated PPP circuit, Link Control Protocol (LCP) has gone down. If the LCP Auto-Restart option was configured as Yes, then the system attempts to restart LCP.

LCP is up

Meaning: For the indicated PPP circuit, Link Control Protocol (LCP) is up. The system now attempts to bring up the appropriate network layer control protocols.

Local disconnected remote

Meaning: The router has disconnected the point-to-point link after first sending a disconnect request to the remote end and receiving an unnumbered acknowledgment.

Local LLC reset remote

Meaning: The router has sent a reset request to the remote end of the point-to-point link.

Local not hearing from remote

Meaning: A disparity exists between the ends of a point-to-point circuit. The circuit's remote signal and sense testing require that both ends of the circuit be designated as "active". This message is generated by the active side of a mismatched pair.

Action: Modify the configuration to ensure that the Remote signal & sense parameter is set to Active on both of the routers.

Local reset of remote succeeded

Meaning: The router has received a reset indication in response to an outstanding reset request.

Event Log Messages
cct: Circuit Event Messages

LQM negotiation rejected by remote station

- Meaning:** For the indicated PPP circuit, the remote station refuses to accept negotiation of the Link Quality Monitor (LQM) parameter. The system cannot bring up the Link Control Protocol (LCP) until the remote station is willing to accept negotiation of the LQM parameter.
- Action:** If it is not considered necessary to receive Link Quality Report (LQR) packets in order to monitor link quality, then modify the configuration so that the LQM Time parameter is set to 0. If the LQM Time parameter is set to 0, then the system will not require the peer (remote) station to send LQR packets.

Management Interface connection established

- Meaning:** The network and the DTE have established the connection necessary for periodic polling and status message exchange on the identified circuit.

mapped inact used since req'd. cct=YYY

- Meaning:** This indicates that an IP-mapped circuit has timed out due to inactivity on circuit **YYY**. The inactivity time set in the map record was used since other requests were queued waiting a free circuit.

Max Pkt Size adjusted down to 1500

- Meaning:** For the indicated PPP circuit, the Max Pkt Size parameter exceeded the maximum value allowed of 1500 bytes. The Max Pkt Size parameter has been automatically adjusted down to 1500 bytes.
- Action:** Modify the configuration so that the Max Pkt Size parameter is within the legal range.

Memory error (MERR) detected

- Meaning:** The LAN controller or link level controller cannot access the router memory. The circuit is effectively disabled.
- Action:** Verify hardware integrity.

min channel number > max (min set to X)

Meaning: The router configuration has the minimum channel number greater than the maximum channel number. The router will correct this.

Action: Correct the router configuration.

Minimum Latency cap being used

Meaning: A minimum latency cap of 3100 bytes is being used because the latency cap time is too small for the current link speed.

missed receiving XX LQRs: link is down

Meaning: For the indicated PPP circuit, **XX** Link Quality Monitor (LQM) time periods elapsed without a Link Quality Report (LQR) packet being received from the peer (remote) station. The link is declared down, the Link Control Protocol (LCP) is brought down, and all active network control protocols are also brought down. If the LCP Auto-Restart option is enabled, then the router attempts to restart LCP.

missed XX Echo Replies: link is down

Meaning: For the indicated PPP circuit, **XX** Echo Request time periods elapsed without an Echo Reply packet being received from the remote station. The link is declared down, the Link Control Protocol (LCP) is brought down, and all Network Control Protocols are also brought down. If the LCP Auto-Restart option is enabled, the router attempts to bring LCP up again.

missed XX LQRs: link is down

Meaning: For the indicated PPP circuit, **XX** Link Quality Monitor (LQM) time periods elapsed without a Link Quality Report (LQR) packet being received from the peer (remote) station. The link is declared down, the Link Control Protocol (LCP) is brought down, and all Network Control Protocols are also brought down. If the LCP Auto-Restart option is enabled, the router attempts to bring LCP up again.

Event Log Messages
cct: Circuit Event Messages

Net sequence num receive recovery

Meaning: The network is now properly sending keep-alive sequence numbers for the identified circuit.

Next hop IP X.X.X.X has no ph #

Meaning: All map items must have at least one configured phone number. The map record with with IP next-hop address **X.X.X.X** has no configured phone #.

Action: Add a phone number to the IP to V.25 bis mapping record.

New DLCI XXX added over existing one

Meaning: For the indicated frame relay circuit, a PVC was marked as new in the PVC status message before it was removed using the management interface. The old PVC is deleted and this new one is put in its place.

No buffers to reconnect to remote

Meaning: The circuit indicated in the **object** field of the event message cannot establish a connection because of insufficient buffer space.

No Pool circuits config for X.X.X.X

Meaning: A IP-mapped circuit was configured, but no pool circuits were configured for the circuit group associated with this static route. **X.X.X.X** is the IP address of the associated static route. This configuration error prevents the V.25 bis to IP map from working. The IP map is left disabled and the associated IP address will not be reachable using this map. A result is that all IP addresses accessed by this map will not be accessible. Attempting to enable the map with the NCL Enipmap command results in the NCL error message "Disabled, no pool ccts cfg for X.X.X.X. (X.X.X.X is the ip address of the next hop associated with the map.)"

Action: Configure the circuit group with V.25 bis pool circuits.

Not receiving seq num on MI enquiry

Meaning: For the indicated frame relay circuit, the other side of the frame relay interface is issuing status enquiry messages with last received keep-alive sequence numbers that are not as expected. That is, this sequence number is not the last sequence number we sent. This indicates that the other side is not receiving our status message response.

out of memory for IP to V.25 bis mapping

Meaning: Either too many IP-mapping records have been configured, or too many other configuration parameters have been set.

Action: Check your configuration and reduce the number of configured items.

out of memory for IP to V.25 bis mapping phone #

Meaning: Either too map records have been configured, or too many other configuration parameters have been set.

Action: Check your configuration file and reduce the number of configured items.

out of message buffers, pkts dropped

Meaning: There are no message buffers available for V.25 bis. These messages are used for internal V.25 bis communication. When this occurs, data packets may be lost or a V.25 bis connection may not be established.

Action: Reduce the overall system resource use. (For example, reduce traffic to the router.)

Out of sequence keep alive (net)

Meaning: The router is not properly receiving the network keep-alive sequence number for the identified circuit name. Usually this means the switch has reset its sequence counter, indicating that it is experiencing difficulties.

Event Log Messages
cct: Circuit Event Messages

Providing quality of service to remote

Meaning: Follows the “circuit in auto-detect mode” message and indicates the Quality of Service parameter setting in the local router for the indicated circuit.

Pkts rcvd while waiting for outbound data

Meaning: The router was waiting for outbound data so that it could establish a connection when inbound data was received from the adapter.

Action: Check the router configuration. In manual adapter mode, the router should only initiate a connection outbound when set up to enable on data available. If this is the side that should initiate the call, check the adapter configuration so that it doesn’t auto answer.

Physical level error

Meaning: The LAN controller or link level controller has detected a Level 1 (physical media) error.

Action: Verify hardware integrity.

Pool cct must enable on data avail

Meaning: V.25 bis pool circuits must be configured to enable when data is available. This is a warning to the user of the misconfiguration. The circuit will be used as if set up to enable when data is available.

Action: Check your configuration file and correct the V.25 bis circuit misconfiguration.

possible loop-back has been detected

Meaning: For the indicated PPP circuit, PPP detected a possible line loopback.

ppp: bad configuration file

Meaning: PPP detected an inconsistency in the configuration.

Action: Modify the configuration.

protocol 0xYY not supported

Meaning: For the indicated PPP circuit, the peer (remote) station sent a packet with a PPP protocol value of YY (hex), but the system does not support PPP protocol YY.

Providing LLC1 service

Meaning: The circuit named in the *object* field of the event message is enabled and providing LLC1 service.

Providing LLC2 service to remote

Meaning: The circuit named in the *object* field of the event message is enabled and providing LLC2 service.

PVC XXX added - Active

Meaning: For the indicated frame relay circuit, a PVC has been added in the active state. This is due to a full status message or an update status message from the management interface. XXX is the DLCI associated with the newly added PVC.

PVC XXX added - Inactive

Meaning: For the indicated frame relay circuit, a PVC has been added in the inactive state. This is due to a full status message or an update status message from the management interface. Usually this indicates that the station at the other side of this connection is not active. XXX is the DLCI associated with the newly added PVC.

PVC XXX deleted

Meaning: For the indicated frame relay circuit, the PVC indicated by the given DLCI XXX has been deleted. Deletion may occur because a PVC status IE was not present in the full status message or because it has been explicitly deleted.

Event Log Messages
cct: Circuit Event Messages

PVC XXX received xoff indication

Meaning: A PVC information element indicated that this PVC has received an Xoff indication. Data will not be transmitted over this particular PVC until it receives an xon indication. This message is only relevant if the Data Link Connection Management type is LMI. Annex D does not use the Xoff/Xon indication. XXX is the DLCI associated with the PVC which has received the Xoff indication.

PVC XXX received xon indication

Meaning: A PVC information element indicated that this PVC has received an Xon indication. Generally, this message follows the Xoff indication. This frees the PVC for data transfer. XXX is the DLCI associated with the PVC which has received the xon indication.

PVC XXX status change to Active

Meaning: For the indicated frame relay circuit, a PVC has changed state to active. This is due to a full status message or update status message from the management interface. XXX is the DLCI associated with the PVC for which the change has occurred .

PVC XXX status change to Inactive

Meaning: For the indicated frame relay circuit, a PVC has changed state to inactive. This is due to a full status message or update status message from the management interface. XXX is the DLCI associated with the PVC for which the change has occurred.

PVC IE out of order f or dlci XXX

Meaning: For the indicated frame relay circuit, a full status message was received for which the PVC status information elements were not in ascending order by DLCI. XXX identifies the first out of order PVC information element.

QOS = quality of service, addr = DCE/BIDTE, compression = Yes/No

Meaning: Follows the “circuit in auto-detect mode” message and indicates the current Quality of Service, Point-to-Point Address, and Compression parameter settings.

Received a connect delay indication (DLC)

Meaning: The terminal terminal adapter issued a delay call to the router. The router will retry the call after the delay time requested.

Received a connect indication (CNX)

Meaning: The router has received a connect indication. (This terminal adapter response is not needed by the router because it uses DSR to indicate when a call has been established.)

Received a connect fail indication (CFI)

Meaning: The router has received a Call Failure indication from the terminal adapter. Depending on the configuration, the router will attempt the connection again automatically.

Action: Check for any logged adapter errors to find out why the call failed, and correct errors as necessary.

Received call

Meaning: The router has received an incoming call.

Received call dropped (number not allowed)

Meaning: The router received an incoming call, but dropped it because the number did not match any allowed incoming number.

Action: No user action required. However, if for the call to be accepted, it must be added to the list of allowed numbers in the configuration file, or the configuration must be changed to allow all incoming calls.

Event Log Messages
cct: Circuit Event Messages

received indication too short, len = *X*

Meaning: The terminal adapter indication is too short. The router will ignore it.

Action: Check the terminal adapter configuration.

Received packets while in the down state

Meaning: The router has received packets from the terminal adapter while the connection is down. These packets will be dropped.

Action: Check the terminal adapter configuration.

Received packets while waiting for CTS

Meaning: The router has received packets from the terminal adapter while waiting for CTS. These packets will be dropped.

Action: Check the terminal adapter configuration.

Received phone number length > *XX*

Meaning: The received phone number was too long. The router will truncate it to the allowed length.

Action: Check the terminal adapter configuration.

Received sub-address length > *XX*

Meaning: The received subaddress is too long. The router will truncate it to the allowed length.

Action: Check the terminal adapter configuration.

received unknown indication -> *XXX*

Meaning: The terminal adapter indication is unknown. The router will ignore it.

Action: Check the terminal adapter configuration.

Receiver overflow detected

Meaning: The Local Area Network Controller, or the Link Level Controller for the circuit identified in the *object* field of the event message has dropped a received packet because of lack of space in the Receiver FIFO buffer.

Remote clearing

Meaning: The remote end of a point-to-point circuit is in the process of resetting.

Remote connection refused by local

Meaning: The router has rejected a call request from the remote end.

Remote disconnect after local FRMR

Meaning: The remote end of a point-to-point circuit has disconnected after receiving a frame reject packet from the local end of the circuit.

Remote disconnect confirmed

Meaning: A local LLC2 circuit has received a positive confirmation of a previously issued disconnect.

Remote disconnect received

Meaning: A local LLC2 circuit has issued a disconnect to a remote circuit, and this disconnect has been received. (Same as “Remote clearing” in this section.)

Remote disconnect retries exhausted

Meaning: A local LLC2 circuit has issued a disconnect to a remote circuit, and the number of retries has been exhausted after N2 (Retry Counter) times of trying.

Remote disconnect timeout

Meaning: A local LLC2 circuit has issued a disconnect to a remote circuit, and this disconnect has timed out and become idle.

Event Log Messages
cct: Circuit Event Messages

Remote disconnected local

Meaning: The router has received (and processed) a disconnect request from the remote end.

Remote reset to local

Meaning: The router has received a reset request from the remote end.

remote station has logged in to Server

Meaning: For the indicated PPP circuit, the remote station has successfully logged in to the system.

remote station rejected ATCP

Meaning: For the indicated PPP circuit, the remote station has rejected the AppleTalk control Protocol (ATCP). No AppleTalk traffic may occur over the link until the remote station is ready to accept the AT Control Protocol.

remote station rejected BNCP

Meaning: For the indicated PPP circuit, the remote station has rejected the Bridge Network Control Protocol (BNCP). No bridge traffic may occur over the link until the remote station is ready to accept the Bridge Network Control Protocol.

remote station rejected DRSCP

Meaning: For the indicated PPP circuit, the remote station has rejected the DECnet Routing Service Control Protocol (DRSCP). No DRS traffic may occur over the link until the remote station is ready to accept the DRS Control Protocol.

Meaning: For the indicated PPP circuit, the remote station has rejected the Bridge Network Control Protocol (BNCP). No bridge traffic may occur over the link until the remote station is ready to accept the Bridge Network Control Protocol.

remote station rejected IPCP

Meaning: For the indicated PPP circuit, the remote station has rejected the IP Control Protocol (IPCP). No IP traffic may occur over the link until the remote station is ready to accept the IP Control Protocol.

remote station rejected IPXCP

Meaning: For the indicated PPP circuit, the remote station has rejected the IPX Control Protocol (IPXCP). No IPX traffic may occur over the link until the remote station is ready to accept the IPX Control Protocol.

remote station rejected LCP

Meaning: For the indicated PPP circuit, the remote station has rejected the Link Control Protocol (LCP). Link initialization cannot continue until the remote station is ready to accept the Link Control Protocol.

remote station rejected UPAP

Meaning: For the indicated PPP circuit, the remote station has rejected the User/Password Authentication Protocol (UPAP). Link initialization cannot continue until the remote station is ready to accept the User/Password Authentication Protocol.

Action: If UPAP is not considered necessary, then modify the configuration to disable UPAP.

remote station's login attempt failed

Meaning: For the indicated PPP circuit, the remote station failed in its attempt to login to the system. The remote station's User ID or Password (or both) were incorrect.

Action: The remote station's User ID and/or Password in the configuration may be modified (if desired) so that the remote station may successfully login to the system.

Event Log Messages
cct: Circuit Event Messages

remote station's LQM time > configuration time

Meaning: For the indicated PPP circuit, the Link Quality Monitor (LQM) time that the remote station is willing to negotiate for is greater than the LQM time configured for the PPP circuit. The higher LQM time is accepted, but it means that the remote station will be sending Link Quality Report packets less often than the system originally requested.

Responded to reset, service continued

Meaning: The router has received (and processed) a reset request from the remote end. Refer also to "Unexpected remote reset to local" on page 17-55 in this section.

Retrying LLC2 connection

Meaning: The circuit identified in the *object* field of the event message has been unable to obtain positive acknowledgment of an outstanding frame. It will continue to retry the connection as specified by the Retry Counter (N2), Retry Timer (T1), and Connect Retries LLC2 parameters.

Sent CIC cmd to connect call

Meaning: The router has sent a CIC command in response to an incoming call to establish a connection.

Sent CRN cmd to XXX

Meaning: The router has sent a CRN command with the listed number XXX.

Sent DIC cmd to disconnect call

Meaning: The router has sent a DIC command in response to an incoming call to prevent establishing a connection.

Server has logged in to remote station

Meaning: For the indicated PPP circuit, the system successfully logged in to the remote station.

Server's login attempt failed

Meaning: For the indicated PPP circuit, the system failed in its attempt to login to the remote station. The system User ID or the System Password (or both) were incorrect.

Action: Modify system User ID and/or System Password in the configuration.

SQE absent (non 802.3 XCVR)

Meaning: The circuit named in the *object* field of the event message has detected a loss of the Signal Quality Error (SQE) signal.

Action: Check transceiver hardware. SQE is not supported by Ethernet version 1.0 transceivers.

SR internal LAN ID not in RIF route

Meaning: A specifically routed frame that did not include the internal LAN ID configured for bridging was received. The packet is dropped.

Action: For information on the Internal LAN ID parameter, refer to chapter 6 in this manual.

SR is_srf_rif_insert: no rif entry

Meaning: A specifically routed frame was received, but the appropriate entry in the source-routing intermediate-station table (sr_is_table) does not contain a routing information field for the destination station. The packet is dropped.

SR max hops exceeded in explorer frame

Meaning: The maximum number of hops for a source-routed packet, seven, was exceeded in an all-routes-explorer (ARE) frame or a spanning-tree-explorer (STE) frame. The packet is dropped.

SR max hops exceeded in Specifically Routed Frames

Meaning: The maximum number of hops for a source-routed packet, seven, was exceeded in a specifically routed frame (SRF). The packet is dropped.

SR max RDs exceeded in explorer packet

Meaning: The maximum number of route descriptors (RDs) for a source-routed packet, eight, was exceeded in an all-routes-explorer (ARE) frame or a spanning-tree-explorer (STE) frame. The packet is dropped.

SR max RDs exceeded in SRF packet

Meaning: The maximum number of route descriptors (RDs) for a source-routed packet, eight, was exceeded in a specifically routed frame (SRF). The packet is dropped.

SR out cg = cg for SRF

Meaning: The specifically routed frame (SRF) is being forwarded through the same interface on which it was received. This can occur if the loop detection time is configured too low to detect an ARE loop, if the network is reconfiguring due to a link failure, or if the router is rebooted.

Action: Increase the Loop Detection Time parameter.

SR out of buffers

Meaning: No packet buffer was available to allocate for flooding an all-routes-explorer (ARE) frame out through an interface. It could not be flooded.

SR possible ARE loop

Meaning: A possible all-routes-explorer (ARE) loop has been detected. This can occur if the loop detection time is configured too low to detect an ARE loop, if the network is reconfiguring due to a link failure, or if the router is rebooted.

Action: Increase the Loop Detection Time parameter.

SR Rif_table out of space

Meaning: The routing information field (RIF) table, which contains the RIFs used to route source-routed packets between the router and the remote token ring nodes, is out of space. It contains RIFs used for both end-station source routing for IP as well as intermediate-station source routing for bridging.

SR sr_es_find: Madr_table out of space

Meaning: The madr_table, the station address table (also called the MAC address table), is out of space. It contains the station addresses of nodes that communicate through token ring interfaces on this router. These addresses are used for both end-station source routing for IP as well as intermediate-station source routing for bridging.

Action: For an HP series 200 or 400 routers: Increase available memory space by deleting any unneeded portions of the configuration, such as configurations for unused ports or protocols.

For an HP router 650: Increase memory on the routing engine from 8 to 16 Mbytes (using the HP J2443A memory upgrade). If this message occurs after a memory upgrade, increase available memory space by deleting any unneeded portions of the configuration, such as configurations for unneeded ports or protocols.

SR Sr_es_table out of space

Meaning: The sr_es_table, the source-routing end-station table, is out of space. It contains indexes into the station address table (madr_table) for destination nodes that communicate through token ring interfaces directly attached to this router. It also contains pointers to the RIF table, which provides the routing information for the destination nodes.

Action: The maximum number of sr_es_table entries supported by the 2-Mbyte processor card is 1K. Upgrade the processor card to 5-Mbytes of memory to allow 4K entries.

Event Log Messages
cct: Circuit Event Messages

SR Sr_is_srf_rif_insert: no rif entry

Meaning: A specifically routed frame was received, but the appropriate entry in the source-routing intermediate-station table (sr_is_table) does not contain a routing information field for the destination station. The packet is dropped.

SR Sr_is_table out of space

Meaning: The sr_is_table, the source-routing intermediate-station table, is out of space. It contains indexes into the station address table (madr_table) for source/destination pairs of nodes. It also contains pointers to the RIF table, which provides the routing information for the source/destination nodes on the network.

SR sr_ring full

Meaning: The SR_ring data structure, used to contain outgoing source-routed packets, is full. No other source-routed packets will be sent out until the next time the bridge task runs.

SR TF forward_ring full

Meaning: The forward_ring data structure, used to contain outgoing source-routed packets that have been filtered through traffic filters, is full. No other source-routed packets that need to be filtered will be sent out until the next time the bridge task runs.

Status msg polling recovery

Meaning: The network is now responding to the status enquiry messages within the given timeout period. After three consecutive status/enquiry-status message exchanges, this message is displayed to indicate that the system is in sync.

Token cable connection fault

Meaning: The token ring interface has detected a faulty cable connection.

Action: Check for a loose or disconnected cable, and verify other hardware.

Token SRA Programming Failure

Meaning: The token ring device failed SRA programming, indicating a possible hardware failure. Source route bridging will not function properly.

Action: Contact your Hewlett-Packard support provider.

too many bytes lost: link unreliable

Meaning: For the indicated PPP circuit, the number of bytes lost (either by the system or by the remote station) exceeded the allowed number of lost bytes as determined using the Desired Link Quality parameter. All Network Control Protocols will be brought down by the system. The system will continue to send and receive Link Quality Report (LQR) packets. When desired link quality is re-established, the Network Control Protocols will be brought up again.

Too many channels to aggregate (max set to X)

Meaning: The router configuration has too many channels to aggregate. The router will set the channel number to X.

Action: Correct the router configuration.

Too many circuits configured for slot XX

Meaning: The configuration contains more than four frame relay interfaces for a single slot. The slot number of the error is included as XX.

Action: Modify the configuration so that there are fewer frame relay interfaces for slot XX.

too many packets lost: link unreliable

Meaning: For the indicated PPP circuit, the number of packets lost (either by the system or by the remote station) exceeded the allowed number of lost packets as determined using the Desired Link Quality parameter. All Network Control Protocols will be brought down by the system. The system will continue to send and receive Link Quality Report (LQR)

Event Log Messages

cct: Circuit Event Messages

packets. When desired link quality is re-established, the Network Control Protocols will be brought up again.

Too many V.25 bis maps defined, limit = %d

Meaning: Too many V.25 bis map records have been defined. The maximum number allowed is 255.

Action: Check your configuration file and reduce the number of configured items.

Too many V.35 circuits configured

Meaning: The configuration contains an excessive number of V.35 line records for this slot.

Action: Modify the configuration.

Transceiver signal loss

Meaning: The LAN controller cannot communicate with the Ethernet/802.3 transceiver.

Action: Verify the integrity of the transceiver.

transmit congestion on cct X

Meaning: Indicates that the flow of data to be transmitted to the given V.25 bis circuit (**cct**) has exceeded the circuit's capacity, and packets have been dropped.

Action: Slow down the information rate or increase the available line bandwidth.

Transmit underflow detected

Meaning: The link level controller has truncated packet transmission because of an interruption in the flow of data from memory.

TR Open Failed

Meaning: The token ring device failed in its attempt to insert into the ring. This usually results from trying to insert to a ring at the wrong speed (4 or 16 Mbits).

Action: Verify and select the proper ring interface speed for this line.

Unable to perform update for dlci

Meaning: For the indicated frame relay circuit, an operator tried to modify a DLCI but the system was unable to perform the requested modification. Possible problems are adding a DLCI that has already been added or deleting a DLCI that isn't present.

unable to read configuration summary

Meaning: Unable to read the V.25 bis map configuration.

Action: Check your IP-mapping configuration for errors.

unable to read ip map record

Meaning: Unable to read the V.25 bis IP-mapping configuration.

Action: Check your IP-mapping configuration for errors.

Unexpected remote reset to local

Meaning: This message occurs at one end of a point-to-point link when the connection is first being established. One end of the link usually comes up before the other end. The first end subsequently receives a reset request from the other end when it comes up. The side that comes up first displays the above message, which always appears in tandem with the "Responded to reset, service continued" event message.

Unexp ring ind, will rcv inbound call

Meaning: Router already received an incoming call message and just got another one. The incoming call will be accepted if it doesn't fail any user-

Event Log Messages

cct: Circuit Event Messages

specified call restrictions placed on inbound calls. This is an unlikely event and may indicate an error by the connected adapter.

Note: In V.25 bis mode, the WAN Net Fail LED lights if the connected adapter does not respond with CTS True within 20 seconds of the router raising DTR. The Net Fail LED turns off if the adapter subsequently does respond.

In manual adapter mode, the WAN Net Fail LED lights if a connection does not come up within the connect wait time on the first attempt to establish an outbound connection. The LED turns off if a connection is established on a subsequent retry.

unknown char *X* in phone number

Meaning: The phone number configured (for terminal adapter) has unexpected characters. These characters will not be used when making or receiving the call.

unknown char *X* in recv phone number

Meaning: The received phone number has unexpected characters. The router will ignore them.

Action: Check the terminal adapter configuration.

unknown char *X* in recv sub-address

Meaning: The received sub-address has unexpected characters. The router will ignore them.

Action: Check the terminal adapter configuration.

unknown char *X* in sub-address

Meaning: The sub-address configured has unexpected characters. These characters will not be used when making or receiving the call.

Unsupported IE value *XXX* found

Meaning: For the indicated frame relay circuit, a valid status update or full status message was received with an unrecognized or unsupported Information Element (IE). *XXX* identifies Information Element identifier code in question.

Unsupported NLPID found *XXX*

Meaning: For the indicated frame relay circuit, a received data packet that included a NLPID value that was not recognized. The NLPID identifies the encapsulated data type. Packets received with unknown NLPIDs are discarded. *XXX* identifies the NLPID value received.

V.25 bis to IP dup next hop, IP *X.X.X.X*

Meaning: A duplicate IP next-hop entry has been configured in the IP to V.25 bis mapping configuration. *X.X.X.X* is the IP address of the duplicate.

Action: Remove the duplicate entry. (If not removed, the first entry is used and the second entry will be ignored.)

V35 circuit record missing

Meaning: A circuit has not been configured.

Action: Modify the configuration to ensure that it includes circuit records for *cct*.

Wrong sequence number on MI enquiry

Meaning: For the indicated frame relay circuit, the other side of the frame relay interface is issuing status enquiry messages with keep-alive sequence numbers that are not as expected. That is, this sequence number is more than one greater than the last one we received.

X - High priority transmit congestion

Meaning: This message is reported when the data packets that were prioritized as high can't be sent over the WAN link due to congestion. This message is reported on the first instance of dropping a packet due to congestion and the first time a packet is dropped after the tx_congestion or total_tx_error statistic is reset.

X Latency cap XXX bytes (XXXms,XXXbps)

Meaning: This reports the calculated number of maximum bytes that will be queued to the given WAN circuit. The numbers in parenthesis are the configured values for Max Link Latency and Clock Speed that were used in the calculation.

X - Low priority transmit congestion

Meaning: This message is reported when the data packets that were prioritized as low can't be sent over the WAN link due to congestion. This message is reported on the first instance of dropping a packet due to congestion and the first time a packet is dropped after the tx_congestion or total_tx_error statistic is reset.

X - Maximum link latency reached

Meaning: This message is reported when packets can't be sent over the WAN link because the maximum link latency configured by the user would be exceeded. This message is reported on the first instance of dropping a packet due to exceeding the latency cap and the first time a packet is dropped after the latency_tx or total_tx_error statistic is reset.

X - Normal priority transmit congestion

Meaning: This message is reported when the data packets that were not prioritized can't be sent over the WAN link due to congestion. This message is reported on the first instance of dropping a packet due to congestion and the first time a packet is dropped after the tx_congestion or total_tx_error statistic is reset.

XNSCP is down

Meaning: For the indicated PPP circuit, XNS Control Protocol (XNSCP) has gone down.

XNSCP is up

Meaning: For the indicated PPP circuit, XNS Control Protocol (XNSCP) is up. XNS packets may now be sent and received on the link.

X - PPP/FR High Pri Tx congestion

Meaning: When PPP is configured over slow WAN links ($\leq 64K$), the PPP control packets have priority over any data packets. This message is reported when these high priority control packets can't be sent over the link due to congestion. This message is reported on the first instance of dropping a packet due to congestion and the first time a packet is dropped after the tx_congestion or total_tx_error statistic is reset.

X - PPP/FR Low Pri Tx congestion

Meaning: When PPP is configured over slow WAN links ($\leq 64K$), the PPP control packets have priority over any data packets. This message is reported when the lower priority data packets can't be sent over the link due to congestion. This message is reported on the first instance of dropping a packet due to congestion and the first time a packet is dropped after the tx_congestion or total_tx_error statistic is reset.

dev: Device Event Messages

These event messages are generated by the system variable “dev” in one of the following formats, depending on the router model you are using:

Series 200 and 400: `dev: 'device event message'`

Router 650: `dev[slot number]: 'device event message'`

Bad module ID

Meaning: The adapter card (module) ID cannot be identified by the driver. These IDs are listed in table 18-1 in the “hw: Hardware Information Base” section in chapter 18.

Action: Verify the adapter card hardware.

CCT *cct*: Bad board id

Meaning: The router has detected that the connector number specified for this token ring port does not physically exist on the hardware. Either the current version of the operating system does not support the hardware type or the line record for this token ring circuit (*cct*) *has an invalid connector number configured*.

Action: Check the connector assignment for this token ring line (*cct*) in the configuration file.

CCT *cct*: Group Address Programming Failure

Meaning: A failure was detected when programming the proprietary token ring group address for the hop count reduction. No source routing hop count reduction will take place. There may be too many protocols configured on this token ring circuit that use functional addresses.

Action: Contact your HP support provider.

CCT cct: Token cable connection fault

Meaning: The router detected a cable fault on this token ring circuit. The circuit is no longer in operation.

Action: Check that the cable is still attached to the router and also to the token ring hub. If the connections are proper, then the cable itself may be bad.

CCT cct: Token Ring circuit record missing

Meaning: This token ring circuit is not completely configured. There may be some corruption of the configuration file.

Action: Reconfigure the token ring circuit and line.

CCT cct: Token Ring line record missing

Meaning: This token ring line is not completely configured. There may be some corruption of the configuration file.

Action: Reconfigure the token ring circuit and line.

CCT cct: Token SRA Programming Failure

Meaning: A failure was detected while trying to program the source route accelerator chip.

Action: There may be a hardware failure. Contact your HP support provider.

CCT cct: Too many lines assigned to the Token connector

Meaning: There can be only one line configured per token ring connector.

Action: Ensure that each line in the configuration file has a unique token ring connector name.

Event Log Messages
dev: Device Event Messages

Connected module is non-link: *nn*

- Meaning:** The adapter card cannot be identified by the driver. These IDs are listed in table A-1 in the “hw: Hardware Information Base” section in chapter 18.
- Action:** Verify the adapter card hardware.

Connector *nn* not on this module

- Meaning:** The configuration record reflects a non-existent physical connector.
- Action:** Modify Connector in the line record in the configuration.

Connector out of range

- Meaning:** The configuration contains an invalid Connector parameter.
- Action:** Use the Configuration Editor to identify and replace the invalid Connector parameter.

Ethernet CAM load failed

- Meaning:** SONIC hardware fault.
- Action:** HP series 200 or 400 router: Replace the router.
HP Router 650: Replace the interface card.

Ethernet circuit assigned to multiple lines

- Meaning:** The same Ethernet circuit has been assigned to multiple lines.
- Action:** Modify the configuration to ensure that circuits are assigned to only one line.

Ethernet Port # carrier sense lost

Action: Check the transceiver and connection to router port #.

Ethernet Port # failed self-test

Meaning: Hardware error.

Action: HP series 200 or 400 router: Replace the router.
HP Router 650: Replace the interface card.

Ethernet Port # transmit failure

Action: Check the LAN cable and connection to the transceiver on port #.

Frame Relay enabled on cct XXX

Meaning: The synchronous driver has enabled the support for frame relay on cct XXX. At this point, the management interface is also initialized for cct XXX if it has been configured.

Internal clock must be the same for ports WAN1 & WAN2

Meaning: On an HP Router 650, synchronous lines using connectors WAN1 and WAN2 share the same clock signal generator. Thus, when using internal clocking on WAN1 and WAN2, the Clock Speed parameter in the lines configuration must have the same value for both connectors. The Clock Speed parameter is meaningless when Clock Source for the line is set to External.

Action: Reconfigure both lines to have the same clock speed.

Internal clock must be the same for ports WAN3 & WAN4

Meaning: On an HP Router 650, synchronous lines using connectors WAN1 and WAN2 share the same clock signal generator. Thus, when using internal clocking on WAN1 and WAN2, the Clock Speed parameter in the lines configuration must have the same value for both connectors. The Clock Speed parameter is meaningless when Clock Source for the line is set to External.

Event Log Messages

dev: Device Event Messages

Action: Reconfigure both lines to have the same clock speed.

Internal clock must be the same on all ports

Meaning: On all HP series 200 and 400 routers, all synchronous lines share the same clock signal generator. Thus, when using internal clocking on more than one line, the Clock Speed parameter in the lines configuration must have the same value for those lines. The Clock Speed parameter is not used when the clock source for the line is set to External.

Action: Reconfigure both lines to have the same clock speed.

Internal clock set to *speed*

Meaning: This is a progress message indicating what clock speed was chosen for the indicated line. The chosen speed is not what was configured because the line shares a clock signal generator with another line. For an HP Router 650, lines using connectors WAN1 and WAN2 share a clock signal generator, and lines using connectors WAN3 and WAN4 share a clock signal generator. For all other products, all synchronous lines share a clock signal generator.

Action: Reconfigure both lines to have the same clock speed.

Invalid MFS, dflt=2

Meaning: The configuration record for the circuit contains a faulty value in the Minimum Frame Spacing field. The router has defaulted to a value of 2.

Action: Modify Minimum Frame Spacing in the configuration.

Invalid N2, dflt=16

Meaning: The configuration record for the circuit contains a faulty value in the Retry Counter (N2) field. The router has defaulted to a value of 16.

Action: Modify Retry Counter (N2) in the configuration.

No buffers available for deadlock processing

Meaning: Indicates a degenerative line condition resulting in the lack of receive buffers at both the line source and termination.

No circuits configured

Meaning: No circuits are configured.

Action: Modify the configuration to include required circuit records.

No configuration summary record

Meaning: A circuit record is missing from the configuration.

Action: Modify the configuration to ensure that all lines and circuits are defined.

No Ethernet circuits configured

Meaning: **HP series 200 and 400 Routers:** No Ethernet circuits are configured in the router.

HP J2435A Four-Port Ethernet Interface Module: No Ethernet circuits are configured in the module.

Action: Modify the line and circuit configuration to include required circuit records.

No lines configured

Meaning: No lines are configured for the circuits on the router or on the indicated slot.

Action: Configure one or more lines for the router or indicated slot.

No Token Ring circuits

Meaning: One or more circuits designated by the Circuit Name parameter in the line record has not been configured.

Event Log Messages

dev: Device Event Messages

Action: Modify the configuration to ensure that it includes circuit records for all circuits.

No Token Ring circuits configured

Meaning: This is a possible error condition in that no circuits have been configured for a router having one or more token ring ports. None of the circuits will be used.

Action: Check your network topology to see if any of the token ring circuits should be configured.

Pass-thru protocol enabled on cct *cct#* driver: (LLAN *local-address* RLAN *remote-address*)

Meaning: The synchronous pass-through protocol is enabled on *cct#*. The configured local and remote station addresses are shown also.

Rx FRMR on circuit *cct #* Frame: *hh hh hh hh hh*

Meaning: Circuit *cct* (running LLC) has received a frame reject frame. *hh hh hh hh hh* is the first five bytes of the frame in hexadecimal format.

SYNC circuit assigned to multiple lines

Meaning: One or more line records contains references to the same point-to-point circuit.

Action: Modify the line configuration to ensure that all line and circuit records are consistent.

Token Ring circuit assigned to multiple lines

Meaning: A circuit has been assigned to more than one line on this router. Proper operation requires that a circuit be configured to only one line.

Action: Check the lines configuration to ensure that the token ring circuit name is assigned to only one token ring line.

Too many Ethernet circuits configured

- Meaning:** The configuration contains more Ethernet circuit records than can be accommodated.
- Action:** Modify the configuration to ensure that no more than the maximum Ethernet/802.3 circuit records are assigned.

Too many lines assigned to Ethernet connector

- Meaning:** The same Ethernet/802.3 line has been assigned to multiple physical connectors.
- Action:** Modify the configuration so that only a single line is assigned to each connector.

Too many lines assigned to V.35 connector

- Meaning:** The configuration contains an excessive number (greater than two) of line records for a single connector.
- Action:** Modify the line configuration to ensure that no more than one line record references a specific physical connector.

Too many Token Ring circuits configured

- Meaning:** There can be no more than one token ring circuit configured for each port on the router. More than one circuit has been configured for a token ring port.
- Action:** Reconfigure the token ring circuit(s) to no more than one per port.

Too many Token Ring circuits configured for slot

- Meaning:** There can be no more than four token ring circuits configured for an HP Router 650 four-port token ring interface module. More than four circuits have been configured.
- Action:** Reconfigure the token ring circuits to no more than one per port.

Event Log Messages
dev: Device Event Messages

Too many V.35 circuits configured

Meaning: The configuration contains an excessive number of V.35 line records.

Action: Modify the line configuration.

Total bandwidth reserved not 100% (XXX% cfg'ed)

Meaning: The bandwidth reserved for each of the priorities for the WAN circuit does not add up to 100%.

Action: Make sure the three percentages configured in the Bandwidth Reservation record for the given WAN circuit add up to 100.

IV.35 circuit record missing

Meaning: A circuit *cct* has not been configured.

Action: Modify the configuration to ensure that it includes circuit records for *cct*.

WAN Port #failed self-test

Meaning: Hardware error.

Action: HP series 200 or 400 router: Replace the router.
HP router 650: Replace the interface card.

XCVR *n* out of range in line record

Meaning: The configuration contains an invalid transceiver number.

Action: Modify the lines configuration.

dls: Data Link Services Event Messages

Bad action

- Meaning:** Internal DLS state machine error.
- Action:** Contact your HP support representative.

Bad cct type configured

- Meaning:** The circuit type configured is not a valid type. It can only be one of:
- Ether/802.3 , 802.5, FDDI, HP Point to Point,
 - LAPB, PPP, SMDS, Frame relay, V.25 bis adaptor,
 - Manual adapter, PPP over V.25 bis
- Action:** Use the Configuration Editor to select a circuit type.

Bad QoS configured for cct type

- Meaning:** The Quality of Service configured for this circuit is not possible with this type of circuit. The valid possibilities are:

Circuit Type	QOS Possibilities
Ether/802.3	LLC 1 (datagram)
802.5	LLC 1 (datagram)
FDDI	LLC 1 (datagram)
HP Point to Point	LLC 1 (datagram) LLC 2 (reliable) Auto
LAPB	X.25
PPP	LLC 1 (datagram)
SMDS	LLC 1 (datagram)
Frame relay	LLC 1 (datagram)
V.25 bis adapter	LLC 1 (datagram)
Manual adapter	LLC 1 (datagram)
PPP over V.25 bis	LLC 1 (datagram)

Event Log Messages

dls: Data Link Services Event Messages

Action: Reconfigure the circuit.

CGM misconfigured

Meaning: DLS was unable to notify the upper layer protocols that the circuit has come up. The Circuit Group Manager module is not active.

Action: Disable the circuit and re-enable it via NCL. If the symptom persists, call your HP support representative.

Clock recovered

Meaning: The router has detected that data has been transmitted on the WAN circuit that had previously lost its clock signal. Service has been restored.

Establishing LLC2 connection

Meaning: Indicates the progress of a circuit configured for LLC2 quality of service; the router is trying to establish the LLC2 connection with a peer over the WAN circuit.

Circuit auto-configuring

Meaning: This circuit was configured to auto-detect WAN parameters like Quality of Service, HDLC addresses, and compression; the router is attempting to negotiate these parameters.

Detected carrier, enabling cct

Meaning: The router has detected the carrier signal on the WAN circuit; the circuit will become operational.

Invalid Configuration: QOS must be LLC2

Meaning: Auto-configuring has detected a remote bridge, but the router's QOS configuration option is not set to LLC2 or auto-configure.

Action: Use the LLC2 or auto-configure option to configure the QOS for the Point-to-Point WAN circuit.

Invalid Configuration: Pt-to-Pt address must be DCE

Meaning: Auto-configuring has detected a remote bridge, but the router's Pt-to-Pt address configuration option is not set to DCE or auto-configure.

Action: Use DCE or auto-configure as the Pt-to-Pt address for the Point-to-Point WAN circuit.

Invalid Configuration: Mismatching QOS

Meaning: The QOS configuration option for the Point-to-Point WAN circuit is not the same on the local and remote device.

Action: Change to QOS configuration option to be the same or to use auto-configure on either the local or the remote device.

Invalid Configuration: Use 'No Compression'

Meaning: Auto-configuring has detected a remote bridge and the router's compression configuration option is not set to 'No Compression' or auto-configure.

Action: Use "No Compression" or auto-configure as the compression method for the Point-to-Point WAN circuit.

Invalid Configuration: Pt-to-Pt addresses are equal

Meaning: The Pt-to-Pt address configuration option for the Point-to-Point WAN circuit is the same on the local and remote device.

Action: Change to Pt-to-Pt address configuration option to be the different or to use auto-configure on either the local or the remote device.

Invalid Configuration: Mismatching Compression

Meaning: The compression configuration option for the Point-to-Point WAN circuit is not the same on the local and remote device.

Action: Change the compression configuration option to be the same or to use auto-configure on either the local or the remote device.

Event Log Messages

dls: Data Link Services Event Messages

Invalid Configuration detected by remote side

Meaning: A Point-to-Point configuration option that was not using auto-configure is incompatible with the remote device.

Action: Use the auto-configure option to configure the Point-to-Point WAN circuit on either the local or the remote device.

Lost carrier, disabling cct

Meaning: The router has detected the loss of the carrier signal on the WAN circuit. The circuit is no longer in service.

Action: Check cable connections, check any modems, CSU/DSUs, and the line itself.

No cct record for FDDI CCT %cct%

Meaning: No line has been configured for this FDDI circuit.

Action: Configure a line for this FDDI circuit.

QOS = *addr*, addr = *addr*, Compression = *compression*

Meaning: Dynamic Link Establishments has negotiated the parameters for this end of the WAN link as shown.

SR sr_es_find: Mdr_table out of space

- Meaning:** The table that stores station addresses of end nodes on a token ring network is full. The router uses a Least-Recently-Used policy to replace entries in this table, so no connectivity is lost. The replacement of entries may only affect the forwarding performance to those nodes that have been replaced. In this case the router must relearn them.
- Action:** You may want to increase the Forwarding Table Size parameter in the bridge configuration.

SR Sr_es_table out of space

- Meaning:** The table that stores adjacent node source routes for token ring interfaces is full. The router uses a Least-Recently-Used policy to replace entries in this table, so no connectivity is lost. The replacement of entries may only affect the forwarding performance to those nodes who have been replaced. In this case the router must relearn them.
- Action:** You may want to increase the Forwarding Table Size parameter in the bridge configuration.

SR max RDs exceeded in explorer frame

- Meaning:** The router has received a source route explorer frame (STE, ARE, or SRF) that is addressed to the router, and there are more than eight routing descriptors in the packet. The node that generated the packet is in violation of the source routing protocol.

SR Rif_table out of space

- Meaning:** The table that stores RIFs for hop count reduction and translational bridging is full. The router uses a Least-Recently-Used policy to replace entries in this table, so no connectivity is lost. The replacement of entries may only affect the forwarding performance to those nodes who have been replaced. In this case the router must relearn them.
- Action:** You may want to increase the Forwarding Table Size parameter in the bridge configuration.

drs: DECnet Event Messages

These event messages are generated by the system variable “drs”, the DECnet routing service.

Adj Down CG *ccg*, Bad Pkt, Adj=*aa.nnnn*

Meaning: An adjacent node (accessible through circuit group *ccg*), whose area and node address is *aa.nnnn*, is declared down because the node transmitted an erroneous packet.

Adj Down CG *ccg*, Chksum error, Adj=*aa.nnnn*

Meaning: An adjacent node (accessible through circuit group *ccg*), whose area and node address is *aa.nnnn*, is declared down because the node transmitted a routing topology packet which contained an invalid checksum.

Adj Down CG *ccg*, Dropped, Adj=*aa.nnnn*

Meaning: In adjacent node (accessible through circuit group *ccg*), whose area and node address is *aa.nnnn*, is declared down because the node transmitted a faulty (misaddressed) hello packet.

Adj Down CG *ccg*, Out of range, Adj=*aa.nnnn*

Meaning: An adjacent node (accessible through circuit group *ccg*), whose area and node address is *aa.nnnn*, is declared down because the node's area and/or node address exceeds the values set by the Max Area and/or Max Nodes parameters.

Action: Modify the configuration to increase the values of Max Area and/or Max Nodes.

Adj Down CG *ccg*, Router Table Full, Adj=*aa.nnnn*

Meaning: An adjacent node (accessible through circuit group *ccg*), whose area and node address is *aa.nnnn*, is declared down. The node information has been deleted from the current adjacent router table.

Adj Down CG *ccg*, Sync lost, Adj=*aa.nnnn*

Meaning: The circuit group manager has declared circuit group *ccg* (which accesses node *aa.nnnn*) to be disabled. Consequently, the DECnet router declares *aa.nnnn* down.

Adj Down CG *ccg*, Timeout, Adj=*aa.nnnn*

Meaning: An adjacent node (accessible through circuit group *ccg*), whose area and node address is *aa.nnnn*, is declared down because the DECnet router has failed to receive three consecutive hello packets from this node.

Adj Down CG *ccg*, Version Skew, Adj=*aa.nnnn*

Meaning: An adjacent system (accessible through circuit group *ccg*), whose Area and Node Address is *aa.nnnn*, has been declared DOWN because the system's DECnet routing software predates Version 2.0.0.

Adj Rej CG *ccg*, node=*aa.nnnn*, Endnode Table Full

Meaning: An adjacent node (accessible through circuit group *ccg*), whose area and node address is *aa.nnnn*, is declared down. The node information could not fit in the current adjacent endnode table.

Adj Rej CG *ccg*, node=*aa.nnnn*, Router Table Full

Meaning: An adjacent node (accessible through circuit group *ccg*), whose area and node address is *aa.nnnn*, is declared down. The node information could not fit in the current adjacent router table.

Adj Up CG *ccg*, Adj=*aa.nnnn*

Meaning: The adjacent node whose area and node address is *aa.nnnn* is declared up.

Area Reach Chg Area *aa*, Reachable

Meaning: The previously unreachable area, whose area address is *aa*, has become reachable.

Event Log Messages
drs: DECnet Event Messages

Area Reach Chg Area *aa*, Unreachable

Meaning: The previously reachable area, whose area address is *aa*, has become unreachable.

CG Down CG *ccg*, Sync lost, node=*aa.nnnn*

Meaning: The circuit group manager has declared circuit group *ccg* (which accesses node *aa.nnnn*) to be unavailable.

CG Up CG *ccg*, Adj=*aa.nnnn*

Meaning: The circuit group manager has declared circuit group *ccg* (which accesses node *aa.nnnn*) up.

Circuit Group misconfigured

Meaning: The configuration file contains an improperly configured circuit group.

Action: Check circuit and circuit group records in the configuration.

Circuit misconfigured

Meaning: The configuration contains an improperly configured circuit.

Action: Check circuit records in the configuration.

DECnet Circuit Group misconfigured

Meaning: The DECnet record in the configuration contains an improperly configured circuit group.

Action: Check DECnet circuit group parameters.

entity disabled

Meaning: DECnet has been disabled in response to NCL's Disable command.

entity enabled

Meaning: DECnet successfully initialized, or has been enabled with the NCL's Enable command.

Init Fail CG *ccg*, Block size small, Ver=*nn.nn.nn*

Meaning: An adjacent host (accessible over circuit group *ccg*) failed to complete initialization because of an insufficient configured block size.

No DECnet Record configured

Meaning: The configuration does not contain a DECnet record.

Action: Modify the configuration to include a DECnet configuration record.

Node Reach Chg Node *aa.nnnn*, Reachable

Meaning: The previously unreachable node, whose area and node address are *aa.nnnn*, has become reachable.

Node Reach Chg Node *aa.nnnn*, Unreachable

Meaning: The previously reachable node, whose area and node address are *aa.nnnn*, has become unreachable.

Pkt Fmt Err CG *ccg*, *ffffffff*, node=*aa.nnnn*

Meaning: The DECnet router received a partially correct packet from node *aa.nnnn* over circuit group *ccg*. *ffffffff* is the hexadecimal representation of the first six bytes of the packet.

remote SMDS address invalid for DRS Area *XX*, Node *YY*

Meaning: The SMDS address in the entry in the DECnet Routing Service (DRS) Remote Address Map for DECnet Area *XX*, system *YY*, is invalid. An SMDS address is 10 digits in length, and each digit must be in the range 0 to 9.

Action: Modify the configuration to correct the SMDS address in the appropriate DECnet Address Map entry.

Event Log Messages
drs: DECnet Event Messages

Routing Pkt CG *ccg*, Highest=*aa.nnnn*, Adj=*aa.nnnn*

Meaning: An adjacent router is configured with an area and/or node number greater than the values for which the router is configured. Adj= contains the source address of the packet. Highest= contains the faulty address data contained in the packet.

egp: Exterior Gateway Protocol Event Messages

These event messages are generated by the system variable “egp”, the Exterior Gateway Protocol.

Already enabled

Meaning: An already enabled EGP has received NCL’s Enable command.

Already disabled

Meaning: An already disabled EGP has received NCL’s Disable command.

Bad AS, local *ip-address* remote *ip-address*

Meaning: EGP has detected a faulty autonomous system address within the configuration.

Action: Verify the integrity of Local ASN and Remote ASN entries in the configuration. A valid entry pair consists of two unique nonzero addresses.

Bad IP address, *ip-address*

Meaning: EGP has detected a faulty IP address within the configuration.

Action: Verify the integrity of the Local Address and Remote Address configuration parameters. Ensure that these parameters do not include broadcast addresses. A valid entry pair consists of two unique, nonzero addresses.

Configuration complete

Meaning: EGP has successfully initialized.

Configuration failed

Meaning: EGP could not initialize because of errors in the configuration.

Event Log Messages

egp: Exterior Gateway Protocol Event Messages

Action: Modify the configuration.

Configuration inconsistency repaired

Meaning: EGP has noted a minor discrepancy in the configuration. It has initialized using default values.

Configuration record not found

Meaning: The configuration does not include an EGP record.

Action: Modify the configuration.

Enable failed

Meaning: EGP failed to enable in response to NCL's Enable command.

Entity disabled

Meaning: EGP has been disabled in response to NCL's Disable command.

Entity disabled, shutdown failed

Meaning: EGP has been disabled in response to NCL's Disable command. Currently existing neighbor connections were terminated abruptly, and not in accordance with EGP protocol.

Entity enabled

Meaning: EGP has been enabled in response to NCL's Enable command.

Entity enabled, startup failed

Meaning: EGP has been enabled in response to NCL's Enable command. EGP, however, has failed to establish connections with neighboring routers.

Entity is still closing connections

Meaning: A "busy" EGP has received NCL's Disable command.

Action: Wait, then re-issue the command.

Entity not initialized

Meaning: EGP has received an NCL command before it has completed initialization.

Error *nnnn* attaching to *ip-address*

Meaning: EGP has encountered an error attempting to attach the neighbor designated by *ip-address*. *nnnn* designates the error listed in table 17-1 on page 17-83.

Error *nnnn* detaching from *ip-address*

Meaning: EGP has encountered an error attempting to detach from the neighbor designated by *ip-address*. *nnnn* designates the error listed in table 17-1 on page 17-83.

Insufficient buffers for operation

Meaning: The router cannot provide sufficient buffers for EGP operations.

Action: Consider reducing the number of neighbors to reduce buffer requirements.

Insufficient memory for operation

Meaning: The router cannot provide sufficient memory for EGP operations.

Action: Consider reducing the number of neighbors to save memory space.

Internal error

Meaning: EGP has encountered an unspecified error attaching to or detaching from a neighbor.

Invalid action

Meaning: EGP received a command, that while otherwise valid, was inappropriate to its current state.

Event Log Messages

egp: Exterior Gateway Protocol Event Messages

Invalid number of neighbors

Meaning: While checking its neighbor table, EGP found too few or too many entries.

Action: Modify the configuration to ensure that the number of neighbors is greater than 1, but less than 20.

IP entity not available

Meaning: The IP entity is not available. EGP cannot function in the absence of IP.

Action: Check if IP routing has been disabled. Check the configuration to verify IP router configuration parameters.

Table 17-1. Error Codes

Code	Explanation
320	Interface not found
321	Requested resource unavailable
322	Router out of memory
323	Router out of buffers
324	Necessary parameter unspecified
325	Option or command not supported
326	Invalid output parameter
327	Connection not established
328	Connection already exists
329	Connection closing
32a	Invalid operation for state
32b	Connection timed out
32c	Unknown network requested
32d	Connection refused
32e	Connection reset locally
32f	Connection reset by peer
320	Interface not found
330	Bad packet checksum
331	Packet too big
332	Unsupported options encountered
333	Unsupported flag encountered
334	Received ill-formed reset
335	Received ill-formed segment
336	Received ill-formed acknowledgment
337	Received duplicate acknowledgment
338	Received duplicate segment
339	Received segment out of sequence
33a	Send window closed
33b	Send (retransmit) ring buffer overflow
33c	Receive window closed
33d	Receive (resequencing) queue overflow
33e	Unknown (network) message code
33f	Unknown (network) message type
340	Internal (fatal) error

Event Log Messages

egp: Exterior Gateway Protocol Event Messages

IP entity not ready

Meaning: The IP entity is not currently available.

Action: Wait for IP to initialize.

Neighbor *ip-address* acquired

Meaning: EGP has acquired a new neighbor.

Neighbor *ip-address* down

Meaning: The EGP neighbor reachability algorithm has declared *ip-address* in the down state. In this state, EGP allocates resources to the neighbor and responds to Request, Cease, and Hello commands.

Neighbor *ip-address* unacquired

Meaning: The EGP neighbor reachability algorithm has declared *ip-address* in the idle state. In this state, EGP allocates no resources to the neighbor, and responds only to a Request command or a node or operator-generated initialization.

Neighbor *ip-address* up, polling disabled

Meaning: The EGP neighbor reachability algorithm has declared *ip-address* in the up state. In this state, EGP allocates resources to the neighbor, and responds to all commands and requests. EGP is in the passive state; it does not issue poll commands.

Neighbor *ip-address* up, polling enabled

Meaning: The EGP neighbor reachability algorithm has declared *ip-address* in the up state. In this state, EGP allocates resources to the neighbor, and responds to all commands and requests. EGP is in the active state; it issues poll commands.

Source address equal to destination

- Meaning:** The configuration contains identical values for the Local Address and Remote Address parameters.
- Action:** Modify the configuration to ensure the accuracy of local and remote addresses.

ip: IP Event Messages

These event messages are generated by the system variable “ip”, the DoD Internet Router.

arp: *ip-address1* / *ip-address2*

Meaning: IP has added a new entry, learned through the Address Resolution Protocol (ARP), to its address translation table. *ip-address1* is the host address; *ip-address2* is the network interface address.

bad cg *ccg* on *ip-address*

Meaning: IP has detected a discrepancy in the circuit group record *ccg*.

Action: Modify the configuration.

bad ip address *ip-address*

Meaning: The IP address *ip-address* (probably a broadcast address) is invalid.

Action: Modify the configuration to repair *ip-address*.

bad mask *mask* / *ip-address*

Meaning: IP has detected a discrepancy between an IP address, *ip-address*, and its associated subnet mask, *mask*.

Action: Modify the configuration to repair *ip-address* and/or *mask*.

bad mtu (*nn*) on circuit *cct*

Meaning: Circuit *cct* # will not support the minimum IP Maximum Transmission Unit (MTU).

Bad rx bcast *bcast* on *ip address*

- Meaning:** The configuration contains an invalid receive broadcast address on the interface designated by *ip address*.
- Action:** No action is required as IP will use a default broadcast address. Note that the Configuration Editor guards against this error. This message should be seen only if a user has attempted to modify the configuration without using the Configuration Editor.

Bad tx bcast *bcast* on *ip address*

- Meaning:** The configuration contains an invalid transmit broadcast address on the interface designated by *ip address*.
- Action:** No action is required as IP will use a default broadcast address. Note that the Configuration Editor guards against this error. This message should be seen only if a user has attempted to modify the configuration without using the Configuration Editor.

duplicate ip address

- Meaning:** Multiple network interfaces have been configured with the same IP address.
- Action:** Modify the configuration to ensure the uniqueness of interface addresses.

entity already disabled

- Meaning:** An already disabled IP has received NCL's Disable command.

entity already enabled

- Meaning:** An already enabled IP has received NCL's Enable command.

entity disabled

- Meaning:** IP has been disabled in response to NCL's Disable command.

Event Log Messages
ip: IP Event Messages

entity enabled

Meaning: IP has been enabled in response to NCL's Enable command.

entity reset

Meaning: IP has reinitialized.

filters configured

Meaning: IP has configured source address, destination address, and/or TCP/UDP port filters.

global broadcasts will not be received

Meaning: The Global Broadcast parameter has been set to No.

Action: If you want to receive global broadcasts, modify the configuration to set the value of Global Broadcast to Yes. If you do not want to receive global broadcasts, no action is required.

icmp: *ip-address* unreachable (host)

Meaning: IP has received an Internet Control Message Protocol (ICMP) Destination Unreachable message from *ip-address*. The message contains a Code field value of 1, indicating that the IP host designated by *ip-address* is unreachable.

icmp: *ip-address* unreachable (net)

Meaning: IP has received an Internet Control Message Protocol (ICMP) Destination Unreachable message from *ip-address*. The message contains a Code field value of 0, indicating that the network designated by *ip-address* is unreachable.

icmp: quench from *ip-address*

Meaning: IP has received an Internet Control Message Protocol (ICMP) source quench message from *ip-address*.

icmp: redirect from *ip-address*

Meaning: IP has received an Internet Control Message Protocol (ICMP) redirect message from *ip-address*.

icmp: Unsolicited Echo Reply from *X.X.X.X*

Meaning: Indicates a reply from IP address *X.X.X.X* to a Ping that was not sent by the local router. A packet may have been duplicated on the network.

Action: If this message occurs frequently, investigate the source of the replies for operating problems.

insufficient memory

Meaning: The router cannot provide sufficient memory for IP operations.

invalid operation for state

Meaning: IP received an otherwise valid command that was inappropriate to its current state.

network disabled on *ip-address*

Meaning: IP has disabled the network interface *ip-address*.

ip: Source Routing not enabled (Token Ring only)

Meaning: The Source Route parameter is set to Yes, but the IP network interface does not use a token ring. End-node source routing is thus not enabled for this IP interface.

Action: Modify the configuration so that Source Route is No for a non-token-ring line.

network enabled on *ip-address*

Meaning: IP has initialized the network interface *ip-address*.

Event Log Messages
ip: IP Event Messages

no network interfaces configured

- Meaning:** The configuration contains no network interface records.
- Action:** Modify the configuration to include network definitions for all network interfaces.

resolved: *ip-address1* / *ip-address2*

- Meaning:** IP has added a new entry, learned through the Address Resolution Protocol (ARP), to its address translation table. *ip-address1* is the host address; *ip-address2* is the network interface address.

SR max RDs exceeded in explorer packet

- Meaning:** The maximum number of Route Descriptors (RDs) was exceeded in an All Routes Explorer (ARE) packet or a Spanning Tree Explorer (STE) packet. The maximum number of Route Descriptors for a source routed packet is eight. The packet cannot be accepted and is dropped.

SR max RDs exceeded in SRF packet

- Meaning:** The maximum number of Route Descriptors (RDs) was exceeded in a specifically routed frame (SRF). The maximum number of Route Descriptors for a source routed packet is eight. The packet cannot be accepted or dropped.

SR Rif_table out of space

- Meaning:** The routing information field (RIF) table is out of space. The Rif_table contains routing information fields that are used to route source routed packets between the HP bridge/router and remote hosts over token ring networks.

SR sr_es_find: Maddr_table out of space

Meaning: The MAC address table (Maddr_table) is out of space. The station address table contains station addresses that are used for both end station (ES) source routing over IP as well as intermediate station (IS) source routing over the bridge.

SR Sr_es_table out of space

Meaning: The source routing end station table is out of space. The Sr_es_table is a table that contains destination station addresses. It contains pointers to the RIF table.

too many networks configured for this circuit group

Meaning: A single network interface has been configured with more than 16 networks.

Action: Modify the configuration for not more than 16 networks in a single circuit group.

ipx: IPX Router Event Messages

These event messages are generated by the the system variable "ipx", the IPX router.

CG *ccg*: Del Rt to *dest net* via *next hop net*: *next hop*

Meaning: *ccg* is the name of the circuit group the route was learned on.
 dest net is the destination network the route referred to.
 next hop net is the directly connected network that was to be used to
 get to the next hop router.
 next hop is the IPX address of the router that was the next hop for
 traffic destined for *dest net*.

CG *ccg*: Del Srv *server* at *ipx-address*

Meaning: The Service Advertising Protocol learned a node has been deleted. The node is specified by *server*, which is a character string truncated after eleven digits, and by the full IPX address, *ipx-address*, which is shown in hexademimal notation (the first eight digits are the network address and the last twelve digits are the host address).

CG *ccg*: NetBIOS Bcast Rt *ee* ignored – bad name

Meaning: A NetBIOS broadcast static route configured on the IPX interface has an invalid NetBIOS Resource Name configured. It may be too long or may contain nonhexadecimal characters following "\", for example. The route is being ignored. The circuit group associated with this network interface is *ccg*, and *ee* is the number of the invalid NetBIOS static route entry configured.

CG *ccg*: NetBIOS Bcast Rt *ee* ignored – bad net

Meaning: A NetBIOS broadcast static route configured on the IPX interface has a destination network (Dest Network parameter) of 00000000 or FFFFFFFF. The route is being ignored. The circuit group associated with this network interface is *ccg*, and *ee* is the number of the invalid NetBIOS static route entry configured.

CG *ccg*: New Rt to *ipxnet* via *ipx-address*

Meaning: The IPX routing module generates a new event message whenever it learns a new route or updates an existing route. The new route is specified by *ipxnet*, which is the destination network to which the new or updated route refers, and by *ipx-address*, which is the full IPX address of the next hop router. The *ipx-address* is shown in hexademimal notation (the first eight digits are the network address and the last twelve digits are the host address).

CG *ccg*: New Srv *server* at *ipx-address*

Meaning: The Service Advertising Protocol learned a new node, *server*, which is a character string that is truncated after eleven digits, and by the full the destination network to which the new or updated route refers, and by *ipx-address*, which is the full IPX address, *ipx-address*, which is shown in hexademimal notation (the first eight digits are the network address and the last twelve digits are the host address).

CG *ccg*: SAP Net Fltr *ee* ignored – bad net num

Meaning: A SAP network-level filter configured on the IPX interface has a Network Number of 00000000. The filter is being ignored. The circuit group associated with this network interface is *ccg*, and *ee* is the number of the invalid SAP network-level filter configured.

CG *ccg*: SAP Srv Fltr *ee* ignored – bad srv type

Meaning: A SAP server-level filter configured on the IPX interface has a Server Type of FFFF. The filter is being ignored. The circuit group associated with this network interface is *ccg*, and *ee* is the number of the invalid SAP server-level filter configured.

ipx: *ccg*: ipxwan info response timed out

Meaning: IPXWAN did not receive an information response packet within 20 seconds and ipxwan then timed out.

Event Log Messages

ipx: IPX Router Event Messages

ipx: ipxwan - Internal Network Number not unique

Meaning: IPXWAN detected the same Internal Network Number configured on both sides of the link.

Action: Modify the configuration. Change the IPX Internal Network Number to be unique.

ipx: ccg: ipxwan is up

Meaning: IPXWAN exchange was successful and IPXWAN is up on this interface.

ipx: ipxwan - out of pkt buffers

Meaning: Out of packet buffers.

ipx: ipxwan - Routing Type Not Accepted

Meaning: Routing protocol RIP/NLSP not accepted by the router.

ipx: ccg: ipxwan slave timed out

Meaning: IPXWAN exchange did not conclude in 60 seconds and ipx then timed out.

ipx: ipxwan - Timer Response received by slave

Meaning: Router has been selected to be a slave and received an incorrect timer response packet.

ipx: ccg: ipxwan trying to connect - not configured

Meaning: Remote router requesting IPXWAN connection. IPXWAN not configured on the router.

Action: Configure IPXWAN on the router.

ipx: *ccg* : New Rt to *ipxnet* via *ipx-address*

Meaning: The IPX routing module generates a new event message whenever it learns a new route or updates an existing route. The new route is specified by *ipxnet*, which is the destination network to which the new or updated route refers, and by *ipx-address*, which is the full IPX address of the next hop router. The *ipx-address* is shown in hexadecimal notation (the first eight digits are the network address and the last twelve digits are the host address).

Note HP Router 650 Only: If the value of *ipxnet* is zero and the second part of *ipx-address* is the station address of the router, then the first part of *ipx-address* is a directly-connected network on the router.

ipx: *ccg* : New Srv *server* at *ipx-address*

Meaning: The Service Advertising Protocol learned a new node, *server*, which is a character string that is truncated after eleven digits, and by the full the destination network to which the new or updated route refers, and by *ipx-address*, which is the full IPX address, *ipx-address*, which is shown in hexadecimal notation (the first eight digits are the network address and the last twelve digits are the host address).

ipx: *ccg* request timed out

Meaning: IPXWAN request sent out but no response received on that interface within the timeout interval.

Action: Check if IPXWAN has been configured on the remote link.

ipxwan - Internal Network Number record not configured

Meaning: IPXWAN detected an unconfigured record in the IPX configuration.

Action: Configure an internal network number and router name in the IPX configuration.

lb: Bridge Event Messages

The event messages are generated by the system variable "lb", the learning bridge.

Circuit Group *ccg* Blocking

Meaning: The spanning tree algorithm has placed circuit group *ccg* in the blocking state. A circuit group in this state does not participate in frame relay. The spanning tree algorithm, however, does include blocked ports in its calculation of the active topology.

Circuit Group *ccg* Disabled

Meaning: The spanning tree algorithm has placed circuit group *ccg* in the disabled state. A circuit group in this state does not participate in frame relay. The spanning tree algorithm does not include disabled ports in its calculation of the active topology.

Circuit Group *ccg* Forwarding

Meaning: The spanning tree algorithm has placed circuit group *ccg* in the forwarding state. A circuit group in this state is participating in frame relay.

Circuit Group *ccg* Learning

Meaning: The spanning tree algorithm has placed circuit group *ccg* in the learning state. A circuit group in this state is participating in frame relay, and has enabled the learning function.

Circuit Group *ccg* Listening

Meaning: The spanning tree algorithm has placed circuit group *ccg* in the listening state. A circuit group in this state is preparing to participate in frame relay.

entity disabled

Meaning: The bridge has been disabled in response to NCL's Disable command.

entity enabled

Meaning: The bridge successfully initialized, or has been enabled with NCL's Enable command.

fwd dlay should be >= XXX

Meaning: The Forward Delay configuration parameter was misconfigured.

Action: For the Forward Delay parameter, configure the value *XXX* or greater, correctly corresponding to the value configured for Max Age.

max age should be >= XXX

Meaning: The Max Age configuration parameter was misconfigured.

Action: For the Max Age parameter, configure the value *XXX* or greater, correctly corresponding to the value configured for Hello Time.

No Bridge Circuit Group configured

Meaning: The bridge record in the configuration contains an improperly configured circuit group.

Action: Check bridge circuit groups.

No Bridge Record configured

Meaning: The bridge protocol has not been configured.

Action: Configure the bridge.

No Bridge Software configured

Meaning: The bridge protocol has not been loaded.

Action: Modify the configuration to include a bridge record.

SR internal LAN ID not in RIF route

Meaning: A specifically routed frame (SRF) was received that did not include the Internal LAN ID of the bridge. The frame cannot be forwarded and must be dropped.

SR is_srf_rif_insert: no rif entry

Meaning: A specifically routed frame (SRF) was received, however, the appropriate entry in the source routing intermediate station table (Sr_is_table) does not contain a routing information field (RIF) for the destination station. The packet is dropped.

SR max hops exceeded in explorer frame

Meaning: The maximum number of hops was exceeded in an all routes explorer (ARE) frame or a spanning tree explorer (STE) frame. The maximum number of hops for a source routed packet is seven. The packet cannot be forwarded and must be dropped.

SR max hops exceeded in Specifically Routed Frames

Meaning: The maximum number of hops was exceeded in a specifically routed frame (SRF). The maximum number of hops for a source routed packet is seven. The packet cannot be forwarded and must be dropped.

SR out cg = cg for SRF

Meaning: The specifically routed frame (SRF) is being forwarded out the same interface on which it was received. This can occur if the Loop Detection Time is set too low, or if the network is reconfiguring (due to a link failure), or if the router is rebooted.

SR out of buffers

Meaning: An attempt was made to allocate a packet buffer to flood an All Routes Explorer (ARE) packet out of a particular interface. However, no packet buffer was available. The ARE cannot be flooded out of the interface.

SR possible ARE loop

Meaning: A possible All Routes Explorer (ARE) loop has been detected. This can occur if the Loop Detection Time is set too low, if the network is reconfiguring (due to a link failure), or if the router is rebooted.

Action: Check the Loop Detection Time parameter in the configuration. The Loop Detection Time may be set too low to detect an ARE loop and may need to be increased.

SR Rif_table out of space

Meaning: The routing information field (RIF) table (Rif_table) is out of space. The RIF table contains RIFs that are used to route source routed packets between routers and remote hosts over token ring networks. The RIF table contains RIFs used for both end station (ES) source routing over IP and intermediate station (IS) source routing over the bridge.

SR sr_is_find: Madr_table out of space

Meaning: The station address table (Madr_table) is out of space. The Madr_table is a table that contains station addresses that are used for both end station (ES) source routing for IP as well as intermediate station (IS) source routing for the bridge.

SR sr_is_table: out cct's cg is 0, sending ARE

Meaning: The specifically routed frame (SRE) was received and the appropriate entry in the source route intermediate station table (Sr_is_table) for the source destination pair does not yet include the route to the destination station. The bridge will now send an All Routes Explorer (ARE) packet in order to discover the route to the destination station. (The route to the destination station is discovered when a response packet is received from the destination station.) This situation can occur if the network is re-configuring (due to a link failure), or if the router was rebooted.

SR sr_is_table out of space

Meaning: The source routing intermediate station table is out of space. The Sr_is_table is a table that contains source-destination pairs of station addresses. It contains pointers to the RIF table.

SR sr_ring full

Meaning: The sr_ring data structure used to contain outgoing source routed packets is full. No other source routed packets will be sent out until the ring has been emptied.

SR TF forward_ring full

Meaning: The forward_ring data structure is used to contain outgoing source routed packets that have been filtered through traffic filters. This data structure is now full. No other source routed packets that need to be filtered through traffic filters will be sent out until the ring has been emptied.

SRT out of buffers

Meaning: No packet buffer was available to allocate for the source-routing transparent (SRT) bridge to process an all-routes-explorer (ARE) frame or a spanning-tree-explorer (STE) frame.

line: Lines Event Messages

Connector *nn* not on this module

- Meaning:** The configuration record reflects a non-existent physical connector.
- Action:** Modify Connector in the line record in the configuration.

Invalid MFS, dflt=2

- Meaning:** The configuration record for circuit *cct #* contains a faulty value in the Minimum Frame Spacing field. The router has defaulted to a value of 2.
- Action:** Modify Minimum Frame Spacing in the configuration.

Invalid N2, dflt=16

- Meaning:** The configuration record for circuit *cct #* contains a faulty value in the Retry Counter (N2) field. The router has defaulted to a value of 16.
- Action:** Modify Retry Counter (N2) in the configuration.

No buffers available for deadlock processing

- Meaning:** Indicates a degenerative line condition resulting in the lack of receive buffers at both the line source and termination.

No V.35 circuits configured

- Meaning:** Circuits designated by the Circuit Name parameter in the line record have not been configured.
- Action:** Modify the configuration to ensure that it includes circuit records for all circuits.

Event Log Messages
line: Lines Event Messages

Sync circuit assigned to multiple lines

- Meaning:** One or more line records contains references to the same point-to-point circuit.
- Action:** Modify the configuration to ensure that all line and circuit records are consistent.

Too many lines assigned to V.35 connector

- Meaning:** The configuration contains an excessive number (greater than two) of line records for a single connector.
- Action:** Modify the configuration to ensure that no more than one line record references a specific physical connector.

Too many V35 circuits configured for slot

- Meaning:** The configuration contains an excessive number of V.35 line records.
- Action:** Modify the Lines configuration.

V35 circuit record missing

- Meaning:** The circuit has not been configured.
- Action:** Modify the configuration to ensure that it includes circuit records for the circuit.

V35 line record missing

- Meaning:** A line record has not been associated with the circuit *cct*.
- Action:** Modify the configuration to ensure that it includes properly associated line and circuit records.

mgr: Manager Event Messages

These event messages are generated by the system variable "mgr".

auto enabling *entity*

Meaning: The manager is auto-enabling the specified device or service. *entity* can be any of the following: a circuit of any type, the IP router, the bridge, the IPX router, EGP, SNMP, TCP, and Telnet.

Config file converted due to OS upgrade

Meaning: When a new operating system (OS) is downloaded to a router, the configuration file is converted to become consistent with the new OS.

Config file updated from network download

Meaning: The configuration file has been updated through the network with a copy of another router's configuration.

Config file updated to default configuration

Meaning: The configuration file has been updated to a default configuration.

Config file updated via configuration editor

Meaning: A change has been made to the configuration file by using the Configuration Editor.

enable *entity* failed

Meaning: The manager could not enable *entity* (which can be any item listed for the preceding message).

Action: Contact your HP support provider.

Event Log Messages
mgr: Manager Event Messages

cct.circuit name reserved as a backup circuit

Meaning: The specified circuit was not auto-enabled because it was reserved as a backup circuit.

No memory for session startup

Meaning: There is insufficient memory available for the indicated activity.

Action: Contact your HP Service provider.

No memory for temp session

Meaning: There is insufficient memory available for the indicated activity.

Out of message buffers

Meaning: There is insufficient memory available for the indicated activity.

Action: Contact your HP Service provider.

password(s) removed via Clear button

Meaning: The router's Clear button was detected. The passwords protecting console (or Telnet) access to the router have been removed.

ospf: OSPF Event Messages

These event messages are generated by the system variable “ospf”, the Open Shortest Path First internet routing protocol.

DD: Extern option mismatch

Meaning: The Hello external/stub option specified does not match the configured option.

DD: Nbr's rtr = my rtrid

Meaning: The OSPF entity has detected another OSPF router with the same router identification in a database description packet.

DD: Nbr state low

Meaning: OSPF has received a database description packet from a neighbor whose state is too low to honor. That is, the router will drop the Ls Req and Ls Update packets from the neighbor whose state is below Exchange in the following list:

Full
Loading
Exchange
Exch Start
2 Way
Init
Attempt
Down

DD: Unknown nbr

Meaning: A database description packet has been received from an unknown neighbor.

Hello: Extern option mismatch

Meaning: The Hello external/stub option specified does not match the configured option.

Event Log Messages
ospf: OSPF Event Messages

Hello: IF dead timer mismatch

Meaning: The dead timer value specified in an incoming Hello packet does not match the configured value.

Hello: IF hello timer mismatch

Meaning: The hello timer value specified in an incoming Hello packet does not match the configured value.

Hello: IF mask mismatch

Meaning: The mask value specified in an incoming Hello packet does not match the configured value.

Hello: Unknown Virt nbr

Meaning: An unknown virtual link neighbor has tried to establish an adjacency with the resident OSPF entity.

IP: Bad IP Dest

Meaning: The OSPF entity received an IP packet that was not destined for it.

IP: Bad IP proto id

Meaning: The protocol ID in this IP packet was incorrect or unknown.

IP: Bad OSPF pkt type

Meaning: An incoming OSPF packet contains an unknown or incorrect OSPF packet type.

IP: Pkt src = my IP addr

Meaning: The source address in the IP packet was found to be the same as the address configured for the OSPF entity.

LS Req: Bad pkt

Meaning: OSPF has received a bad link state request.

LS Req: Empty request

Meaning: OSPF has received an empty link state update request.

LS Req: Nbr state low

Meaning: The state of a neighbor sending a link state request is too low to honor. That is, the router will drop the Ls Req and Ls Update packets from the neighbor whose state is below Exchange in the following list:

Full
Loading
Exchange
Exch Start
2 Way
Init
Attempt
Down

LS Req: Unknown nbr

Meaning: An unknown neighbor has sent a link state request to the OSPF entity.

LS Update: Bad LS chksum

Meaning: The checksum calculated for the contents of this incoming link state update packet does not agree with the specified value.

LS Update: less recent rx

Meaning: The OSPF entity has received a link state advertisement that is less recent than the current internal copy.

Event Log Messages
ospf: OSPF Event Messages

LS Update: Nbr state low

Meaning: The OSPF entity has received a link state update from a neighbor in a state too low to be processed. That is, the router will drop the Ls Req and Ls Update packets from the neighbor whose state is below Exchange in the following list:

Full
Loading
Exchange
Exch Start
2 Way
Init
Attempt
Down

LS Update: Newer self-gen LSA

Meaning: The OSPF entity has received a self-generated link state advertisement that appears to be newer than the internal copy.

LS Update: Unknown nbr

Meaning: A link state update has been received from an unknown neighbor.

LS Update: Unknown type

Meaning: The OSPF entity has received an unknown link state update type.

OSPF: Area mismatch

Meaning: The OSPF entity discerns that one of its interfaces has been mismatched with a configured area.

OSPF: Auth key != area key

Meaning: There is a mismatch between the authentication key specified in the packet and the configured value.

OSPF: Bad intf area id

Meaning: The interface area identification specified in this packet does not match the one configured for this OSPF interface. Or, the packet was received on an interface belonging to another area.

OSPF: Bad OSPF checksum

Meaning: The checksum calculated for this packet does not agree with the value specified in the packet.

OSPF: Bad OSPF version

Meaning: The version of OSPF as specified in this packet is incompatible with the version supported by the OSPF entity. Versions 1 and 2 are compatible; this software complies with Version 2.

OSPF: Bad virt link info

Meaning: The OSPF entity has interpreted information from a non-backbone source as incorrectly appearing on the backbone.

OSPF: BDR = *ip-address*

Meaning: OSPF is performing the designated router algorithm with respect to interface *ip-address*. DR and BDR indicate the results of the algorithm.

OSPF: Choosing DR INTF *ip-address*

Meaning: OSPF is performing the designated router algorithm and is in the process of choosing a designated router on the interface at *ip-address*.

OSPF: DR = *ip-address*

Meaning: OSPF has selected the router at *ip-address* to be the designated router.

OSPF: Entity enabled

Meaning: The OSPF entity has initialized correctly and has reached the enabled state.

Event Log Messages
ospf: OSPF Event Messages

OSPF: Packet is too small

Meaning: OSPF has received a packet that is too small.

OSPF: Packet size > IP length

Meaning: OSPF has received a packet exceeding the allowable IP datagram length.

OSPF: Received on down IF

Meaning: OSPF has received a packet on an interface that was considered to be down.

OSPF: TQ_IFCHECK: Interface if_name (*ip-address*) is down

Meaning: When the OSPF entity was enabling, it found the specified interface in the down state. OSPF periodically checks the status of its interfaces and therefore is capable of recognizing state changes.

OSPF: Transmit bad

Meaning: OSPF was unable to transmit a packet.

OSPF: TRANS [IF/NBR] ID = *ip-address* Event: *X* States: *Y*-> *Z*

Meaning: The transit interface or neighbor (*ip-address*) has received an event (*X*) that caused it to pass through a state change from state *Y* to state *Z*. The following events can cause state machine changes for interfaces or neighbors:

Events Received by Neighbors:	Events Received by Interfaces:
Hello Received	Interface UP
Start	Wait Timer
Two Way Received	Backup Seen
Adjacency OK	Neighbor Change
Negotiation Done	Loop Indication
Bad LS Request	Unloop indication
Exchange Done	Interface Down
Seq # Mismatch	
Loading Done	
One Way	
Reset Adjacency	
Kill Neighbor	
Inactivity Timer	
Lower Level Down	

The associated states that affected neighbors or interfaces can pass through are:

States Associated with Neighbors:	States Associated with Interfaces:
Down	Down
Attempt	Loopback
Init	Waiting
2 Way	P to P
Exch Start	DR
Exchange	Backup DR
Loading	DR Other
Full	
SC Virtual	

pm: Port Module Manager Event Messages

These event messages are generated by the system variable “pm”, which is the port module manager for the HP Router 650.

Can't allocate re-boot message, restart impossible

Meaning: The router software was unable to allocate a message needed to initiate the reboot process of a port module. The port module will not be restarted automatically.

Action: Restart the port module by enabling it from the NCL prompt.

Card in slot *slot #* removed

Meaning: The router software has detected the removal of a port module in the specified slot.

Disabling Port Module

Meaning: The NCL Disable command was successful and the process of disabling the port module has begun.

Disabling Port Module slot *slot #*

Meaning: The port module in the specified slot is being disabled.

Download failure on slot *slot #*

Meaning: The port module in the specific slot was not able to be downloaded because of a lack of memory or a CRC error in the download file in Flash memory.

Action: Manually restart the port module by enabling it from NCL. For example, if a download failure is indicated for slot 4, you can attempt to manually enable it by executing this NCL command:

```
enable dev[4]
```

If the condition persists, contact you HP support provider.

Downloading Port Module type *type #* in slot *slot #*

Meaning: The software for the port module in slot # is being downloaded. The port module *type #* is a numeric identifier (1, 2, etc.).

Enabling Port Module

Meaning: The NCL Enable command was successful and the process of enabling the port module has begun.

Enabling Port Module slot *slot #*

Meaning: The port module in the specified slot is being enabled.

Failure to disable slot *slot #*

Meaning: Software was unable to disable the port module in the specified slot. The port module may already be disabled.

Action: If the hot swap LED is illuminated, extract the port module.

Port Module hot swap in slot *slot #* initiated

Meaning: An operator has pressed the hot swap button on the specified port module and started the hot swap process. The port module will shut down all functions and illuminate the hot swap LED when it is safe to extract the port module.

Port Module slot *slot #* Initialized

Meaning: The software download and initialization of the port module in the specified slot is successful and complete.

Port Module slot *slot #* boot fail

Meaning: The port module in the specified *slot #* did not boot after being successfully downloaded. If the router has Auto Enable set, the port module will automatically be restarted.

Port Module inserted in slot *slot #*

Meaning: The router software has detected the insertion of a port module in the specified slot.

Port Module in slot *slot #* ready for hot swap

Meaning: The port module in the specified slot has been successfully shut down and is ready to be removed.

Action: To restart a module in *slot #*, extract the shut down port module and insert a new port module, or re-enable the existing port module using the NCL Enable command.

Port Module slot *slot #* critical failure detected

Meaning: The router software has detected a critical failure on the port module in the specified slot. A crash record will be uploaded, possibly indicating the reason for the failure. If the system has Auto Enable set, the port module will automatically be restarted.

Port Module slot *slot #* presence mismatch

Meaning: The router software has detected an improperly seated port module. The port module is not completely inserted into the backplane which may lead to unexpected router behavior.

Action: Verify that the port module is properly inserted, and reboot if the module must be re-inserted.

Port module slot *slot #* removed and not re-installed

Meaning: The router software has detected an inconsistency in the presence of a port module in the indicated slot after a reset.

Action: Cycle the power to the router.

Port Module slot *slot #* state *state* incorrect for enable

Meaning: The port module in the specified slot is not in the correct state to be enabled. It may already be enabled.

Action: Attempt to disable the port module or perform a hot swap.

Port Module slot *slot #* state mismatch

Meaning: The router software has detected an inconsistency with state of the port module after power-on selftest.

Action: Reboot the router.

Port Module slot *slot #* unexpected swap

Meaning: The port module in the specified slot has been removed without adhering to the hot swap procedure. Unexpected router behavior may occur.

Action:

Reboot limit exceeded on slot *slot #*

Meaning: The port module has exceeded the maximum number of reboot attempts within a short period of time and will not be restarted. The router software has detected a continuous reboot loop.

Action: Manually restart the port module by enabling it from NCL. For example, if a reboot limit is indicated for slot 4, you can try to manually enable it by executing this NCL command:

```
enable dev[4]
```

If the reboot limit condition persists, contact your HP support provider.

Rebooting Slot *slot #*

Meaning: The port module in the specified slot is being rebooted.

Event Log Messages

pm: Port Module Manager Event Messages

Selftest failed on slot *slot #*

- Meaning:** The port module in the specified slot of an HP Router 650 has failed selftest.
- Action:** Determine the source of the failure by using the procedure described under “Card/Slot Failure During Self-Test” in the “Troubleshooting” chapter of the router installation manual. If the test indicates failure of either the slot or the port module, contact your HP service provider.

Selftesting Port Module slot *slot #*

- Meaning:** The port module in the specified slot is being self-tested.

Selftest passed on slot *slot #*

- Meaning:** The port module in the specified slot has completed selftest successfully.

slot *slot #* HW ID and line configuration mismatch

- Meaning:** The port module inserted in the specified slot does not match the expected value and will not be initialized.
- Action:** Change the configuration for the slot and reboot.

Uploading crash record from slot *slot #*

- Meaning:** After detecting a critical failure on the port module, the router software will upload a crash record and make an entry in the crash log. You can view the crash record using the NCL Crash command.

ppp: Point-to-Point Protocol

These event messages are generated by the PPP managed object.

bad configuration file

Meaning: PPP detected an inconsistency in the configuration.

Action: Modify the configuration.

XXX is up

Meaning: The PPP protocol *XXX* has been successfully negotiated with the peer PPP.

XXX is down

Meaning: The PPP protocol *XXX* has stopped communicating with the peer PPP.

LQM negotiaion rejected by remote station

Meaning: The peer PPP has rejected the LQM option.

Action: Configure the local PPP for no LQM (LQM time of zero).

Max Pkt Size adjusted down to XX

Meaning: The negotiated PPP maximum receive size (MRU) is larger than the router can manage.

Action: Reconfigure peer PPP for a smaller PPP MRU.

Event Log Messages

ppp: Point-to-Point Protocol

missed *NN* Echo Replies: link is down

Meaning: The local PPP has not received a response for *NN* echo replies. The link is going down. PPP will automatically retry opening the PPP link.

missed *NN* LQRs: link is down.

Meaning: The link quality of the WAN is not conducive to data transfers.

possible loop-back has been detected

Meaning: It is possible that the router has a loop-back cable attached or the telephone company has an error that causes a loop-back condition to exist.

Action: Remove the loop-back condition.

protocol *NNN* not supported

Meaning: The local PPP received a packet with an unknown protocol. The protocol *NNN* will be displayed in hex.

remote station has logged in to Server

Meaning: The peer PPP Password Authentication Protocol (PAP) has successfully logged into the local PPP PAP.

remote station's login attempt failed

Meaning: The peer PPP Password Authentication Protocol (PAP) was unsuccessful in logging into the local PPP PAP.

Action: Check the PPP PAP password configurations.

remote station rejected XXX

- Meaning:** The peer PPP reject PPP protocol XXX.
- Action:** There is a configuration mismatch between the local router's PPP and the peer PPP. For example, the local router may be configured for Appletalk on the PPP link while the peer PPP is not configured for Appletalk. In this example you would either delete the Appletalk on the local PPP link or add Appletalk to the peer PPP link's router.

Server has logged in to remote station

- Meaning:** The PPP Password Authentication Protocol (PAP) has successfully logged into the peer PPP PAP.

Server's login attempt failed

- Meaning:** The PPP Password Authentication Protocol (PAP) was unsuccessful in logging into the peer PPP PAP.
- Action:** Check the PPP PAP password configurations.

too many bytes lost: link unreliable

- Meaning:** The PPP link is unreliable because too many bytes have been lost. This is measured only when running LQM.

too many packets lost: link unreliable

- Meaning:** The PPP link is unreliable because too many packets have been lost. This is measured only when running LQM.

Event Log Messages

rok: Router Operating Kernel Event Messages

rok: Router Operating Kernel Event Messages

These event messages are generated by the system variable "rok", the router operating kernel.

Boot count = *nnn*

Meaning: The router has been booted *nnn* times.

connection dropped due to inactivity

Meaning: No console input has been received for the time set for the Connection Inactivity Time configuration parameter. The modem has been hung up or the terminal has been logged out.

connection established

Meaning: Console connection is made, using a terminal or modem.

connection establishment timed out

Meaning: Call received, but not all modem lines came up in the time allotted by the Modem Connection Time configuration parameter. All lines have been dropped.

incoming call

Meaning: Initiating connection establishment.

lost CD/RR signal

Meaning: Carrier Detect or Receiver Ready: A modem line has been lost for longer than the time set for the Modem Lost Receive Ready Time configuration parameter. Therefore all modem lines are dropped (modem disconnected).

lost DSR/DM signal

Meaning: Data Set Ready or Data Mode line dropped and modem disconnected.

momentary drop in CD/RR line

Meaning: Carrier Detect/Receiver Ready line lost, for less than the time set for the Modem Lost Receive Ready configuration parameter.

Action: Check the phone lines.

SMDS Event Messages

This section contains an alphabetical list of event messages generated by the SMDS managed object. Each message is followed by an explanation of the message contents and a recommended action (if any is required).

bad configuration file

Meaning: SMDS detected an inconsistency in the configuration.

Action: Modify the configuration.

illegal packet received

Meaning: A packet was received that did not conform to standard SMDS format. The packet was dropped. No further action is necessary. cct identifies the SMDS circuit.

invalid SMDS ARP group address for cct

Meaning: The SMDS Address Resolution Protocol (ARP) group address in the SMDS circuit record for cct # is invalid. An SMDS address is ten digits in length, and each digit must be in the range of 0 to 9.

Action: Modify the configuration.

invalid SMDS group address for cct

Meaning: A group address in the SMDS circuit record for cct # is invalid. An SMDS address is ten digits in length, and each digit must be in the range of 0 to 9.

Action: Modify the configuration.

invalid SMDS individual address for cct #

Meaning: The individual address in the SMDS circuit record for cct # is invalid. An SMDS address is ten digits in length, and each digit must be in the range of 0 to 9.

Action: Modify the configuration.

Madr_table is full

Meaning: The station Address Table (Madr_table) is out of space. The station address table is a hash table that contains station addresses used by the router.

no SMDS Address for DRS area XX, node YY

Meaning: An attempt was made to transmit a DECnet Routing Service (DRS) packet to DECnet area XX, system YY, but no DECnet Address Map record exists that specifies which remote SMDS address should be used for the packet.

Action: Modify the configuration to add the appropriate DECnet Address Map entry.

Smads_bridge_table is full

Meaning: The SMDS Bridge Table (Smads_bridge_table) is out of space. The SMDS Bridge Table contains the mapping between remote station addresses and remote SMDS addresses.

tcp: Transmission Control Protocol Event Messages

These messages are generated by the system variable "tcp".

bad configuration, using defaults

Meaning: TCP has rejected user-supplied protocol parameters; TCP will initialize using default parameters.

Action: Modify the configuration to accept default parameters.

configuration complete

Meaning: TCP has completed configuration using valid user-supplied parameters.

no configuration, using defaults

Meaning: TCP has completed configuration using default parameters in the absence of user-supplied parameters.

telnet: Telnet Event Messages

These messages are generated by the system variable "telnet".

port 23 connected to *ip-address*

Meaning: A Telnet virtual terminal connection between the router and *ip-address* has been established through the well-known Telnet port.

port 23 disconnected from *ip-address*

Meaning: A Telnet virtual terminal connection between the router and *ip-address* has been disconnected.

tftp: TFTP and Fget Event Messages

These event messages are generated by the system variable "tftp", the Trivial File Transfer Protocol.

An FGET is already in progress, request denied

Meaning: Only one Fget command can be satisfied at a time.

Action: Try the command again. Ensure that no other session is using TFTP.

Can't allocate a connection, request denied

Meaning: Not enough global memory to allocate a connection block.

can't find destination net *ip-address*, request denied

Meaning: The destination IP address cannot be reached.

Action: Check that the remote system is still up, and that the routing protocol is operating correctly.

CONFIG transfer aborted, no ID string found

Meaning: The configuration file being received did not have the configuration file identification string in it.

Action: Ensure that the file is a valid configuration file for your router.

could not allocate pkt buf for FGET OS request

Meaning: Buffer memory ran out, so the Fget command could not be executed.

could not disable entity for FGET OS

Meaning: In order to receive the operating system image, we disable all the entities other than IP and the circuit over which the file will be transferred. This frees up enough memory to store the image in memory before burning into non-volatile memory. In this case, one of the configured entities named entity could not be disabled.

could not disable entities for OS GET

Meaning: In order to receive the operating system image, we disable all the entities other than IP and the circuit over which the file will be transferred. This frees up enough memory to store the image in memory before burning into non-volatile memory. In this case, some of the configured entities could not be disabled.

could not find an IP_NW config record for FGET OS request

Meaning: Could not find any IP network interface definition in the configuration.

Action: Check that IP is configured correctly.

could not find cct group config for FGET OS request

Meaning: Could not find the circuit group configuration record for the circuit group specified in the IP network interface definition.

Action: Check that IP is configured correctly.

could not find IP configuration for FGET OS request

Meaning: Could not find a configuration record for IP.

Action: Check that IP is configured correctly.

don't know how to reach dest for FGET OS request

Meaning: The IP address specified in the Fget command is not reachable.

Action: Check that the IP routing protocol is operating correctly and that you used the correct IP address of the TFTP server in the Fget command.

Event Log Messages
tftp: TFTP and Fget Event Messages

entity already disabled

Meaning: An already disabled TFTP entity has received NCL's Disable command.

entity already enabled

Meaning: An already enabled TFTP entity has received NCL's Enable command.

entity disabled

Meaning: The TFTP entity was disabled in response to NCL's Disable command.

entity enabled

Meaning: The TFTP entity was enabled in response to NCL's Enable command.

entity not enabled, request denied

Meaning: The Fget or Fput request requires that TFTP be configured and enabled.

Action: Check that TFTP is configured and enabled.

ERR = *error-pdu-string*

Meaning: This is the message string referred to by the event message "RCVD ERR from *ip-address*, error: #msg follows" or the event message "SENT ERR to *ip-address*, error: #msg follows".

FGET OS aborted

Meaning: The Fget request has been aborted for the reason indicated by the message listed immediately prior to this message in the event log.

FGET OS aborted, destination address unknown

Meaning: The specified destination IP address cannot be reached.

Action: Ensure that the referenced system is available.

FGET Waiting for route to destination *IP_address*

Meaning: The destination IP address was unavailable. The system is retrying the request.

GET *remote-filename* from *ip-address*, file *local-filename*
GET CONFIG from *ip-address*, file CONFIG

Meaning: Echoes the Fget command request.

Insufficient resources for Enable

Meaning: Couldn't allocate a message buffer to register TFTP's port with UDP.

ip_ctrl_id not valid for FGET OS request

Meaning: The IP entity is not in a state to accept requests from upper layers, so the Fget command could not be executed.

Action: Check that IP is configured correctly and is enabled.

IP not in valid state to accept FGET OS request

Meaning: The IP entity may not be enabled. We cannot invoke TFTP without IP being in the running state.

Action: Ensure that IP is enabled.

Not enough free memory for OS after reclamation!

Meaning: The operating system image is too large for the current configuration.

Action: Reconfigure the entire router for IP only, and reconfigure only the TFTP port.

Not enough memory for OS - - will retry

Meaning: The operating system image is too large for the current configuration. TFTP is rebooting to reclaim memory and try again.

Event Log Messages
tftp: TFTP and Fget Event Messages

No pkt buffers for TFTP data send, transfer aborted

Meaning: Ran out of packet buffers during TFTP transfer.

No such action

Meaning: Internal entity action error.

Action: Call your local product support provider.

OS file checksum failed, GET failed

Meaning: The operating system image has a CRC in it that is checked after the Fget transfer has completed. The calculated CRC did not match that transferred with the file. One of the TFTP packets may have been corrupted during the transfer.

Action: Retry the "Fget os" command.

OS transfer aborted, no memory to hold file

Meaning: There is not enough global memory available to hold the operating system.

Out of resources for UDP port registration

Meaning: Couldn't allocate a message buffer to register TFTP's port with UDP.

PUT *local-filename* to *ip-address*, file *remote-filename*

Meaning: Echoes the Fput command request.

RCVD ERR from *ip-address*, error: #msg follows

Meaning: We received a TFTP error PDU during the file transfer with the system whose IP address is *ip-address*. The error number # is TFTP-specific, and its meaning can be found in RFC 783. The message string that was sent back in the error PDU follows this message in the event log.

REBOOTING THE SYSTEM FOR FGET OS MEMORY

Meaning: The operating system needs more memory than the current configuration can supply. TFTP is rebooting to reclaim memory and try again.

receipt of *filename* file complete

Meaning: The file *filename* specified in the Fget command has been successfully received.

received pkt on deleted connection

Meaning: A stray, duplicate, or retransmitted packet has been received after the full transmission related to that packet has been received and TFTP completed. This may be a retransmitted packet that got delayed in the network. Indicates the possibility of network congestion.

RRQ from *ip-address* for file *filename*

Meaning: A TFTP Read request from a system with IP address *ip-address* for file *filename* was received.

SENT ERR to *ip-address*, error: #msg follows

Meaning: We sent a TFTP error PDU during the file transfer with the system whose IP address is *ip-address*. The error number # is TFTP-specific, and its meaning can be found in RFC 783. The message string that was sent back in the error PDU follows this message in the event log.

TFTP Entity not enabled, request denied

Meaning: The Fget or Fput request requires that TFTP be configured and enabled.

Action: Check that TFTP is configured and enabled.

TFTP_ip_ctrl_id not valid for FGET OS request

Meaning: The IP entity is not in a state to accept requests from upper layers, so the Fget command could not be executed.

Event Log Messages

tftp: TFTP and Fget Event Messages

Action: Check that IP is configured correctly and is enabled.

TFTP REBOOTING THE SYSTEM FOR FGET OS MEMORY...

Meaning: The operating system needs more memory than the current configuration can supply. TFTP is rebooting to reclaim memory and try again.

TFTP: Received pkt on deleted connection

Meaning: A stray, duplicate, or retransmitted packet has been received after the full transmission related to that packet has been received and TFTP completed. Indicates the possibility of network congestion.

transfer of *filename* aborted

Meaning: The TFTP entity was disabled during a transfer. The transfer was aborted.

transfer of file *filename* aborted after #retransmissions

Meaning: The receiver of the file stopped sending acknowledgements before the transfer was complete. The connection was timed out.

Action: Check that the remote system is still up.

transfer of file *filename* aborted for inactivity

Meaning: The sender of the file stopped sending data before the transfer was complete. The connection was timed out.

Action: Check that the remote system is still up.

transfer of file *filename* complete
transfer of file CONFIG complete

Meaning: The file *filename* specified in the Fput command has been successfully transferred.

timep: Time Protocol Event Messages

These messages are generated by the system variable "timep".

can't reach time server *ip-address*

- Meaning:** The client cannot reach the server with the *ip-address*. The normal cause is that the subnet of the server is not yet known by IP. However, if the condition persists for several minutes, it indicates that some part of the path is down or that the configured address is incorrect.
- Action:** Check that the correct address for the Timep server is configured. Check that the server's subnet is entered in the IP routing table by using NCL's Rgetr command.

changing time

- Meaning:** The time fields in front of this event message indicate what the time was before it was changed by a request from the Timep server, and to what the time was changed. (See the description of the message entry at the beginning of this chapter.)

entity already disabled

- Meaning:** An already disabled Time Protocol has received NCL's Disable command.

entity already enabled

- Meaning:** An already enabled Time Protocol has received NCL's Enable command.

entity disabled

- Meaning:** Time Protocol has been disabled in response to NCL's Disable command.

Event Log Messages

timep: Time Protocol Event Messages

entity enabled

Meaning: Time Protocol has been enabled in response to NCL's Enable command.

new time set

Meaning: The time fields in front of this event message indicate what the time was before it was changed by a request from the Timep server, and to what the time was changed. (See the description of the message entry at the beginning of this chapter.)

request from *ip-address*

Meaning: The server received a request for the current time from client *ip-address* and will respond (unless it can't reach the node).

X.25 Event Messages

These event messages are generated by the system variable “x25”, that is, X.25.

bad configuration

Meaning: X.25 had detected an inconsistency in the configuration.

Action: Examine and modify the X.25 configuration.

bad LAPB packet window value

Meaning: The Pkt Window parameter in the ‘Circuits’ configuration is outside the legal range of 1 through 127.

Action:

bad Point-to-Point Service packet window value

Meaning: The Negotiated Packet Window parameter in the X.25 Virtual Circuits screen for Point-to-Point Service is outside the legal range of 1 through 127.

Action:

bad PDN Service packet window value

Meaning: The Negotiated Pkt Window parameter in the X.25 Address Map for PDN service is outside the legal range of 1 through 127.

Action:

call accepted from DTE *x121-address*

Meaning: An incoming call was accepted from remote DTE address *x121-address*.

Event Log Messages
X.25 Event Messages

call attempt: *cct* . *ip-address*

Meaning: A call has been made to the destination with IP address *ip-address* on circuit *cct*.

call attempt on *virtual-cct*

Meaning: A call has been made on the virtual circuit named *virtual-cct*.

call: *cct* . *ip-address* . #

Meaning: A DDN or PDN call has been established with the remote host or gateway identified by *ip-address*. *cct* identifies the X.25 DDN or PDN circuit and # identifies the logical connection number.

call cleared on *svc* (C=*mm*) (D=*nn*)

Meaning: A call has been properly cleared on point-to-point virtual circuit *svc*. C (*mm*) contains the decimal contents of the Cause field (octet 4) of the supervisory header of the packet that cleared the call. D (*nn*) contains the decimal contents of the Diagnostic Code field (octet 5) of the same packet. The values are listed in tables 17-2 and table 17-3, at the end of this X.25 section.

call established on *svc*

Meaning: A call has been properly established on point-to-point virtual circuit *svc*. A call is established by a call request, incoming call, call accepted, or call connected packet sequence.

call fail on *cct* (C=*CAUSE*) (D=*DIAGNOSTIC*)

Meaning: The call made on virtual circuit *cct* has failed. C (*Cause*) contains the decimal contents of the Cause field (octet 4) of the supervisory header of the packet that failed. D (*Diagnostic*) contains the decimal contents of the Diagnostic Code field (octet 5) of the same packet. The values are listed in tables 17-2 and table 17-3, at the end of this X.25 section.

clr: *cct* . *ip-address* . # (C=*mm*) (D=*nn*)

Meaning: An established DDN or PDN call to the remote host or gateway identified by *ip-address* has been cleared. *cct* identifies the X.25 DDN or PDN circuit and # identifies the logical connection number. C (*mm*) contains the decimal contents of the Cause field (octet 4) of the supervisory header of the packet that cleared the call. D (*nn*) contains the decimal contents of the Diagnostic Code field (octet 5) of the same packet. The values are listed in tables 17-2 and table 17-3, at the end of this X.25 section.

clr call from DTE *x121-address* (address not found)

Meaning: The incoming call from DTE address *x121-address* has been cleared because the remote DTE address was not found in the X.25 address map.

Action: Modify the configuration by adding an entry for the remote node in the X.25 PDN Address Map for the appropriate X.25 circuit.

clr call from DTE *x121-address* (max calls active)

Meaning: The incoming call from DTE address *x121-address* has been cleared because the maximum number of calls is already active between the X.25 circuit and the remote node.

Action: Modify the configuration by increasing the Max Conns/Dest parameter in the X.25 PDN Address Map for the appropriate X.25 circuit.

clr call from DTE *x121-address* (no host found)

Meaning: The incoming call from DTE address *x121-address* has been cleared because no host circuit was found for the call. For example, if the call was received on a line connected to a DDN network and the line has not been configured for a DDN network, then the call cannot be accepted.

Action: Modify the configuration by configuring the appropriate Quality of Service and PDN types for your network.

Event Log Messages
X.25 Event Messages

clr call from DTE *x121-address* (no idle circuits)

Meaning: The incoming call from DTE address *x121-address* has been cleared because an idle circuit is not available to receive the incoming call.

clr: *cct.ip_addr.#* (C=*nn*) (D=*nn*)

Meaning: An established DDN or PDN call to the remote host or gateway identified by *ip_addr* has been cleared. *cct* identifies the X.25 DDN or PDN circuit and # identifies the logical connection number. (C=*nn*) contains the decimal contents of the Cause field (octet 4) of the supervisory header of the packet that CLEARED the call. (D=*nn*) contains the decimal contents of the Diagnostic Code field (octet 5) of the same packet. The tables at the end of this chapter provide a summary listing of these decimal values.

disable ignored for *virtual-cct*, still processing a previous request

Meaning: NCL's Disable command was issued for the busy virtual circuit, *virtual-cct*.

disable in progress for *virtual-cct*

Meaning: Virtual circuit *virtual-cct* is being disabled.

enable ignored for *virtual-cct*, still processing a previous request

Meaning: NCL's Enable command was issued for an already enabled (and busy) virtual circuit, *virtual-cct*.

enable in progress for *virtual-cct*

Meaning: Virtual circuit *virtual-cct* is being enabled.

fail: *cct . ip-address* (C=*mm*) (D=*nn*)

Meaning: A call to the destination with IP address *ip-address* on the circuit *cct* has failed. C (*mm*) contains the decimal contents of the Cause field (octet 4) of the supervisory header of the packet that failed. D (*nn*) contains the decimal contents of the Diagnostic Code field (octet 5) of the same

packet. The values are listed in tables 17-2 and table 17-3, at the end of this X.25 section.

high lcn (xx) < low lcn (yy); using (yy) for both

- Meaning:** The high LCN (logical channel number) is lower than the low LCN configured for an X.25 circuit. The value given by the low LCN (yy) will be used for both LCNs.
- Action:** Modify the configuration to configure Low LCN and High LCN parameters correctly.

high lcn – low lcn > max lcns (xx); using (yy) for high lcn

- Meaning:** The difference between the high LCN (logical channel number) and low LCN values is greater than the maximum number of LCNs allowed for the circuit. The high LCN will be adjusted downward to yy to allow the maximum number of LCNs to be configured.
- Action:** Modify the configuration to configure Low LCN and High LCN parameters correctly.

high LCN (XXXX) > 4095: now High = YYYY & Low = ZZZZ

- Meaning:** The High LCN value XXXX entered by the user exceeded the maximum value allowed of 4095. The High LCN value has been adjusted downwards to YYYY, and the Low LCN value has been adjusted downwards to ZZZZ to bring them within legal range. For example, if the Low LCN value entered by the user was 5000, and the High LCN value entered by the user was 5010, then the Low LCN and High LCN values are adjusted downwards to 4085 and 4095, respectively. Thus, the actual number of LCNs desired by the user (in this case, 5010 - 5000 = 10) remains unchanged (4095 - 4085 = 10).
- Action:** Modify the configuration.

ioctl error xx occurred in state yy

- Meaning:** A status request of the packet-level interface has generated an error.

Event Log Messages
X.25 Event Messages

read error *xx* occurred in state *xx*

Meaning: A read of the packet-level interface has generated an error.

switch call - *xxx* to *xxx*

Meaning: An incoming Call Request has been switched.

switched call reset *slot n*. cir = clearing code diag = diagnostic

Meaning: A virtual circuit has been reset.

switched VC clear requested

Meaning: A switched virtual circuit is being cleared.

switched VC close timeout detected - retrying *slot n*

Meaning: An internal close request has been lost between slots.

virtual-cct is already disabled

Meaning: NCL's Disable command was issued for the already disabled virtual circuit, *virtual-cct*.

virtual-cct is already enabled

Meaning: NCL's Enable command was issued for the already enabled virtual circuit, *virtual-cct*.

virtual-cct is disabled

Meaning: Indicates that virtual circuit *virtual-cct* is disabled.

virtual-cct is enabled

Meaning: Indicates that virtual circuit *virtual-cct* is enabled and ready to establish or receive a call.

Table 17-2. Cause Field Codes

Code	DCE-generated
1	Number busy
3	Invalid facility request
5	Network congestion
9	Out of order
11	Access barred
13	Not obtainable
17	Remote procedure error
19	Local procedure error
21	RPOA out of order
25	Reverse charging not available
33	Incompatible destination
41	Fast select not available
57	Ship absent

Code	DTE-generated
129	Number busy
131	Invalid facility request
133	Network congestion
137	Out of order
139	Access barred
141	Not obtainable
145	Remote procedure error
147	Local procedure error
149	RPOA out of order
153	Reverse charging not available
161	Incompatible destination
169	Fast select not available
185	Ship absent

Event Log Messages

X.25 Event Messages

Table 17-3. Diagnostic Field Codes

Code	Point-to-Point Service
0	No additional information
1	Invalid P(S)
2	Invalid P(R)
3–15	Not assigned
16	Packet type invalid
17	For state r1
18	For state r2
19	For state r3
20	For state p1
21	For state p2
22	For state p3
23	For state p4
24	For state p5
25	For state p6
26	For state p7
27	For state d1
28	For state d2
29	For state d3
30–31	Not assigned
32	Packet not allowable
33	Unidentifiable packet
34	Call on one-way logical channel
35	Invalid packet type on permanent SVC
36	Packet on unassigned logical channel
37	Reject not subscribed to
38	Packet too short
39	Packet too long
40	Invalid general format identifier (GFI)
41	Restart or registration packet with non-zero values in inappropriate bits
42	Packet type not compatible with facility
43	Unauthorized interrupt confirmation
44	Unauthorized interrupt
45	Unauthorized reject
46–47	Not assigned

Table 17-3. Diagnostic Field Codes (*Continued*)

Code	Point-to-Point Service (<i>Continued</i>)
48	Time expired
49	for incoming call
50	for clear indication
51	for reset indication
52	for restart indication
53–63	Not assigned
64	Call setup, call clearing, or registration problem
65	Facility/registration code not allowed
66	Facility parameter not allowed
67	Invalid called address
68	Invalid calling address
69	Invalid facility/registration length
70	Incoming call barred
71	No logical channel available
72	Call collision
73	Duplicate facility request
74	Nonzero address length
75	Nonzero facility length
76	Facility not provided when expected
77	Invalid CCITT-specified DTE facility
78–79	Not assigned
80	Miscellaneous
81	Improper Cause code from DTE
82	Misaligned octet
83	Inconsistent Q-bit setting
84–111	Not assigned
112	International problem
113	Remote network problem

Event Log Messages

X.25 Event Messages

Table 17-3. Diagnostic Field Codes (Continued)

Code	Point-to-Point Service (Continued)
114	International protocol problem
115	International link out-of-order
116	International link busy
117	Transit network facility problem
118	Remote network facility problem
119	International routing problem
120	Temporary routing problem
121	Unknown DNIC
122	Maintenance action
123–127	Not assigned
241	Call cleared because circuit was disabled or because of failure in X.25 protocol levels 1, 2, or 3
242	Call cleared because SVC was disabled
Code	DDN Service
84	Invalid EE error code received
85	Invalid (out-of-range) PSN number
86	Software error
128	DCE dropped the ready line. Network forwarding mechanisms are not available.
129	Link level sent BREAK
130	Link came up
131	Link went down
132	Remote DTE restarted
133	Local resources not available for call establishment
134	Remote resources not available for call establishment
135	Remote call collision
136	Remote host dead
137	Remote DCE dead
138	Logical subnet access barred. The remote DTE cannot be reached because of a communities-of-interest prohibition.
139	Connection lost
140	Response lost
141	Calling logical name not authorized or enabled
142	Calling logical name incorrect for this DTE
143	Called logical name not authorized
144	Called logical name not enabled

Table 17-3. Diagnostic Field Codes (Continued)

Code	DDN Service (Continued)
145	Called logical name has no effective translations
146	Invalid address; logical addressing not used in this network
147	Declared logical name is now enabled
148	Declared logical name was already enabled
149	Declared logical name is not disabled
150	Declared logical name was already disabled
151	Incoming calls are barred
152	Outgoing calls are barred
153	Cause field is nonzero
154	VC timeout because of idleness (in call between X.25 and AHIP hosts)
155	Destination DTE uses standard X.25 service
156	Invalid protocol ID (in calls between X.25 and AHIP hosts)
157	Error occurred while opening connection at the AHIP source)
160	PVC endpoints are incompatible
161	NAS reselection was completed while the local DCE was waiting for a RESET CONFIRMATION from the local DCE
162	No response by DTE after attempt to bring up virtual circuit
163	PVC is up and restart is complete
164	Network-caused PVC error
165	CPS aggregation deadlock was detected
166	Local DCE received an invalid packet while waiting for a response to a call request from the remote DTE
167	Connection closed because of network error
Code	Reserved for Network-Specific Information
168	Cannot intercept fast select
169	Cannot intercept RPOA
170	Cannot intercept X.75 call
171	Too much data is intercepted call
172	Bad NAS address
173	Invalid facility for normal CLEAR packet
174	Invalid local reselection address
175	Invalid remote local reselection address
176	Reselection request with fast selection
177	Too much data in reselection request
178	Reselection request NUI is greater than fast select
179	Cannot renegotiate fixed facilities

Event Log Messages

X.25 Event Messages

Table 17-3. Diagnostic Field Codes (Continued)

Code	Network-Specific information (Continued)
180	Invalid packet received during NAS select
181	Call opened while the local DCE was waiting for a reply to a CALL REQUEST from DTE and a RESET CONFIRMATION from the local DTE
192	Call cleared because of local pre-emption by a higher-precedence connection
193	Call cleared because of remote pre-emption by a higher-precedence connection
194	Requested precedence is too high
195	PVC take-up collision
196	Remote end-point of the PVC is not initialized with the specified LCN
197	Hunt groups are not used
198	Hunt group number is not valid
199	No port in hunt group is available
200	SVC was killed by MC command
201	PVC was reset by MC command
202	Call redirection took too long or too many tries
205	Call cut off because the precedence level was too low
Code	BFE Information
224	Entering emergency mode
225	Leaving emergency mode
226	Emergency window is open
227	Call failed because address translation information is required
228	Call failed because emergency window was not open

xrx: XNS Router Event Messages

These event messages are generated by the system variable “xrx”, the Xerox XNS router.

xrx: ccg : New Rt to *xrxnet* via *ipx-address*

Meaning:

The XNS routing module generates a new event message whenever it learns a new route or updates an existing route. The new route is specified by *xrxnet*, which is the destination network to which the new or updated route refers, and by *ipx-address*, which is the full IPX address of the next hop router. The *ipx-address* is shown in hexadecimal notation: the first eight digits are the network address and the last twelve digits are the host address.

If the value of *xrxnet* is zero and the second part of *ipx-address* is the station address of the router, then the first part of *ipx-address* is a directly connected network.

Note

If *xrxnet* is zero and the second part of the *ipx-address* is the station address of the box, then the first part of the *ipx-address* is also a directly connected network.

Event Log Messages

xrx: XNS Router Event Messages

xrx: *ccg*: Rcvd Err Pkt – *err#*, Param = *errparam*

Meaning: An error packet has been received by the XNS router. *ccg* is the circuit group on which the error packet was received. *err#* is the error number (in decimal) of the error packet. *errparam* is the error parameter (in decimal) of the error packet.
Valid error numbers are:

0	Unspecified error at destination.
1	Bad checksum or other packet inconsistency at destination.
2	Unknown socket at destination.
3	Destination resource limitations.
512	Unspecified error before reaching destination.
513	Bad checksum or inconsistency before reaching destination.
514	Destination host cannot be reached.
515	Packet exceeded hop count of 15.
516	Packet too large to forward; the <i>errparam</i> is the maximum acceptable length.

xrx: CG *ccg*: Del Rt to *dest_net* via *next_hop_net*: *next_hop_gw*

where:

<i>ccg</i>	is the name of the circuit group on which the route was learned.
<i>dest_net</i>	is the destination network to which the router referred.
<i>next_hop_net</i>	is the directly connected network that was to be used to get to the next hop router.
<i>next_hop_gw</i>	is the XNS or IPX address of the router that was the next hop for traffic destined for <i>dest_net</i> .

zmodem: Zmodem Event Messages

These event messages are NCL error codes that can occur when using the Zmodem commands Zput and Zget.

Display-Only Zmodem Event Messages

These messages are not listed in the event log. They appear only on the console display. For messages that are also logged, see page 17-150.

Command only allowed from the Console Port

Meaning: The Zmodem commands are allowed only from the console port. Telnet sessions cannot use them.

The Configuration Editor is in use by another session

Meaning: Indicates that the a transfer of the configuration file is not allowed because the Configuration Editor is currently accessing it.

Action: Check for Telnet sessions running the Configuration Editor.

The Configuration file is being TFTP'd by another session

Meaning: Indicates that a transfer of the configuration file is not allowed because it is currently being transferred using TFTP.

Action: Check for Telnet sessions running TFTP.

Missing local file name

Meaning: The local file name (or command) was not included with the Zput command.

Action: The local file name to transfer must be entered. (For example, the configuration file.)

Event Log Messages

zmodem: Zmodem Event Messages

Missing remote file name

Meaning: The remote file name was not included with the Zput command.

Action: The remote file name to transfer into must be entered.

NCL ERR — invalid command (ignored)

Meaning: This is a generic error indicating that either the command was mistyped or that manager capability is required to use the command. For Zmodem, this occurs with Zget if you did not use the manager password when you started the console session.

Unable to allocate memory for zmodem protocol

Meaning: The buffer space required for the zmodem protocol transfers is not available currently. This indicates that all the router memory is currently in use for other tasks or for the routing table.

Action: Wait for the router traffic load to decline, then try again.

Logged and Displayed Zmodem Event Messages

The following messages appear in the log file and in the console display. For messages that appear only in the console display, see page 17-149.

Bad escape sequence received %x

Meaning: Indicates that an unknown escape sequence was received by the router. Either the packet was corrupted during transmission or the host was running another protocol.

Action: Check the serial line for a poor connection or source of noise. Also verify that the host is running Zmodem.

CONFIG transfer aborted, no ID string found

Meaning: The router rejected the reception of a new configuration file because it lacked the proper configuration ID at the beginning of the file. This error only can occur with the Zget command.

Action: Try again with the proper configuration file.

Data subpacket too long from remote

Meaning: Indicates that the packet received by the router was longer than expected. Either the packet was corrupted during transmission or the host was running another protocol.

Action: Check the serial line for a poor connection or source of noise. Also verify that the host is running Zmodem.

Received a bad 16 bit CRC on a data packet
Received a bad 32 bit CRC on a data packet.

Meaning: Indicate that a data packet received by the router had a bad CRC. (That is, the packet was damaged in transit.)

Action: Check the serial line for a poor connection or source of noise.

Received a bad 16 bit CRC on binary header
Received a bad 32 bit CRC on binary header

Meaning: Indicate that a binary header received by the router had a bad CRC. (That is, the packet was damaged in transit.)

Action: Check the serial line for a poor connection or source of noise.

Received a bad 16 bit CRC on hex header

Meaning: Indicates that a hex header received by the router had a bad CRC. (That is, the packet was damaged in transit.)
Note: There is no 32-bit CRC defined for hex headers.

Action: Check the serial line for a poor connection or source of noise.

Event Log Messages

zmodem: Zmodem Event Messages

Terminal connection broken

Meaning: Indicates that the serial port between the router and the host has been disconnected.

Timeout on initialization response

Meaning: The router issued an initialization response and did not receive an acknowledgement within ten seconds.

Action: Check that the host is running the Zmodem protocol.

Timeout waiting for remote status

Meaning: The router issued a status request that was not responded to after six attempts that were spaced at ten-second intervals.

Action: Check that the host is running the Zmodem protocol.

Too many bytes before SOF

Meaning: Indicates that the Zmodem start of a frame character was not received within a reasonable amount of characters. Either the packet was corrupted during transmission or the host was running another protocol.

Action: Check the serial line for a poor connection or source of noise. Also verify that the host is running Zmodem.

Transfer terminated by remote

Meaning: Indicates that the host machine has terminated the Zmodem connection to the router.

Action: Check for log messages on the host to understand why the transfer was terminated.

Transfer terminated due to timeout

- Meaning:** Indicates that the router did not receive a Zmodem message from the host for 10 seconds. This message also occurs if the host did not respond to the router when it attempted to connect using the Zget command. (Zget tries for up to 70 seconds before timing out).
- Action:** Check the host configuration.

Unable to allocate memory for read

- Meaning:** The buffer space required for the Zmodem protocol configuration read is not currently available. This indicates that all the router memory is tied up in other tasks or in the routing table. This error can occur only with the Zget command.
- Action:** Wait for the router traffic load to decline, then try again.

Unable to connect to remote

- Meaning:** The router issued an initialization response and did not receive a valid header. The packet may have been corrupted during transmission.
- Action:** Check that the host is running the Zmodem protocol. Also check the serial line for a poor connection or source of noise.

Unable to execute command to create output

- Meaning:** The information requested in the Zput command could not be gathered. This error can occur only with the Zput command.
- Action:** Check for proper syntax, try to display the data on the console without using Zput. Then try Zput again.

Unable to get remote init parameters

- Meaning:** The router issued a status request that was not responded to after ten attempts that were spaced at ten-second intervals.
- Action:** Check that the host is running the Zmodem protocol.

Management Information Base
Variables

This chapter provides descriptions of all variables contained in the enterprise-specific management information base (MIB) on the router. Routers from Hewlett-Packard use the Wellfleet private-enterprise branch of the MIB:

“iso.org.dod.internet.private.enterprises.wellfleet.commServer.wfmib”
or 1.3.6.1.4.1.18.1.1.

At the next level down are the router’s highest-level MIB branches. This appendix is divided into a section for each of those branches, organized alphabetically. The hierarchical structure of those branches and their variables are described in each section. The variables at the end of each branch are listed alphabetically.

- To construct the pathname to the variable for use in NCL’s List and Get commands, separate the names of each level in the structure with periods. For example:

```
get cct.wan1.frames_rx_ok
```

- For a name surrounded by square brackets, omit the period preceding it. For example:

```
get alarm[1].set_cnt
```

Square brackets are commonly used to indicate a slot number for certain pathnames.

To learn more about accessing the MIB:

- Refer to the *User’s Guide* for:
 - Instructions on how to use pathnames and the List, Get and Reset commands
 - A quick reference to the full set of MIB commands.

(Located under “Accessesing the Management Information Base” and in subsequent sections in chapter 7 of the *User’s Guide*.)

- Refer to chapter 16, “Using the Network Control Language”, in this manual for a detailed description of each MIB command.

*Series 200 and 400 routers always use [1] where a slot number is required. For the HP Router 650, [2] through [5] may be used where a slot number is required. The actual number used for a Router 650 corresponds to the slot in which the desired variable occurs.

alarm: Alarm Information Base

The “alarm” information base contains variables that describe the scheduling and issuance of router-generated alarms. The structure is the following:

alarm

[*slot #*]

variables

listed below

The pathname is constructed as follows:

alarm [*slot #*].*variable*

The variables are listed alphabetically:

cancel_cnt contains the number of alarms cancelled by the router prior to the expiration of the alarm timer.

expire_cnt contains the number of alarm-related interrupts. Such an interrupt is generated when the alarm timer reaches zero.

race_cnt contains the number of simultaneous occurrences of the expiration of the alarm timer and the cancellation of a previously scheduled alarm.

set_cnt contains the number of alarms scheduled by the router.

at: AppleTalk Information Base

The “at” information base contains variables that describe transmission and reception activities across each AppleTalk circuit group and rejection of certain packets by the AppleTalk router. The structure is the following:

at

<i>cgc</i>	AppleTalk circuit group name
<i>protocol</i>	specific AppleTalk protocol (see subheadings)
<i>variables</i>	listed below

The pathname is constructed as follows:

at.cgc.protocol.variable

The variables are listed alphabetically under each protocol:

AppleTalk Address Resolution Protocol (ARP)

amt_overflow contains the number of times the circuit group tried unsuccessfully to store a node address and its corresponding station address in the ARP mapping table.

probe_rx contains the number of ARP PROBE packets received by circuit group *cgc*.

probe_tx contains the number of ARP PROBE packets transmitted by circuit group *cgc*.

req_rx contains the number of ARP REQUEST packets received by circuit group *cgc*.

req_tx contains the number of ARP REQUEST packets transmitted by circuit group *cgc*.

rsp_rx contains the number of AARP RESPONSE packets received by circuit group *ccg*.

rsp_tx contains the number of AARP RESPONSE packets transmitted by circuit group *ccg*.

AppleTalk Echo Protocol (AEP)

reply_tx contains the number of AEP REPLY packets transmitted by circuit group *ccg*.

req_rx contains the number of AEP REQUEST packets received by circuit group *ccg*.

Datagram Delivery Protocol (DDP)

ddp_bad_cksum contains the number of AppleTalk packets dropped by circuit group *ccg* because the packet contained an incorrect DDP checksum value.

ddp_fwd contains the number of AppleTalk packets forwarded by circuit group *ccg*.

ddp_hop_ct_exceed contains the number of AppleTalk packets dropped by circuit group *ccg* because the packet's hop count was too large.

ddp_no_ir_addr contains the number of AppleTalk packets dropped by circuit group *ccg* because the next router's station address could not be resolved.

ddp_pkts_dropped_no_aarp_rsp contains the number of AppleTalk packets dropped by circuit group *ccg* because the packet's destination node did not respond to AARP REQUEST packets issued by the router.

ddp_pkts_sent_by_aarp contains the number of AppleTalk packets forwarded after the destination address was resolved by AARP.

Management Information Base Variables

at: AppleTalk Information Base

ddp_rx contains the number of valid AppleTalk packets received by circuit group *cgc*.

ddp_total_drop contains the total number of AppleTalk packets dropped by circuit group *cgc*.

ddp_unknown_netwk contains the number of AppleTalk packets dropped by circuit group *cgc* because the destination network was unknown.

ddp_upper_protocol contains the number of AppleTalk packets sent to an upper-layer protocol by circuit group *cgc*.

Name Binding Protocol (NBP)

nbp_breq_rx contains the number of NBP BROADCAST REQUEST packets received by circuit group *cgc*.

nbp_fwdreq_rx contains the number of NBP FORWARD REQUEST packets received by circuit group *cgc*.

nbp_fwdreq_tx contains the number of NBP FORWARD REQUEST packets transmitted by circuit group *cgc*.

nbp_lkup_tx contains the number of NBP LOOKUP packets transmitted by circuit group *cgc*.

Routing Table Maintenance Protocol (RTMP)

cable_range_conflicts contains the number of times an RTMP DATA packet (received on circuit group *cgc*) contained a routing tuple (a target network and a hop count) with a network range that overlapped a routing entry in the AppleTalk routing table.

data_rx contains the number of RTMP DATA packets received by circuit group *cgc*.

data_tx contains the number of RTMP DATA packets transmitted by circuit group *cgc*.

network_type_conflicts contains the number of RTMP DATA packets (received by circuit group *cgc*) whose routing tuples (a target network and a hop count) conflicted with network entries in the AppleTalk routing table.

nonextended_netwk contains the number of nonextended routing tuples (a target network and a hop count) received by circuit group *cgc*.

rdr_rx contains the number of RTMP ROUTE DATA REQUEST packets received by circuit group *cgc*.

req_rx contains the number of RTMP REQUEST packets received by circuit group *cgc*.

routing_tbl_overflow contains the number of times circuit group *cgc* tried unsuccessfully to store a new routing tuple (a target network and a hop count) in the AppleTalk routing table.

rsp_tx contains the number of RTMP RESPONSE packets transmitted by circuit group *cgc*.

ver_mismatch contains the number of RTMP DATA packets (received by circuit group *cgc*) that were not for AppleTalk Phase 2.

Zone Information Protocol (ZIP)

getlclzones_rx contains the number of ZIP GETLOCALZONES packets received by circuit group *cgc*.

getlclzones_tx contains the number of ZIP GETLOCALZONES packets transmitted by circuit group *cgc*.

getlclzonesreply_rx contains the number of ZIP GETLOCALZONES-REPLY packets received by circuit group *cgc*.

getlclzonesreply_tx contains the number of ZIP GETLOCALZONES-REPLY packets transmitted by circuit group *cgc*.

getnetinfo_rx contains the number of ZIP GETNETINFO packets received by circuit group *cgc*.

Management Information Base Variables

at: AppleTalk Information Base

getnetinfo_tx contains the number of ZIP GETNETINFO packets transmitted by circuit group *cgc*.

getzonelist_rx contains the number of ZIP GETZONELIST packets received by circuit group *cgc*.

getzonelistreply_tx contains the number of ZIP GETZONELISTREPLY packets transmitted by circuit group *cgc*.

netinfoforeply_rx contains the number of ZIP NETINFOFOREPLY packets received by circuit group *cgc*.

netinfoforely_tx contains the number of ZIP NETINFOFOREPLY packets transmitted by circuit group *cgc*.

reply_rx contains the number of ZIP REPLY packets received by circuit group *cgc*.

reply_tx contains the number of ZIP REPLY packets transmitted by circuit group *cgc*.

req_rx contains the number of ZIP REQUEST packets received by circuit group *cgc*.

req_tx contains the number of ZIP REQUEST packets transmitted by circuit group *cgc*.

atmib: AppleTalk MIB Information Base

The “atmib” information base contains variables that describe transmission and reception activities of the AppleTalk router. The structure is the following:

atmib

<i>protocol</i>	stands for the specific AppleTalk protocol (see subheadings)
<i>variables</i>	listed below

The pathname is constructed as follows:

atmib.*protocol.variable*

The variables are listed alphabetically under each *protocol*.

AppleTalk Echo Protocol (AEP)

aep_Reply_tx contains the total number of AEP REPLY packets transmitted by the AppleTalk router.

aep_Req_rx contains the total number of AEP REQUEST packets received by the AppleTalk router.

Datagram Delivery Protocol (DDP)

ddp_bad_cksum contains the total number of AppleTalk packets dropped by the AppleTalk router because the packet contained an incorrect DDP checksum value.

ddp_fwd contains the total number of AppleTalk packets forwarded by the AppleTalk router.

ddp_hop_ct_exceed contains the total number of AppleTalk packets dropped by the AppleTalk router because the packet’s hop count was too large.

Management Information Base Variables

atmib: AppleTalk MIB Information Base

ddp_rx contains the total number of AppleTalk packets received by the AppleTalk router.

ddp_total_drop contains the total number of AppleTalk packets dropped by the AppleTalk router.

ddp_tx contains the total number of AppleTalk packets transmitted by the AppleTalk router.

ddp_unknown_netwk contains the total number of AppleTalk packets dropped by the AppleTalk router because the destination network was unknown.

ddp_upper_prot contains the total number of AppleTalk packets sent to an upper-layer protocol by the AppleTalk router.

Name Binding Protocol (NBP)

nbp_breq_rx contains the total number of NBP BROADCAST REQUEST packets received by the AppleTalk router.

nbp_fwdreq_rx contains the total number of NBP FORWARD REQUEST packets received by the AppleTalk router.

nbp_fwdreq_tx contains the total number of NBP FORWARD REQUEST packets transmitted by the AppleTalk router.

nbp_lkup_tx contains the total number of NBP LOOKUP packets transmitted by the AppleTalk router.

Routing Table Maintenance Protocol (RTMP)

rtmp_req_rx contains the total number of RTMP REQUEST packets received by the AppleTalk router.

rtmp_rsp_tx contains the total number of RTMP RESPONSE packets transmitted by the AppleTalk router.

Zone Information Protocol (ZIP)

zip_getlclzones_rx contains the total number of ZIP GETLOCALZONES packets received by the AppleTalk router.

zip_getlclzones_tx contains the total number of ZIP GETLOCALZONES packets transmitted by the AppleTalk router.

zip_getlclzonesreply_rx contains the total number of ZIP GETLOCALZONESREPLY packets received by the AppleTalk router.

zip_getlclzonesreply_tx contains the total number of ZIP GETLOCALZONESREPLY packets transmitted by the AppleTalk router.

zip_getnetinfo_rx contains the total number of ZIP GETNETINFO packets received by the AppleTalk router.

zip_getnetinfo_tx contains the total number of ZIP GETNETINFO packets transmitted by the AppleTalk router.

zip_getzonelist_rx contains the total number of ZIP GETZONELIST packets received by the AppleTalk router.

zip_netinforeply_rx contains the total number of ZIP NETINFOREPLY packets received by the AppleTalk router.

zip_netinforeply_tx contains the total number of ZIP NETINFOREPLY packets transmitted by the AppleTalk router.

zip_reply_rx contains the total number of ZIP REPLY packets received by the AppleTalk router.

zip_reply_tx contains the total number of ZIP REPLY packets transmitted by the AppleTalk router.

zip_req_rx contains the total number of ZIP REQUEST packets received by the AppleTalk router.

zip_req_tx contains the total number of ZIP REQUEST packets transmitted by the AppleTalk router.

buf: Buffers Information Base

The buffers “buf” information base contains variables that describe the router’s use of two types of global memory buffers: message buffers, which facilitate internal process-to-process communication, and packet buffers, which facilitate external communications by temporarily storing incoming or outgoing data packets. The structure is the following:

buf

[*slot #*] *

type

stands for either *msg* or *pkt*, both containing the same variables

variables

listed below

The pathname is constructed as follows:

buf[*slot #*].*type*.*variable*

The variables are listed alphabetically:

corrupted contains the number of times a corrupted buffer was deleted.

free contains the number of message or packet buffers available for internal VME transfers or external transfers, respectively. Because router operations and application software modules impose some overhead on global memory buffers, the number of buffers available for data transfers is less than the total number of buffers allocated when the router boots.

init contains the number of message or packet buffers allocated when the router booted.

min contains the smallest number of message or packet buffers available since the router booted.

miss contains the number of times that the router was unable to obtain either a message buffer or a packet buffer. Failure to obtain a buffer indicates that all buffers were busy. This parameter is directly related to `min`. If `miss` is greater than 0, `min` must equal 0. Conversely, if `miss` equals 0, then `min` must be greater than 0.

size contains the size of the message or packet buffer in bytes.

*Refer to the footnote on page 18-2

cct: Circuits Information Base

The circuits “cct” information base contains variables that describe transmission and reception activities across each LAN and point-to-point circuit. The structure is the following:

cct

cct stands for the circuit name, usually indicating circuit type (see subheadings)

variables for each type of circuit, as listed below

The pathname is constructed as follows:

cct.cct.variable

The variables are listed alphabetically under each type of circuit:

WAN Circuits

This subsection describes variables common to all WAN circuit types. For variables specific to certain WAN circuit types, refer also to the following:

- PPP--the industry-standard Point-to-Point Protocol-- page 18-35
- Frame Relay--page 18-22.

bad_frames_rx contains the aggregate number of erroneous frames received by circuit *cct*.

cable_type contains a code indicating the type of cable detected on the port for circuit *cct*, as follows:

0	loopback hood	4	RS-232/V.24/V.28 cable
1	V.35 cable	5	n/a
2	RS-422/449/V.36 cable	6	n/a
3	X.21 cable	7	no cable

dls_ret_rx contains the number of frames, received by circuit *cct*, that were later returned by the data-link service (DLS) software. Within the router software architecture, DLS resides between the driver software and the application software. It performs such services as

multiplexing/demultiplexing and encapsulation/deencapsulation. DLS can return frames for numerous reasons (many of which are application-specific): for example, because of unknown internal service-access points (ISAPs), because of user-specified filtering requirements contained within the configuration, or because of lack of enabled entities (for example, IP, IPX, etc.).

dls_ring_cnt contains the current number of packets received by circuit *cct* and transferred to the data-link service (DLS) receiver queue.

frames_rx_ok contains the number of frames received without error by circuit *cct*.

frames_rx_per_sec contains the number of frames that this circuit has received in the last second.

frames_tx_ok contains the number of packets transmitted without error by circuit *cct*. This value equals the sum of *highpri_tx*, *normpri_tx*, and *lowpri_tx*.

frames_tx_per_sec contains the number of frames that this circuit has transmitted in the last second.

frams_incomp_rx contains the number of incomplete frames received by circuit *cct*. An incomplete frame is identified by failure to set the end-of-long-frame bit in the receive message descriptor.

frmr_frames_rx contains the count of unnumbered FRMR (Frame Reject) frames received by circuit *cct*. A FRMR frame reports an error condition. The remote end of the point-to-point circuit transmits a FRMR frame in response to a previous command requesting an unavailable action or service. Because the service or command is unavailable, a FRMR frame does not request retransmission of the erroneous frame.

highpri_congestion contains the number of high priority packets dropped due to congestion.

highpri_tx contains the number of high priority packets transmitted without error.

Management Information Base Variables

cct: Circuits Information Base

lack_resc_error_rx contains the number of instances that circuit *cct* lost a frame because it could not obtain a receive buffer.

latency_tx contains the number of packets (of all priorities) dropped due to exceeding the maximum link latency configured by the user.

Link_SetUps contains the number of times the link has been set up.

Link_UpTime contains how long the link has been up since the router has been booted.

lowpri_congestion contains the number of low priority packets dropped due to congestion.

lowpri_tx contains the number of low priority packets transmitted without error.

mac_addr contains the 12-digit hexadecimal representation of the 48-bit station address used by circuit *cct*.

merr contains the number of memory errors. A memory error indicates that the link level controller, after becoming bus master, failed to receive a ready signal within 256 increments of the system clock after asserting a memory address on the data/address bus. A memory error disables the link level controller.

normpri_congestion contains the number of normal priority packets dropped due to congestion.

normpri_tx contains the number of normal priority packets transmitted without error.

octets_rx_ok contains the number of octets (bytes) received without error by circuit *cct*.

octets_rx_per_sec contains the number of octets that this circuit has received in the last second.

octets_tx_ok contains the number of octets (bytes) transmitted without error by circuit *cct*.

octets_tx_per_sec contains the number of octets that this circuit has transmitted in the last second.

oflo_rx contains the total number of overflows on circuit *cct*. An overflow occurs when the receiver FIFO buffer is full when the link level controller was ready to input data.

peak_frames_rx contains the peak number of frames that this circuit has received in any given second since the last reboot.

peak_frames_tx contains the peak number of frames that this circuit has transmitted in any given second since the last reboot.

peak_octets_rx contains the peak number of octets that this circuit has received in any given second since the last reboot.

peak_octets_tx contains the peak number of octets that this circuit has transmitted in any given second since the last reboot.

rcv_desc_cnt contains the current number of receiver data buffers available to the link level controller.

rejects_rx contains the count of supervisory REJ (Reject) frames received by circuit *cct*. A REJ frame is a negative acknowledgment and requests the retransmission of specified I (Information) frames.

rejects_tx contains the number of supervisory REJ (Reject) frames transmitted by circuit *cct*. A REJ frame is a negative acknowledgment and requests the retransmission of specified I (Information) frames.

runts_rx contains the aggregate number of frames of insufficient length received by circuit *cct*.

rx_peak_rate contains the peak data receive rate in bits per second.

rx_rate contains the current data receive rate in bits per second.

t1_tos contains the number of T1 timeouts. The T1 timer measures the interval between command transmission and the receipt of a response. If a response is not received within this interval, the link level controller increments this counter and then retransmits the command with the P bit set to require an immediate response.

Management Information Base Variables

cct: Circuits Information Base

total_rx_error contains the total number of receive errors on circuit *cct*. This value equals the sum of *bad_frames_rx*, *frams_incomp_rx*, *frmr_frames_rx*, *lack_resc_error_rx*, *oflo_rx*, *rejects_rx*, and *runts_tx*.

total_tx_error contains the total number of transmission errors, which is the sum of *uflo_tx*, *latency_tx*, and *tx_congestion*.

tx_congestion contains the total number of packets dropped due to congestion, which is the sum of *hipri_congestion*, *normpri_congestion*, and *lowpri_congestion*.

tx_peak_rate contains the peak data transmission rate in bits per second.

tx_queue_len contains the number of octets (of all priorities) currently queued to the circuit. This statistic is used as a parameter for controlling latency when Max Link Latency is configured for the circuit.

tx_rate contains the current data transmission rate in bits per second.

uflo_tx contains the total number of underflows on circuit *cct*. An underflow occurs when the transmitter portion of the link level controller truncates a frame because of late receipt of data from memory.

xmt_desc_cnt contains the current number of frames awaiting transmission by the link level controller.

FDDI Circuit

canonical_addr Contains the address of this station in canonical form.

cfm_state Contains the state of the configuration management state machine.

downstream_mac Contains the 48-bit address of the FDDI downstream neighbor.

elm_a_pcm Contains the state of ELM A's physical connection machine (PCM).

elm_b_pcm Contains the state of ELM B's physical connection machine (PCM).

err_gsr_host Contains the number of parity errors detected during a write access to FDDI System Interface (FSI).

err_gsr_internal_op Contains a count of FSI internal operation errors.

err_gsr_llc_rx_rer Contains the number of ring errors that occurred for the ring that controls receive LLC frames.

err_gsr_llc_tx_rer Contains the number of ring errors that occurred for the ring controlling transmit LLC frames.

err_gsr_llc_rx_rov Contains the number of ring overruns on the receive LLC.

err_gsr_port_op Contains the number of FSI port operation errors.

err_gsr_smt_rx_rer Contains the number of ring errors that occurred for the ring that controls receive SMT frames.

err_gsr_smt_rx_rov Contains the number of ring overruns on the receive SMT frame.

Management Information Base Variables

cct: Circuits Information Base

err_rx_crc Contains the number of received frames with a faulty FCS value.

err_rx_mac_status Contains a count of receive frame indication errors (those that are not parity or overrun errors).

err_rx_overrun Contains the number of circuit overruns. An overrun

occurs when the FDDI receive circuitry cannot keep pace with the incoming flow of traffic.

err_rx_parity Contains the number of receive frames with parity errors.

err_tx_abort Contains the number of transmit frame aborts.

err_tx_underrun Contains the number of circuit underruns. An underrun occurs when the FDDI transmit truncates a frame because of late receipt of data from memory.

frames_rx_oc Contains the number of error-free frames received.

frames_rx_per_sec Contains the number of frames that this circuit has received in the last second.

frames_tx_ok Contains the number of error-free frames transmitted.

frames_tx_per_sec Contains the number of frames that this circuit has transmitted in the last second.

ieee_addr Contains the address of the station in IEEE format.

ioe_mov FSI experienced an internal memory overrun error.

mac_mla Contains the MAC's 48-bit long address.

mac_ring_op States whether the ring is operational or not.

mac_ring_op_cnt Contains the number of times the FDDI ring changes states.

missed_cmd Contains a count of commands issued to the FSI that were missed (not executed).

missed_crf Contains a count of commands not executed because the FSI register did not become free.

net_fail Indicates whether net fail LED is lit for the circuit.

octets_rx_ok Contains the number of error-free octets received.

octets_rx_per_sec contains the number of octets that this circuit has received in the last second.

octets_tx_ok Contains the number of error-free octets transmitted.

octets_tx_per_sec contains the number of octets that this circuit has transmitted in the last second.

peak_frames_rx Contains the peak number of frames that this circuit has received in any given second since reboot.

peak_frames_tx Contains the peak number of frames that this circuit has transmitted in any given second since reboot.

peak_octets_rx Contains the peak number of octets that this circuit has received in any given second since reboot.

peak_octets_tx Contains the peak number of octets that this circuit has transmitted in any given second since reboot.

rmt_state Contains the ring management state.

rr_on_rov Contains the number of ring resets issued in response to receive ring overrun errors.

source_mac Contains the source address of the received/transmitted frame.

total_rx_error Contains the number of receive errors.

total_tx_error Contains the number of transmit errors.

Management Information Base Variables

cct: Circuits Information Base

tx_congestion Contains the number of times where a buffer wasn't available to transmit a frame.

upstream_mac Contains the 48-bit address of the FDDI upstream neighbor.

Frame Relay Management Information Base

The Frame Relay MIB tables are organized under the experimental MIB ("exmib"--number 26) in a six-level tree (instead of under the cct MIB).

exmib	Information base identifier
fr	Frame Relay managed object
<i>table variable</i>	dlctble or errtbl listed below
entry	Fixed entry
<i>data variable</i>	Data type
[cct #]	Circuit number
<i>table variable</i>	ccttbl listed below
entry	Fixed entry
<i>data variable</i>	Data type
[cct #]	Circuit number
<i>ddd</i>	dlci

The table variables are:

- Data Link Connection Management Interface Table (dlctble)
- Error Table (errtbl)
- Circuit Table (ccttbl)

Each circuit number ([cct #]) corresponds to the number assigned to that circuit in the "Circuit Name" listing in the first level of the "Circuits" menu in the main screen of the Configuration Editor.

Figure 18- shows this organization.

The Management Information Base for Frame Relay contains the values for these tables, which are described in the following sections.

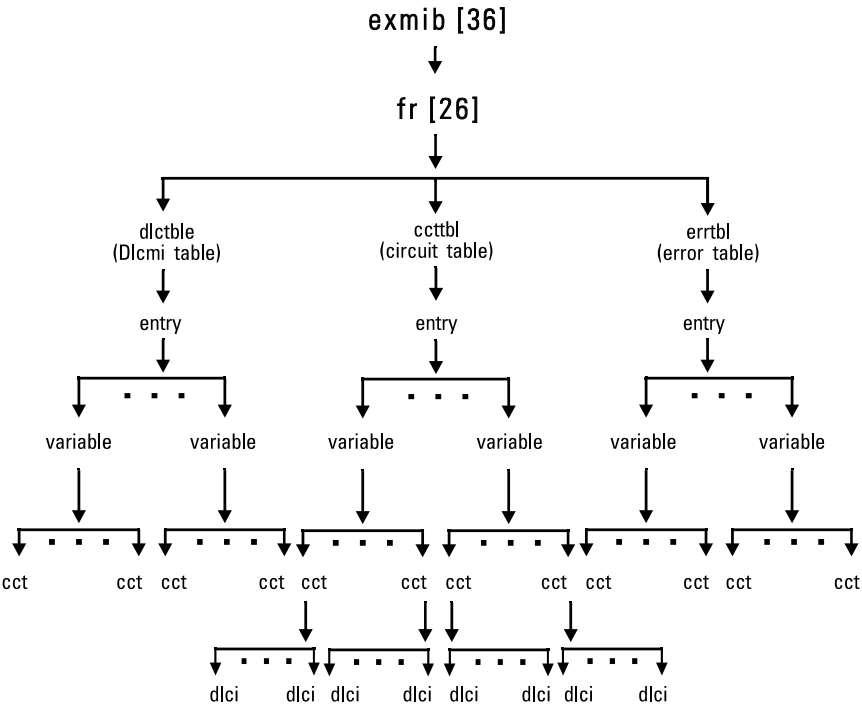


Figure 18-1. Frame Relay Exmib

Management Information Base Variables

cct: Circuits Information Base

Each frame relay MIB item can be accessed through the Network Command Language (NCL) from the console screen. Use the NCL list command to display all or a portion of the frame relay information base. Use the NCL get command to obtain the value of any variable within the information base. There are two methods of access, one using the names of the branches and the other using the numbers.

exmib.fr *table name.table entry*

where:

table name

is the name of the fr table, and

table entry

is the actual value of the table entry.

Or, using the second method of access:

36.26.1.1.5.8

where:

8 is the frame relay circuit number (which is system-assigned), and

5 is the MIB variable.

Data Link Connection Management Interface Table (dlctble)

The frame relay MIB variables, in alphabetical order, for the Data Link Connection Management Interface Table are as follows:

active States which data link connection management scheme is active and, by implication, which DLCI it uses, on the frame relay interface. There are four possible values:

Disabled (1) indicates that there is no interface management running on this interface.

LmiRev1 (2) is the original Local Management Interface (LMI).

ansiT1-617-D (3) indicates the use of ANSI Annex D of ANSI T1-617.

ansiT1-617-B (4) indicates the use of ANSI Annex D of ANSI T1-617 (not supported by HP).

Access methods:

exmib.fr.dlctble.entry.active.cct #

36.26.1.1.2.cct #

where *cct #* indicates the circuit.

addr States that address format are in use on this frame relay interface. There are four possible values:

Q921 (1) specifies use of the first frame relay address format with support for a 13-bit DLCI with no DE, FECN, or BECN bit support. It is mostly obsolete with two-byte support only.

Q922March90 (2) specifies use of March 1990 draft of CCITT specification Q922 with support for an 11-bit DLCI with no DE bit.

Q922November90 (3) specifies use of November 90 draft of CCITT specification Q922 with support for all of Q922November90 plus a control byte in the extended address format.

Q9222 (4) specifies use of the final draft of CCITT specification Q922 with support for all of Q922November90 plus a control byte in the extended address format.

Access methods:

xmib.fr.dlctble.entry.addr.cct #

36.26.1.1.3.cct #

where *cct #* indicates the circuit.

addrlen States the address length, in octets, to be used over this interface. By agreement, all PVCs within a given interface must use the same encoding and encoding length for the DLCI (addresses). In the case of Q922 format, the length indicates the entire length of the address including the control portion.

exmib.fr.dlctble.entry.addrlen.cct #

36.26.1.1.4.cct #

where *cct #* indicates the circuit.

errthr Is the number of errors within a given monitored number of events necessary to cause the interface to be shut down. The default is three errors:

Management Information Base Variables

cct: Circuits Information Base

exmib.fr.dlctble.entry.errthr.cct #

36.26.1.1.7.cct #

where *cct #* indicates the circuit.

index Is the index into the Dlcmi table. It corresponds to the frame relay circuit for which table information is requested.

exmib.fr.dlctble.entry.index.cct #

36.26.1.1.1.cct #

where *cct #* indicates the circuit.

enqlnt Is the number of status enquiry intervals that pass before issuance of a full status enquiry message. The default is six intervals.

exmib.fr.dlctble.entry.enqlnt.cct #

36.26.1.1.6.cct #

where *cct #* indicates the circuit.

maxpvc Indicates the maximum number of permanent virtual circuits (PVCs) allowed for this interface. This is usually dictated by the frame relay network.

exmib.fr.dlctble.entry.maxpvc.cct #

36.26.1.1.9.cct #

where *cct #* indicates the circuit.

monevnt Is the number of events for which errors are collected in order to monitor for an interface shutdown due to excessive error. The default is four events.

exmib.fr.dlctble.entry.monevnt.cct #

36.26.1.1.8.cct #

where *cct #* indicates the circuit.

multicast Indicates whether the frame relay provider offers a multicast service. There are two possible values for this field:

nonBroadcast (1) for those networks that do not support multicasting, and broadcast (2) for those that do.

exmib.fr.dlctble.entry.multicast.cct #

36.26.1.1.10.cct #

where *cct #* indicates the circuit.

pollint Is the number of seconds between successive status enquiry messages. The default value is ten seconds.

exmib.fr.dlctble.entry.pollint.cct #

36.36.1.1.5.cct #

where *cct #* indicates the circuit.

Frame Relay Circuit Table Variables (ccttbl)

The circuit table contains information about the various connections (PVCs) that are presently defined within the frame relay interface. The frame relay MIB variables, in alphabetical order, for the circuit table are:

becn Is the number of frames received from the network indicating backward congestion since the circuit was created.

exmib.fr.ccttbl.entry.becn.cct #.ddd

36.26.2.1.5.cct #.ddd

where *cct #* indicates the circuit and *ddd* indicates the dlci.

crted Is the value of sysUpTime when the circuit was created, whether by the data link connection management or by a set request.

exmib.fr.ccttbl.entry.crted.cct #.ddd

36.26.2.1.10.cct #.ddd

where *cct #* indicates the circuit and *ddd* indicates the dlci.

dlci Is the data link connection identifier for this circuit.

exmib.fr.ccttbl.entry.dlci.cct #.ddd

36.26.2.1.2.cct #.ddd

where *cct #* indicates the circuit and *ddd* indicates the dlci.

fecn Is the number of frames received from the network indicating forward congestion since the circuit was created.

Management Information Base Variables

cct: Circuits Information Base

exmib.fr.ccttbl.entry.fecn.*cct #.ddd*

36.26.2.1.4.*cct #.ddd*

where *cct #* indicates the circuit and *ddd* indicates the dlci.

f_rcvd Is the number of frames received over this circuit since it was created.

exmib.fr.ccttbl.entry.f_rcvd.*cct #.ddd*

36.26.2.1.8.*cct #.ddd*

where *cct #* indicates the circuit and *ddd* indicates the dlci.

f_sent Is the number of frames sent from this circuit since it was created.

exmib.fr.ccttbl.entry.f_sent.*cct #.ddd*

36.26.2.1.6.*cct #.ddd*

where *cct #* indicates the circuit and *ddd* indicates the dlci.

index Is the circuit corresponding to the Frame Relay interface.

exmib.fr.ccttbl.entry.index.*cct #*

36.26.2.1.1.*cct #*

where *cct #* indicates the circuit.

change Is the value of sysUpTime when last there was a change in the circuit state.

exmib.fr.ccttbl.entry.change.*cct #.ddd*

36.26.2.1.11.*cct #.ddd*

where *cct #* indicates the circuit and *ddd* indicates the dlci.

octets Indicates the number of octets received over this circuit since it was created.

exmib.fr.ccttbl.entry.o_rcvd.*cct #.ddd*

36.26.1.9.*cct #.ddd*

where *cct #* indicates the circuit and *ddd* indicates the dlci.

o_sent Indicates the number of octets sent from this circuit since it was created.

exmib.fr.ccttbl.entry.o_sent.cct #.ddd

36.26.2.1.7cct #.ddd

where *cct #* indicates the circuit and *ddd* indicates the dlci.

state Indicates whether the particular circuit is operational. These entries are created by the Data Link Connection Management exchange. There are three possible values for this entry:

Invalid (1) is used to delete an entry manually.

Active (2) is an indication that the circuit is up and ready for use.

Inactive (3) is used to show that the circuit is present but not ready for use.

exmib.fr.ccttbl.entry.state.cct #.ddd

36.26.2.1.3.cct #.ddd

where *cct #* indicates the circuit and *ddd* indicates the dlci.

Frame Relay Error Table Variables

This table describes errors encountered on the Frame Relay interface. It is indexed by circuit number. The error table variables, in alphabetical order, are as follows:

data Is an octet string containing as much of the error packet as possible. As a minimum, it must contain the two octets of the DLCI.

exmib.fr.errtbl.entry.data.cct #

36.26.3.1.3.cct #

where *cct #* indicates the circuit.

index Is the index into the error table that corresponds to the circuit number.

exmib.fr.errtbl.entry.index.cct #

36.26.3.1.1.cct #

where *cct #* indicates the circuit.

Management Information Base Variables

cct: Circuits Information Base

time Is the value of sysUpTime at which the error was detected.

exmib.fr.errtbl.entry.time.cct #

36.26.3.1.4.cct #

where *cct #* indicates the circuit.

type Is the type of error that was last seen on this interface. The following values are valid for this field:

- unknownErr (1)
- receiveShort (2)
- receiveLong (3)
- illegalDLCI (4)
- unknownDLCI (5)
- ImiProtoErr (6)
- ImiUnknownIE (7)
- ImiSequenceErr (8)
- ImiUnknownRpt (9)

exmib.fr.errtbl.entry.type.cct #

36.26.3.1.2.cct #

where *cct #* indicates the circuit.

Ethernet/802.3

alig_error_rx contains the number of non-aligned frames received by circuit *cct*. A non-aligned frame does not end on a byte boundary.

babl_error_tx contains the number of babbles on circuit *cct*. A babble occurs when the transmitter portion of the local area controller (SONIC) transmits an Ethernet or IEEE 802.3 frame containing more than 1518 bytes (this byte count does *not* include the 64-bit frame preamble and synchronization bits). In such an instance, the transmitter completes sending the entire frame, and increments this counter.

buferr_tx contains the number of transmit buffer errors. A transmit buffer error indicates corruption of the transmit descriptor ring associated with circuit *cct*. Usually such corruption takes the form of a break in the data chain (a series of pointers to multiple buffers that contain consecutive portions of a lengthy frame). A transmit buffer error disables the transmitter portion of the local area controller (SONIC).

byte_cnt_mismatch contains the number of times a packet is dropped due to the transmit packet size field not being equal to the transmit packet fragment size field.

cerr contains the number of transceiver self-test failures on circuit *cct*. Some transceivers assert the collision signal during the interpacket delay period to verify the channel between the transceiver and the local area controller (SONIC). Such self-tests are usually referred to as SQE (Signal Quality Error) or “heartbeat”. A test failure (defined as the absence of a collision signal within 2.0 μ s of the cessation of transmission) may indicate transceiver malfunction or a faulty transmission path between the SONIC and the transceiver.

deferred_tx contains the number of deferred transmissions on circuit *cct*. A deferred transmission indicates that the physical medium was busy (the carrier sense signal was *.TRUE.*) when the local area controller (SONIC) had a frame for transmittal. In such an instance, the SONIC waits for the carrier sense signal to go to *.FALSE.*, pauses for an interframe spacing interval, and then attempts to transmit the waiting frame.

dls_ret_rx contains the number of frames, received by circuit *cct*, that were later returned by the data-link service (DLS) software. Within the router software architecture, DLS resides between the driver and application software. It performs such services as multiplexing/demultiplexing or encapsulation/deencapsulation. DLS can return frames for numerous reasons (many of which are application-specific): for example, because of unknown internal service access points (ISAPs), because of user-specified filtering requirements contained within the configuration, or because of lack of enabled entities (for example, IP, IPX, etc.).

dls_ring_cnt contains the current number of packets received by circuit *cct* and currently in transit to data-link service (DLS).

excessv_colln_tx contains the number of excessive collision errors on circuit *cct*. An excessive collision error occurs when the local area controller (SONIC) has detected collisions on the medium in 16 successive attempts to transmit a frame. After 16 unsuccessful transmission attempts, the SONIC drops the frame, increments this counter, and transmits the next frame on its transmit queue.

Management Information Base Variables

cct: Circuits Information Base

fcs_error_rx contains the number of frames received by circuit *cct* that contained an erroneous checksum.

frames_rx_per_sec contains the number of frames that this circuit has received in the last second.

frames_tx_per_sec contains the number of frames that this circuit has transmitted in the last second.

frames_rx_ok contains the number of frames received without error by circuit *cct*.

frames_tx_ok contains the number of frames transmitted without error by circuit *cct*.

frams_incomp_rx contains the number of incomplete frames received by circuit *cct*. An incomplete frame is identified by failure to set the end-of-packet bit in the receive message descriptor.

lack_resc_error_rx contains the number of times circuit *cct* lost frames because of insufficient buffer space.

late_colln_tx contains the number of late collisions on circuit *cct*. A late collision is one detected after the transmission of at least 64 bytes. In such an instance, the local area controller (SONIC) does *not* retransmit the frame. Rather, it terminates the transmission, increments this counter, and transmits the next frame in its transmit queue.

lcar_tx contains the number of instances of carrier loss on *cct*. Loss of carrier indicates that the input (receive enable signal) went *.FALSE.* during a controller-initiated transmission.

mac_addr contains the 12-digit hexadecimal representation of the 48-bit station address used by circuit *cct*.

merr contains the number of memory errors. A memory error indicates that the local area controller (SONIC), after becoming bus master, failed to receive a ready signal within 25.6 μ s of asserting a memory address on the data/address bus. A memory error disables the SONIC.

octets_rx_per_sec contains the number of octets that this circuit has received in the last second.

octets_tx_per_sec contains the number of octets that this circuit has transmitted in the last second.

octets_rx_ok contains the number of octets (bytes) received without error by circuit *cct*.

octets_tx_ok contains the number of octets (bytes) transmitted without error by circuit *cct*.

oflo_rx contains the total number of overflows on circuit *cct*. An overflow occurs when the local area controller (SONIC) could not keep pace with flow of incoming data and lost part or all of an incoming frame.

peak_frames_rx contains the peak number of frames that this circuit has received in any given second since reboot.

peak_frames_tx contains the peak number of frames that this circuit has transmitted in any given second since reboot.

peak_octets_rx contains the peak number of octets that this circuit has received in any given second since reboot.

peak_octets_tx contains the peak number of octets that this circuit has transmitted in any given second since reboot.

to_long_error_rx contains the number of frames received by circuit *cct* that exceeded 1518 bytes in length (this count does *not* include the 64-bit frame preamble and synchronization bits).

total_rx_error contains the total number of receive errors on circuit *cct*. This value equals the sum of *alig_error_rx*, *fcs_error_rx*, *frams_incomp_rx*, *lack_resc_error_rx*, *oflo_rx*, and *to_long_error_rx*.

total_tx_error contains the total number of transmit errors on circuit *cct*. This value equals the sum of *babl_error_tx*, *bufferr_tx*, *excessv_colln_tx*, *late_colln_tx*, *deferred_tx*, *lcar_tx*, and *uflo_tx*.

tx_congestion contains the number of times a buffer wasn't available to transmit a frame.

Management Information Base Variables

cct: Circuits Information Base

uflo_tx contains the total number of underflows on circuit *cct*. An underflow occurs when the transmitter portion of the local area controller (SONIC) truncates a frame because of the late receipt of data from memory.

PPP (Industry-Standard Point-to-Point Protocol) Circuits

The PPP information contains the PPP MIB Link Quality Table and PPP circuit event messages. The PPP MIB variables for the Link Quality Table are organized under

`exmib.ppp.link_quality_table.entry`

and are separate from the general WAN Circuits variables (page 18-14). Use NCL's List command to display all or a part of the ppp information base, and use NCL's Get command to obtain the value of any variable within the information base.

The structure is the following:

```
exmib
  ppp
    link_quality_table.entry
      variables          listed below
      cct #             stands for the PPP circuit number
```

The pathname is constructed as follows:

`exmib.ppp.link_quality_table.entry.variable.cct`
or `36.18.4.1.variable#.cct#`

The variables are listed alphabetically:

index Is a unique value for each PPP link interface. The index value is the circuit number of the PPP circuit.

in_rx_bytes Is a 32-bit state variable indicating the number of bytes that were received on the inbound link during the last period.

in_rx_pkts Is a 32-bit state variable indicating the number of packets that were received on the inbound link during the last period.

in_tx_bytes Is a 32-bit state variable indicating the number of bytes that were transmitted on the inbound link during the last period. In other words, `in_tx_bytes` indicates the number of bytes the remote peer station transmitted during the last period.

Management Information Base Variables

cct: Circuits Information Base

in_tx_lqrs Is an eight-bit state variable indicating the number of Link Quality Report (LQR) packets that the remote peer remote station had to transmit so that the local end could receive exactly one LQR. The `in_tx_lqrs` variable defines the length of the period over which `in_tx_packets`, `in_tx_bytes`, `in_rx_packets`, and `in_rx_bytes` were measured.

in_tx_pkts Is a 32-bit state variable indicating the number of packets that were transmitted on the inbound link during the last period. In other words, `in_tx_pkts` indicates the number of packets the remote peer station transmitted during the last period.

last_out_tx_bytes Is a 32-bit state variable storing the value of the `Out-Tx-Octets-Ctr` from the last received Link Quality Report packet. In other words, `last_out_tx_bytes` indicates the total number of bytes transmitted by the remote peer station since the LCP reached the *open* state.

last_out_tx_pkts Is a 32-bit state variable storing the value of the `Out-Tx-Packets-Ctr` from the last received Link Quality Report packet. In other words, `last_out_pkts` indicates the total number of packets transmitted by the remote peer station since the LCP reached the *open* state.

last_in_rx_bytes Is a 32-bit state variable storing the value of the `In-Rx-Bytes-Ctr` from the last received Link Quality Report packet. In other words, `last_in_rx_bytes` indicates the total number of bytes received by the peer (remote) station since the LCP reached the *open* state.

last_in_rx_bytes

last_in_rx_pkts Is a 32-bit state variable storing the value of the `In-Rx-Packets-Ctr` from the last received Link Quality Report packet. In other words, `last_in_rx_pkts` indicates the total number of packets received by the peer (remote) station since the LCP reached the *open* state.

pppLinkQualityEntry {pppLinkQualityTable1} Provides Link Quality Management information about a particular PPP link.

Token Ring Circuits

adpt_bad_dio_par contains the number of times the token-ring adapter detected a bad parity value on data passed to the adapter through a direct I/O access.

adpt_dma_rd_abort contains the number of times the token-ring adapter aborted a direct-memory-access read operation. This could be caused by excessive parity errors, excessive bus errors, or the expiration of a 10-second timer while waiting for a directory-memory-access bus operation to complete.

adpt_dma_wr_abort contains the number of times the token-ring adapter aborted a direct-memory-access write operation. This could be caused by excessive parity errors, excessive bus errors, or the expiration of a 10-second timer while waiting for a directory-memory-access bus operation to complete.

adpt_parity_err contains the number of times the token-ring adapter detected a bus parity error on the adapter's internal bus.

adpt_ring_underrun contains the number of times the token-ring adapter detected an internal direct-memory-access underrun when receiving from the ring.

frames_rx_per_sec contains the number of frames that this circuit has received in the last second.

frames_tx_per_sec contains the number of frames that this circuit has received and transmitted in the last second.

log_ari_fci_err contains the number of times the token-ring adapter detected that its upstream neighbor was unable to set the address-recognized indicator or frame-copied indicator bit of received frames.

log_burst_err contains the number of times the token-ring adapter detected the absence of signal transitions for five half-bit times between the starting and ending delimiters, or between the ending and starting delimiters.

Management Information Base Variables

cct: Circuits Information Base

log_dma_bus_err contains the number of direct-memory-access bus errors that do not exceed the abort threshold.

log_dma_par_err contains the number of direct-memory-access parity errors that do not exceed the abort threshold.

log_frm_cpy_err contains the number of times the token-ring adapter (while in the receive/repeat mode) recognized a frame addressed to its specific address but found the address-recognized-indicator bits not equal to zero. This indicates a possible line hit or duplicate address.

log_line_err contains the number of times the token-ring adapter (while in the receive/repeat mode) recognized a line error. A line error is recorded when (1) a code violation exists between the starting and ending delimiters of a frame, (2) a code violation exists in a token, or (3) a frame check sequence error exists.

log_lost_frm contains the number of times the token-ring adapter (while in the transmit/stripping mode) failed to receive the end of a frame that it had previously transmitted.

log_rx_congest contains the number of times the token-ring adapter (while in the repeat mode) recognized a frame addressed to its specific address.

log_token_err contains the number of times a token-ring adapter in an active monitoring station detected an error with the token protocol. The errors may be the following:

- A token with a nonzero priority has the monitor count bit equal to one, indicating a circulating high-priority token.
- A frame has the monitor count bit equal to one, indicating a circulating frame.
- No token or frame is received within a 10-millisecond window.
- The starting delimiter/token sequence has a code violation in an area where code violations must not occur.

octets_rx_per_sec contains the number of octets that this circuit has received in the last second.

octets_tx_per_sec contains the number of octets that this circuit has transmitted in the last second.

peak_frames_rx contains the peak number of frames that this circuit has received in any given second since reboot.

peak_frames_tx contains the peak number of frames that this circuit has transmitted in any given second since reboot.

peak_octets_rx contains the peak number of octets that this circuit has received in any given second since reboot.

peak_octets_tx contains the peak number of octets that this circuit has transmitted in any given second since reboot.

ring_auto_rem contains the number of times the token-ring adapter detected an internal hardware error, either within the chip set itself, or within the physical-star wiring (*lobe*) between the adapter and the wire concentrator. The token-ring adapter is removed from the ring after detecting the error.

ring_cnt_overflow contains the number of times the token-ring adapter error counter incremented from 254 to 255.

ring_hard_err contains the number of times the token-ring adapter transmitted or received beacon frames to or from the ring. The beacon processor is used to recover the ring after a ringstation has sensed a hard error, which renders the ring inoperable. Hard errors are caused by (1) wire faults, (2) frequency errors, or (3) incoming signal loss. The station that detects such a hard error transmits, or "beacons", information that isolates the failure location.

ring_lobe_wire contains the number of times the token-ring adapter detected a short or open circuit between the adapter and the wire concentrator.

ring_one_station contains the number of times the token-ring adapter sensed that it was the only station on the ring.

ring_recover contains the number of times the token-ring adapter observed claim token frames on the ring. A ring station transmits a

Management Information Base Variables

cct: Circuits Information Base

claim token frame when it detects that the ring does not contain an active monitor, or that the active monitor is not functioning properly.

ring_rem_station contains the number of times the token-ring adapter removed itself from the ring after receiving a remove ring station frame. A remove ring station frame is issued from the network manager and forces an adapter to remove itself from the ring.

ring_sig_loss contains the number of times the token-ring adapter detected a loss of signal on the ring.

ring_soft_err contains the number of report error frames transmitted by the token-ring adapter. A report error frame is transmitted in response to a soft error. A soft error is one that temporarily degrades system performance but may be recovered using standard adapter protocols.

ring_tx_beacon contains the number of times the token-ring adapter transmitted beacon frames to the ring. A beacon frame indicates a hard error. This count specifies the number of hard errors detected by the adapter; the difference between this count and ring_hard_err specifies the number of hard errors detected by other ring stations.

rx_frm_cmpi (rint) contains the number of times the token-ring adapter received a frame and then generated an adapter-to-attached-system interrupt. Such an interrupt is enabled or disabled by the frame interrupt bit (bit 4 of RECEIVE_CSTAT). Because frames can be received faster than the adapter can cause the interrupts, each increment of this counter can report the reception of one or multiple frames.

rx_suspended contains the number of times the token-ring adapter processed a receive parameter list containing both an odd address in the forward pointer field (indicating the end of the list) and an end frame bit equal to 0 (indicating more to follow).

total_adapt_error contains the aggregate count of token-ring adapter hardware or software errors, the sum of the counts of adpt_bad_dio_par, adpt_dma_rd_abort, adpt_dma_wr_abort, adpt_parity_err, and adpt_ring_underrun variables.

total_log_error contains the aggregate count of token-ring adapter log errors, the sum of the counts of log_ari_fci_err, log_burst_err, log_dma_bus_err, log_dma_par_err, log_frm_cpy_err, log_line_err, log_lost_frm, log_rx_congest, and log_token_err variables.

total_ring_error contains the aggregate count of ring errors, the sum of the counts of ring_auto_rem, ring_cnt_overflow, ring_hard_err, ring_lobe_wire, ring_one_station, ring_recover, ring_rem_station, ring_sig_loss, ring_soft_err, and ring_tx_beacon variables.

total_rx_error contains the sum of the counts of log_rx_congest and rx_suspended variables.

total_tx_error contains the sum of the counts of tx_frm_cmpl, tx_frm_err, tx_frm_size_err, tx_ill_frm_fmt, tx_list_err, tx_odd_adr, and tx_threshold variables.

tx_frm_cmpl (tint) contains the number of times the token-ring adapter transmitted a frame and then generated an adapter-to-attached-system interrupt. Such an interrupt is enabled or disabled by the frame interrupt bit (bit 4 of TRANSMIT_CSTAT). Because frames can be transmitted faster than the adapter can cause the interrupts, each increment of this counter can report the transmission of one or multiple frames.

tx_frm_err contains the number of times the token-ring adapter recorded a transmit frame error. A transmit frame error occurs when the token-ring adapter finds an erroneous start frame bit (bit 2 of TRANSMIT_CSTAT). Either the bit is equal to 1 on a list that is not the anticipated start of a frame, or the bit is equal to 0 on an anticipated start of a frame.

tx_frm_size_err contains the number of times the token-ring adapter recorded a transmit frame size error. A transmit frame size error occurs when (1) the frame size count (bytes 7 and 8 of the transmit parameter list) is not equal to the sum of the data count fields contained in the parameter list, (2) when the frame size count is less than the required header plus one byte of the I (Information) field date, or (3) when the frame size count is equal to 0 (except in lists that define I frames).

Management Information Base Variables

cct: Circuits Information Base

tx_ill_frm_fmt contains the number of times the token-ring adapter recorded an illegal frame format error. An illegal frame format error occurs when bit 0 of the frame control (FC) field is equal to 1.

tx_list_err contains the number of times the token-ring adapter recorded an error in one of the lists that compose the frame. The token-ring adapter terminates the Transmit command; the attached system must issue another Transmit command to continue.

tx_odd_adr contains the number of times the token-ring adapter processed a transmit parameter list containing both an odd address in the forward pointer field (indicating the end of the list) and an end frame bit equal to 0 (indicating more to follow).

tx_threshold contains the number of times the token-ring adapter recorded a transmit threshold error. A transmit threshold error occurs when the frame size count (bytes 7 and 8 of the transmit parameter list) exceeds the buffer capacity allocated at system initialization.

chassis: Chassis Information Base

The chassis information base contains variables that describe various chassis elements in the HP Router 650. The structure is the following:

```
chassis
  id[0]
  slots[0]
  slot_table.entry
    variables
    instance
  entity_table.entry
    variables
    instance
  slotmap_table.entry
    variables
    instance
  sensor_table.entry
    variables
    instance
```

Examples of pathname constructions are:

```
chassis.id.0
chassis.slot_table.entry.variable[instance]
or 58.3.1.variable#[instance]
```

The variables are listed alphabetically under each table type.

Management Information Base Variables

chassis: Chassis Information Base

ID[0] contains a unique identifier for this chassis.

slots[0] contains the number of slots in this chassis.

Slot_Table

Example:

```
get chassis.slot_table.entry.objectid.slot#
```

descr[slot#] contains a textual description of the card plugged into *slot#*.

index[slot#] contains the index number for *slot#*.

lastchange[slot#] contains a time stamp showing the time interval between initialization of the router engine module and the module in *slot#*.

objectid[slot#] contains the authoritative identification of the card plugged into *slot#*.

Entity_Table

Example:

```
get chassis.entity_table.entry.entity_table variable.1
```

descr[1] contains a textual description of the HP Router 650.

function[1] contains the generic function provided by the HP Router 650.

index[1] contains the entity number for the HP Router 650.

Name[1] contains the local name by which entity i is known.

objectid[1] contains the authoritative identification of the HP Router 650.

timestamp[1] should always be 0.

Slotmap_Table

Example:

```
get chassis.slotmap_table.entry.slot[slot#][1]
```

entity[slot#][1] contains the entity number for slot# on the HP Router 650.

slot[slot#][1] contains the slot number for slot# on the HP Router 650.

Sensor_Table

These variables report the status of the power supply, fan, and internal temperature in HP Router 650 chassis.

Example:

```
get chassis.sensor_table.entry.sensor_table variable[sensor #]
```

descr[sensor#] contains a textual description of the sensor.

failures[sensor#] contains the number of times the sensor's status has changed to BAD.

index[sensor#] contains the sensor index number for *sensor#*.

number[sensor#] contains a unique number for similar sensors.

objectid[sensor#] contains the authoritative identification of the indicated sensor.

status[sensor#] contains the status of the sensor. Status categories are:

Management Information Base Variables

chassis: Chassis Information Base

- 1: UNKNOWN Status of the object monitored by the sensor is unknown.
- 2: BAD The object monitored by the sensor may be inoperable or operating outside of the proper range.
- 3: WARNING The object monitored by the sensor is operating close to the limit of the proper range.
- 4: GOOD The object monitored by the sensor is within the proper operating range.

warnings[*sensor#*] contains the number of times the sensor's status has changed to WARNING.

config: Configuration Information Base

The “config” information base contains variables identifying router hardware and software. The major structure for config (excluding variables) is:

version[0]	the version variable, listed first below
key	Key to available services
cct_table	Circuit branch
cct_tbl_entry	
cgr_table	Circuit Group branch
cgr_tbl_entry	
lb_table	Bridge branch
lb_cgtbl_entry	
at_table	AppleTalk branch
at_cgtbl_entry	
drs_table	DECnet branch
drs_cgtbl_entry	
ip_table	IP branch
ip_iftbl_entry	
xrx_table	XNS branch
xrx_iftbl_entry	
ipx_table	IPX branch
ipx_iftbl_entry	
num_egp[0]	

Management Information Base Variables

config: Configuration Information Base

Pathnames for the List and Get commands are constructed as shown in the following examples:

```
get config.version.0
list config.key.*
list config.cct_table.*
get config.ip_table.ip_iftbl_entry.*
get 35.14.1.3.cct #
```

Version

version[0] contains the operating code version number (also known as software or firmware). For example, a software version such as A.08.01 is described as follows:

A the function set available in your router
08 the common release number
01 updates to the current common release

Key

The Key variables inform you of whether a particular variable can be configured on the router. For each of the variables:

- A value of 1 means the service can be configured
- A value of 0 means the service is not available for configuration on this model router

at AppleTalk routing service

drs DECnet routing service

fr Frame Relay circuit services

ip IP routing service (the TCP/IP protocol suite)

ipx IPX routing service

lb Bridge service

osi OSI routing

smlds SMDS services

x25 X.25 circuit services

xns XNS routing service

Circuit Table

cct_indx[*cct #*] circuit number

cct_type[*cct #*] circuit type.

cct_name[*cct #*] circuit name, such as “Ether 1”

cct_slot[*cct #*] slot number

cct_pam[*cct #*] physical access method

cct_port[*cct #*] physical port number, viewing from left to right and from top to bottom

Circuit Group Table

cgr_indx[*cgt #*] contains circuit group number

cgr_name[*cgt #*] contains circuit group name, such as “WAN1G”

Bridge Table

lb_indx[*index*] index

lb_cgr_num[*index*] circuit group number

Management Information Base Variables

config: Configuration Information Base

AppleTalk Table

at_indx[*interface* #] AppleTalk interface index

at_cgr_num[*interface* #] AppleTalk interface index

at_if_addr[*interface* #] address for interface

DECnet Table

drs_indx[*interface* #] DECnet interface number

drs_cgr_num[*interface* #] circuit group number

adrsif_addr[*interface* #] address for interface

IP Table

ip_if_indx[*interface* #] interface num

ip_cgr_num[*interface* #] circuit group number

ip_if_addr[*interface* #] IP address for interface

XNS Table

xrx_if_indx[*interface* #] XNS interface number

xrx_cgr_numx[*interface* #] circuit group number

xrx_if_addrx[*interface* #] XNS address for interface

IPX Table

- px_if_indx[*interface*]** IPX interface number
- ipx_cgr_num[*interface*]** circuit group number
- ipx_if_addr[*interface*]** address for interface

dev: Device Information Base

The “dev” information base contains a single control object whose sole function is to generate system management messages. The single-level structure is the following:

dev

decnet: DECnet Configuration Information Base

The DECnet configuration “decnet” information base contains variables that describe DECnet global and interface-specific configuration parameters. The structure is the following:

decnet	
<i>variables</i>	the global variables, listed below (see “Global” subheading)
iftab.if	the interface-specific branch (see “Interface Specific” subheading)
<i>variables</i>	the interface-specific variables, listed below
[n]	the interface number assigned by the router

The pathnames are constructed as follows:

decnet.*variable*
decnet.iftab.if.*variable*[*n*]

The variables are listed alphabetically under the two branches:

Global

- amaxcst** contains the maximum inter-area transit cost.
- amaxhop** contains the maximum number of areas that a packet can traverse from source to destination.
- area** contains the number of the local DECnet area.
- bcrtimer** contains the time interval between topology packets.
- enadj** contains the maximum number of adjacent nodes.
- maxarea** contains the number of areas in the network.

Management Information Base Variables

decnet: DECnet Configuration Information Base

maxnode contains the maximum number of nodes per network area.

maxvisit contains the maximum number of times a packet can pass through the same router.

nmaxcst contains the maximum node-to-node transit cost.

nmaxhop contains the maximum number of hops that a packet can transit from source to destination.

node contains the router's DECnet node number.

state contains the router state: 1 indicates that the router is enabled and forwarding packets; 2 indicates that the router is disabled.

Interface Specific

cost contains the relative circuit cost assigned to the interface.

cname contains the name of the circuit group that enables the DECnet interface.

htime contains the time interval between DECnet hello packets.

index contains the router-assigned interface number.

numrtr contains the number of routers associated with the interface.

rprior contains the router priority.

state contains the interface state: 1 indicates that the router is enabled and forwarding packets; 2 indicates that the router is disabled.

dls: Data Link Services Information Base

The Data Link Services information base contains variables that access the data link statistics for configured circuits. The structure is:

dls
 cct name circuit name
 variables listed below

The pathnames are constructed as shown in the following examples:

dls.*variable*
dls.*cct name.variable*

re_rx_dma_ring_cnt This stat shows the number of packets in the circuit's DLS receive ring. This statistic exists only on the routing engine for HP series 600 routers. There is a DLS receive ring per circuit. The circuit's DLS RX ring is filled by the routing engine as it pulls global packet buffer pointers from the interface module that owns the circuit.

rx_dma_drops These are the number of received packets dropped by an interface module due to global packet memory congestion (that is, lack of global packet buffers). This situation occurs when the routing engine cannot keep up with the aggregate packet input rate. The interface module sees that the RE is out of global buffers, so it drops the incoming packets.

test_cmd_rx contains the number of 802.2 Logical Link Control (LLC) Test commands received by circuit cct. Test commands seek to provide a basic verification of the LLC-to-LLC transmission path. The value contained in this variable should equal the value contained in test_rsp_tx.

test_cmd_tx contains the number of 802.2 Logical Link Control (LLC) Test commands issued on circuit cct. The value contained in this variable should be 0, as should the value of test_rsp_rx.

Management Information Base Variables

dls: Data Link Services Information Base

test_rsp_rx contains the number of 802.2 Logical Link Control (LLC) Test responses received by circuit cct. Receipt of a Test response requires the previous transmission of a Test command. The value contained in this variable should be 0, as should the value of test_cmd_tx.

test_rsp_tx contains the number of 802.2 Logical Link Control (LLC) Test responses issued on circuit cct. Test responses reply to Test commands and verify the LLC-to-LLC transmission path. The value contained in this variable and the value contained in test_cmd_rx should be equal.

tx_cct_ring_cnt This statistic shows the number of packets in the circuit's transmit ring. The protocols dump packets whose forwarding decision has been made into the transmit rings (1 per circuit). The drivers pull the packets out of the transmit rings and queue them to the network interface device for transmitting on the media. This statistic is valid on HP series 200 or 400 routers, and for interface modules on HP series 600 routers.

tx_dma_drops These are the number of transmit packets dropped by an interface module due to local port module packet memory congestion (that is, a lack of local packet buffers). This occurs when the output link on the interface module cannot keep up with the rate at which packets are being sent to it by the routing engine.

unrecog_pdu contains the number of unrecognized 802.2 Logical Link Control protocol data units (PDUs) received by circuit cct. An unrecognized PDU is one whose control field indicates other than a UI (Unnumbered Information) frame, an XID (Exchange Identification) frame, or a Test frame.

xid_cmd_rx contains the number of 802.2 Logical Link Control (LLC) XID (Exchange Identification) commands received by circuit cct. XID commands request LLC service-type and receive-window-capacity data from a remote host. The value contained in this variable should equal the value contained in xid_rsp_tx.

xid_cmd_tx contains the number of 802.2 Logical Link Control (LLC) XID commands issued on circuit cct. The value contained in this variable should be 0, as should the value of xid_rsp_rx.

Management Information Base Variables
dlis: Data Link Services Information Base

xid_rsp_rx contains the number of 802.2 Logical Link Control (LLC) XID responses received by circuit cct. Receipt of an XID response requires the previous transmission of an XID command. The value contained in this variable should be 0, as should the value of xid_cmd_tx.

xid_rsp_tx contains the number of 802.2 Logical Link Control (LLC) XID responses issued on circuit cct. XID responses reply to XID commands and provide LLC service-type and receive-window-capacity data. The value contained in this variable should equal the value contained in xid_cmd_rx.

drs: DECnet Circuit Group Information Base

The DECnet routing service “drs” information base contains variables that describe transmission and reception activities across each DECnet circuit group; it also contains variables that describe the rejection of certain packets by the DECnet router. The structure is the following:

drs	
cg	circuit-group-specific branch (see subheading)
cgg	circuit group name
variables	listed below
total	the aggregate rejection branch (see subheading)
variables	listed below

The pathnames are constructed as follows:

 drs.cg.cgg.variable
 drs.total.variable

The variables are listed alphabetically under the two branches:

Circuit Group Specific

drop	contains the number of packets dropped by circuit group cgg.
trans_pkts_recv	contains the number of data packets received by circuit group cgg.
trans_pkts_sent	contains the number of data packets sent by circuit group cgg.

Aggregate Rejection

aged_pkt_loss contains the number of packets dropped by the DECnet router because the packet had transited too many routers prior to reaching its destination. The maximum number of routers that a packet can transit is determined by the Area Max. Hops and Max. Hops parameters. Area Max. Hops specifies the number of routers that a packet can transit before reaching its destination area; Max. Hops specifies the number of routers within an area that a packet can transit before reaching its destination node.

node_unreach contains the number of packets dropped by the DECnet router because the destination node (while within range) was unreachable.

node_out_of_range contains the number of packets dropped by the DECnet router because the destination node resided in an area having a number greater than that designated by the Max. Area parameter, or because the destination node number exceeded that designated by the Max. Nodes parameter.

oversized_pkt_loss contains the number of packets dropped by the DECnet router because the packet size exceeded the capacity of the transmission media.

pkt_format_error contains the number of packets dropped by the DECnet router because some portion of the packet header could not be parsed.

route_update_loss contains the number of topology packets dropped by the DECnet router because the packet contained information beyond the router's capacity.

echo: Echo Service Information Base

The TCP “echo” information base contains variables that describe the Transmission Control Protocol echo service. The structure is the following:

echo

variables listed below

The pathname is constructed as follows:

echo.*variable*

The variables are listed alphabetically:

mem_err contains the number of memory errors.

mem_use contains the total number of bytes used by the echo service.

no_mem contains the number of times echo was unable to function because of lack of memory resources.

rx_bytes contains the total number of bytes transmitted during echo sessions.

sess_cur contains the current number of echo sessions.

sess_tot contains the total number of echo sessions since the router last booted.

tx_bytes contains the total number of bytes received during echo sessions.

egp: EGP Information Base

The Exterior Gateway Protocol “egp” information base contains variables that describe the transmission and reception of messages by the EGP protocol. The structure is the following:

egp

variables listed below

The pathname is constructed as follows:

egp.variable

The variables are listed alphabetically:

bad_asn contains the number of received EGP messages that contained an unrecognized autonomous system number in the EGP header.

bad_cod contains the number of received EGP messages that contained an unrecognized value in the Code field of the EGP header.

bad_hel contains the number of unexpected Hello neighbor reachability messages received by EGP. A Hello message is unexpected when received from a passive peer.

bad_ihu contains the number of unexpected I Hear You neighbor reachability messages received by EGP. An I Hear You message is unexpected when received in the absence of a prior Hello message.

bad_stt contains the total number of received EGP messages that contained an unrecognized value in the Status field of the EGP header.

bad_sum contains the total number of received EGP messages that contained a faulty checksum in the EGP header.

bad_type contains the total number of received EGP messages that contained an unrecognized value in the Type field of the EGP header.

bad_ver contains the total number of received EGP messages that contained an invalid EGP version number in the EGP header. The router's EGP implementation supports EGP version 2.

Management Information Base Variables

egp: EGP Information Base

cmdoos contains the number of times EGP received an out-of-sequence command message. An out-of-sequence message indicates that a prior message, issued by an EGP peer, has been missed.

cmdrej contains the number of times EGP refused to respond to a received command. Such refusal could be generated by receipt of a neighbor acquisition message from an unknown autonomous system, or by receipt of a faulty EGP message (for example, one with a bad checksum) from a known neighbor.

err contains the number of times EGP received a message that, while appropriate for the router's current state, was otherwise erroneous.

mem_use contains the number of memory bytes used by the EGP protocol. Memory requirements include protocol overhead, the state machine model, and timers.

mem_wait contains the number of instances in which EGP delayed operations because of unavailable memory resources.

no_mem contains the number of instances in which EGP was unable to function because of insufficient memory resources.

nop contains the number of instances that EGP received an otherwise valid EGP message inappropriate or inapplicable to its current state.

pkts_rcv contains the total number of received EGP messages.

pkts_snt contains the total number of transmitted EGP messages.

sess_cur contains the current number of EGP peers. An EGP peer is a remote routing device with which the router exchanges routing information.

sess_tot contains the aggregate number of EGP peers. This counter is incremented when the router moves from the EGP Idle state to either the Acquisition state or Down state.

tmrrej contains the number of T3 (abort timer) timeouts.

hw: Hardware Information Base

The structure of the hardware “hw” information base is the following:

hw

[*slot #*] always “1” for HP Series 200 and 400 routers
 “1” through “5” for the HP Router 650

variables listed below

The pathname is constructed as follows:

hw[*slot #*].*variable*

The variables are listed alphabetically:

dram_size contains the number of bytes of DRAM (dynamic RAM) on this router.

flash_size contains the number of bytes of flash EPROM (electrically programmable ROM) on this router.

id contains the hardware model identification number.

prod_nm contains the HP product number for this router.

rom_ver contains the version number of the ROM used on this router.

sram_size contains the number of bytes of SRAM (static RAM) on this router.

ip: IP Information Base

The IP router “ip” information base contains variables that describe transmission and reception activities across each IP interface; it also contains variables describing the IP routing table. The structure is the following:

ip	
ip_interface	the interface-specific branch (see subheading)
ip-address	the IP address in dotted decimal notation
variables	the interface-specific variables
ip_route_table	the routing table branch (see subheading)
net_tree	
variables	the routing table variables

The pathnames are constructed as follows:

 ip.ip_interface.ip-address.variable
 ip.ip_route_table.net_tree.variable

The variables are listed alphabetically under the two branches:

Interface Specific

address contains the 32-bit IP address of interface *ip-address* expressed as a decimal integer.

drop.dest_unknown contains the number of IP datagrams dropped by interface *ip-address* because the IP header contained an unknown or corrupt IP destination address.

drop.filtered contains the number of IP datagrams dropped by interface *ip-interface* in response to source-address or destination-address filters established at router configuration.

drop.frag_error contains the number of IP datagrams dropped by interface *ip-interface* because of its inability to fragment a datagram. *ip-interface* forwards datagrams up to 1500 bytes in length; longer datagrams must be fragmented. Should the datagram originator forbid fragmenting (by setting the DF bit--Do Not Fragment--in the IP header), interface *ip-address* drops the datagram, increments this counter, and issues an Internet Control Message Protocol (ICMP) destination unreachable message.

drop.header_format contains the number of IP datagrams dropped by interface *ip-address* because of an unparseable or corrupt IP header.

drop.reassembly_busy contains the number of IP datagrams dropped by interface *ip-interface* because of the lack of resources at the message destination.

drop.ttl_exceeded contains the number of IP datagrams dropped by interface *ip-interface* because the IP header Time field had reached 0.

drop.xsumerror contains the number of IP datagrams dropped by interface *ip-interface* because of a faulty IP header checksum.

icmp_rx.dest_unreachable contains the number of ICMP destination unreachable messages received by interface *ip-address*. Such messages indicate that the originating node cannot route or deliver datagrams.

icmp_rx.echo_request contains the number of ICMP echo request messages received by interface *ip-address*. Such messages test whether a destination node is reachable.

icmp_rx.frag_error contains the number of ICMP destination unreachable messages with a Code field value of 4 (indicating that a datagram could not be fragmented) received by interface *ip-address*. Such messages indicate that an IP datagram previously routed through interface *ip-address* cannot be handled by a subsequent router.

icmp_rx.param_problem contains the number of ICMP parameter problem messages received by interface *ip-address*. Such messages report faulty IP datagram headers.

Management Information Base Variables

ip: IP Information Base

icmp_rx.redirect contains the number of ICMP redirect messages received by interface *ip-address*. Such messages inform the recipient of a more optimum IP route.

icmp_rx.ttl contains the number of ICMP time exceeded messages received by interface *ip-address*. Such messages are generated when a datagram's hop count reaches 0.

icmp_rx.xsum_error contains the number of received ICMP messages dropped by interface *ip-interface* because of a faulty ICMP checksum.

icmp_tx.dest_unreachable contains the number of ICMP destination unreachable messages transmitted by interface *ip-address*. Such messages indicate that the originating node cannot route or deliver datagrams.

icmp_tx.echo_reply contains the number of ICMP echo reply messages transmitted by interface *ip-address*. Such messages test whether a destination node is reachable.

icmp_tx.frag_error contains the number of ICMP destination unreachable messages with a Code field of 4 (indicating that a datagram could not be fragmented) transmitted by interface *ip-address*. Such messages indicate that *ip-address* cannot fragment an IP datagram longer than 1500 bytes, or that the DF bit (Do Not Fragment) of the IP datagram was set.

icmp_tx.param_problem contains the number of ICMP parameter problem messages transmitted by interface *ip-address*. Such messages report faulty IP headers.

icmp_tx.redirect contains the number of ICMP redirect messages transmitted by interface *ip-address*. Such messages inform the recipient of a more optimum IP route.

icmp_tx.ttl contains the number of ICMP time exceeded messages transmitted by interface *ip-address*. Such messages are generated when a datagram's hop count reaches zero.

mask contains the 32-bit subnet mask of interface *ip-address* expressed as an unformatted decimal integer.

rx contains the total number of IP datagrams received by interface *ip-address*.

tx contains the total number of IP datagrams transmitted by interface *ip-address*.

ulp contains the total number of IP datagrams delivered by the router to one of three upper-level protocols (Internet Control Message Protocol, Transmission Control Protocol, or User Datagram Protocol) for processing.

Routing Table

cache_hits contains the number of times the IP address was not found in the forwarding table and was found in the IP address cache, which contains the previous IP address found.

mem_used contains the number of bytes of memory used by the IP routing table.

node_count contains the current number of networks contained in the IP routing table.

node_depth contains the number of levels in the IP routing table.

search_count contains the number of searches through the IP routing table. Upon receiving a packet for forwarding, the router first checks its cache to determine the next hop to the destination address. If not found there, the router then accesses the IP routing table.

search_depth contains the total depth of searches through the routing tree.

ipx: IPX Information Base

The “ipx” information base is composed of: (1) a set of variables that describe transmission and reception of packets across each IPX interface, (2) a set of variables that describe aggregate Internet Datagram Protocol (IDP) activity, (3) an IPX addressing table, (4) a SAP table, and (5) an IPX routing table. You can also use NCL's Rgetir and Rgetis commands to access the tables. The structure is the following:

ipx	
if	the interface-specific IPX address (hexadecimal) branch (see subheading)
<i>variables</i>	the interface-specific variables
mib	the IDP protocol branch (see subheading)
idp	
<i>variables</i>	the IDP protocol variables

The pathnames are constructed as follows:

`ipx.if.variable`

`ipx.mib.idp.variable`

The variables are listed alphabetically under two branches:

Interface Specific

drop contains the total number of IDP datagrams dropped (for whatever reason) by interface *if*.

rx contains the total number of IDP datagrams received by interface *if*.

tx contains the total number of IDP datagrams transmitted by interface *if*.

ulp contains the total number of IDP datagrams delivered to be processed by an upper-level protocol (for example, RIP, Echo, Error).

Internet Datagram Protocol (IDP)

forwarding contains an integer switch indicating the node's function within the extended IPX network. A value of 1 indicates that the node is acting as a gateway (routes and forwards datagrams); a value of 2 indicates that the node is acting as a host (does not route and forward datagrams).

forwdatagrams contains the number of received IDP datagrams not addressed to the IPX router. The router attempts to forward these datagrams to their ultimate destination.

inadderrors contains the number of IDP datagrams discarded because of invalid destination address fields.

indelivers contains the number of IDP datagrams delivered to IDP user protocols (including Error Protocol).

indiscards contains the number of valid input IDP datagrams discarded because of insufficient router resources (lack of buffer space).

inherrors contains the number of IDP datagrams discarded because of errors in their IDP headers. Such errors include faulty checksums, format errors, and transport control (hop count) errors.

inreceives contains the total number of all IDP datagrams (including those received in error) received from all interfaces.

inunknownprotos contains the number of IDP datagrams discarded because of an incorrect or corrupted value in the Protocol Type field in the IDP header.

outdiscards contains the number of valid output IDP datagrams discarded because of insufficient router resources (lack of buffer space).

outnoroutes contains the number of IDP datagrams discarded because no route could be found to transmit them to their destination.

outrequests contains the number of IDP datagrams generated by local IDP user protocols (including Error).

isdn: ISDN (V.25 bis) Information Base

The “isdn” information base contains variables for V.25 bis lines through a terminal adapter (manual or automatic dialing). The structure is the following:

isdn	V.25 bis
adapter	the terminal adapter branch (see subheading)
ccttbl	V.25 bis circuit table
<i>variables</i>	the terminal adapter variables, listed below
<i>cct #</i>	the circuit number as an index
mapping	the IP-mapping branch
ipmapping	
<i>variables</i>	the IP-mapping variables, listed below
<i>instance</i>	map entry or other variable

The pathnames are constructed as follows:

```
isdn.adapter.ccttbl.variable.cct#  
or 49.1.1.variable#[cct#]  
isdn.mapping.ipmapping.variable[instance]  
or 49.2.1.variable#[instance]
```

The variables are listed alphabetically under two branches:

V.25 bis Adapter

bandwidth[*cct#*] contains the maximum bandwidth allowed for an outbound connection. This value is only used when the V.25 bis extensions are set for per channel bandwidth and maximum channels to aggregate. (Value = per channel Bandwidth * Max channels to aggregate.)

cctname[*cct#*] contains the name configured for this circuit, such as WAN1.

ccttype[*cct#*] contains the circuit type defined in the V.25 bis circuit group definition, either Circuit Group Member, Backup Member, Pool Member, or Misconfigured Circuit.

connecttime[*cct#*] contains the value indicating the time in seconds that the current V.25 bis connection has been alive. If there is no current connection, then this value indicates the total time that the last connection was up. If a connection has never been established, the value is 0.

index[*cct#*] contains the circuit number for this V.25 bis circuit. This variable is used with the index number for the first circuit, to find all the circuit numbers for use in the other variables.

lasterror[*cct#*] contains the last two ASCII character errors issued by the terminal adapter. If no error has been set, then it contains None.

lastlog[*cct#*] contains the last V.25 bis event message for this circuit.

phonenum[*cct#*] contains the last phone number called on outbound connections and the last phone number received on inbound connections. (On manual connections, this value is set to Unknown. On inbound connections where the receive number is not passed, it is also set to Unknown. If no connection has been established since the router was booted, the value is set to Never used.

state[*cct#*] indicates the state of this V.25 bis circuit, one of the following:

Current outbound means the connection was opened in the outbound direction and is currently open.

Current inbound means the connection was opened in the inbound direction and is currently open.

Previous outbound means the last connection was opened in the outbound direction and is currently closed.

Previous inbound means the last connection was opened in the inbound direction and is currently closed.

Never used means no V.25 bis connection has been established since the last time the router was booted.

Management Information Base Variables

isdn: ISDN (V.25 bis) Information Base

subaddr[*cct#*] contains the last subaddress sent on an outbound connection or received on an inbound connection. If not known, the value is set to `Unknown`. If no connection has been established since the router was booted, the value is set to `Never used`.

IP Mapping

ip_networks[*IP-addr-for-hop*] contains the IP network map to the circuit. Each IP address accessible for this hop is a separate index (the instance within the square brackets).

ipmapcctname[*map#*] contains the actual circuit name associated with the map. This indication is valid only when the map state is `Connecting` or `Connect`. In other states the variable contains "No circuit mapped".

ipmapconndrop[*map#*] contains the number of packets dropped for this map while the map was connecting and during the connected state.

ipmapconnectnum[*map#*] contains the number of separate successful calls made on behalf of this map.

ipmapconnecttime[*map#*] contains the amount of time this map has been in the connected state (that is, total connect time for the map).

ipmapdownndrop[*map#*] contains the number of packets dropped for this map while the map was going down. This occurs when packets are queued to be sent and either the user disables the map or the connection is lost during data transfer.

ipmaprcvpkt[*map#*] contains the number of packets successfully received for this map.

ipmapstate[*map#*] indicates the state of the IP map. The possible states are the following:

disconnected means the map is disconnected; the circuit is available.

disabled means the circuit has been disabled by NCL's Disipmap command.

connecting means the map is in the process of making a V.25 bis connection.

connected means the map is connected and the circuit is in use.

queue wait means the map has data to send, but no pool circuits are currently available. When a circuit becomes available, the map will go into the connecting state. (Refer to the VC inactivity time parameter in chapter 14.)

hold down means the map has failed to connect. It cannot be used until the Hold down time expires. The IP address will again be accessible and the map will go into the disconnected state. (Refer to the Hold down time and VC inactivity time parameters in chapter 14.)

ipmapxmitpkt[*map#*] contains the number of packets successfully transmitted for this map.

nexthop[*map#*] contains the address of the network that has a static route through the next hop address. There is a separate entry for each network reachable using the static route. That is, there can be several entries per next hop (For this reason there is a separate instance for each address). The format of the message associates the next hop with the given address. (For example, `ip_networks_1` indicates that this IP address is associated with `nexthop[1]`).

key: Key Information Base

The “key” information base indicates whether specific HP router services are available to be configured on this model router.

- A value of 1 means the service can be configured.
- A value of 0 means the service is not available.

key

variables listed below

The pathname is constructed as follows:

key.variable

The variables are listed alphabetically:

at AppleTalk routing service

drs DECnet routing service

fr Frame Relay circuit services

ip IP routing service (the TCP/IP protocol suite)

ipx IPX routing service

lb Bridge service

osi OSI routing

smlds SMDS services

x25 X.25 circuit services

xns XNS routing service

lb: Bridge Information Base

The bridge “lb” information base contains variables that describe the reception and transmission of packets across each bridging circuit group. The structure is the following:

lb
 cgc bridge circuit group name
 variables listed below

The pathname is constructed as follows:

lb.*cgc.variable*

The variables are listed alphabetically:

block_ste indicates the disposition of STE frames received by the circuit group. A value of 1 indicates that received STE frames are blocked (dropped); a value of 0 indicates that received STE frames are forwarded. If either NCL's Blockste or Unblockste command has been executed after the most recent reboot of the router, this variable indicates which is currently in effect. Conversely, if neither Blockste nor Unblockste have been used since the last reboot, then this variable indicates the setting of the Block STE configuration parameter in the Bridge Circuit Group Parameters Screen at the last reboot.

drop_dst_addr contains the number of packets dropped by circuit group *cgc* in accordance with global destination address filters specified within the configuration.

drop_dst_local contains the number of packets dropped by circuit group *cgc* because the source and destination address were on the same (local) network.

drop_interval contains the number of packets dropped by circuit group *cgc* because more than one packet was flooded to a (particular) unlearned address during a Flood Interval time period. A packet is flooded to all networks if the destination of the packet is unknown to the router. The flood can be controlled by the Flood Interval parameter in the Bridge menu of the Configuration Editor. If packets are received with the same destination as the first packet and within the Flood

lb: Bridge Information Base

Interval time, those packets are dropped if the destination of the first packet has not yet replied. The router will not flood packets more than once within the Flood Interval time if the Flood interval time is set to a value other than zero.

drop_invalid_ringid increments when an explorer frame is received and the last ring ID in the RIF does not match the configured ring ID on which it was received. If this occurs, verify that the configured ring ID matches the actual ring ID.

drop_listen contains the number of packets dropped by circuit group *ccg* while it was in the spanning-tree learning state. While in the learning state, *ccg* receives both network-generated bridge protocol data units (BPDUs) and end-node-generated traffic. This traffic is subjected to the learning process but not relayed. Time spent in the learning state is governed by the *Forward Delay* parameter. Upon expiration of the forward delay timer, circuit group *ccg* enters the forwarding state.

drop_loadbal_noprotcf contains the number of packets dropped by circuit group *ccg* because the protocol contained in the *Type* field did not match the expected protocol value.

drop_no_cg_from_cgm contains the number of packets dropped by circuit group *ccg* because of a change in state of the circuit group during processing time. This usually indicates that a circuit group has gone down (been disabled) during packet processing.

drop_protocol contains the number of packets dropped by circuit group *ccg* in accordance with global or local protocol filters specified by the configuration.

drop_src_addr contains the number of packets dropped by circuit group *ccg* in accordance with local source address filters specified by the configuration.

flood contains the number of packets flooded by circuit group *ccg*; *ccg* floods packets if it has not yet learned the location of the packet's destination address.

fwd_dst_addr contains the number of packets forwarded by circuit group *ccg* in accordance with global destination-address filters specified by the configuration.

fwd_load_bal contains the number of packets forwarded by circuit group *ccg* in accordance with load balancing options specified by the configuration.

fwd_mcast_addr contains the number of packets forwarded by circuit group *ccg* in accordance with global multicast-address filters specified by the configuration.

fwd_protocol contains the number of packets forwarded by circuit group *ccg* in accordance with global or local protocol filters specified by the configuration.

max_hops contains the value assigned to the Max Hops configuration parameter on the Bridge Circuit Group Parameters Screen. (Refer to the Max Hops parameter in chapter 6.)

recv contains the number of packets received by circuit group *ccg*.

recv_cfg contains the number of configuration BPDUs received by circuit group *ccg*.

recv_tcn contains the number of topology-change notification BPDUs received by circuit group *ccg*.

srbcast_fwd contains the total number of all-paths-broadcasting-routing and spanning-tree-broadcast-routing frames forwarded on circuit group *ccg*.

srbcast_rx contains the total number of all-paths-broadcasting-routing and spanning-tree-broadcast-routing frames received on circuit group *ccg*.

srf_dropnotinroute contains the number of specifically routed frames dropped on circuit group *ccg* because the bridge was not contained in the routing path.

srf_fwd contains the number of specifically routed frames forwarded on circuit group *ccg*.

srf_rx contains the number of specifically routed frames received on circuit group *ccg*.

Management Information Base Variables

lb: Bridge Information Base

xmit contains the number of packets transmitted by circuit group *ccg*.

xmit_cfg contains the number of configuration BPDUs sent by circuit group *ccg*.

xmit_tcn contains the number of topology-change notification BPDUs sent by circuit group *ccg*.

lbmib: Bridge Address Table Information Base

The bridge address table “lbmib” information base contains data on the forwarding and filtering of bridge frames. Use NCL’s Rgetb command to access the “lbmib” address table.

The structure is the following:

```
lbmib
  fwdtable
    entry
      variables listed below
    count
  riftable
    rifentry
      variables listed below
```

The variables are listed alphabetically:

address contains a station (MAC-level, or physical) address of a connected LAN device, expressed as a 12-digit hexadecimal number.

cg contains the name of the circuit group that provides a connection to *address*.

dst contains the disposition of frames containing *address* in the destination address field of the Ethernet header. F indicates they are forwarded; D indicates they are dropped.

dstaddr contains the station (MAC-level, or physical) address of the destination node.

if contains the interface number the router assigned to *cg*.

Management Information Base Variables

lbmib: Bridge Address Table Information Base

rif describes the path used to source route packets between the source route and the destination. The first two bytes contain the routing control (RC) field that describes the routing type, field length, direction bit, and largest frame size, as follows:

- bits 1-2: RIF type
 - 00: Specifically Routed Frame (SRF)
 - 11: Spanning Tree Explorer (STE)
 - 10: All Routes Explorer (ARE)
- bit 3: Reserved
- bits 4-8: Length of RIF (maximum = 18 bytes)
- bit 9: Direction that frames traverse LAN
 - 0: Forward
 - 1: Reverse
- bits 13-16: Reserved

src contains the disposition of frames containing *address* in the source address field of the Ethernet header. F indicates they are forwarded; D indicates they are dropped.

src_addr contains the station (MAC-level, or physical) address of the source interface.

xs_flood denotes whether frames destined for **address** are (1) forwarded, (2) flooded, or (3) dropped.

log: Event Log Information Base

The event log information base contains data on the event log and enables access to certain events. You can use the NCL List command to display all or a part of the event log information base, and the NCL Get command to obtain the value of any variable within the information base. The MIB number for log is 57. The structure is:

log	
<i>variable</i>	listed below
table.entry.text	listed below

Examples of the pathname are as follows:

```
list log.*
list 57.*
list log.bootpoint.*
get log.*
get log.bootpoint.*
get 57.2.*
```

bootpoint[0] contains the event number of the first event that occurred on this router when it was booted.

events[0] contains the number of events that have occurred on this router.

lastevent[0] contains the last event message to occur on this router.

maxtablesize[0] contains the maximum number of events the log can hold.

table.entry.text[event#] is only available through SNMP. It contains the event message for event number %event%.

```
get log.table.entry.text
get 57.4.1.1
```

mem: Memory Information Base

The memory “mem” information base contains variables that describe system memory management. The structure is the following:

mem

[*slot #*] always “1” for an HP Series 200 or 400
router; “1” to “5” on an HP Router 650

type either *local* or *global*,
both with the same variables

variables listed below

The pathname is constructed as follows:

mem[*slot #*].*type.variable*

The variables are listed alphabetically:

alloc_bytes contains the number of currently allocated bytes.

alloc_seg_cnt contains the number of currently allocated memory
segments.

free_bytes contains the number of available (unallocated) bytes.

free_seg_cnt contains the current number of free memory
segments. A free memory segment is an unused contiguous memory
block of greater than 16 bytes. Generally, an increase in the number of
free memory segments indicates an increase in memory fragmentation.

slab_cnt contains the current number of discretely managed
memory areas. Each slab is further broken down into smaller
contiguous areas called segments.

total_bytes contains the number of currently installed bytes.

mgr: Manager Information Base

The System manager “mgr” information base contains a single control object whose function is to generate system management and entity enabling messages. NCLs List and Get commands provide no additional information regarding the “mgr” information base.

mib: Internet MIB

This IP routing information base, the “mib” branch, within the private-enterprise section, contains the same variables as the standard Internet MIB I section, as defined in Internet Request for Comments (RFC) 1156. The variables in the private-enterprise section have different names but have the same identification codes (following the private-enterprise prefix “1.3.6.1.4.1.18.1.1”) as the router variables in the standard MIB section.

NCL's Rgets and Rgetms commands are the most efficient means to obtain the values of variables within the standard Internet MIB. Rgeta, Rgeti, and Rgetr can be used to retrieve specific MIB addressing and routing tables. List and Get, however, can be used to obtain the pathnames, variables, and their values, from this “mib” branch within the private-enterprise section. (See chapter 15 for these commands.)

name: Name Information Base

The “name” information base contains variables that describe the operations and structure of the name server. The structure is the following:

name

[*slot #*] always “1” for an HP Series 200 or 400
router; “1” to “5” on an HP Router 650

variables listed below

The pathname is constructed as follows:

name[*slot #*].*variable*

The variables are listed alphabetically:

alias_cnt contains the number of aliased objects added to the name server table. This variable should always contain 0.

create_cnt contains the number of objects added to the name server table.

cur_cnt contains the current number of objects in the name server table.

cur_mem_used contains the current number of bytes occupied by the name server table.

delete_cnt contains the number of objects deleted from the name server table.

find_cnt contains the number of name server table accesses that resulted in successful resolutions.

list_cnt This counter is not currently implemented. It should always contain 0.

update_cnt contains the number of updates to name server table entries.

pm: Port Module Manager Information Base

The “pm” port module manager information base contains variables that describe port interface modules that may be installed in the HP Router 650.

pm

total_ports_modules

slot #

variables

module-specific branch and variables

Examples of pathname constructions are:

pm.*slot #.variable*

pm.total_ports_modules

or

53.1

Chassis

total_ports_modules the current number of operational port modules in the chassis.

Module

Example:

```
get pm.slot2.state
```

state The current state of the port module. The following values are possible.

- 0 = Dead
- 1 = Absent
- 2 = Hard Reset
- 3 = Soft Reset
- 4 = Selftest Pass
- 5 = Selftest Fail
- 6 = Downloading
- 7 = Booting
- 8 = Alive
- 9 = Running

hwid the type of port module in the slot. The following values are possible.

- 0 = Empty Slot (i.e. No Card)
- 1 = Ethernet Port Module
- 2 = Synchronous WAN Port Module
- 3 = Token Ring Port Module
- 4 = FDDI Port Module

msg_tx the number of messages transmitted from the routing engine to the port module.

msg_rx the number of messages received by the routing engine from the port module.

msg_fail the number of message transmissions and receptions which have failed.

trans_depth the maximum depth of the transactional message log.

Management Information Base Variables
proprietary: Proprietary Information Base

proprietary: Proprietary Information Base

This is a proprietary Information Base used by HP network management applications. If further information is desired, please contact your HP representative.

rok: Router Operating Kernel Information Base

The structure of the router operating system “rok” information base is the following:

rok

[*slot #*] always “1” for an HP Series 200 or 400
 router; “1” to “5” on an HP Router 650

variables listed below

The pathname is constructed as follows:

rok[*slot #*].*variable*

The variables are listed alphabetically:

boot_count contains the number of times the router has been booted. It is never reset as long as battery-backed RAM is intact.

console_connects contains the number of times the console has made a modem connection.

cpu contains the CPU utilization averaged over the last 2 seconds.

false_buserrs contains the number of false bus errors seen by the CPU. It should normally contain 0.

ready_tasks contains the total number of processes currently ready to run.

spurious_ints contains the total number of spurious interrupts received by the CPU. It should normally contain 0.

total_tasks contains the total number of existing operating system processes. It cannot be reset.

snmp: SNMP Information Base

The Simple Network Management Protocol “snmp” information base contains variables that describe the transmission and reception of User Data Protocol (UDP) datagrams delivered to or originated by the SNMP management agent. The structure is the following:

snmp

variables listed below

The pathname is constructed as follows:

snmp.*variable*

The variables are listed alphabetically:

snmpbadcommunity contains the number of incoming requests dropped by the SNMP management agent because either (1) the community name was unknown or (2) the originating host was not a member of a known community.

snmpbadtype contains the number of incoming requests dropped by the SNMP management agent because the protocol data unit (PDU) specified an invalid operation code.

snmpinpkts contains the number of User Data Protocol (UDP) datagrams delivered to the SNMP management agent.

snmpoutpkts contains the number of User Data Protocol (UDP) datagrams originated by the SNMP management agent.

snmpprocerrs contains the number of syntactically correct SNMP messages that could not be processed; such messages might request an unknown variable, contain an invalid instance identification, or contain a violation of access-control restrictions.

snmptotalrequested contains the total number of individual variables whose values have been requested in incoming SNMP PDUs. An approximation of the number of variables requested in each SNMP PDU can be computed by dividing `snmptotalrequested` by `snmpinpkts`.

svc: System Services Information Base

The system services “svc” information base contains variables that describe the private memory management function of system management. This function maintains dynamic information on the memory space available to active tasks. The next level identifies the memory management instance (*sme*). The next level identifies one of four specific memory management tables. The lowest level contains the actual *svc* memory management variables. The router maintains identical variable sets for all tables. The structure is the following:

svc	
[<i>slot #</i>]	always “1” for an HP Series 200 or 400 router; “1” to “5” on an HP Router 650
<i>sme</i>	memory management
<i>type</i>	table type; either: <i>ref</i> reference table <i>act</i> action table <i>syn</i> symbol table <i>txt</i> text string table
<i>variables</i>	listed below

The pathname is constructed as follows:

svc.[*slot #*].*sme.type.variable*

The variables are listed alphabetically:

- alloc** contains the number of objects allocated, and in use, in space.
- install** contains the current number of objects contained in space.
- space** contains the size of the memory area in bytes.

tcp: TCP Information Base

The Transmission Control Protocol “tcp” information base contains variables that describe the exchange of TCP segments between communicating TCP peer entities. The structure is the following:

tcp

variables listed below

The pathname is constructed as follows:

tcp.*variable*

The variables are listed alphabetically:

acks_snt contains the number of positive acknowledgments transmitted by the router during TCP sessions.

app_dropped contains the number of TCP segments dropped because of invalid segment, port, and/or protocol information.

app_notcb contains the number of instances the TCP port was not found in the hash table. Consequently, TCP drops the segment.

badack contains the number of received faulty acknowledgment segments.

badflg contains the number of received TCP segments that contained unknown or faulty flags.

badopt contains the number of received TCP segments that requested unknown/unsupported TCP options.

badrst contains the number of received faulty TCP reset segments.

badseg contains the number of faulty received TCP segments.

badsum contains the number of received TCP segments that contained a bad checksum value.

- dupack** contains the number of duplicate acknowledgment segments.
- dupseg** contains the number of duplicate received TCP segments.
- erract** contains the total number of error messages sent by TCP.
- hashcolls** contains the number of times hashing of the TCP port information produced a collision with a previous port.
- hashhits** contains the number of times the hash was successful when matching TCP ports.
- hashmiss** contains the number of times the hash was missed during a TCP port search.
- mem_err** contains the number of memory errors.
- mem_use** contains the number of bytes of memory required for TCP operations.
- net_dropped** contains the number of TCP segments dropped because of an invalid data path.
- net_notcb** contains the number of times the hash table search of active TCP ports failed, and reset of the connection was attempted.
- no_mem** contains the number of instances TCP could not function because of lack of memory resources.
- nopact** contains the number of times a received TCP segment required no action.
- pkts_rcv** contains the number of TCP segments received by the router during TCP sessions.
- pkts_snt** contains the number of TCP segments transmitted by the router during TCP sessions.
- rcv_full** contains the number of times TCP segments were dropped because the receive window was closed.

Management Information Base Variables

tcp: TCP Information Base

rehashes contains the number of times the TCP port table was rehashed. This happens when a connection is closed, or when the control block hash table requires rehashing.

reseq contains the number of packets resequenced by the router.

reseq_drop contains the number of elements dropped because of resequencing.

reseq_full contains the number of times TCP had a full resequencing queue.

reseq_mgr contains the number of resequenced packets linked to form a larger packet.

retx contains the number of packets retransmitted by the router.

retx_full contains the number of times the TCP retransmit buffer was full.

rx_bytes contains the number of bytes received by the router during TCP sessions.

segoos contains the number of segments received out of sequence.

sess_cur contains the current number of TCP connections.

sess_tot contains the number of TCP connections since the router last booted.

snd_full contains the number of times the TCP send window was full.

toobig contains the number of times a TCP segment was not sent because the receive window size was too small.

tx_bytes contains the number of bytes transmitted by the router during TCP sessions.

telnet: Telnet Information Base

The “telnet” information base contains variables that describe virtual-terminal connections between the router and a remote device. The structure is the following:

telnet

variables listed below

The pathname is constructed as follows:

telnet.*variable*

The variables are listed alphabetically:

inp.bad_opt contains the number of incoming TCP segments that requested unknown or unsupported Telnet options.

inp.dropped contains the number of incoming TCP segments that were dropped because of lack of processing resources.

inp.no_if contains the number of incoming TCP segments that were dropped for lack of an interface.

inp.too_big contains the number of incoming TCP segments that were dropped because they exceeded the mtu.

mem_err contains the number of memory errors.

mem_use contains the number of bytes of memory used by Telnet.

no_mem contains the number of instances Telnet was unable to function because of the lack of memory resources.

out.dropped contains the number of outgoing TCP segments that were not sent because of lack of processing resources.

out.iac_fnd contains the number of outgoing Telnet escape sequences that were not transmitted.

Management Information Base Variables

telnet: Telnet Information Base

out.no_if contains the number of outgoing TCP segments that were dropped for lack of an interface.

out.too_big contains the number of outgoing TCP segments that were dropped because they exceeded the MTU.

rx_bytes contains the number of bytes received by the router while connected to a remote terminal by means of Telnet.

sess_cur contains the current number of Telnet connections. The router supports a maximum of two simultaneous Telnet sessions.

sess_tot contains the number of Telnet connections since the router last booted.

tx_bytes contains the number of bytes transmitted by the router while connected to a remote terminal by means of Telnet.

tftp: TFTP Information Base

The Trivial File Transfer Protocol “tftp” information base contains variables that describe file transfers between the router and a remote device. The structure is the following:

tftp

variables listed below

[*n*] the interface number assigned by the router

The pathnames are constructed as follows:

tftp.*variable* [*n*]

The variables are listed alphabetically:

aborted contains the number of TFTP sessions that were prematurely terminated.

errin contains the number of received TFTP ERROR packets (Opcode=5).

errout contains the number of transmitted TFTP ERROR packets (Opcode=5).

filesin contains the number of files successfully transmitted to the router from a remote device by means of the TFTP.

filesout contains the number of files successfully transmitted by the router to a remote device by means of the TFTP.

rrqin contains the number of received TFTP READ REQUEST packets (Opcode=1).

rrqout contains the number of transmitted TFTP READ REQUEST packets (Opcode=1).

rxmits contains the total number of TFTP packets retransmitted by the router.

Management Information Base Variables

tftp: TFTP Information Base

wrqin contains the number of received TFTP WRITE REQUEST packets (Opcode=2).

wrqout contains the number of transmitted TFTP WRITE REQUEST packets (Opcode=2).

timep: Time Protocol Information Base

The “timep” information base contains variables that count two Time Protocol events. The structure of the information base is the following:

timep

variables listed below

The pathname is constructed as follows:

timep.*variable*

The variables are listed alphabetically:

requests contains the number of times the Timep server received a request.

retries contains the number of times the Timep client retries obtaining the time.

timer: Timer Information Base

The “timer” information base contains variables that describe the scheduling and issuance of router-generated timers. The structure of the information base is the following:

timer
 [slot #] always “1” for an HP Series 200 or 400
 router; “1” to “5” on an HP Router 650
 variables listed below

The pathname is constructed as follows:

timer[slot #].variable

The variables are listed alphabetically:

cancel_cnt contains the number of timers cancelled by the router prior to the expiration of the timer.

expire_cnt contains the number of timers that have expired.

race_cnt contains the number of simultaneous occurrences of the expiration of the timer and the cancellation of the timer.

set_cnt contains the number of timers scheduled by the router.

xrx: Xerox XNS Information Base

The “xns” information base is composed of: (1) a set of variables that describe transmission and reception of packets across each XNS interface, (2) a set of variables that describe aggregate Internet Datagram Protocol (IDP)/Error Protocol activity, (3) an XNS addressing table, and (4) an XNS routing table. You can also use NCL’s Rgetxr command to access the tables. The structure is the following:

xns	
if	the interface-specific XNS address (hexadecimal) (see subheading)
variables	the interface-specific variables, listed below
mib	(along with idp) the IDP/error protocol branch
idp	(along with mib) the IDP/Error Protocol branch (see subheading)
variables	the IDP/Error Protocol variables, listed below

The pathnames are constructed as follows:

xns.if.*variable*
xns.mib.idp.*variable*

The variables are listed alphabetically under two branches:

Interface

- drop** contains the total number of IDP datagrams dropped (for whatever reason) by interface if.
- rx** contains the total number of IDP datagrams received by interface if.
- tx** contains the total number of IDP datagrams transmitted by interface if.

Management Information Base Variables

xrx: Xerox XNS Information Base

ulp contains the total number of IDP datagrams delivered by the router to an upper-level protocol (for example, RIP, Echo, Error) for processing.

Protocol

errsdestbadsock contains the number of destination-host-generated Error Protocol packets, with an Error Number of 2, that were relayed by the router. This error number indicates that the destination host received an IDP packet addressed to an unknown socket.

errsdestchksum contains the number of destination-host-generated Error Protocol packets, with an Error Number of 1, that were relayed by the router. This error number indicates that the destination host received an IDP packet that contained a faulty or corrupted checksum.

errsdesthdrlen contains the number of packets rejected by a destination host because the packet header was of insufficient length.

errsdestnoresrcs contains the number of destination-host-generated Error Protocol packets, with an Error Number of 3, that were relayed by the router. This error number indicates that the destination host discarded an IDP packet because of lack of processing resources.

errsdestproto contains the number of packets rejected by a destination host because the protocol type field contained an invalid or unknown value.

errsdestunspec contains the number of destination-host-generated Error Protocol packets, with an Error Number of 0, that were relayed by the router. This error number indicates that the destination host rejected an IDP packet for unspecified reasons.

errssuppressed contains the number of packets dropped because of length below minimum.

errsxitchksum contains the number of router-generated Error Protocol packets with an Error Number of 1001. This error number indicates that the router received an IDP packet that contained a faulty or corrupted checksum.

errsxithopcnt contains the number of router-generated Error Protocol packets with an Error Number of 1003. This error number indicates that the packet had passed through more than the maximum number of routers before arriving at its destination.

errsxittoobig contains the number of router-generated Error Protocol packets with an error number of 1004. This Error Number indicates that the packet is too long for the router to relay.

errsxitunreach contains the number of router-generated Error Protocol packets with an Error Number of 1002. This error number indicates that the router cannot reach the packet destination.

errsxitunspec contains the number of router-generated Error Protocol packets with an Error Number of 1000. This error number indicates that the router rejected an IDP packet for unspecified reasons.

forwarding contains an integer switch indicating the node's function within the extended XNS network. A value of 1 indicates that the node is acting as a gateway (routes and forwards datagrams); a value of 2 indicates that the node is acting as a host (does not route and forward datagrams).

forwdatagrams contains the number of received IDP datagrams not addressed to the XNS router. The router attempts to forward these datagrams to their ultimate destination.

inadderrors contains the number of IDP datagrams discarded because of invalid destination address fields.

indelivers contains the number of IDP datagrams delivered to IDP user protocols (including Error Protocol).

indiscards contains the number of valid input IDP datagrams discarded because of insufficient router resources (lack of buffer space).

inherrors contains the number of IDP datagrams discarded because of errors in their IDP headers. Such errors include faulty checksums, format errors, and transport control (hop count) errors.

inreceives contains the total number of all IDP datagrams (including those received in error) received from all interfaces.

Management Information Base Variables

xrx: Xerox XNS Information Base

inunknownprotos contains the number of IDP datagrams discarded because of an incorrect or corrupted value in the Protocol Type field in the IDP header.

outdiscards contains the number of valid output IDP datagrams discarded because of insufficient router resources (lack of buffer space).

outnoroutes contains the number of IDP datagrams discarded because no route could be found to transmit them to their destination.

outrequests contains the number of IDP datagrams generated by local IDP user protocols (including Error).

x25: X.25 Information Base

The “x25” information base contains variables that describe frame-level and packet-level transmission and reception activities across each X.25 circuit; it also contains variables that describe packet-level transmission and reception activities across each X.25 point-to-point dedicated switched virtual circuit. The structure is the following:

x25	
<i>cct</i>	an X.25 circuit name
<i>type</i>	either frame or pkt
<i>variables</i>	the circuit frame- or packet-level variables, listed below (see subheading)
<i>svc</i>	stands for an X.25 virtual circuit name (see subheading)
<i>variable s</i>	the X.25 virtual circuit variables, listed below

The pathnames are constructed as follows:

x25.cct.type.variable

x25.svc.variable

The variables are listed alphabetically under the different branches on the following pages.

Circuit Frame Level

bad_len_rx contains the number of supervisory FRMR (Frame Reject) frames received by X.25 circuit cct that contained W and X bits set to 1. This bit pattern indicates that the remote end has rejected a supervisory or unnumbered frame issued by X.25 circuit cct because the frame length was faulty.

bad_len_tx contains the number of supervisory FRMR (Frame Reject) frames transmitted by X.25 circuit cct that contained W and X bits set to 1. This bit pattern indicates that X.25 circuit cct has rejected a previously received supervisory or unnumbered frame because the frame length was faulty.

bad_nr_rx contains the number of supervisory FRMR (Frame Reject) frames received by X.25 circuit cct that contained a Z bit equal to 1. This bit pattern indicates that the remote end has rejected a frame issued by X.25 circuit cct because it contained a faulty receive sequence number.

bad_nr_tx contains the number of supervisory FRMR (Frame Reject) frames transmitted by X.25 circuit cct that contained a Z bit value equal to 1. This bit pattern indicates that X.25 circuit cct has rejected a previously received frame because the frame contained a faulty receive sequence number.

disc_rx contains the count of unnumbered DISC (Disconnect) frames received by X.25 circuit cct. DISC frames terminate the DCE/DTE link.

disc_tx contains the count of unnumbered DISC frames transmitted by X.25 circuit cct. DISC frames terminate the DCE/DTE link.

dm_rx contains the count of unnumbered DM (Disconnected Mode) frames received by X.25 circuit cct. DM frames indicate that the sending node is logically disconnected.

dm_tx contains the count of unnumbered DM (Disconnected Mode) frames transmitted by X.25 circuit cct. DM frames indicate that the sending node is logically disconnected.

frmr_rx contains the aggregate number of FRMR (Frame Reject) frames received by X.25 circuit cct. FRMR frames report specific error conditions.

frmr_tx contains the aggregate number of FRMR (Frame Reject) frames transmitted by X.25 circuit cct. FRMR frames report specific error conditions.

ignore_rx contains the aggregate number frames, received on X.25 circuit cct, that were not processed, generally because of insufficient length or because of a faulty address field (containing values other than 01 or 03).

info_rx contains the number of I (Information) frames received by X.25 circuit cct. I frames carry user data packets.

info_tx contains the number of I (Information) frames transmitted by X.25 circuit cct. I frames carry user data packets.

lev2_down contains the number of times that X.25 circuit cct went down in accordance with X.25 frame-level protocol.

lev2_up contains the number of times that X.25 circuit cct came up in accordance with X.25 frame-level protocol.

rej_rx contains the number of REJ (Reject) frames received by X.25 circuit cct. A REJ frame is a negative acknowledgment calling for the retransmission of specified I frames.

rej_tx contains the number of REJ (Reject) frames transmitted by X.25 circuit cct. A REJ frame is a negative acknowledgment calling for the retransmission of specified I frames.

rnr_rx contains the number of RNR (Receiver Not Ready) frames received by X.25 circuit cct. An RNR frame denotes a busy condition, indicating a temporary inability to accept I frames from the remote end of the circuit.

rnr_tx contains the number of RNR (Receiver Not Ready) frames transmitted by X.25 circuit cct. An RNR frame denotes a busy condition, indicating a temporary inability to accept I frames from the remote end of the circuit.

Management Information Base Variables

x25: X.25 Information Base

rr_rx contains the number of RR (Receiver Ready) frames received by X.25 circuit cct. An RR frame either indicates the readiness to receive I frames, or acknowledges the receipt of I frames.

rr_tx contains the number of RR (Receiver Ready) frames transmitted by X.25 circuit cct. An RR frame either indicates the readiness to receive I frames, or acknowledges the receipt of I frames.

sabm_rx contains the number of SABM (Set Asynchronous Balanced Mode) frames received by X.25 circuit cct. SABM frames initiate the establishment of the DCE/DTE link.

sabm_tx contains the number of SABM (Set Asynchronous Balanced Mode) frames transmitted by X.25 circuit cct. SABM frames initiate the establishment of the DCE/DTE link.

ua_rx contains the number of UA (Unnumbered Acknowledgment) frames received by X.25 circuit cct. UA frames acknowledge receipt of SABM or DISC frames, and complete the establishment or termination of the DCE/DTE link.

ua_tx contains the number of UA (Unnumbered Acknowledgment) frames transmitted by X.25 circuit cct. UA frames acknowledge receipt of SABM or DISC frames, and complete the establishment or termination of the DCE/DTE link.

unknown_rx contains the number of FRMR (Frame Reject) frames received by X.25 circuit cct that contained a W bit set to 1. This bit setting indicates that the remote end has rejected a frame issued by cct because the frame contained an invalid, or unimplemented, command or response.

unknown_tx contains the number of FRMR (Frame Reject) frames transmitted by X.25 circuit cct that contained a W bit set to 1. This bit setting indicates that cct has rejected a previously received frame because the frame contained an invalid, or unimplemented, command or response.

Circuit Packet Level

call_cfm_rx contains the number of CALL CONNECTED packets received by X.25 circuit cct. A CALL CONNECTED packet completes the call- setup procedure.

call_cfm_tx contains the number of CALL ACCEPTED packets transmitted by X.25 circuit cct. A CALL ACCEPTED packet indicates readiness to accept an incoming call, and generates a CALL CONNECTED packet at the remote end of the circuit.

call_rx contains the number of INCOMING CALL packets received by X.25 circuit cct. An INCOMING CALL packet indicates that a remote node is attempting to establish a connection.

call_tx contains the number of CALL REQUEST packets transmitted by X.25 circuit cct. A CALL REQUEST packet initiates the call-setup procedure, and generates an INCOMING CALL packet at the remote end of the circuit.

clear_cfm_rx contains the number of CLEAR CONFIRMATION packets received by X.25 circuit cct. A CLEAR CONFIRMATION packet acknowledges that the previously requested clear action has been implemented.

clear_cfm_tx contains the number of CLEAR CONFIRMATION packets transmitted by X.25 circuit cct. A CLEAR CONFIRMATION packet acknowledges that the previously requested clear action has been implemented.

clear_rx contains the number of CLEAR INDICATION packets received by X.25 circuit cct. A CLEAR INDICATION packet acknowledges the receipt of a CLEAR REQUEST packet.

clear_tx contains the number of CLEAR REQUEST packets transmitted by X.25 circuit cct. A CLEAR REQUEST packet disconnects the virtual circuit.

diagnostic_rx contains the number of DIAGNOSTIC packets received by X.25 circuit cct. The DCE generates DIAGNOSTIC packets for fault isolation purposes.

Management Information Base Variables

x25: X.25 Information Base

data_rx contains the number of DATA packets received by X.25 circuit cct. DATA packets contain user data.

data_tx contains the number of DATA packets transmitted by X.25 circuit cct. DATA packets contain user data.

dropped_tx contains the count of IP datagrams dropped by the circuit because of X.25 failures or queue clipping.

error_rx contains the number of erroneous packets (for example, packets with a bad length, REGISTRATION packets if registration is not enabled, and RESTART packets not directed to LCN0) received by X.25 circuit cct.

reset_cfm_rx contains the number of RESET CONFIRMATION packets received by X.25 circuit cct. A RESET CONFIRMATION packet acknowledges that the previously requested reset action has been implemented.

reset_cfm_tx contains the number of RESET CONFIRMATION packets transmitted by X.25 circuit cct. A RESET CONFIRMATION packet acknowledges that the previously requested reset action has been implemented.

reset_rx contains the number of RESET INDICATION packets received by X.25 circuit cct. A RESET INDICATION packet informs the recipient that the remote node has reset the send and receive packet sequences to 0.

reset_tx contains the number of RESET REQUEST packets transmitted by X.25 circuit cct. A RESET REQUEST packet sets the send and receive packet sequences to 0, and generates a RESET INDICATION packet at the remote end of the circuit.

restart_cfm_rx contains the number of RESTART CONFIRMATION packets received by X.25 circuit cct. A RESTART CONFIRMATION packet acknowledges that the previously requested restart action has been implemented.

restart_cfm_tx contains the number of RESTART CONFIRMATION packets transmitted by X.25 circuit cct. A RESTART CONFIRMATION

packet acknowledges that the previously requested restart action has been implemented.

restart_rx contains the number of RESTART INDICATION packets received by X.25 circuit cct. A RESTART INDICATION packet informs the recipient that the remote node has cleared all switched virtual circuits.

restart_tx contains the number of RESTART REQUEST packets transmitted by X.25 circuit cct. A RESTART REQUEST packet clears all switched virtual circuits, and generates a RESTART INDICATION packet at the remote end of the circuit.

rnr_rx contains the number of RNR (Receiver Not Ready) packets received by X.25 circuit cct. An RNR packet denotes a busy condition, indicating a temporary inability to accept DATA packets from the remote end of the circuit.

rnr_tx contains the number of RNR (Receiver Not Ready) packets transmitted by X.25 circuit cct. An RNR packet denotes a busy condition, indicating a temporary inability to accept DATA packets from the remote end of the circuit.

rr_rx contains the number of RR (Receiver Ready) packets received by X.25 circuit cct. An RR packet either indicates the readiness to receive DATA packets, or acknowledges the receipt of DATA packets.

rr_tx contains the number of RR (Receiver Ready) packets transmitted by X.25 circuit cct. An RR packet either indicates the readiness to receive DATA packets, or acknowledges the receipt of DATA packets.

t20_tmout contains the number of T20 timer expirations. The T20 timer starts when a RESTART REQUEST packet is issued, and terminates when a RESTART CONFIRMATION packet is received. If a RESTART CONFIRMATION is not received within T20 seconds (typically 180 seconds), the RESTART REQUEST is reissued.

t21_tmout contains the number of T21 timer expirations. The T21 timer starts when a CALL REQUEST packet is issued, and terminates when a CALL CONNECTED, CLEAR INDICATION, or INCOMING CALL packet is received. If such a packet is not received within T21 seconds (typically 200 seconds), a CLEAR REQUEST is issued.

x25: X.25 Information Base

t22_tmout contains the number of T22 timer expirations. The T22 timer starts when a RESET REQUEST packet is issued, and terminates when a RESET CONFIRMATION or RESET INDICATION packet is received. If such a packet is not received within T22 seconds (typically 180 seconds), the RESET REQUEST is reissued.

t23_tmout contains the number of T23 timer expirations. The T23 timer starts when a CLEAR REQUEST packet is issued, and terminates when a CLEAR CONFIRMATION or CLEAR INDICATION packet is received. If such a packet is not received within T23 seconds (typically 180 seconds), the CLEAR REQUEST is reissued.

Virtual Circuits

data_rx contains the number of DATA packets received by X.25 virtual circuit svc. DATA packets contain user data.

data_tx contains the number of DATA packets transmitted by X.25 virtual circuit svc. DATA packets contain user data.

dropped_tx contains the number of packets dropped by X.25 virtual circuit cct because of resource limitations (no buffer space available, or the virtual circuit was down).

reset_cfm_rx contains the number of RESET CONFIRMATION packets received by X.25 virtual circuit svc. A RESET CONFIRMATION packet acknowledges that the previously requested reset action has been implemented.

reset_cfm_tx contains the number of RESET CONFIRMATION packets transmitted by X.25 virtual circuit svc. A RESET CONFIRMATION packet acknowledges that the previously requested reset action has been implemented.

reset_rx contains the number of RESET INDICATION packets received by X.25 virtual circuit svc. A RESET INDICATION packet informs the recipient that the remote node has reset the send and receive packet sequences to 0.

reset_tx contains the number of RESET REQUEST packets transmitted by X.25 virtual circuit svc. A RESET REQUEST packet sets the send and receive packet sequences to 0, and generates a RESET INDICATION packet at the remote end of the circuit.

rnr_rx contains the number of RNR (Receiver Not Ready) packets received by X.25 virtual circuit svc. An RNR packet denotes a busy condition, indicating a temporary inability to accept DATA packets from the remote end of the circuit.

rnr_tx contains the number of RNR (Receiver Not Ready) packets transmitted by X.25 virtual circuit svc. An RNR packet denotes a busy condition, indicating a temporary inability to accept DATA packets from the remote end of the circuit.

rr_rx contains the number of RR (Receiver Ready) packets received by X.25 virtual circuit svc. An RR packet either indicates the readiness to receive DATA packets, or acknowledges the receipt of DATA packets.

rr_tx contains the number of RR (Receiver Ready) packets transmitted by X.25 virtual circuit svc. An RR packet either indicates the readiness to receive DATA packets, or acknowledges the receipt of DATA packets.

DDN and PDN Virtual Circuit Variables

X.25 DDN and PDN service maintain a set of variables identical to those in the previous section. However, they are ephemeral. These variables can be accessed only for currently established DDN or PDN virtual circuits.

Access the event log to identify currently established virtual circuits. Established calls are indicated by event log entries that take the following form:

call: cct_name.ip_addr.#

where:

cct_name is the name of the X.25 DDN or PDN circuit.

ip_addr is the dotted-decimal IP address of the remote device.

is the logical connection number.

Management Information Base Variables

x25: X.25 Information Base

After verifying that a call has been established, scan the log to ensure that the call (and switched virtual circuit) is still active (has not been cleared). Cleared calls are indicated by an event log entry that takes the following format:

```
clr: cct_name.ip_addr.#(C=nn)(D=nn)
```

where:

cct_name is the name of the X.25 DDN or PDN circuit.

ip_addr is the dotted-decimal IP address of the remote device.

is the logical connection number.

(C=nn) is the encoded clearing cause.

(D=nn) is encoded diagnostic information.

To display all virtual circuit variables for an established DDN or PDN virtual circuit, enter the following at the NCL prompt:

```
x25.cct_name.ipaddr.#.*
```

where:

x25 is the X.25 managed object

cct_name.ip_addr.# is taken from the event log.

* is the wildcard character.

To display a single virtual circuit variable for an established DDN or PDN virtual circuit, enter the following at the NCL prompt:

```
x25.cct.ip_addr.#.code
```

where:

x25 is the X.25 managed object.

cct_name.ip_addr.# is taken from the event log.

code is the pathname code for the variable.

See the "X.25 Event Messages" in chapter 3.

A

Parameter Finder

How To Use the Parameter Finder

The parameter finder is a tool you can use to help determine the menu path to any parameter in the Configuration Editor by listing each parameter according to its position in the Configuration Editor hierarchy.

The parameters are grouped according to the menu items under which they occur in the main screen of the Configuration Editor.

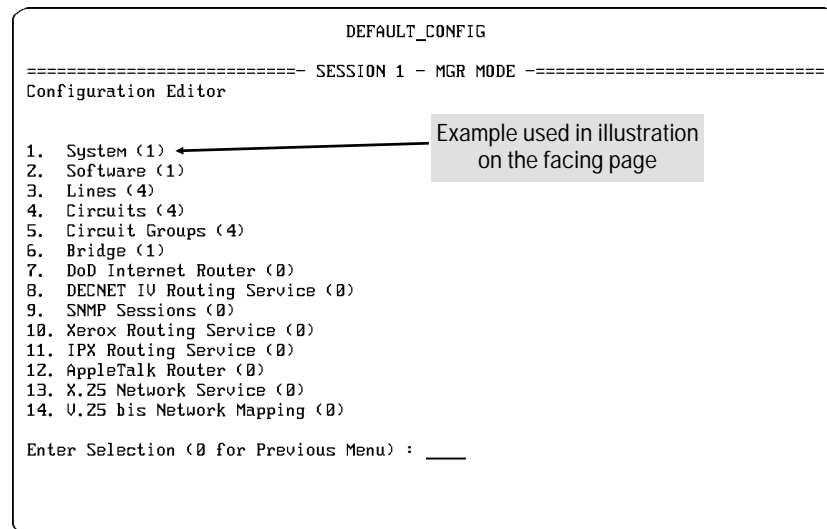


Figure A-1. The Main Screen of the Configuration Editor

For example, in “1. System (1)”, shown above and in the menu tree on the facing page:

- “Automatic Reboot” and “System Contact” are just two of several parameters you’ll find as soon as you select the “1. System” menu item.
- “Beginning month” is a parameter that you will find only when the “Daylight Time Rule” parameter is set to “User defined”.
- “Event Filter Level” is a parameter that you will find only if you access the “1. System Session” menu item.

1. System (1)

System Name

Auto Enable

Automatic Reboot

Timezone

Daylight Time Rule

Daylight Time Rule = User defined

Beginning month

Ending month

Beginning day

Ending day

System Contact

System Location

1. System Session

Event Filter Level

Session Mode (*User, Telnet*)**Typographical Conventions**

- Parameter names appear as:

System Name

Auto Enable

- Numbered menu items appear as:

1. System (for Main menu items)

1. System Session (for submenu items)

- Parameters that appear only when a certain condition is met are listed under a line describing that condition. For example, Beginning month, Ending month, Beginning day, and Ending day appear only when the “Daylight Time Rule” parameter is set to “User defined”, as shown below:

Daylight Time Rule = User defined

Beginning month

Ending month

Beginning day

Ending day

1. System

1. System

System Name

Auto Enable

Automatic Reboot

Timezone

Daylight Time Rule

Daylight Time Rule = User defined

Beginning month

Ending month

Beginning day

Ending day

System Contact

System Location

1. System Session

Event Filter Level

Session Mode

Terminal

Screen Refresh Rate

Session Mode = User

Baud Rate

Flow Control

Parity

Bit / Char

Stop Bits

Connection inactivity time (min)

Modem connection time (sec)

Modem lost receive ready time (msec)

Modem disconnection time (sec)

2. Software

3. Lines

2. Software

Protocol

3. Lines

Physical Access Method

Physical Access Method = CSMA/CD

Connector

Physical Access Method = FDDI

Bridge Type

Physical Access Method = SYNC

Connector

Clock Source

Clock Speed

Physical Access Method = TOKEN RING

Connector

Ring Interface

1. Circuit Name

Circuit Name

4. Circuits

4. Circuits

Circuit Name

Auto Enable

Quality of Service

Circuit Type

Circuit Type = Ether/802.3

LAN Address

XCVR signal polling

Circuit Type = PPP over V.25 bis

LQM Time (secs)

Echo Request Time (secs)

Desired Link Quality

Min Frame Spacing

Extended (32-bit) CRC

Max Pkt Size

IP Address

LCP Active-Open

LCP Auto-Restart

Max Link Latency (ms)

Use UPAP

Compression

1. Adapter record

Connect when

Call restrictions

Minimum connect duration (sec)

Connect retry count

Connect wait time (sec)

Connect inactivity time (sec)

Send CIC on all allowed INC's

Delay after connect failure (min)

Per channel Bandwidth

4. Circuits (Continued)***Circuit Type = PPP over V.25 bis (Continued)***

1. Adapter record (Continued)
 - Min channels to aggregate
 - Max channels to aggregate
 - Channel Management
1. Outbound call number
 - Remote station Number
 - Subaddress
2. Allowed inbound call numbers
 - Allowed Number
 - Subaddress
3. Local number (Used for collision avoidance)
 - Remote Station Number
 - Subaddress
2. Bandwidth Reservation
 - Percent of queue reserved for high priority pkts
 - Percent of queue reserved for normal priority pkts
 - Percent of queue reserved for low priority pkts

Circuit Type = Manual Adapter

- Min Frame Spacing
- Max Link Latency (ms)
- Connect when
- Minimum connect duration (sec)
- Connect retry count
- Connect wait time (sec)
- Connection inactivity time (sec)
- Delay after connect failure (min)
- 1. Bandwidth Reservation
 - Percent of queue reserved for high priority pkts
 - Percent of queue reserved for normal priority pkts
 - Percent of queue reserved for low priority pkts

Circuit Type = V.25 bis adapter

- Min Frame Spacing
- Max Link Latency (ms)

A: Parameter Finder

4. Circuits (Continued)

Circuit Type = V.25 bis adapter (Continued)

1. Adapter record
 - Connect when
 - Minimum connect duration (sec)
 - Connect retry count
 - Connect wait time (sec)
 - Connect inactivity time (sec)
 - Send CIC on all allowed INC's
 - Delay after connect failure (min)
 - Per channel Bandwidth
 - Min channels to aggregate
 - Max channels to aggregate
 - Channel Management
1. Outbound call number
 - Remote station Number
 - Subaddress
2. Allowed inbound call numbers
 - Allowed Number
 - Subaddress
3. Local number (Used for collision avoidance)
 - Remote Station Number
 - Subaddress
2. Bandwidth Reservation
 - Percent of queue reserved for high priority pkts
 - Percent of queue reserved for normal priority pkts
 - Percent of queue reserved for low priority pkts

Circuit Type = Frame Relay

- DLCI Encoding Type
- DLCI Encoding length
- Maximum packet size
- Provide InARP
- Max Link Latency (ms)
- Management Type

4. Circuits (Continued)

Circuit Type = Frame Relay (Continued)

Management Type = ANSI Annex D or LMI

- Poll Interval (seconds)
- Intervals between Full Polls
- Monitored Events
- Events for Error
- Alarm Timer

Management Type = LMI Switch or Annex D Switch

- Provide Update Status
- Maximum Poll Interval (seconds)
- Monitored Events
- Events for Error

1. Permanent Virtual Circuits

- DLCI

2. Multicast Support

- ARP multicast DLCI
- AppleTalk multicast DLCI
- Bridge Flood multicast DLCI
- DECNet multicast DLCI
- OSI multicast DLCI
- General multicast DLCI

3. Bandwidth Reservation

- Percent of queue reserved for high priority pkts
- Percent of queue reserved for normal priority pkts
- Percent of queue reserved for low priority pkts

Circuit Type = SMDS

- Min Frame Spacing
- Individual Address
- Group Address
- ARP Group Address
- Extended (32-bit) CRC
- Max Pkt Size
- Use SNAP
- Use DXI v3.2

A: Parameter Finder

4. Circuits (Continued)

Circuit Type = SMDS (*Continued*)

Use Heartbeat Poll

Heartbeat Polling Interval

Heartbeat Down Count

Max Link Latency (ms) (0=none)

1. Bandwidth Reservation

Percent of queue reserved for high priority pkts

Percent of queue reserved for normal priority pkts

Percent of queue reserved for low priority pkts

Circuit Type = Pt to Pt Protocol (PPP)

LQM Time (secs)

Echo Request Time (secs)

Desired Link Quality

Min Frame Spacing

Extended (32-bit) CRC

Max Pkt Size

IP Address

LCP Active-Open

LCP Auto-Restart

Max Link Latency (ms)

Use UPAP

Compression

1. Bandwidth Reservation

Percent of queue reserved for high priority pkts

Percent of queue reserved for normal priority pkts

Percent of queue reserved for low priority pkts

Circuit Type = LAPB (X.25)

PDN

T1 (0.1 secs)

N2

Min Frame Spacing

Flow Ctrl

Pkt Window

Pkt Size

4. Circuits (Continued)

Circuit Type = LAPB (X.25) (Continued)

- SVC
- Low SVC LCN
- High SVC LCN
- PVC
- Low PVC LCN
- High PVC LCN
- Max Link Latency (ms) (0=none)
- 1. Bandwidth Reservation
 - Percent of queue reserved for high priority pkts
 - Percent of queue reserved for normal priority pkts
 - Percent of queue reserved for low priority pkts

Circuit Type = HP Point to Point

- Point to Point Address
- Minimum Frame Spacing
- Max Link Latency (ms)
- Compression
- Remote signal & sense
- Data Link Layer Protocol
- 1. Bandwidth Reservation
 - Percent of queue reserved for high priority pkts
 - Percent of queue reserved for normal priority pkts
 - Percent of queue reserved for low priority pkts

Circuit Type = FDDI

- LAN Address
- XCVR signal polling

Circuit Type = 802.5

- LAN Address
- XCVR signal polling

5. Circuit Groups

5. Circuit Groups

Circuit Group Name

Circuit Group Speed

1. Circuit Group Members

Circuit Name

2. Circuit Group Backup Members

Circuit Name

3. Circuit Group Pool Members

Circuit Name

6. Bridge

6. Bridge

- Auto Enable
- Forwarding Table Size
- STP Priority
- Max Age
- Flood Interval (sec)
- Bridge ID (Hex)
- Hop Count Reduction
- Table Age Interval (min)
- Spanning Tree Enable
- Hello Time
- Forward Delay
- Internal LAN ID (Hex)
- Loop Detection Time (ms)
- Group LAN ID
- 1. Lists
 - 1. MAC Address Lists
 - List Name
 - 1. List Members
 - MAC Address (low)
 - MAC Address (high)
 - 2. Ethernet Type Lists
 - List Name
 - 1. List Name
 - Ethernet Type (low)
 - Ethernet Type (high)
 - 3. SAP Lists
 - List Name
 - 1. List Members
 - SAP (low)
 - Sap (high)

A: Parameter Finder

6. Bridge (Continued)

1. Lists (Continued)

4. Protocol ID/Org. Code Lists

List Name

1. List Members

Protocol ID/Org. Code (low)

Protocol ID/Org. Code (high)

2. Circuit Groups

Circuit Group Name

Cost

LAN ID (Hex)

Max hops

Learning Bridge

Translational Bridge

STP Priority

Src Rte

Block STE

Traffic Priority

1. Traffic Filters

Precedence

MAC dest (low)

MAC dest (high)

Effect

MAC source (low)

MAC source (high)

Effect

DL Format

DL Format = 802.2 SNAP

Protocol ID/Org. Code (low)

Protocol ID/Org. Code (high)

Effect

Ethertype (low)

Ethertype (high)

Effect

6. Bridge (Continued)

- 2. Circuit Groups (Continued)
 - 1. Traffic Filters (Continued)
 - DL Format = 802.2 LLC*
 - DSAP (low)/(high)/Effect
 - SSAP (low)/(high)/Effect
 - DL Format = Ethernet*
 - Type (low)/(high)/Effect
 - Action
 - 1. User Defined Fields
 - Header
 - Offset
 - Length
 - Effect
 - 1. Values
 - Low Value (hex)
 - High Value (hex)
 - 2. Outgoing Circuit Group Assignment
 - Circuit Group Name
- 3. Circuit Group Load Balancing
 - Circuit Group Name
 - 1. Load Balancing Definitions
 - 1. Load Balancing Selections
 - Protocol Type
 - Circuit Name
- 4. Source Route Bridge IDs
 - Bridge ID (hex)
- 5. Translational Bridge
 - Aging Timer (min)
 - Default Conversion Type
 - 1. Alternate Conversion List
 - MAC Address

7. DoD Internet Router

7.DoD Internet Router

Auto Enable

RIP Network Diameter

Management Priority

Global Broadcast

Mode

Drop Non-Local Arp

Suppress Authentication Traps

1. Lists

1. IP Address Lists

List Name

1. List Members

IP Address (low)

IP Address (high)

2. IP Port Lists

List Name

IP Port (low)

IP Port (high)

2. Network Interface Definition

Internet Address

Subnet Mask

Circuit Group

Receive Broadcast

Transmit Broadcast

Address Resolution

Normal ARP

Proxy ARP

Host Cache

UDP Checksum

RIP Supply

RIP Listen

7. DoD Internet Router (Continued)

2. Network Interface Definition (Continued)

- Default Route Supply
- Default Route Listen
- Poisoned Reverse
- RIP Interface Cost
- Address Mask Reply
- MTU Discovery Option
- Load Balancing
- ASB Flood
- Source Route (Token Ring)

1. Traffic Filters

- Precedence
- IP Dest (low)
- IP Dest (high)
- Effect
- IP Source (low)
- IP Source (high)
- Effect
- Protocol
- UDP/TCP Dest Port (low)/(high)
- Effect
- UDP/TCP Source Port (low)/(high]
- Effect
- Action

1. User Defined Fields

- Header
- Offset
- Length
- Effect
- 1. Values
 - Low Value (hex)
 - High Value (hex)

A: Parameter Finder

7. DoD Internet Router (Continued)

2. Network Interface Definition (Continued)

1. Traffic Filters (Continued)

2. Next Hop Assignment

Next Hop Address

Drop if Next Hop is Down

3. Static Routes

Internet Address

Type (*Static Route, Static Adjacency, Adjacent Host*)

Type = Static Route

Subnet Mask

Next Hop

Cost

Preference

Propagate to RIP

Propagate to EGP

Propagate to OSPF

Make route conditional on an alternate circuit group

Type = Static Adjacency

DLCI

Type = Adjacent Host

LAN Address

Subnet Mask

Encapsulation

4. OSPF

Auto Enable

Router ID

AS Boundary

SPF Hold Down Timer

1. Areas

Area ID

Authentication Type

Stub Area

7. DoD Internet Router (Continued)

4. OSPF (Continued)

1. Areas (Continued)

1. Network Summaries

IP Address

Network Map

2. Interfaces

Circuit Group Name

Password

1. Interface Definition

Interface Type

IP Address

Metric

Interface Type = Broadcast

1. Broadcast Definition

Hello Interval

Dead Interval

Retransmit Interval

Priority

Interface Type = Point-to-Point

1. Point-to-Point Definition

Hello Interval

Dead Interval

Retransmit Interval

Interface Type = Non-Broadcast Multi-Access

1. Non-Broadcast Multi-Access Definition

Priority

Hello Interval

Dead Interval

Retransmit Interval

Poll Interval

1. Neighbors

IP Address

Priority

7. DoD Internet Router (Continued)

5. EGP Configuration

Auto Enable

1. EGP Neighbors

Local Mode

local Address

Remote ASN

Remote Address

Aquisition Mode

Polling Mode

Hello Timer

Polling Timer

6. TCP Configuration

Number of Connections

Transmit Window Size

Receive Window Size

Open/Close Timeout (ms)

Activity Timeout (ms)

Minimum Retransmit Interval

Auto Enable

7. TFTP Configuration

Max Retransmissions

Retransmission Time Out

Connection Close Time Out

Auto Enable

Allow Router to Accept Files

1. Client Address(es)

Internet Addresses

8. Time Protocol Configuration

Auto Enable

Mode

9. BOOTP Configuration

Relay Auto Enable

Max relay hops

7. DoD Internet Router (Continued)

9. BOOTP Configuration (Continued)

1. BOOTP Request Destinations

Dest IP Address

10. Import Route Filters

Network Address

Network Mask

Import Action

From Protocol (*RIP, OSPF, EGP*)

From Protocol = RIP

From Gateway

From Interface

Preference (*If Import Action = Accept*)

From Protocol = OSPF

Type

Tag

Preference (*If Import Action = Accept*)

From Protocol = EGP

From Peer

From Autonomous System

Preference (*If Import Action = Accept*)

11. Export Route Filters

Network Address

Network Mask

Export Action

From Protocol

To Protocol

To Protocol = RIP

To Interface

Metric

To Protocol = OSPF

Type

Tag

A: Parameter Finder

7. DoD Internet Router (Continued)

11. Export Route Filters (Continued)

To Protocol = EGP

To Peer

To Autonomous System

Metric

8. DECNET IV Routing Service

8. DECNET IV Routing Service

- Auto Enable
- Max Nodes
- Max. Area
- Node
- Area
- Max. Hops
- Area Max. Hops
- Max. Cost
- Area Max. Cost
- Max. Bcast Endnodes
- Max. Visits
- Bcast. Routing Timer
- 1. Lists
 - 1. Area Lists
 - List Name
 - 1. List Members
 - Area (low)
 - Area (high)
 - 2. Node Lists
 - List Name
 - 1. List Members
 - Node (low)
 - Node (high)
 - 3. Packet Type Lists
 - List Name
 - 1. List Members
 - Packet Type (low)
 - Packet Type (high)

A: Parameter Finder

8. DECNET IV Routing Service (Continued)

2. Circuit Groups

Circuit Group Name

Cost

Hello Timer

Router Priority

Number of Routers

1. Traffic Filters

Precedence

Dest Area (low) / (high) / Effect

Dest Node (low) / (high) / Effect

Source Area (low) / (high) / Effect

Source Node (low) / (high) / Effect

Packet Type (low) / (high) / Effect

Action

3. Remote Address Map

Remote Area

Remote Node

Remote WAN Address

WAN Protocol

Circuit Name

9. SNMP Sessions

9. **SNMP Sessions**

Community Name

Session mode

Session type

Session type = Trap

Send Event Messages As Traps

Event Filter Level

1. Node Addresses

Node Address

10. Xerox Routing Service

10. Xerox Routing Service

Host Number

Auto Enable

1. Lists

1. Network Lists

List Name

1. List Members

Network Number (low)

Network Number (high)

2. Host Lists

List Name

1. List Members

Host (low)

Host (high)

3. Socket Lists

List Name

1. List Members

Socket (low)

Socket (high)

3. Packet Type Lists

List Name

1. List Members

Packet Type (low)

Packet Type (high)

10. Xerox Routing Service (Continued)

2. Network Interface Definitions

Network Number

Circuit Group

RIP Supply

RIP Listen

RIP Interface Cost

Checksums On

Source Route (Token Ring)

RIP and SAP split horizon

Random load balancing

1. Traffic Filters

Precedence

Dest Network (low) / (high) / Effect

Dest Host (low)/(high)/Effect

Dest Socket (low) / (high) / Effect

Source Network (low) / (high) / Effect

Source Host (low) / (high) / Effect

Source Socket (low)/(high)/Effect

Packet Type (low) / (high) / Effect

Action

3. Static Route Definitions

Target Net

Next Hop Host

Next Hop Net

RIP Table Cost

11. IPX Routing Service

11. IPX Routing Service

Auto Enable

1. Lists

1. Network Lists

List Name

1. List Members

Network Number (low)

Network Number (high)

2. Host Lists

List Name

1. List Members

Host (low)

Host (high)

3. Socket Lists

List Name

1. List Members

Socket (low)

Socket (high)

4. Packet Type Lists

List Name

1. List Members

Packet Type (low)

Packet Type (high)

2. Network Interface Definitions

Network Number

Circuit Group

RIP Supply

RIP Listen

RIP Interface Cost

Encapsulation Type

WAN SAP Period (mins)

11. IPX Routing Service (Continued)**2. Network Interface Definitions (Continued)**

Accept NETBIOS Bcasts from net
Deliver NETBIOS Bcasts to net
Source Route (Token Ring)
SAP driven RIP supply
RIP and SAP split horizon
Random load balancing
IPXWAN

1. SAP Network Level Filter Definitions

Action
Network Number (Hex)
Server Type (Hex)

2. SAP Server Level Filter Definitions

Action
Server Type (Hex)
Server Name

3. NETBIOS Broadcast Static Routes

Dest Network (Hex)
NetBIOS Resource Name

4. Traffic Filters

Precedence
Dest Network (low) / (high) / Effect
Dest Host (low)/(high)/Effect
Dest Socket (low) / (high) / Effect
Source Network (low) / (high) / Effect
Source Host (low) / (high) / Effect
Source Socket (low)/(high)/Effect
Packet Type (low) / (high) / Effect
Action

3. Static Route Definitions

Target Net
Next Hop Host
Next Hop Net
RIP Table Cost

A: Parameter Finder

11. IPX Routing Service (Continued)

4. Internal Network Number and Router Name

Internal Network Number

Internal Router Name

12. AppleTalk Router

12. AppleTalk Router

- Auto Enable
- AARP Mapping Table Size
- Routing Table Size
- Zone Table Size
 - 1. Lists
 - 1. Network Lists
 - List Name
 - 1. List Members
 - Network (low)
 - Network (high)
 - 2. Node Lists
 - List Name
 - 1. List Members
 - Node (low)
 - Node (high)
 - 3. Socket Lists
 - List Name
 - 1. List Members
 - Socket (low)
 - Socket (high)
 - 4. DDP Type Lists
 - List Name
 - 1. List Members
 - Network (low)
 - Network (high)

A: Parameter Finder

12. AppleTalk Router (Continued)

2. Circuit Groups

Circuit Group Name

Probe

Checksum

Node ID

Source Route (Token Ring)

Seed Router

Seed Router = Yes

Network Min

Network Max

Network

Default Zone Name

Zone Filter

Cost

Seed Router = Yes

1. Zone Name List

Zone Name

2. Traffic Filters (*Same as "1. Traffic Filters", below*)

1. Traffic Filters (*Numbered "2" if Seed Router = Yes*)

Precedence

Dest Net (low) / (high) / Effect

Dest Node (low)/(high)/Effect

Dest Sock (low) / (high) / Effect

Source Net (low) / (high) / Effect

Source Node (low) / (high) / Effect

Source Sock (low)/(high)/Effect

DDP Type (low) / (high) / Effect

Action

13. X.25 Network Service

13. X.25 Network Service

Auto Enable

1. PDN Service

Lower Circuit Name

Max Queue Size

MTU Size

Upper Circuit Name

Local DTE Address

Closed User Group

Closed User Group = Yes

Outgoing Access

Group Number

1. X.25 Address Map

IP Address

X.121 Address

Broadcast

Max Conns

Min Idle Time (secs)

Max Idle Time (secs)

Call Retry Time (secs)

Flow Ctrl

Flow Ctrl = Negot

Negotiated Pkt Window

Negotiated Pkt Size

A: Parameter Finder

13. X.25 Network Service (Continued)

2. DDN IP Service

Lower Circuit Name
Precedence
Max Queue Size
Max Conns/Dest
Min Idle Time (secs)
Max Idle Time (secs)
Upper Circuit Name
Internet Address

3. HP Point to Point Service

Lower Circuit Name
Max Queue Size
Local DTE Address

1. X.25 Virtual Circuits

Circuit Name
Remote DTE Addr
Connection ID
Flow Ctrl

Flow Ctrl = Negot

Negotiated Pkt Window
Negotiated Pkt Size
Permanent Circuit

14. V.25 bis Network Mapping

14. V.25 bis Network Mapping

1. Phone # to IP mapping

IP Next Hop

Connect retry count

Connect wait time (sec)

Hold down time (sec)

VC inactivity time (sec)

1. Outbound call number

Remote Station Number

Subaddress

Index

!

!...16-4
32-bit encapsulation...4-15
802.2 LLC...6-8
802.2 SNAP...6-8

A

A.08 code...16-21, 16-23
AARP Mapping Table Size...12-6
Accept NETBIOS Bcasts from net...11-5
Acquisition Mode...7-6
Action...6-5, 7-6, 8-4, 10-4, 11-5
Action on circuit group enable/disable...7-6
Adapter Record...4-5, A-6, A-8
Address Mask Reply...7-6
Address Resolution...7-7
AEP...16-4
Aging Timer (min)...6-5
Alarm...16-32
Alarm Timer...4-5
Allowed inbound call numbers...A-7
Annex D switch...4-19
ANSI Annex D...4-19
ANSI terminal...16-98
AppleTalk
 AARP Mapping Table Size ...12-6
 Checksum...12-6
 Circuit Group...12-6
 DDP Type Lists...12-6
 Default Zone Name...12-7
 Dest Sock (low)...12-9
 List Name...12-11
 Multicast DLCI...4-5
 Network Number (low)...12-12
 Node Lists...12-13
 Seed Router...12-14
 Source Node (low)...12-16
 Source Route (Token Ring)...12-17
 Zone Name...12-18
ARE...6-13, 6-16, 18-80

- Area...8-4
- Area (high)...8-4
- Area (low)...8-4
- area list, DECnet...8-4
- Area Max. Cost...8-5
- Area Max. Hops...8-5
 - ...8-5
- ARP
 - Group Address...4-5
 - Circuits...4-5
 - multicast DLCI...4-5
 - table...16-41
 - unpredictable results...7-20
- ASB Flood...7-8
- at (AppleTalk)...16-32
- atmib...16-32
- Atping...16-4
- authentication key...7-21
- Authentication Type...7-8
- Auto Enable...11-5, 13-4
 - AppleTalk...12-5
 - Bridge...6-5
 - Circuits...4-5
 - DECnet...8-5
 - global...1-4, 6-6
 - IP...7-9
 - X.25...4-5
 - XNS...10-4
- Automatic Reboot...1-4

B

- bandwidth...4-2
- Bandwidth Reservation...4-6
- Baud Rate...1-4, 1-9
- Bcast Routing Timer...8-6
- Beginning Day...1-4
- Beginning Month...1-5
- Bit/Char...1-5
- bitmap table...4-22
- Block STE...6-6
- boot...1-4, 1-9, 16-5
- BOOTP...7-25
- BPDU...6-11, 6-16
- Bridge Flood multicast DLCI...4-6
- Bridge ID (hex)...6-6

Bridge parameters
 Action...6-5
 Aging Timer...6-5
 Block STE...6-6
 Bridge ID (Hex)...6-6
 Circuit Group Name...6-7
 Default Conversion Type...6-7
 DSAP (low)...6-8
 Flood Interval (sec)...6-10
 Forward Delay...6-10
 Hello...6-12
 High Value (hex)...6-12
 Hop Count Reduction...6-12
 LAN ID (Hex)...6-13
 Length...6-13
 List Name...6-13
 Loop Detection Time (hex)...6-13
 MAC Address (high)...6-14
 MAC Address (low)...6-14
 MAC dest (high)...6-15
 Max Hops...6-16
 Protocol ID/Org. Code (high)...6-17
 Protocol ID/Org. Code (low)...6-17
 SAP (high)...6-18
 Spanning Tree Enable...6-19
 SSAP (high)...6-20
 SSAP (low)...6-20
 STP Priority...6-21
 Type (high)...6-22
Bridge Type...3-3
bridge type, FDDI...3-3
Broadcast...13-4
Browse...16-6
Buf...16-31 - 16-32
buf object...16-30
buffers...15-8

C

cable, F1047-80002...16-100
cache table, ARP...16-41
Call restrictions...4-6
Call Retry Timer (secs)...13-4 - 13-5
cct...16-32
Channel Management...4-6
Chassis...16-32

- Checksum...12-6
- checksum, faulty...15-15
- Checksums On...10-4
- Circuit Group...7-9, 10-4, 11-6, 12-6
- Circuit Group Name...6-7, 8-6, 12-14
 - Circuits...5-3
- Circuit Group Speed...5-3
- Circuit Name...6-7, 13-5
 - Circuits...3-3, 4-7, 5-3
- Circuit Type...4-7, 13-5
- Circuits
 - ARP Group Address...4-5
 - Auto Enable...4-5
 - Call restrictions...4-6
 - Channel Management...4-6
 - Circuit Group Name...5-3
 - Circuit Group Speed...5-3
 - Circuit is enabled...4-11
 - Circuit Type...4-7
 - Compression...4-9
 - Connect inactivity time (sec)...4-10
 - Connect Retries...4-10
 - Connect retry count...4-10
 - Connect wait time (sec)...4-10
 - Connect when...4-11
 - Data is available or on incoming calls...4-11
 - Data Link Layer Protocol...4-11
 - Desired Link Quality...4-12
 - DLCI Encoding Length...4-13
 - Echo Request Times (sec)...4-14
 - Events for Error...4-14
 - Extended (32-bit) CRC...4-14
 - Group Address...4-15
 - Hearbeat Down Count...4-15
 - Hearbeat Polling Interval...4-15
 - Individual Address...4-15
 - Interval Between Polls...4-15
 - IP Address...4-15
 - LAN Address...4-15
 - LCP Active-Open...4-17
 - LCP Auto Restart...4-17
 - Link Idle Time (T3)...4-17
 - LQM Time (secs)...4-17
 - Management Type...4-18
 - Max channels to aggregate...4-19
 - Max Link Latency (ms)...4-19

- Maximum Packet Size...4-20
- Min Frame Spacing...4-20
- Minimum connect duration (sec)...4-21
- Modulus...4-21
- Monitored Events...4-22
- Multicast Support...4-22
- Password of Remote Station...4-23
- Perchannel bandwidth...4-23
- Permanent Virtual Circuit...4-23
- Point-to-Point Address...4-23
- Poll Interval (seconds)...4-24
- Provide InARP...4-24
- Quality of Service...1-5, 4-24
- Relay Timer (T1)...4-26
- Remote Address...1-5, 4-25
- Remote signal & sense timeout (sec)...4-26
- Remote Signal and Sense...4-25
- Remote Station Number...4-26
- Send CIC on all allowed INCs...4-26
- Server Password...4-27
- Server User ID...4-27
- Subaddress...4-27
- Use DXI v3.2...4-27
- Use Heartbeat Poll...4-27
- Use SNAP...4-28
- Use UPAP...4-28
- User ID of Remote Station...4-28
- Xcvr Signal Polling...4-29
- Clear button...16-15
- Clock Source...3-3
- Clock Speed...3-3 - 3-4
- clock speed limit, RS-232 cable...3-4
- clock, at boot...1-9
- Community Name...9-3
- Compression...4-9
- compression limitation...4-9
- Conditional Circuit Group...7-9
- Config...16-6, 16-32
- Configuration editor
 - menu path...A-2
 - parameters, finding...A-2
- configuration, changing...16-21
- configuration, download...16-100
- configuration, remote...16-20
- Conflict Alert...16-26
- Connect inactivity time (sec)...4-10

- Connect Retries...4-10
- Connect retry count...4-10, 4-12, 14-3
- Connect wait time (sec)...4-10, 14-3
- Connect when...4-11
- Connection Close Time Out...7-9
- Connection ID...13-5
- Connection Inactivity Time...1-5
- connector...3-3 - 3-4
- connector name, default...3-4
- console port, connecting...1-5
- Cost...6-7, 7-9, 8-6
- Crash...16-7
- crash, software...1-4
- CUG (Closed Users Group)...13-5

D

- Data is available or on incoming calls...4-11
- Data Link Layer Protocol...4-11, 4-25
- data-link layer...4-2
- datagram field...12-10
 - DDP type...12-10
 - destination network...12-10
 - destination node...12-10
 - destination socket...12-10
 - source network...12-10
 - source node...12-10
 - source socket...12-10
- Date
 - See Time
- daylight savings time...1-5
- Daylight Time Rule...1-5
- DCE, frame relay...4-5
- DDN (Defense Data Network)...13-10
- DDP Type (high)...12-6
- DDP type (low)...12-7
- DDP type field...12-10
- DDP Type Lists...12-6
 - AppleTalk...12-10
- Debug (event log)...1-6
- decnet...16-32
- DECnet multicast DLCL...4-11
- DECnet parameters
 - Area (high)...8-4
 - Area (low)...8-4
 - Area Max. Cost...8-5

- Bcast Routing Timer...8-6
- Circuit Group Name...8-6
- Dest Network (low)...8-7
- Dest Node (high)...8-7
- Max. Area...8-9
- Max. Bcast End nodes...8-9
- Max. Cost...8-9
- Max. Hops...8-9
- Max. Nodes...8-9
- Node...8-10
- Node (high)...8-10
- Node (low)...8-10
- Packet Type (low)...8-11
- Precedence...8-11
- Remote WAN Address...8-12
- Source Area (low)...8-12
- Source Node (high)...8-13
- WAN Protocol...8-14
- Default Conversion Type...6-7
- Default Route Listen...7-10
- Default Route Listen, prerequisite...7-10
- Default Route Supply...7-10
- Default Route Supply, prerequisite...7-10
- Default Zone Name...12-7
- Defense Data Network (DDN)...13-10
- Delay after connect failure (min)...4-12
- Deliver NETBIOS Bcasts to net...11-6
- Desired Link Quality...4-12
- Dest Host (high)...10-5, 11-6
- Dest Host (low)...10-5, 11-6
- Dest IP Address...7-10
- Dest Net (high)...12-7
- Dest Net (low)...12-8
- Dest Network (Hex)...11-7
- Dest Network (high)...8-6, 10-5, 11-7
- Dest Network (low)...8-7, 10-6, 11-7, 12-8
- Dest Node (low)...8-8, 12-9
- Dest Sock (high)...12-9
- Dest Sock (low)...12-9
- Dest Socket (high)...10-6, 11-8
- Dest Socket (low)...10-7, 11-8
- Destination Network...12-10
- destination node field...12-10
- destination socket field...12-10
- Disable...16-8
- DL Format...6-7

- DLCI...4-23 - 4-24, 7-10
- DLCI Encoding Length...4-13
- DLCI Encoding Type...4-13
- dls...16-32
- driver...16-32
- Drop If Next Hop is Down...7-10
- drs...16-32
- DSAP (high)...6-8 - 6-9
- DSAP (low)...6-8
- DSU...4-15
- DSU/CSU...4-27
- DTR...4-10
- duplicate station address...4-16
- DXI...4-27

E

- echo...16-33
- Echo Request Times (sec)...4-14
- Edit...16-8
- Effect...6-9, 8-8, 10-7, 11-9, 12-10
 - Don't Match...12-10
 - Ignore...12-10
 - IP...7-10
 - Match...12-10
- EGP connections...7-6
- Enable...16-9
- enabling software modules...1-4
- encapsulation...4-14, 7-11
- Encapsulation Type...7-11, 11-9
- Ending day...1-6
- Ending month...1-6
- Ethernet...6-8
- Ethernet Type (high)...6-9
- Ethernet Type (low)...6-10
- Ethernet V2 format...6-7
- Event Filter Level...1-6, 9-3
- event log...16-11, 17-2
- Event Log message levels...1-6
- Events for Error...4-14
- Exit...16-10
- exmib...16-32
- explorer frames...16-84
- explorer frames...6-6
- Export Action...7-11
- export route filter...7-20

Extended (32-bit) CRC...4-14
external clock source...3-3

F

F1047-80002 cable...16-100
factory default...15-3
FDDI bridge type...3-3
file
 NCL command output...16-100
 print to...16-19
 upload...16-99
filter rule...6-5
filter, priority values...6-17
filtering, frames...6-9
filtering, IP...7-17
filters, in bridging...6-7
Flood Interval (sec)...6-10
flooding...15-7
Flow Control...1-7
Flow Control Parameter Negotiation...13-6
Flow Ctrl...13-6
Forward Delay...6-10, 6-21
Forwarding Table Size...6-11, 6-20
forwarding table, bridge...6-19
frame relay address field...4-13
frame relay DCE...4-5
Frame type
 See Encapsulation type
frames, bridged...6-5
From Autonomous System...7-12
From Gateway...7-12
From Interface...7-12
From Peer...7-12
From Protocol...7-12
full-status inquiry messages...4-15

G

- General Multicast DLCI...4-15
- Get...16-34
- global auto enable...1-4
- Global Broadcast...7-13
- GMT...1-9
- Grenwich Mean Time...1-9
- Group Address...4-15
- Group LAN ID...6-11
- Group Number...13-6

H

- HDLC...4-8, 4-20 - 4-21
- Header...6-11, 7-13
- Heartbeat Down Count...4-15
- heartbeat polling...4-27
- Heartbeat Polling Interval...4-15
- heartbeat polling messages...4-15
- Hello Interval...7-13
- Hello Time...6-12, 6-21
- Hello Timer...7-13, 8-9
- Help...16-10
- High LCN...13-7
- High PVC LCN...13-6
- High SVC LCN...13-6
- High Value (hex)...6-12
- Hold down time...14-3
- Hop Count Reduction...6-12
- Host (high)...10-8
- Host (high)...10-8
- Host (low)...10-8
- Host Cache...7-14
- Host lists...10-8, 11-10
- Host Number...10-8
- Host Number (high)...11-10
- Host Number (low)...11-10
- hotswap...16-25 - 16-26
- HP 700 series terminal...16-19
- HP Remote Bridge...4-25, 16-28
- hpn...16-32
- hw...16-32

I

- ICMP address mask reply message...7-6
- ICMP datagram...15-15
- IEEE 802.2 test packet...16-28
- IHU response...7-21
- Import Action...7-14
- Individual Address...4-15
- Information (event log)...1-6
- interface module...4-27
- Interface Type (OSPF)...7-14
- internal clock source...3-3
- Internal LAN ID (Hex)...6-12
- Internal Network Number...11-11
- Internal Router Name...11-11
- Internet Address...7-15, 13-7
- Intervals Between Polls...4-15
- ip...16-32
- IP Address...4-15, 7-15, 13-7
- IP Address (high)...7-15
- IP Address (low)...7-15
- IP datagram, disposition...7-6
- IP datagrams...15-15
- IP Dest (high)...7-15
- IP Dest (low)...7-16
- IP filters per interface...7-22
- IP Next Hop...14-4
- IP parameters
 - Action on circuit group enable/disable...7-6
 - Address Mask Reply...7-6
 - ASB Flood...7-8
 - Auto Enable...7-9
 - Default Route Supply...7-10
 - Drop If Next Hop is Down...7-10
 - Effect...7-10
 - Encapsulation Type...7-11
 - Export Action...7-11
 - From Gateway...7-12
 - From Interface...7-12
 - From Protocol...7-12
 - Header...7-13
 - Host Cache...7-14
 - IP Source (high)...7-16
 - IP Source (low)...7-17
 - Max Relay Hops...7-19
 - Max Retransmissions...7-19

- Metric...7-19
- MTU Discovery Option...7-19
- Next Hop...7-20
- Offset...7-21
- Poisoned Reverse/Split Horizon...7-21
- Preference...7-22
- Propagate to RIP...7-23
- Receive Broadcast...7-24
- RIP Interface Cost...7-25
- RIP Supply...7-26
- SNAP...7-11
- Source Route (Token Ring)...7-26
- To Interface...7-27
- To Protocol...7-27
- Transmit Broadcast...7-28
- Type...7-28
- UDP Checksum Off...7-29
- UDP/TCP Dest Port (low)...7-29
- UDP/TCP Source Port (high)...7-30
- UDP/TCP Source Port (low)...7-30
- Value (hex)...7-13
- IP Port (high)...7-16
- IP Port (low)...7-16
- IP Source (high)...7-16
- IP Source (low)...7-17
- IPX...16-32
 - Action...11-5
 - Auto Enable...11-5
 - Circuit Group...11-6
 - Deliver NETBIOS Bcasts to net...11-6
 - Dest Network (Hex)...11-7
 - Dest Network (high)...11-7
 - Dest Socket (high)...11-8
 - Effect...11-9
 - Encapsulation Type...11-9
 - Host Number (high)...11-10
 - Network Number (high)...11-11
 - Network Number (low)...11-12
 - Next Hop Host...11-12
 - Packet Type (high)...11-12
 - Packet Type (low)...11-13
 - Precedence...11-13
 - Random load balancing...11-13
 - RIP and SAP split horizon...11-14
 - RIP Listen...11-14
 - RIP Supply...11-14

- SAP driven RIP supply...11-15
- Socket (low)...11-16
- Source Route (Token Ring)...11-18
- Source Socket (low)...11-18
- IPXWAN...11-11
- isdn...16-33
 - See v.25 bis

K - L

- key...16-32

- LAN Address...4-15, 7-17
- LAN ID (Hex)...6-13
- latency...4-19
- lb...16-32
- lbmib...16-32
- LCO Auto Restart...4-17
- LCP Active-Open...4-17
- LCP connection...4-17
- Learning Bridge...6-13
- Length...6-13, 7-17
- line charges, minimizing...4-21
- Lines menu...A-5
- Link Idle Time (T3)...4-17
- link verification...4-5
- List...16-35
- List Members...12-10
- List Name...6-13, 7-17, 8-9, 11-11, 12-11
- List Name...11-11
- LLC2 connection...4-10
- LMI...4-23
- LMI (Local Management Interface)...4-19
- LMI switch...4-19
- Load Balancing...7-17
- Local Address...7-18
- Local ASN...7-18
- Local DTE Address...13-8
- Log...16-11, 16-32
- LOG BOTTOM...16-19
- Logi...16-13
- Logout...16-15, 16-27
- Loop Detection Time (Hex)...6-13
- Low LCN...13-6 - 13-7
- Low PVC LUN...13-8
- Low SVC LCN...13-8

Low Value (hex)...6-13, 7-18
Lower Circuit Name...13-8
LQM Time...4-18
LQM Time (secs)...4-17

M

MAC address
 See also *station address*
MAC Address (high)...6-14
MAC Address (low)...6-14
MAC data link header...6-14
MAC dest (high)...6-14
MAC dest (low)...6-15
MAC source (high)...6-15
MAC source (low)...6-15
Major (event log)...1-6
Make route conditional...7-18
manage object...16-31
Managed objects table...16-32
Management information base
 See MIB
Management Priority...7-18
Management Type
 ANSI Annex D...4-19
 Circuits...4-18
 LMI (Local Management Interface)...4-19
 Unsupported...4-19
manager password
 See password
map, object identification...16-36
Max Age...6-16, 6-21
Max channels to aggregate...4-19, A-8
Max Conns...13-8
Max Hops...6-16
Max Idle Time (secs)...13-8
Max Link Latency (ms)...4-19 - 4-20
Max Link Latency (X.25)...13-9
Max Queue Size...13-9
Max Relay Hops...7-19
Max Retransmissions...7-19
Max. Area...8-9
Max. Bcast End nodes...8-9
Max. Cost...8-9
Max. Hops...8-9
Max. Nodes...8-9

- Max. Visits...8-10
- Maximum Packet Size...4-20
- mem...16-32
- Menu path...A-2
- Metric...7-19
- mgr...16-32
- MIB...16-32, 16-36
 - variables...16-31
 - foreign...16-51
 - remote...16-48
- Min Channels to Aggregate...4-20
- Min Frame Spacing...4-20, 13-9
- Min Idle Time (secs)...13-9
- Minimum connect duration (secs)...4-21
- Minimum Frame Spacing...4-21
- Mode...7-19
- Mode (normal or end-node)...7-19
- Mode (time protocol)...7-19
- modem...1-7
- Modem Connction Time...1-7
- Modem Disconnection Time...1-7
- Modem Lost Receive Ready Time...1-8
- Modulus...4-21, 4-28
- Monitored Events...4-22
- More...16-6, 16-14
- MTU Discovery Option...7-19
- MTU Size...13-9
- MTU, probe/reply...7-19
- multicast address...4-5, 4-16
- Multicast Support...4-22

N

- N2...13-10
- name...16-32
- NCL commands...16-2
- NCL ERR--invalid...16-5, 16-15
- Negotiated Pkt Size...13-10
- Negotiated Pkt Window...13-10
- Neighbor ID...7-20
- neighbor-reachability...7-21
- net fail LED...4-29, 17-56
- Net Hop Host...10-9
- net mask...16-42
- NET2...13-10
- NetBIOS Resource Name...11-12

- Network...12-11
- Network Address...7-20
- Network lists...10-9, 11-11, 12-10,12-11
- Network Mask...7-20
- Network Max...12-11
- Network Min...12-12
- Network Number...10-9, 11-11
- Network Number (Hex)...11-12
- Network Number (high)...10-8, 11-11
- Network Number (low)...10-9, 11-12, 12-12
- Next Hop...7-20
- Next Hop Address...7-20
- Next Hop Host...11-12
- Next Hop Net...10-9, 11-12
- Node...8-10
- Node (high)...8-10, 12-12
- Node (low)...8-10, 12-13
- Node Address...9-3 - 9-4
- Node Address (SNMP)...9-3
- Node ID...12-13
- Node Lists...12-10, 12-13
- Non Local ARP Source...7-20
- Non-local ARP...7-20
- Normal ARP...7-21
- Novell...6-8
- Number of Routers...8-11

O

- object identification codes...16-35 - 16-36
- Offset...6-16, 7-21
- operating code...16-96
- operating code version...16-21
- operating code, download...16-93, 16-95
- operating code, version...16-95
- OSI multicast DLCI...4-23
- OSPF...16-32
 - backbone...7-20
 - commands...16-72
 - Hello packets...7-13
 - interface type...7-14
 - prerequisite...7-10
- Ospf Intf...16-74
- Ospf Errs...16-73
- Ospf Lsdb...16-76
- Ospf Nbrs...16-78

Ospf Rtab...16-80
Ospf Tq...16-82
Outgoing Access...13-10

P

Packet Type (high)...8-11, 10-9, 11-12
Packet Type (low)...8-11, 10-10, 11-13
Packet type lists specify...11-12
Page...16-14
parameter finder...A-2
Parameter finder, how to use...A-2
Parity...1-8
pass-thru...4-11
Password...7-21, 16-15
 incorrect...16-21
 manager...16-96
 of Remote Station...4-23
PC host file...16-98
PC upload...16-99
PC, terminal...16-19
PDN...13-10
Percent of queue reserved...4-23
Perchannel Bandwidth...4-23
Performance (event log)...1-6
Permanent Virtual Circuit...4-23
Physical Access Method...3-4
physical address
 See station address
Ping...16-18
Pkt Size...13-11
Pkt Window...13-11
pm...16-32
Point-to-Point Address...4-23
Point-to-Point WAN links...4-9
Poisoned Reverse/Split Horizon...7-21
Poll Interval...4-5, 7-22
Poll Interval (seconds)...4-24
Polling Mode...7-21
Polling Timer...7-22
PPP address...4-23
Precedence...6-17, 7-22
 8-11, 10-10, 11-13, 12-13
Precedence (X.25)...13-11
Preference...7-22
Print...16-19

- print to file...16-19
- priorities for different packet types...6-22
- Priority...6-17, 7-23
- Probe...12-14
- Procomm Plus...16-98 - 16-100
- Propagate to OSPF...7-23
- Propagate to RIP...7-23
- propagated route...7-12
- Protocol...2-3, 7-23
- Protocol ID/Org. Code (high)...6-17
- Protocol ID/Org. Code (low)...6-17
- Protocol Type...6-18
- Provide InARP...4-24
- Proxy ARP...7-24
- PVC...13-11

Q - R

- Quality of Service...13-11
 - circuits...1-5, 4-24
- Quick...16-20
- Quick Configuration...3-3, 16-20
- Quick Remote...16-20
- Random load balancing...11-13
- Rboot...16-21
- Receive Broadcast...7-24
- redirect output...16-93
- Relay Auto Enable...7-24
- Relay Time (T1)...4-26
- Remote Address...1-5, 4-25, 7-25
- Remote Area...8-12
- Remote ASN...7-25
- Remote DTE Address...13-11
- Remote LAN Address...4-25
- Remote Node...8-12
- Remote Signal and Sense...4-25
- Remote signal and sense timeout...4-25 - 4-26
- Remote Station Number...4-26, 14-4
- Remote WAN Address...8-12
- Repeat...16-22
- repeat command...16-4
- Reset...16-39
- response time sensitivity...4-19
- Retransmission Time Out...7-25
- Retransmit Interval...7-25
- Retry Counter (N2)...4-26

RFC 1156...16-40
Rget...16-52
Rgeta...16-41
Rgetat...16-55
Rgetata...16-57
Rgetatr...16-58
Rgetb...16-59
Rgetd...16-60
Rgetda...16-61
Rgetdn...16-63
Rgeti...16-42
Rgetif...16-68
Rgetir...16-64
Rgetis...16-66
Rgetm...16-53
Rgetms...16-43
Rgetmw...16-49
Rgetr...16-45
Rgets...16-47
Rgetw...16-50
Rgetxr...16-70
rif...18-80
Ring Interface...3-5
RIP...7-13
RIP and SAP split horizon...11-14
RIP Interface Cost...7-25, 10-10, 11-14
RIP Listen...7-26, 10-10, 11-14
RIP Network Diameter...7-25
RIP Supply...7-26, 10-11, 11-14
RIP Table Cost...11-14
RIP updates...7-12
rok...16-32
Router ID...7-26
Router Priority...8-12
Routing Table Size...12-14
RS-232 cable, clock speed...3-4

S

SAP (high)...6-18
SAP (low)...6-18
SAP driven RIP supply...11-15
Screen Refresh Rate...1-8
security, console...16-15
Seed Router...12-14
Send CIC on all allowed INC's...4-26

- Send Event Messages As Traps...9-4
- Server Name...11-15
- Server Password...4-27
- Server Type
- Server Type (Hex)...11-15
- Server User ID...4-27
- services, routing...1-4
- Session mode...1-8, 9-4, A-4
- Session type...9-4
- severity, event log...16-11
- severity, event log message...17-2
- single-route explorer frames...6-6
- Slot Number...4-27
- slot number, HP router 650...16-31
- slot number, series 200/400...16-31
- SNA packets...6-22
- SNAP...7-11
- SNMP...16-32
 - Community Name...9-3
 - Send Event Messages As Traps...9-4
 - Session Mode...9-4
- SNMP agent...16-54
- Socket (high)...10-11, 11-15, 12-15
- Socket (low)...10-11, 11-16, 12-15
- Socket Lists...12-10, 12-14
- Software...2-3
- Source Area (high)...8-12
- Source Area (low)...8-12
- Source Host (high)...10-12, 11-16
- Source Host (low)...10-12, 11-16
- Source Net (high)...12-15
- Source Net (low)...12-15
- Source Network (high)...10-12, 11-17
- Source Network (low)...10-13, 11-17
- source network field...12-10
- Source Node (high)...8-13, 12-16
- Source Node (low)...8-13, 12-16
- source node field...12-10
- Source Route (Token Ring)...6-20, 7-26, 10-11, 11-18, 12-17
- source route entries, aging...6-5
- Source Route Translation Bridging
 - See TRNSB
- source routing...6-6, 6-19
- source routing, parallel bridges...6-7
- Source Sock (high)...12-17
- Source Sock (low)...12-17

- Source Socket (high)...10-13, 11-18
- Source Socket (low)...10-14
- source socket field...12-10
- source-route bridging...16-84, 16-86
- source-route packets...18-80
- spanning tree...16-84 - 16-85
- spanning tree algorithm...6-7, 6-21
- Spanning Tree Enable...6-19
- spanning tree parameter values...6-19
- speed sense...1-4
- Split horizon...7-21
- Src Rte...6-20
- SRF...18-80
- SRF (specially routed froma...6-11
- SSAP (high)...6-20
- SSAP (low)...6-20
- Stamp...16-23
- static route...7-11
- station address...4-15 - 4-16, 4-25, 7-7, 7-17
- Stats...16-24
- status inquiry messages...4-24
- STE...16-84, 18-80
- Stop Bits...1-8
- STP Priority...6-21
- stub area...7-9, 7-26
- Subaddress...4-27, 14-4
- Subnet Mask...7-27
- Summary...16-25
- Suppress Authentication Traps...7-27
- SVC...13-12, 16-32
- synchronous line...3-4
- synchronous timing signals, origin...3-3
- System Contact...1-9
- System Location...1-9
- System Name...1-9
- System Session...1-9

T

- T1...4-26, 13-12
- Table Age Interval...6-21
- Tag...7-27
- Target Net...10-14, 11-19
- TCP...15-15, 16-32
- TCP connections...16-27
- TCP segments, disposition...7-6

- TELENET...13-10
- Telnet...16-27, 16-32
- Telnet Mode...1-8
- Terminal...1-9
- terminal emulation...1-9
- terminal, ANSI...16-98
- terminal, VT100...16-98
- Test...16-28
- TFTP...7-9, 16-33, 16-93, 16-95 - 16-96
- Time...16-29
- time rule...1-4 - 1-6
- Timeout...16-21
- timep...16-32
- timer...16-32
- timer, OSPF...16-82
- Timezone...1-9
- TIP Table Cost...11-14
- To Interface...7-27
- To Protocol...7-27
- token ring service...3-5
- Traffic Priority...6-22
- transferring configuration...16-98 - 16-104
- transferring NCL display...16-98 - 16-104
- Transit Area...7-28
- Transitional Bridge...6-22
- Translational Bridge...6-22
- translational bridging (TRNSB)...6-5
- transmission rate, data...1-4
- Transmit Broadcast...7-28
- TRNSB...6-22
- TT output line...3-3
- Type...7-28
 - for IP import route filters...7-28
 - of static route...7-28
- Type (high)...6-22
- Type (high), Ethernet...6-22
- Type (low)...6-23

U

- UDP...15-15
- UDP Checksum Off...7-29
- UDP datagram, disposition...7-6
- UDP/TCP Dest Port (high)...7-29
- UDP/TCP Dest Port (low)...7-29
- UDP/TCP Source Port (high)...7-30

- UDP/TCP Source Port (low)...7-30
- UK-PSS...13-10
- UPAP...4-28
- Upper Circuit Name...13-12
- Use Bitmap...13-11
- Use DXI v3.2...4-27
- Use Heartbeat Poll...4-27
- Use SNAP...4-28
- Use UPAP...4-28
- User ID of Remote Station...4-28
- user password
 - See Password

V - W

- v.25 bis map entry...16-87 - 16-90
- v.25 bis, net fail LED...17-56
- Value (hex)...7-13
- VC inactivity time (sec)...14-4
- version, operating code...16-23, 16-95
- vertical frequency rate...1-8
- VT100 terminal...16-98
- VT100 terminal emulation...1-9
- WAN net fail LED...17-56
- WAN Protocol...8-14
- WAN SAP Period...11-19
- Warning (event log)...1-6
- wild card...16-34, 16-39
- Window Size...4-28

X - Z

- X.121 Address...13-12
- x.25...16-33
- X.25 parameters
 - Broadcast...13-4
 - PVC...13-11
 - SVC...13-12
 - Use Bitmap...13-11
- Xcvr Signal Polling...4-29
- XNS
 - Action...10-4
 - Checksums On...10-4
 - Circuit Group...10-4
 - Dest Host (high)...10-5
 - Dest Host (low)...10-5
 - Dest Network (high)...10-5

Dest Network (low)...10-6
Dest Socket (high)...10-6
Dest Socket (low)...10-7
Effect...10-7
Host (low)...10-8
Network Number...10-9
Network Number (high)...10-8
Next Hop Host...10-9
Next Hop Net...10-9
Packet Type (high)...10-9
RIP Interface Cost...10-10
RIP Listen...10-10
RIP Supply...10-11
Socket (high)...10-11
Source Network (low)...10-13
Source Route (Token Ring)...10-11
Source Socket (high)...10-13
Source Socket (low)...10-14
XON/XOFF...1-7
xrx...16-33
zmodem...16-98 - 16-100, 16-102 - 16-103
Zone Filter...12-18
Zone Name...12-18
Zone Table Size...12-18



©Copyright 1994
Hewlett-Packard Company
Printed in Singapore 7/94

Manual Part Number
5962-8305