Release Notes

Software Releases A.09.60 and B.09.60

HP AdvanceStack Routers

Part Number: 5963-6569, E0895
Edition 3, August 1995
Printed in Singapore

Product Numbers and Software Version

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

- A.09 series,
  - including A.09.60
- B.09 series,
  - including B.09.60

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.

Hewlett-Packard
8000 Foothills Boulevard
Roseville, California 95747-6588
U.S.A.
916-786-8000

Preface

This document supplements your router manual set:

- *Installation Guide*
- *User's Guide*
- *Operator's Reference*
- *HP Routing Services and Applications*
- *Documentation Map*
- *HP AdvanceStack Routers Documentation and Technical Reference* CD-ROM

It includes:

- Hardware and software differences among specific router models
- What's new and changed for software releases A.09 and B.09, including specific versions *x*.09.01, *x*.09.5*x*, x.09.6*x*
- Manual update information
- Case study and application note supplements

This document obsoletes the following manuals:

- *Release Notes*
  Software Releases A.09 and B.09
  HP AdvanceStack Series 200 and Series 400 Routers
  E1194 (p/n 5962-8308)

- *Release Notes*
  Software Release A.09
  HP AdvanceStack Router 650
  E1194 (p/n 5962-8319)

- *Release Note Supplement*
  Software Releases A.09.50 and B.09.50
  HP AdvanceStack Routers
  E0195 (p/n 5963-2678)

Contents

Part 1

Software Releases and Hardware Compatibility

Updating to Release A.09.60 or B.09.60

Versions A.09.60 and B.09.60 of HP router operating code software replace all earlier versions for the routers listed on page 13.

If you already have an HP router running version A.09.5*x* or B.09.5*x* or earlier, use the HP AdvanceStack Router Update A.09.60 or B.09.60 diskettes and a PC to update your router. Follow the instructions in the README.TXT file (included with the files) for using the utility provided to download the new software. After you do so, booting the router converts your operating code to version A.09.60 or B.09.60 for the router model you have.

Notes

When you update to the new release, the function set you need for the configuration is automatically updated to work with the new operating code.

A special issue for upgrading a release previous to A.09.00 on the HP 27289A Router FR (a discontinued hardware version replaced by the HP 27289B Router 240) occurs when the configuration contains X.25 configuration information. You may be required to temporarily save this large configuration file on another server or on your PC router console and temporarily use a simpler configuration while upgrading the operating system to release A.09.60. The original configuration file can then be restored to the upgraded router.

Reverting to the Previous Release

After updating to the new release (A.09, B.09), it is possible to revert to a previous release (A.08 or B.08) by downloading it using NCL's Fget command or using update files with a PC. Doing so deletes your configuration for the new version and substitutes a factory default configuration to match the previous release. This is necessary because the updated configuration is not compatible with the previous release.

Before you lose your updated configuration in the process of reverting, you may want to use NCL's Browse command to first print the configuration information, to make it easier to later re-enter it into the factory default configuration.

Caution Do not perform the reversion by *pushing* an older operating code release onto a router having the new release! This keeps the updated configuration, which is incompatible with the old release.

Using the Software Manuals with This Release

The router software manuals have been updated for releases A.08 and B.08. The *Release Notes* (this document) contain the additional information for releases A.09 and B.09. The *Documentation Map* illustrates the organization of the manual set. The manuals include the features of both functional sets A and B; how to use the manuals for set B is described in "Features Available Only in the A.09 Functional Set (and Not in B.09)" on page 12.

Version Numbering

HP router operating code versions are numbered in three fields:

function . release# . version#

Example: A.09.01

"A" and "B" The letter in the first field of the version number identifies the functional set of the software. "A" refers to the "advanced" set of functions, which is the five routing services plus bridging. "B" refers to the "basic" set of router functions, including two routing services plus bridging. That is, "A" has a few more features than B. Most models of HP routers operate with the "A" set of functions.

"09" The two-digit number in the second field identifies a major *release* of the software, numbered consecutively. Major new features are added when a new release is issued. For example, the most recent major release is the *x*.09 release (that is, A.09 and B.09; December 1994).

"01" The two-digit number in the third field identifies the maintenance update version, numbered consecutively. The initial version of release "09" may be "01" (that is, A.09.01 and B.09.01). Later update versions may be "02", "03", etc.

For example, the current update version is *x*.09.60, (that is, A.09.60 and B.09.60; October 1995). This version of *Release Notes* for all of release *x*.09 includes the minor new features added in *x*.09.5*x* and *x*.09.60.

Features Available Only in the A.09 Functional Set (and Not in B.09)

The manuals you receive with your router—*Operator's Reference*, *User's Guide*, *Installation Guide*, and *HP Routing Services and Applications* as well as these *Release Notes*—describe all software features available in Hewlett-Packard routers, including features that are not available in all router models.

- Routers using release B.09 (the HP J2540B Router 230 and the HP J2540A Router PR) do not offer the features in the table below.
- Routers using release A.09 offer all of the features in the table below *except any features requiring specific network media for which an individual router has no port, such as FDDI, 100VG, token ring, or synchronous WAN.*

Features Unavailable for the HP Router 230

Feature	A.09	B.09
Quick Remote, to SmartBoot other routers	Yes	No
DECnet routing service	Yes	No
AppleTalk routing service	Yes	No
XNS routing service	Yes	No
EGP (Exterior Gateway Protocol) routing protocol for the IP routing service	Yes	No
OSPF (Open Shortest Path First) routing protocol for the IP routing service	Yes	No
X.25 packet switching	Yes	No
Frame Relay	Yes	No
SMDS (Switched Multi-megabit Data Service)	Yes	No
Token ring, 100VG, and FDDI, since the HP Router 230 has no such ports	Yes	No

Hardware and Software Compatibilityhardware

Router Models for Releases A.09 and B.09

Hewlett-Packard router software releases A.09 and B.09 operate on the router models listed below. Each router model can transfer a functional set from another of the same model, and from certain other models; before you update the functional set on a router using another router as the source, refer to the “Release x.09 Software Compatibility Matrix” on page 15. Note that series 200 and 400 routers have been renamed to allow easier identification with their respective router families.

Series 200 Models	A.09	B.09[1]	Former Name	Notes
HP J2628A Router 210	✓	–	–	
HP J2540B Router 230	–	✓	HP J2540A Router PR	The discontinued A version of this product—HP J2540A Router PR—also can use B.09.
HP 27289B Router 240	✓	–	HP 27289A Router FR	The discontinued A version of this product—HP 27289A Router FR—also can use A.09.
HP J2543A Router 245	✓	–	HP J2543A Router TFR	
Series 400 Models	**A.09**	**B.09**	**Former Name**	
HP 27288A Router 430	✓	–	HP 27288A Router SR	
HP 27285A Router 440	✓	–	HP 27285A Router ER	
HP 27286A Router 445	✓	–	HP 27286A Router TR	
HP 27287A Router 470	✓	–	HP 27287A Router LR	
HP 27290A Router 480	✓	–	HP 27290A Router BR	
Series 600 models	**A.09**	**B.09**	**Former Name**	
HP J2430A Router 650	✓	–	n/a	

1 Release B.09 contains a subset of the features in A.09 to make the Router 230 a lower-cost branch router. The subset is described on page12 in “Features...Not in B.09”.

Operating Code Release History

The following table lists the software releases applicable to each router model.

Router Model	Product Number	OS Releases
210	J2628A	A.08.03, A.09.60
PR-A *	J2540A	B.07.01 through B.09.60
230 (PR-B)	J2540B	B.08.02 through B.09.60
FR-A *	27289A	5.74 through A.09.60
240 (FR-B)	27289B	A.08.02 through A.09.60
245 (TFR)	J2543A	A.08.02 through A.09.60
430 (SR)	27288A	5.74 through A.09.60
440 (ER)	27285A	5.43 through A.09.60
445 (TR)	27286A	5.70.04 through A.09.60
470 (LR)	27287A	5.76 through A.09.60
480 (BR)	27290A	5.76 through A.09.60
650	J2430A	A.08.02 through A.09.60
CR*	27270A, 27270B	5.41 through 5.76 (only)

* Discontinued hardware. There are B versions of the PR-A and FR-A.

Software Compatibility Matrix

Use this matrix to determine which router(s) having version A.09.60 or B.09.60 operating code you can use as sources for updating the operating systems of other routers having older versions. This matrix applies to operating code updates, but not to configuration updates.

Release *x*.09 Software Compatibility Matrix

	210	PR-A*	230 (PR-B)	FR-A*	240 (FR-B)	245 (TFR)	430 (SR)	440 (ER)	445 (TR)	470 (LR)	480 (BR)	650	CR*
210	Y	-	-	-	Y	Y	-	-	-	-	-	-	-
PR-A*	-	Y	-	-	-	-	-	-	-	-	-	-	-
230	-	-	Y	-	-	-	-	-	-	-	-	-	-
FR-A *		-	-	Y	-	-	Y	Y	Y	Y	-		
240 (FR-B)	Y	-	-	-	Y	Y	-	-	-	-	-	-	-
245 (TFR)	Y	-	-	-	Y	Y	-	-	-	-	-	-	-
430 (SR)	-	-	-	Y	-	-	Y	Y	Y	Y	-	-	-
440 (ER)	-	-	-	Y	-	-	Y	Y	Y	Y	-	-	-
445 (TR)	-	-	-	Y	-	-	Y	Y	Y	Y	-	-	-
470 (LR)	-	-	-	Y	-	-	Y	Y	Y	Y	-	-	-
480 (BR)	-	-	-	-	-	-	-	-	-	-	Y	-	-
650	-	-	-	-	-	-	-	-	-	-	-	Y	-
CR*	-	-	-	-	-	-	-	-	-	-	-	-	Y

*** Discontinued hardware versions.**

Example: If you have just updated an HP Router 470 to A.09.60, and the network also includes an HP Router 440 and an HP Router 245, which of these two routers can you update using TFTP from the 470?

Answer: Only the 440 can be updated from the 470. To update the 245 using TFTP, you must have access to a 210, 240, or another 245 containing the A.09.60 update.

Router Hardware

Port Configurations

Each router model has a different selection of networking ports:

Type and Number of Ports

Router Model	Ethernet/ 802.3 LAN	100VG LAN	FDDI LAN	Token Ring LAN	Synch. WAN	Total Count
HP J2628A Router 210	1 (internal to hub)	—	—	—	1	2
HP J2540B Router 230	1 AUI & BNC	—	—	—	1	2
HP 27289B Router 240	1 AUI & BNC	—	—	—	1	2
HP J2543A Router 245	—	—	—	1	1	2
HP 27288A Router 430	1 AUI & BNC	—	—	—	3	4
HP 27285A Router 440	2 AUI	—	—	—	2	4
HP 27286A Router 445	1 AUI	—	—	1	2	4
HP 27287A Router 470	4 AUI & BNC	—	—	—	—	4
HP 27290A Router 480	4 AUI & BNC	—	1	—	—	5
HP J2430A Router 650	Increments of 4	Increments of 1	Increments of 1	Increments of 4	Increments of 4	varies max. 16

The *Installation Guide* for your router describes each type of port the router offers, its cabling, and its LEDs.

Height

The enclosure for each series 200 or 400 router (except the HP Router 210 module, which is installed in an HP AdvanceStack hub) is either 4.3 cm (1.7") high (one 4.3-cm rack space), called a *single-height* router, or 8.9 cm (3.5") high (two 4.3-cm rack spaces), called a *double-height* router.

Enclosure Height

Single-Height	Double-Height
HP J2540B Router 230	HP 27287A Router 470
HP 27289B Router 240	HP 27290A Router 480
HP J2543A Router 245	
HP 27288A Router 430	
HP 27285A Router 440	
HP 27286A Router 445	

The *Installation Guide* for your series 200 or 400 router illustrates the single-height and double-height enclosures and examples of the different rear LED layouts.

Using the Software Manuals with the HP Router 210 Module

The HP AdvanceStack Router 210 module runs the same software that other, stand-alone HP routers run. The router software and how to use it is described in the following three manuals provided with all HP routers: *User's Guide*, *Operator's Reference*, and *HP Routing Services and Applications*. Startup of the router software is described in the *Installation Guide* for the HP AdvanceStack Router 210 Module.

The HP AdvanceStack Router 210 Module is an auxiliary module installed in an HP AdvanceStack 10Base-T hub; some of its ports are different from those described in the router software manuals. The console port differences are described below. One of the network ports—the Ethernet/802.3 LAN port—is not externally visible but is inside the hub. How that port fits into the network is described below, so that you can use the router software manuals to configure it. Note that if the router module is configured and entirely managed, using SmartBoot and Telnet, from another router attached on an HP-Point-to-Point link, then you will not interact with the router software at your site.

Console Port

You interact with the router software by using the router console interface. Chapter 1 of the *User's Guide*, on page 1-6, states "You can access a router's console interface either by directly connecting your terminal to the router's console port or by using Telnet or a modem connection."

What this means for the router module in the hub is that you connect a PC to the RS-232 Distributed Management port on the front of the hub, and you reach the router's console interface by going through the hub's HP Stack Manager interface. Making a direct serial connection or a modem connection is described in the procedure on the next page.

Telnet connections, however, involve a network connection from another router or host. They do not involve a console connected to the hub; they do not involve HP Stack Manager. This is true for all routers.

1. Make the direct serial or modem connection according to step 5 in chapter 2 of the hub's *Installation & Reference Guide*.

2. Once you have connected the console, start HP Stack Manager as described in chapter 3, "Installing and Using HP Stack Manager", in the hub's *Installation & Reference Guide*.

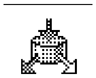
3. On the HP Stack Manager main window, click on the Connect button.

   After a few seconds, a list of connected hubs appears in the Device Chain List window. Identify a particular hub by its entry in the Station Address column. For hubs containing a router module, "SNMP/Router" appears in the column headed "Exp Slot".

4. Do either of the following:

   - Press and hold down the Shift key while you double-click on the hub in the Device Chain List.

   - Highlight the hub in the Device Chain List, and then press and hold down the Shift key while you click on the Access button.

   If you don't hold down the Shift key in the preceding step, HP Stack Manager displays a graphical representation of the hub. To continue, click on the Router icon (shown at left) that is in the tool bar.

5. After a few seconds, the Copyright screen appears. (Ignore references to speed sensing in the *User's Guide*, such as on page 2-3.) If you are prompted for "`Password:`" type the password and press Enter. After the Copyright screen, the Main Menu screen appears. Once you reach the Main Menu, this router module operates the same as all other routers, as described in the *User's Guide*.

Network Ports

The router module has one WAN port and one LAN port. Its WAN port uses the connector showing through the cover plate on the expansion slot at the back of the hub. Its Ethernet/802.3 LAN port is inside your hub; it uses the connector between the SNMP module and the router module. The WAN and the LAN ports must be configured for routing, either by using SmartBoot (Quick Remote or a Bootp server) or by using the router console interface at this hub. Figures 1 and 2 illustrate the structure of the hub, the router, and their connections.

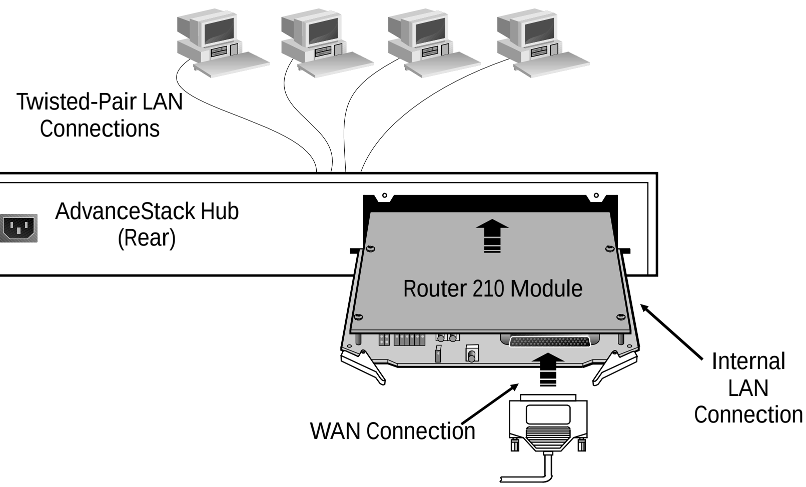


Figure 1. Physical View of Hub and Router Connections

The topology of this extended network can be visualized with an internal LAN bus inside the hub, as illustrated in figure 2. The internal LAN port for the router is on the same LAN as the nodes attached to the hub.

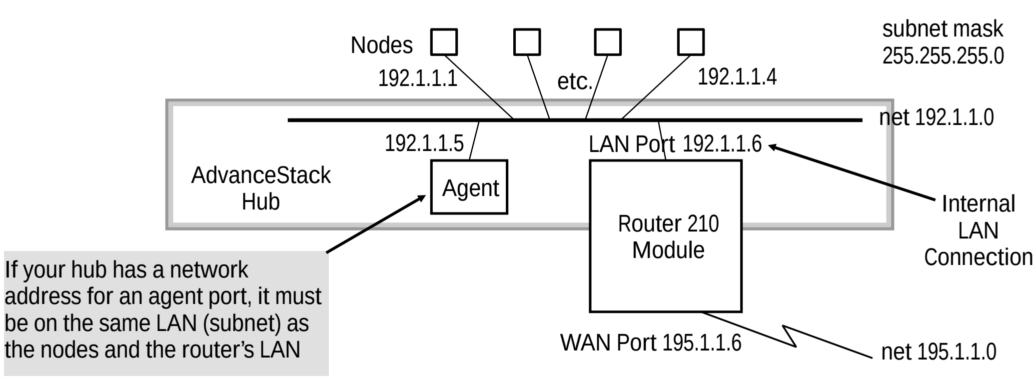


Figure 2. Topological View of Hub and Router Connections

Figure 2 illustrates an example of how the router is to be configured with network addresses, in this example for the Internet Protocol (IP). Both the LAN and WAN ports must be configured for the router.

Part 2

New Features

The features listed in this section were added to the software for releases beginning with A.09 and B.09, but have not yet been incorporated into the manual set.

Features Added with *x*.09.5*x* and *x*.09.6*x*

Some of the features were added beginning with versions A.09.**5***x* and B.09.**5***x* *or* versions A.09.**6***x* and B.09.**6***x*. These features are new to this latest edition of the *Release Notes*—since *Release Notes: Software Releases A.09 and B.09*, Edition 11/94, p/n 5962-8319 or 5962-8308, and *Release Notes Supplement: Software Releases A.09.50 and B.09.50*, Edition 0195, p/n 5963-2678. These features are summarized in the table below.

Version Number Label *x*.09.*xx*

Also, the complete descriptions of these features follow in this Part 2, where they are marked in the left margin with a note giving the first complete version number incorporating that feature. Features not marked with a version number (and not listed in this table) are incorporated into all A.09 and B.09 releases.

Feature	First Version Supporting	Pages for Description
100VG on the Router 650	A.09.60	23, 104–106
IPX Ping	*x*.09.60	64
IPX SNAP Encapsulation Type	*x*.09.60	67–69
SmartBoot Helper: LCNs & other X.25 options	A.09.52	46–48
SmartBoot Helper options for saving without booting	A.09.50	37, 39, 41, 49
FDDI on the Router 650	A.09.50	33

100VG for the HP Router 650

A.09.60

With the release of A.09.60, a new media type has been added for the HP Router 650—100VG-AnyLAN. This is available on the new HP J2438A 100VG Port Module, which features a 100VG LAN port.

The connector name for this port is “VG1”. The default circuit and circuit group names used are “VG#1” and “VG#1G”, respectively. (The number of the module’s slot appears where “#” appears here.)

For more information about 100VG and about the ease of migrating your networks to this new100-Mbit/s technology, please refer to the *100VG-AnyLAN Technology Guide* on the *HP AdvanceStack Routers Documentation and Technical Reference* CD-ROM, included in your documentation package. A general reference is *Planning and Designing High Speed Networks Using 100VG-AnyLAN*, 2nd edition, 1995, by Janis Furtek Costa.)

Quick Configuration for 100VG

On the Quick Configuration screen, illustrated in figure 3 on the next page, you would see a row beginning with “3:VG 1” if the module were in slot 3. When you use Quick Configuration, the line, circuit, and circuit group will be configured automatically just as they are for the existing LAN media such as Ethernet. You configure the routing addresses for your networks, just as you would for any other IEEE 802.3/Ethernet LAN.

```
HP J2430A Router 650                                        2-Oct-1995  11:21:00

==========================- SESSION 1 - MGR MODE -=============================
IP address:  17.150.16.1
--------------------------------------- Use arrow keys to move, / for hot keys -
System name:    CENTRAL
IP host-only:   NO           SNMP enabled:  YES    Inbound Telnet enabled: YES
               |Brg  DoD IP           DoD IP          IPX      Port   WAN Port
               |Enab Address          Subnet Mask     Network  Conf   Parameters
2:Ethernet 1   |
2:Ethernet 2   |YES  17.100.16.1      255.255.248.0
2:Ethernet 3   |
2:Ethernet 4   |
3:VG 1         |YES  17.150.16.1      255.255.248.0
               |
               |
               |
--------------------------------------------------------------------------------
Enter an IP address if you wish to route DoD IP traffic through this port.  Use
`dotted decimal' notation X.X.X.X where each X is a decimal number between 0
and 255.  Even if you are not routing IP traffic, you need to configure IP if
you have SNMP or inbound Telnet enabled, or you wish to use outbound Telnet.
```

Figure 3. Quick Configuration Screen with 100VG

Configuration Editor Parameters for 100VG

A.09.60

In the Configuration Editor, the initial Lines, Circuits, and Circuit Groups screens now provide for the 100VG module.

Configuration Editor Access to the Line Parameters

`3. Lines` (see figure 4)

And for an additional parameter, Circuit Name:

`1. Circuit Name` (see figure 5)

```
HP JZ430A Router 650                                        Z-Oct-1995  11:03:17

==========================- SESSION 1 - MGR MODE -=============================
Configuration Editor
Slot Number : 3
Physical Access Method : VG

Connector : VG1
1. Circuit Name (1)













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

Figure 4. The Primary Lines Screen

```
HP JZ430A Router 650                                        Z-Oct-1995   1:06:18

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




Circuit Name : VG31________
```

Figure 5. The Secondary Lines Screen for the Circuit Name

Lines Parameters and Options

Physical Access Method	The type of physical line connected to the port selected by the setting of the Connector parameter (see below). **Note:** Any available option for this parameter can be selected, regardless of whether it exists on the router being configured and corresponds to the port selected by the Connector parameter. Make sure your selection is valid for the selected port. Default: CSMA/CD
VG	(New option) The type of physical line for a 100VG-AnyLAN port.
CSMA/CD Token Ring FDDI SYNC etc.	(Previously existing options)
Connector	The physical port being configured on the router. Depending on the options selected for the Slot number parameter and the Physical Access Method parameter (above), the default will be selected to match that type.
VG1	(New option) The corresponding connector for the VG physical access method.
ETHER1 TOKEN1 FDDI1 WAN1 etc.	(Previously existing options)
Circuit Name	Identifies the circuit for the associated connector (see the Connector parameter above). Select the Circuit Name menu item and use the secondary Lines screen shown in figure 5.
VG#1	(where ***#*** is the number of the slot containing the 100VG Port Module) (New name.) The recommended name for the circuit connecting the first VG port in slot ***#***. The use of Quick Configuration sets up this name as the default for the 100VG connector. **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 and port numbers for the connector.

Configuration Editor Access to the Circuit Parameters

```
4. Circuits
```

```
HP JZ430A Router 650                                        2-Oct-1995   1:09:45

==========================- SESSION 1 - MGR MODE -============================
Configuration Editor
Circuit Name : VG31                       Auto Enable : Yes
Quality of Service : LLC 1 (datagram)     Circuit Type : Ether/802.3


LAN Address : ____________                XCVR signal polling : Inactive
```

Figure 6. The Circuits Screen

Circuits Parameters and Options

Circuit Name

Use the same circuit name you used in the Lines configuration (see page 26.)

VG#1 — (where *#* is the number of the slot containing the 100VG Port Module)
The use of Quick Configuration sets up this name as the default for the 100VG connector.

Circuit Type

Specifies the circuit type.

Ether/802.3 — (Previously existing option.) The frame format for the transmission channel for IEEE 802.3 or Ethernet or 100VG-AnyLAN networks.

Note: 100VG uses the same setting that is used for 10-Mbit/s IEEE 802.3 and Ethernet media.

802.5
FDDI
HP Point to Point
etc. — (Previously existing options)

Configuration Editor Access to the Circuit Group Parameters

`5. Circuit Group` (see figure 7)

And for an additional parameter, Circuit Name:

`1. Circuit Group Members` (see figure 8)

```
HP JZ430A Router 650                                      Z-Oct-1995   1:15:01

==========================- SESSION 1 - MGR MODE -============================
Configuration Editor
Circuit Group Name : VG31G
Circuit Group Speed : 56000


1. Circuit Group Members (1)
2. Circuit Group Backup Members (0)
3. Circuit Group Pool Members (0)









Enter Selection (0 for Previous Menu) : 1__
```

Figure 7. The Primary Circuit Groups Screen

```
HP JZ430A Router 650                                      Z-Oct-1995   1:18:23

==========================- SESSION 1 - MGR MODE -============================
Configuration Editor
Circuit Name : VG31________
```

Figure 8. The Primary Circuit Group Members Screen

Circuit Group Parameters and Options

Circuit Group Name

The name identifying the circuit group, up to a maximum of 12 alphanumeric characters.

VG#1G

(where *#* is the number of the slot containing the 100VG Port Module)
(New name.) The recommended name for the group containing circuit VG#1. The use of Quick Configuration sets up this name as the default for the 100VG connector.

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

Circuit Name

Select the Circuit Group Members menu item (number 1) and use the secondary Circuit Groups screen shown in figure 8. Use the same circuit name you used in the Lines configuration (see page 26.)

VG#1

(where *#* is the number of the slot containing the 100VG Port Module)
The use of Quick Configuration sets up this name as the default for the 100VG connector.

New Event Messages for 100VG

A.09.60

For a listing of the new VG-related event messages, refer to "New and Changed Event Messages" on pages 104 to 106.

New MIB Variables for 100VG

A.09.60

These MIB objects have been added to the “cct: Circuits Information Base”, documented in the *Operator’s Reference* starting on page 18-14. The following new subsection should appear following page 18-18.

The pathname to these variables is:

`cct.`*`cct.`* *where* *`cct`* is the 100VG circuit name.

VG Circuits

dls_ring_cnt contains the current number of packets received by this circuit and currently in transit to the data-link service (DLS).

err_rx_align counts alignment errors found in stored packets. They occur when a non-octet is received.

err_rx_badsym counts symbols received that did not decode properly.

err_rx_balance counts balance symbols received that were not the correct symbols.

err_rx_crc counts frames received with a faulty FCS value.

err_rx_ipm counts packets received with an Invalid Packet Marker (IPM).

err_rx_runt counts packets with less than the minimum length required.

err_rx_sdf counts Start of Frame errors received.

err_rx_skew counts occurrences of wire skew (a cable fault) greater than the allowed signal offset between two pairs and the other two pairs of twisted wire.

err_rx_trunc counts stored packets that were truncated at 8064 bits, while the status bits remain valid.

frames_rx_ok contains the number of error-free frames received through this circuit.

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 through this circuit.

frames_tx_per_sec contains the number of frames that this circuit has transmitted in the last second.

mac_addr contains the 12-digit hexadecimal representation of the 48-bit station address (MAC address, LAN address, etc.) used by this circuit.

net_fail indicates whether the Net Fail LED is lit for the circuit.

octets_rx_ok contains the number of error-free octets received through this circuit.

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 through this circuit.

octets_tx_per_sec contains the number of octets that this circuit has transmitted in the last second.

peak_frames_rx contains the greatest number of frames that this circuit has received in any one second since last booting of the router.

peak_frames_tx contains the greatest number of frames that this circuit has transmitted in any one second since last booting of the router.

peak_octets_rx contains the greatest number of octets that this circuit has received in any one second since last booting of the router.

peak_octets_tx contains the greatest number of octets that this circuit has transmitted in any one second since last booting of the router.

rx_dropped contains the number of packets that were dropped when received, due to lack of resources.

total_rx_error contains the total number of receive errors on this circuit

total_tx_error contains the total number of transmission errors on this circuit

tx_congestion contains the number of times a buffer wasn't available to transmit a frame.

FDDI for the HP Router 650

A.09.50

With the release of A.09.50, the HP Router 650 now supports the LAN media type FDDI. This is available on the new HP J2436A FDDI Interface for the HP Router 650, which features an FDDI LAN port.

The connector name for this port is "FDDI1". The default circuit and circuit group names used are "FDDI#1" and "FDDI#1G", respectively. (The number of the module's slot appears where "#" appears here.).)

On the Quick Configuration screen, illustrated in figure 9 on the next page, you would see a row beginning with "4:FDDI 1" if the module were in slot 4. When you use Quick Configuration, the line, circuit, and circuit group will be configured automatically just as they are for the other LAN media such as Ethernet. You configure the routing addresses for your networks, just as you would for any other LAN.

```
HP J2430A Router 650                                         1-Oct-95  10:05:13

==========================- SESSION 1 - MGR MODE -============================
Bridge on this port (y/n)?
--------------------------------------- Use arrow keys to move, / for hot keys -
System name:    ERIC-650
IP host-only:   NO           SNMP enabled:  YES    Inbound Telnet enabled: YES
               |Brg  DoD IP          DoD IP          IPX      Port   WAN Port
               |Enab Address         Subnet Mask     Network  Conf   Parameters
2:Ethernet 1   |
2:Ethernet 2   |YES  17.100.16.1     255.255.248.0
2:Ethernet 3   |
2:Ethernet 4   |
3:VG 1         |YES  17.150.16.1     255.255.248.0
4:FDDI 1       |
               |
               |
-------------------------------------------------------------------------------
Answer yes to enable bridging through this port.  You might need to enable
bridging if your network carries traffic for a protocol that is not routed by
this system.  If your topology contains loops, you will need to enable spanning
tree using the Configuration Editor.
```

Figure 9. Quick Configuration Screen with FDDI

All other FDDI functions, such as configuration, event messages, and MIB objects, are already incorporated in the other router manuals, since FDDI has been available for the HP Router 480.

New Default Configuration

To enable support for SmartBoot Helper (page 36), the factory default configuration has been modified. The table below shows the defaults as they appear in Quick Configuration.

The New Factory Default for Routers

Quick Configuration field	Default	New?
System name	DEFAULT_CONFIG	
IP host-only	YES	yes
SNMP enabled	NO	
Inbound TELNET enabled	NO	
Brg Enab	YES	
DoD IP Address	127.*x.x.x*	yes
DoD IP Subnet Mask	255.255.255.0	yes
IPX Network	—	
Port Conf:		
Ring interface (token ring)	16	
Link type (WAN)	HP (Point to Point)	
Bridge type (FDDI)	TR (Translating)	
WAN Port Parameters:		
Quality of service	AUTO	
Point-to-Point address	AUT	
AppleTalk Net Range	—	
AppleTalk Zone Name	—	
DECnet area.node	—	

The router is set to “factory default” configuration when shipped from the factory and whenever you clear the router using the Clear/Reset button combination. For more on clearing the router, refer to the installation guide you received with the router.

SmartBoot Enhancement on the HP Router 650

Beginning with release A.09, the HP Router 650 can use SmartBoot to download a configuration in the same way as HP Series 200/400 routers. That is, when the HP Router 650 boots from the factory default, it transmits Bootp requests over all operating links for approximately one minute. If a response is received from either a Quick Remote source or a Bootp server, the router configures itself accordingly. If no response is received, the router continues its boot-up process in the default configuration. (Refer to “New Default Configuration” on page 34.)

For more information on SmartBoot operation, refer to the following in the *User’s Guide* you received with your router:

- Chapter 8, “How To Use Quick Remote To Configure a Remote Router”
- Appendix A, “BOOTP Notes”

The SmartBoot Helper

```
                                DEFAULT_CONFIG

==========================- SESSION 1 - MGR MODE -============================
                                   Main Menu

         -->   1.  Statistics Screen Menu
               2.  Network Control Language Interpreter
               3.  Configuration Editor
               4.  Event Log
               5.  LOGOUT
               6.  Quick Configuration
               7.  Quick Remote
               8.  SmartBoot Helper









PRESS: ? for help, Down, Up, <- to exit, <RETURN> to select
```

Figure 10. Access to SmartBoot Helper from the Main Menu

Why Use SmartBoot Helper? Using SmartBoot Helper (termed *Helper* in the remainder of this manual), a central site operator can set up automatic configuration retrieval for HP routers. Such routers can then be sent to a remote site for installation in networks using any one of several HP router WAN link services. This feature enables a central site to manage a remote router without having specially trained personnel at the remote site. An operator at a remote site can also use SmartBoot Helper for automatic configuration retrieval without having to know extensive configuration parameter data.

What Are SmartBoot and SmartBoot Helper? SmartBoot is a component of Hewlett-Packard's "Instant On" branch office router installation feature that uses HP Point-to-Point WAN links and LAN links to automatically configure the router. SmartBoot Helper is a minimal interface used to extend SmartBoot functionality to other types of WAN links. That is, when an HP router boots in the factory default configuration or a SmartBoot Helper configuration, the router automatically attempts to download a configuration from another device in one of the following ways:

- If the router boots from its factory default configuration, it uses Bootp to search for a configuration from either another HP router (using Quick Remote over an HP Point-to-Point WAN link) or from a Bootp server (using TFTP over a WAN or LAN link).
- If the router boots from a configuration created in the Helper, it uses Bootp to search for a configuration in Quick Remote or a Bootp server over the following types of WAN links:
  - PPP
  - Frame Relay
  - X.25 Point to Point
  - X.25 PDN
  - Manual Adapter (V.25 bis)
  - PPP over V.25 bis
  - V.25 bis

(For more on configuration downloading using Quick Remote or TFTP, refer to the *User's Guide* you received with your router.)

How the Helper Operates

The Helper creates a configuration and then automatically invokes SmartBoot operation when the router boots using any of the following options:

- The operator selects the “Save and Reboot” option when exiting from Helper.
- The operator selects the “Save and Exit” option when exiting from Helper, and then executes the Boot command in NCL.

A.09.50
B.09.50

- The operator selects the “Save and Exit” option when exiting from Helper, then subsequently cycles power to the router. (This option enables a central site operator to create a Helper configuration and then ship the router to a remote site for installation.)

Bootp Features. SmartBoot invoked by using the Helper (or booting from the factory default configuration) uses Bootp to retrieve a configuration from either of the following sources:

- A full configuration from a TFTP (Bootp) server.
- A minimal configuration provided by Quick Remote from another HP router.

In both cases, after the router receives a new configuration, it boots and begins operating with that configuration. (For more information, refer to the *User's Guide* you received with your router.)

Operator Control. The Helper requires central or remote site operator intervention through one of the following:

- A terminal connected to the client router either directly or using a modem. (Refer to the *Installation Guide* you received with your router.)
- A central site terminal access to the remote router using Telnet.
  In this case, the client router must already be configured with a valid IP address on at least one port, with Telnet enabled. (The factory default IP address, 127.*X.X.X*, will not serve this purpose.)

Boot Errors. If the operator saves a Helper configuration, then exits from SmartBoot and uses the Boot command in NCL or cycles power to the router without first connecting the router to a properly configured network, then:

- The current router configuration will be replaced by the Helper configuration.
- SmartBoot Helper returns to its default state.
- It will be necessary to re-configure SmartBoot Helper in order to reset the automatic configuration feature.

Note

If SmartBoot operation fails in an attempt to download a configuration, the router configures itself in one of the following ways:

- If SmartBoot was invoked by using the Helper, the router replaces the current configuration with the configuration specified by the Helper and then boots. That is, the WAN port specified in the Helper is assigned a random IP address derived from its station (MAC) address; the subnet mask for that port is set to 255.255.255.0; and the port configuration is set to the WAN protocol specified in Helper. Also, the system name is set to HELPER_CONFIG. All other parameters are set to defaults by Helper.
- If SmartBoot was invoked by booting the router from its factory default condition, it configures itself as a bridge, as described under "New Default Configuration" on page 21 above.

Using the Helper to Download a Quick Remote Configuration

Quick Remote configures only the first WAN port on a client router. Thus, when using Helper on the client router with the server router set up for a Quick Remote response, you should normally:

1. Connect the client's *first* WAN port to the link used for accessing Quick Remote on the server router.

2. Use Helper to configure the first WAN port on the client.

Note Regardless of which port that Helper uses for access to Quick Remote on a server router, a Quick Remote configuration downloaded to a client router is always used to configure the first WAN port and (if included) the first LAN port on the client.

With the following exceptions, using Helper to invoke SmartBoot for Quick Remote operates in the same way as using the factory default configuration to invoke SmartBoot.

Differences Between Factory Default/SmartBoot Operation and Helper/SmartBoot Operation$Idefault configuration

Application	Factory Default/SmartBoot	Helper/SmartBoot
Links used for Bootp request	All active WAN and LAN links	Any active WAN link selected by the operator
WAN Protocols	HP Point to Point	PPP X.25 Point to Point Manual Adapter (for V.25 bis) Frame Relay X.25 PDN PPP over V.25 bis V.25 bis
Execution	Executes automatically when booted from the factory default condition.	Executed by operator from a directly connected console or in Telnet, using Helper's "Save and Reboot" exit option. OR If operator exits by using Helper's ''Save and Exit'' option, executed by the first subsequent power cycle or Boot command.

A.09.50
B.09.50

If you need information on how to use Quick Remote, refer to chapter 8, "How To Use Quick Remote To Configure a Remote Router", in the *User's Guide* you received with your router.

Using the Helper to Download a Configuration from a TFTP (Bootp) Server

SmartBoot invoked by the Helper operates with TFTP (Bootp) servers over the network in the same way that SmartBoot does when it is invoked by booting the router while in the factory default condition. The only difference is that Helper uses one of the WAN link types listed on page 37, while booting from the factory default condition uses only an HP Point-to-Point WAN link and/or an Ethernet link. (Refer to appendix A, "Notes on Configuring from a Bootp Server", in the *User's Guide* you received with your router.)

Importance of the Client's Station (MAC) Address. The Bootp server uses the station address of the client router to find the client's entry (previously created by the system operator) in the Bootp database (`/etc/bootptab` on a Unix machine). Thus, to prepare the Bootp server to respond to the client router's Bootp request, the system operator must first learn the client's WAN or LAN port station address. To determine the station address, connect a console to the client router and use the Get command in NCL. For example, to get the WAN port's station address on an HP Router 430, execute the following NCL command:

```
get cct.wan1.mac_addr
```
[Return]

Sequence of Helper Events for a TFTP (Bootp) Download.

1. The system operator uses Helper to configure the client router. This configuration specifies:
   - The WAN port to use on the client router (and, on an HP Router 650, the slot number)
   - The WAN protocol type and associated (minimal) parameters

   All other parameters are defaulted internally by the Helper. When the operator exits from Helper by using either the "Save and Reboot" or "Save and Exit" option, the router's current configuration is overwritten by the newly generated Helper configuration. The name of this new configuration is HELPER_CONFIG, which appears in the System Name parameter.

2. When one of the following occurs, the client router boots itself with the HELPER_CONFIG configuration and transmits Bootp requests over the selected WAN port:
   - The operator uses the “Save and Reboot” option to exit from the Helper.
   - The operator uses the “Save and Exit” option to exit from the Helper. Later, the operator executes the Boot command in NCL or cycles power to the router.

A.09.50
B.09.50

3. If the client router receives a Bootp response from a Bootp server, the router boots itself with an intermediate configuration that uses the following parameters (received in the Bootp response):
   - IP address of the client router
   - IP address of the Bootp server containing the full configuration file (previously created by the system operator for the client router)
   - Pathname for the router configuration file stored in the Bootp server

   (The system name for this intermediate configuration is BOOT_CONFIG.)

4. The router then initiates a TFTP retrieval of its configuration file from the TFTP server specified in the Bootp response. (The Bootp server and the TFTP server can be the same machine.)

5. After retrieving the specified configuration file, the client router then boots a final time and begins networking with the new configuration.

Network Preparation

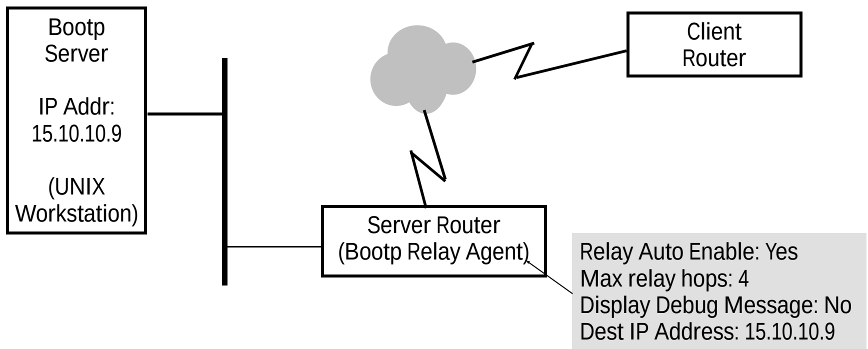


Figure 11. Example of a Network Providing Bootp Access to a Specific Server (15.10.10.9)

For Helper to operate, a Bootp server (typically a Unix machine) on the network must be prepared to respond to Bootp requests from the router. This requires an operator experienced in Unix administration and able to set up and manage Bootp services. The server must be set up to receive Bootp requests, to transmit Bootp replies, and to TFTP router configuration files. Because Helper operates only on WAN links, the client router and Bootp server are likely to be on different networks, making it necessary to configure an adjacent router as a Bootp relay agent. (Refer to figure 11, above.) To do so, configure the parameters under the "Bootp Configuration" menu item under the "DoD Internet Router" menu item in the router's Configuration Editor.

Note

In the above example, if the "Dest IP Address" field is empty, the server router performing the Bootp relay agent function broadcasts the client router's Bootp requests to all subnetworks.

For more information on network preparation for Bootp, refer to:

- Appendix A, “Notes on Configuring from a Bootp Server” in the *User’s Guide* you received with your router
- “Bootp and DHCP” in chapter 2 of the *HP Routing Services and Applications* manual you received with your router
- Appendix A, “Using Bootstrap Protocols in an Internet Environment”, in this manual on page 123
- Unix MAN pages on `bootpd`

For more on Bootp operation, refer to the following Requests for Comment:

- RFC 951
- RFC 1533
- RFC 1534
- RFC 1542

How To Use the Helper

This procedure assumes the following:

- An operator has access using a terminal or PC emulating a terminal to the client router, either through a direct connection from the terminal or PC to the router's console port, or (if the router has already been configured for IP operation on at least one port), using Telnet from another HP router (running version A.09.50 or later operating code).
- If you are using SmartBoot Helper to download a minimal configuration from a Quick Remote source on another HP router (the server):
  - The necessary WAN connection between the client router and the server router is in place and configured for one of the services listed on page 37. (This can be any WAN port on the client.)
  - Quick Remote on the server router is configured for the port through which it is connected to the client router. (For Quick Remote information, refer to chapter 8, "How To Use Quick Remote", in the *User's Guide* you received with your router.)
- If you are using SmartBoot Helper to download a configuration file from a Bootp server:
  - The necessary WAN and LAN connections between the client router, the Bootp relay agent, and the Bootp server are in place. (For an example, refer to figure 11 on page 42.)
  - The Bootp relay agent is configured to forward the Bootp request from the client to the Bootp server. (Refer to "Network Preparation" on page 42.)
  - The Bootp server is configured to send a Bootp reply and, subsequently, a configuration file to the client. (For more on this topic, refer to the earlier pages in this section and to appendix A, "Notes on Configuring from a Bootp Server", in the *User's Guide* you received with your router.)

1. From the Main menu in the client router, select item 8, "SmartBoot Helper".

   ```
   8. SmartBoot Helper
   ```

   You will then see the display shown in figure 12.

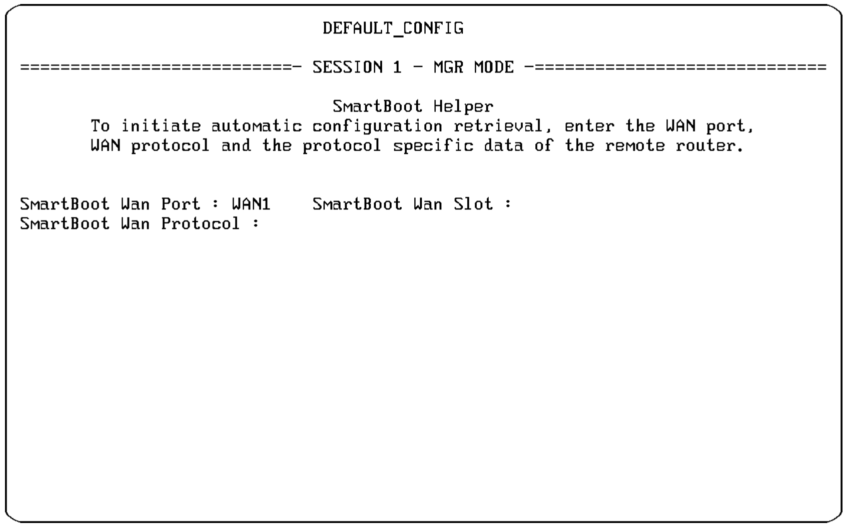


Figure 12. The Main SmartBoot Screen (HP Router 650)

Note

In the display illustrated in figure 12, the `SmartBoot Wan Slot` entry appears only for the HP Router 650.

2. Use the → key to select the name of the `SmartBoot Wan Port` you want to use. (The default is WAN1.) Then press Return.

3. If the client router is an HP Router 650, use the → key to select the `SmartBoot Wan Slot` number. (The default is 2.) Press Return.

4. Use the → key to select the `SmartBoot Wan Protocol`. (The default is PPP.) Your selection should match the WAN protocol that has been configured for this link from the server router or the Bootp relay agent. Then press Return.

5. Depending upon which WAN protocol you select, you are then prompted for additional parameters, as shown on the following pages. If a default option is already filled in for a parameter, use the → key to toggle to the desired option and press Return when the correct one appears. If no option is already filled in, then enter the appropriate text and press Return to move on to the next parameter. See the table on the next page for protocols and parameters available.

SmartBoot WAN Protocols and Parameters

See pages 47–48 for an explanation of the options for each parameter shown in the table below.

A.09.52
A.09.60

A.09.52
A.09.60

Protocol	Parameters
PPP (the default)	[none]
Frame Relay	Management Type
Manual Adapter	[none]
V.25 bis	Remote Phone Number
PPP over V.25 bis	Remote Phone Number
X.25 Point to Point	PDN Type
	Local X.121 Address
	Remote X.121 Address
	Connection ID
	Flow Ctrl
	Pkt Window
	Pkt Size
	SVC parameter
	SVC LCN Number
	PVC
	PVC LCN Number
X.25 PDN	PDN Type
	Local X.121 Address
	Remote IP Address
	Remote X.121 Address
	Flow Ctrl
	Pkt Window
	Pkt Size
	SVC
	SVC LCN Number

Parameter Options Available

Use the [→] key to toggle to a listed option, and press [Return] when the desired one appears. For a fill-in field, enter the text and press [Return] when it is correct. (Pressing [Return] moves on to the next parameter.)

`Management Type:`
`LMI` (the default)
`Unsupported`
`CCITT Annex A`
`ANSI Annex D`

(See “Management Type” in the *Operator’s Reference*, chapter 4.)

`Remote Phone Number:` Enter the telephone number used by the terminal adapter to dial out to the server.

(Same as “Remote Station Number” in the *Operator’s Reference*, chapter 4.)

`PDN Type:`
`TELENET` (the default)
`NET2`
`UK-PSS`
`TRANSPAC`
`Use Bitmap`
`OTHER`

(See “PDN” in the *Operator’s Reference*, chapter 13.)

`Local X.121 Address:` Enter the network-supplied decimal number assigned to the interface between this router and the X.25 network.

(Same as “Local DTE Address” in *Operator’s Reference*, chapter 13.)

`Remote X.121 Address:` Enter the network-supplied decimal number assigned to the interface between the X.25 network and the server router.

(Same as “Remote DTE Address” in the *Operator’s Reference*, chapter 13.)

`Remote IP Address:` Enter the IP address of the interface on the server router to the X.25 network.

(See “IP Address” in the *Operator’s Reference*, chapter 13.)

`Connection ID:` Enter the same decimal number configured for `Connection ID` on the server router for its X.25 point-to-point connection to this client router.

(See “Connection ID” in the *Operator’s Reference*, chapter 13.)

A.09.52
A.09.60
for all on
this page

`Flow Ctrl:` `Negot` (the default)
Packet window and size parameters will be initiated as below and then negotiated, if negotiation is a subscription option from the service provider.
`Deflt`
Packet window and size parameters will be configured as below.

`Pkt Window:` `2` (the default)
Or enter another number between 1 and 127.

Use the same packet window size configured for the line from the service provider.

`Pkt Size:` `16`
`32`
`64`
`128` (the default)
`256`
`512`
`1024`
`2048`

Select the size in bytes of the packet layer data field, as configured for the line from the service provider.

`SVC:` `Yes` (the default)
`No`

For X.25 PDN, accept `Yes`. For X.25 Point to Point, accept `Yes` if using switched virtual circuits, or select `No` if not.

`SVC LCN Number:` Enter the LCN number for the call to the server, within the range of switched virtual circuit LCNs for the line from the service provider.

`PVC:` `Yes`
`No` (the default)

Select `Yes` to use a permanent virtual circuit; `SVC` above must be `No`.

`PVC LCN Number:` `0` (the default; used when no permanent virtual circuits are used) or:
If PVCs *are* used, enter the LCN number used for the PVC, within the range of PVC LCNs for the line from the service provider.

6. After the last parameter is accepted, you are prompted with:

    `Back to Helper?`

    You can use the [→] key to toggle to one of three other options:

    A.09.50
    B.09.50

    ```
    Save and Exit?
    Save and Reboot?
    Exit without Saving?
    ```

`Back to Helper?` (Default.) Press [Return] when this option is displayed to either re-configure the port just configured or (if the router has more than one WAN port) to replace the current port selection and configuration with another choice. This procedure will repeat starting with step 2 (page 45).

`Save and Exit?`

A.09.50
B.09.50

Use the [→] key to display this option and press [Return] to save the Helper configuration and return to the point from which you entered Helper. (The Helper itself is reset to its default values.) The next time that the Boot command is executed or the power is cycled, the router incorporates the Helper configuration and begins SmartBoot operation. This feature enables an operator at a central site to prepare the router for automatic configuration before sending it to a remote site for installation.

Note: If the subsequent configuration download attempt fails, the router retains the configuration with which it was last booted, which will be the HELPER_CONFIG configuration generated by Helper. (See "Boot Errors" on page 38.)

`Save and Reboot?`

A.09.50
B.09.50

Use the [→] key to display this option and press [Return] to incorporate the new Helper configuration and begin SmartBoot operation. SmartBoot attempts to download a final configuration from either Quick Remote or a Bootp server, depending upon how the network has been prepared. Regardless of the result, the Helper configuration overwrites the router's current configuration and resets itself to its default values. (See "Boot Errors" on page 38.)

`Exit Without Saving?` Use the [→] key to display this option and press [Return] to cancel the Helper configuration and to return to the point from which you entered Helper.

Notes

When SmartBoot executes with a Helper configuration, if a problem exists somewhere in the network to prevent the server from downloading the final configuration, then the client router can remain in either of the following configurations, depending on the nature of the network problem:

- The HELPER_CONFIG configuration that is created when the operator exits from Helper by using either the “Save and Exit” or “Save and Reboot” option.
- The BOOT_CONFIG configuration that results from SmartBoot operation.

If the SmartBoot operation invoked by Helper fails for any reason, it will be necessary to (1) determine and remedy the source of the problem and (2) use Helper again to attempt another SmartBoot procedure.

X.25 Service Enhancements

X.25 features have been added to support a switching service and to make permanent virtual circuit (PVC) configuration more flexible.

X.25 Switching

The X.25 service has been enhanced to include a switch feature that eliminates the need for a separate hardware switch (DCE) in order for nodes (DTEs) on an X.25 network to communicate with each other.

The X.25 switch service supports up to 64 DTEs, and is based on a static configuration of DTEs in the network. For each DTE, you configure an X.121 address, a circuit name (for the DTE's physical port), full or partial address matching, and call latency. The address matching feature gives you the option of using one partial address to route an incoming call to one of several end nodes connected to the same addressable device, such as a multiplexer, on one of the router's WAN ports.

Note

X.25 switching operates on any HP Series 200/400/600 router that is using version *x*.09.00 or later software, *except* the HP Router 210 Module.

Event Messages for the X.25 Switch Service

For descriptions of X.25 event messages, refer to "X.25 Event Messages" on page 109.

Configuration Editor Parameters for X.25 Switching

Configuration Editor Access to the X.25 Switch Service

```
13. X.25 Network Service
    4. Switch Service
        1. Switch Address Map
```

You will then see the display shown in figure 13. Use this screen to configuration the parameters for each individual DTE for which the router is acting as a switch.

```
                              DEFAULT_CONFIG

===========================- SESSION 1 - MGR MODE -============================
Configuration Editor
X.121 Address : _______________         Lower Circuit :

Match : Full                            Call Latency Time (secs) : 10
```

Figure 13. X.25 Switch Service Parameters

Parameters and Options

Call Latency Time (secs)
Specifies how long in seconds to wait for a response to an outgoing call.

Default: 10 seconds

Lower Circuit
Specifies the name of the physical WAN port through which the DTE is configured. For example, in figure 14 below, the Lower Circuit name is WAN3. In an HP Router 650, if you used the first WAN port in a four-port synchronous module installed in slot 2, the default name would be WAN21.

Match

Defines how to use the value of the X.121 Address parameter. Using a partial address reduces the number of DTEs to configure and the search time needed by the software to process a switching operation.

Default: Full

Full — Forces the service to exactly match the full X.121 address in the ''called address'' field of an incoming Call Request Packet in order for the switch to route the call to the proper DTE.

Partial — Enables the X.25 service to route the call to a device containing several DTE connections, and relies on the device to determine which DTE receives the call. Requires that the X.121 Address be configured with only the digits needed to form the partial address. In this case, the X.121 address is compared to the corresponding most-significant digits of the ''called address'' field of incoming call packets to determine where to route the call.

In the example illustrated in figure 14, consider a multiplexer connected to the WAN3 port and having six DTEs attached to it.

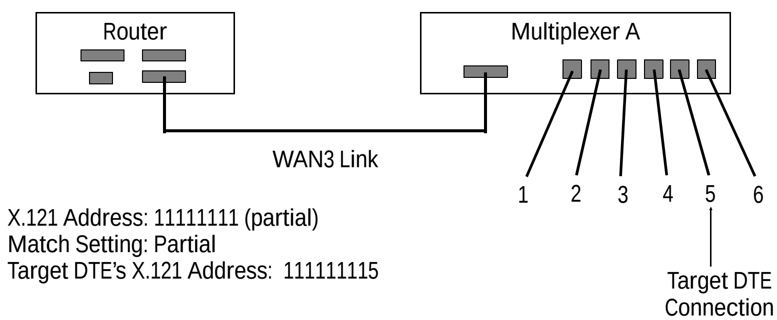


Figure 14. Example System Usage of Partial Address Matching

If the X.121 address of multiplexer A is the eight-digit number 11111111, with a ninth digit (*X*) used to address the device lines, then any call destined for address 11111111*X*, such as 111111115, goes to multiplexer A, and the multiplexer itself routes the call to device line 5.

For more information on using Match with a ''partial'' setting, refer to the X.121 Address parameter on page 54.

X.121 Address

Specifies the X.121 address of the DTE (node on the X.25 network). This address can be up to 15 digits in length and is stored in the X.25 routing table along with the name of the corresponding physical WAN port that you specify with the Lower Circuit parameter. When the router subsequently receives a call requesting this address (the ''called address''), the router locates the address in the X.25 routing table, determines the name of the corresponding physical WAN port, and forwards the call to that port.

If you are using full address matching (refer to Match, above) you should enter one, complete (unique) address for each DTE you want to configure for X.25 switching. However, if you are using partial address matching, enter only the digits necessary to identify the partial address.

Note: Addresses you specify with the X.121 Address parameter are stored in the X.25 routing table in the order in which they are entered. When the router receives an incoming call packet. Thus, the X.121 address(es) should be entered in a sequence determined by their lengths, with the longest address(es) entered first, the second longest addresses entered second, and so on. If this order of precedence is not observed, and one or more of the stored address are configured for a partial match, it is possible for a call to be misdirected. For example, suppose a router has three WAN ports:

X.121 Address	Lower Circuit	
2222	WAN1	(Match: Partial)
22222	WAN2	(Match: Partial)
22223	WAN3	(Match: Partial)

In the above case, an incoming call addressed for node 5 on port 3 (222235) would be misdirected to node 5 on port 1 because the incoming address would meet the Match criteria of the first routing table entry (partial address 2222). The solution to this problem is to rebuild the X.25 routing table with the addresses ordered from longest to shortest, as follows:

X.121 Address	Lower Circuit	
22222	WAN2	(Match: Partial)
22223	WAN3	(Match: Partial)
2222	WAN1	(Match: Partial)

New PDN Parameter Options for X.25 Switching

New options have been added to the existing options for the (X.25) PDN circuit parameter to simplify configuring an X.25 circuit as a DCE.

Configuration Editor Access to the X.25 PDN Circuit Parameter

```
4. Circuits
```

When the main Circuits screen is displayed, set Circuit Type to "LAPB (X.25)" to access the PDN parameter.

Parameters and Options

PDN	Identifies the supplier of X.25 services. New in this release A.09 are the ''_DCE'' options that have been added to the existing PDN option set. Default: TELENET
TELENET	This provider of PDN subscription service (DTE).
DDN	"
UK-PSS	"
NET2	"
TRANSPAC	"
OTHER	Use this option if your X.25 service provider is not listed. It configures the router to interface with a non-specific packet-switched network.
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) in the *Operator's Reference* shows how to construct the status word. Enter the status word in eight-digit hexadecimal form.
TELENET_DCE	[new for A.09] Specifies the TELENET provider of the PDN subscription service (for DCE operation); use this option when the X.25 switch service will be configured for the circuit and the remote host is configured for TELENET (operating as the DTE device).
DDN_DCE	[new for A.09] Specifies Defense Data Network (DDN) service (for DCE operation); use this option when the X.25 switch service will be configured for the circuit and the remote host is configured for DDN (operating as the DTE device). For more information on DDN, refer to the PDN parameter description in chapter 13 of the *Operator's Reference*.
PSS_DCE	[new for A.09] Specifies the PSS provider of the PDN subscription service (for DCE operation); use this option when the X.25 switch service will be configured for the circuit and the remote host is configured for UK-PSS (operating as the DTE device).
NET2_DCE	[new for A.09] Specifies the NET2 provider of the PDN subscription service(for DCE operation); use this option when the X.25 switch service will be configured for the circuit and the remote host is configured for NET2 (operating as the DTE device).

Quick Configuration Changes for X.25 Switching

Release *x*.09 adds X.25 switching to the available routing services. (Refer to "X.25 Service Enhancements" on page 51.) Quick Configuration has been modified to include this addition. If you are unfamiliar with Quick Configuration operation, refer to chapter 3 in the *User's Guide* you received with your router.

Quick Configuration Access to the X.25 Switch Service

1. Start a Quick Configuration session. (Type the menu number in front of the item "Quick Configuration", such as [6].)

2. When the "Welcome..." screen appears, press [Return] to display the Quick Configuration screen.

3. Move the cursor to the "Port Conf" column for the WAN port you want to configure for X.25 switching.

4. Specify X.25 service by typing:

   `lapb` [Return]

5. "SW" (for "switching") will appear in the adjacent WAN Port parameters field for the selected port. The following message will appear:

   ```
   Type '/X' to add an X.25 switch record and/or
   address maps.
   ```

6. Type [/] [X] (a hot key) to enter the Configuration Editor at the X.25 routing service level.

7. Press [Return] to accept the default Auto Enable setting ("Yes") and display the screen shown in figure 15.

```
                              DEFAULT_CONFIG

==========================- SESSION 1 - MGR MODE -============================
Configuration Editor
Auto Enable          : Yes


1. PDN Service (0)
2. DDN IP Service (0)
3. HP Point to Point Service (0)
4. Switch Service (1)










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

Figure 15. X.25 Service Menu

8. Type 4 and press Return. Then select an action option—either Browse, Modify, or Add—to display the switch address menu item:

   ```
   1. Switch Address Map
   ```

9. Type 1 and press Return to display the "X.25 Switch Service Parameters" screen. (If you have previously configured X.25 switching, you must select an action option, as in the preceding step.)

10. For information on configuring the individual X.25 switching parameters, use the list of parameters and options starting on page 52 in the section for "Configuration Editor Access to the X.25 Switch Service".

11. When you finish configuring the X.25 switching parameters, press Return as many times as needed to return to the Quick Configuration screen. When finished with Quick Configuration, type Ctrl C and then Y to exit from Quick Configuration and boot the router.

Operating Note

X.25 switching does not operate with bridging or the other routing service parameters available in Quick Configuration. For this reason, leave the Brg Enab, IP, IPX, AppleTalk, and DECnet fields blank for the port you are configuring for X.25 switching.

PVC Configuration Enhancement

This enhancement increases the flexibility of permanent virtual circuit (PVC) operation by eliminating the need to determine the PVC logical circuit number (LCN) on the order of configuration of the individual circuits. This eliminates the possibility that the LCN could automatically be assigned a value outside of the range specified by the low and high PVC LCN parameters in the Circuits configuration. Additionally, the Flow Control parameter in the X.25 Address Map and X.25 Virtual Circuits menus of the X.25 Network Service is eliminated.

Configuration Editor Access to PVC Configuration

```
13. X.25 Network Service
   3. HP Point to Point Service
      1. X.25 Virtual Circuits
```

```
                              DEFAULT_CONFIG

===========================- SESSION 1 - MGR MODE -============================
Configuration Editor
Circuit Name :                        Remote DTE Addr :
Connection ID :
Permanent Circuit : Yes
                                      LCN Number : 0___
```

Figure 16. The X.25 Permanent Circuit and LCN Number Parameters

Parameters and Options

Permanent Circuit

Determines whether the circuit specified under HP Point to Point Service in the X.25 Network Service menu operates as a permanent connection to an external packet-switching device or a connection activated by calls.

Default: No

Yes

Configures the circuit to remain permanently open. Configuring ‘‘Yes’’ also requires that you configure an LCN number corresponding to the LCN number configured in the external packet-switching device.

Note: If you select ‘‘Yes’’, you must also configure the PVC LCN range for this circuit to match the LCN range you specify in the external packet-switching device. The PVC LCN range for the selected circuit is defined by the Low PVC LCN and High PVC LCN parameters found in the Circuits configuration when the Circuit Type is ‘‘LAPB (X.25)’’.

No

Configures the circuit to respond to calls.

LCN Number

Appears when the Permanent Circuit parameter is enabled (set to ‘‘Yes’’). This value must be within the range specified by the Low PVC LCN and High PVC LCN parameters found in the Circuits configuration when the Circuit Type is ‘‘LAPB (X.25)’’.X.25;PVC (permanent virtual circuit)

Default: 0

TCP Configuration

The Transmission Control Protocol (TCP) is the DoD Internet standard transport-level protocol. TCP is used for Telnet service. The TCP configuration is basically a set of "tuning" parameters used in the local host:

- To control how long to wait for a TCP communications timeout in a connection to a remote host
- To detect and recover from a network failure

When a failure is detected, TCP terminates the Telnet connection to the remote host and returns you to local host control. The effectiveness of TCP in carrying out these functions depends on the stability of the network. (Factors such as congestion can affect actual TCP response times.) It is recommended that you initially leave the TCP parameters at their defaults, and adjust them only if doing so avoids unnecessary timeouts in Telnet connections to a remote host. (For more on Telnet, refer to the *User's Guide* and the *Operator's Reference*.) Release *x*.09 replaces the former set of TCP parameters with a smaller, modified set.

TCP "guarantees" that each packet will be delivered by requiring the receiver to send an "acknowledgment" for each packet or series of packets received. If no acknowledgment is received, TCP retransmits the packet(s). The parameters described in this section control the retry interval (how long TCP waits before retransmitting), and the number of retransmission retries (how many retransmissions occur before terminating the connection).

The retry interval is based on how much time TCP expects to allow for sending a packet and receiving an acknowledgment. This is known as the "round-trip" time. Upon receiving each acknowledgment, TCP updates this estimate, and thus the retry interval itself.

New Event Messages for TCP

For a listing of the new TCP-related event messages, refer to "Transmission Control Protocol Event Messages" on page 108.

Configuration Editor Access to the TCP Parameters

```
7. DoD Internet Router
    6. TCP Configuration
```

```
                              DEFAULT_CONFIG

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

Auto Enable : Yes

Retranmission Retries : 5
Initial Retry Interval (ms) : 1000
Minimum Retry Interval (ms) : 500
Maximum Retry Interval (ms) : 16000

Activity Poll Interval (secs) : 300
```

Figure 17. The TCP Configuration Screen

Parameters and Options

Activity Poll Interval (sec)

Specifies the number of seconds between ‘‘keep-alive’’ packets. (A keep-alive packet is an empty packet that elicits a response from the remote host to ensure that the host is still connected.) A keep-alive packet is sent only when there has been no activity (packets transmitted between hosts) for a period equal to the current activity poll.

Default: 300 (seconds)

Auto Enable

Enables or disables TCP upon booting of the router.

Default: Yes

Yes — Enables TCP upon booting of the router.

No — Disables TCP upon booting of the router.

Initial Retry Interval (ms)

When a TCP connection begins, specifies the initial interval to wait before re-sending a keep-alive packet via TCP. Set this parameter to a value equal to the estimated round-trip packet time; that is, the time it should take to send a TCP keep-alive packet and receive an acknowledgment from the remote host.

Default: 1000 (milliseconds)

Range: Between the Maximum Retry Interval and the Minimum Retry Interval

After each unsuccessful retry of a keep-alive packet, the router increases or decreases the actual interval used, depending upon whether the last successful keep-alive transmission was actually larger or smaller than the retry interval in use for that packet. For example, if the Initial Retry Interval parameter is set to 1000 ms. but the actual interval of the last successful keep-alive packet is 878 ms., then the retry interval will be internally adjusted to a value smaller than 1000, but larger than 878. If the next retry also fails, then the retry interval will again be internally adjusted to a value closer to 878. This pattern will be repeated until there is a successful retry or until the maximum number of retries allowed has been exhausted.

Note: The actual interval used after the initial attempt will remain within the range you specify in the Maximum Retry Interval and Minimum Retry Interval parameters. Also, regardless of what interval is being used internally, this parameter value does not change; it serves as the first interval to use for sending keep-alive packets each time a new TCP connection is established.

Maximum Retry Interval (ms)

Specifies the upper limit for the TCP retry interval. For the first retry interval, the router uses the value specified by the Initial Retry Interval parameter. Subsequent retries may be at a larger or smaller retry interval. (Refer to the Initial Retry Interval for more on this topic.)

Default: 16000 (milliseconds)

Range: Greater than Minimum Retry Interval; less than 30 seconds

Minimum Retry Interval (ms)

Specifies the lower limit for the TCP retry interval. This parameter is available to prevent the retry interval from becoming too short due to extremely fast round-trip times (which can result in unnecessary retransmissions). For the first retry interval, the router uses the value specified by the Initial Retry Interval parameter. Subsequent retries may be at a larger or smaller retry interval. (Refer to the Initial Retry Interval for more on this topic.)

Default: 5000 (milliseconds)

Range: Between 500 ms and the Maximum Retry Interval

Retransmission Retries

Specifies the number of times TCP will retransmit a packet before terminating the connection.

Default: 5

Range: 1–30

Telnet Logout Changes

There are two methods for logging out of a Telnet session:

- `LOGOUT` selected from the Main menu
- [Ctrl] [D] typed at the NCL prompt

Prior to release x.09, [Ctrl] [D] would disconnect your Telnet session with a remote router and return you to your local router session, regardless of any other sessions on intermediate routers. That is, if you had "cascaded" Telnet sessions (from router A to B to C, etc.), then [Ctrl] [D] would return you to the first router session (router A), and disconnect you from the Telnet sessions on both routers B and C. Figure 18 illustrates the cascaded sessions.

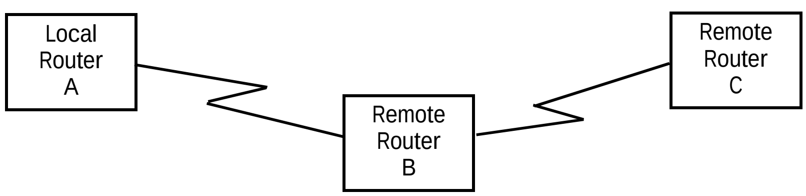


Figure 18. Example Topology for Cascaded Telnet Sessions

Beginning with release x.09, Telnet logout options are as follows:

- `LOGOUT` Returns you to the previous Telnet session.
- [Ctrl] [D] Returns you to the previous Telnet session.
  For example, if you have cascaded Telnet sessions from your local router A through remote router B to remote router C (and if both A and C are running release x.09), then executing [Ctrl] [D] returns you to router B. See figure18.
- [Ctrl] [R] Always returns you to your local router session, regardless of how many Telnet sessions are cascaded from the local router.

IPX Ping, a New NCL command

A.09.60
B.09.60

Before the *x*.09.60 version release, the IP protocol was required to make use of the "Ping" function: to send a packet requiring direct response, to test the reachability of another node on the network. It is used for verification of network configuration and for troubleshooting. Now all HP routers provide this function with IPX routing, without need for IP, through a new NCL command named Ipxping.

Novell's Netware Link Services protocol (NLSP) Specification, Revision 1.0, includes the IPX Ping Protocol, Version 1, for a simple, end-to-end network-layer reachability test. HP's implementation of IPX Ping follows that specification. Additionally, the implementation of Ipxping is very similar to that of the Internet Control Message Protocol's (ICMP) echo request message in NCL's Ping command. Ipxping includes one addition, however, in allowing the specification of packet size.

Ipxping: Sending a IPX Ping Protocol Packet

Use NCL's Ipxping command to send a test packet(s) to an IPX node that you specify. You can address a single node, including this router (loop-back), but broadcast addresses are not supported. This router issuing the test packet must have IPX routing configured.

After transmitting the packet to the addressed node, the router waits for a response. If a response is received within the specified or default wait period, the console displays a message indicating that the target is alive. If a response is not received within that period, the console displays a message indicating that the target did not respond.

Syntax

```
ipxping network.node [count] [wait] [size]
```

`network.node` is the IPX address of the target node—the network number of the network on which the target node resides, followed by a period, followed by the node (host) number of the target node.

`count` (optional) is the number of times to repeat the packet transmission. If an integer is not included, one (1) packet is transmitted.

`wait` (optional) is how many seconds to wait for a response. If a second integer is not included, a response must be received in five (5) seconds (for each packet transmitted) to be successful.

`size` (optional) is the size, in number of bytes, of the packet to transmit. If a third integer is not included, each packet transmitted will be 40 bytes in length.

Examples

```
ipxping 108.08000922583e
```

Sends out one 40-byte packet to node 0800922583e on network 108. Waits up to five seconds before timing out. The response might be:

```
108. 800922583e is alive, time=1 ms
```

```
ipxping 108.08000922583e 3 20
```

Sends out three 40-byte packets to node 0800922583e on network 108. Waits up to 20 seconds for each response to be received. The response might be:

```
108. 800922583e is alive, iteration 1, time=0 ms
108. 800922583e is alive, iteration 2, time=1 ms
108. 800922583e is alive, iteration 3, time=0 ms
```

```
ipxping 108.08000922583e 10 30 60
```

Sends out ten 60-byte packets to node 0800922583e on network 108. Waits up to 30 seconds for each response to be received. The response would report the same information as for the preceding example; size is not echoed.

New MIB Variables for IPX Ping

A.09.60
B.09.60

Two MIB objects have been added to the “ipx: IPX Information Base”, documented in the *Operator’s Reference* starting on page 18-68. The new items would be included within the “Interface Specific” subsection.

The pathname to these variables is:

`ipx.`*`if.net#.`*	*where* `if` is the IPX circuit name. *where* `net#` is the IPX network number of this network interface.

ping_rx contains the total number of IPX Ping datagrams received by this interface. Such messages are sent from another network node to test whether this router is reachable.

ping_tx contains the total number of IPX Ping datagrams transmitted over this interface. Such messages test whether a destination node is reachable.

IPX Encapsulation Type Additions and Changes

Existing Encapsulation Types Renamed

A.09.60
B.09.60

The default setting and the other options for the IPX parameter Encapsulation Type have been renamed to better match Novell's conventions for naming encapsulation types, also called frame types. Also, the option set now better accommodates the new Ethernet SNAP encapsulation addition (see the next subsection starting on page 67).

The Encapsulation Type parameter is described on pages 11-9 to 11-10 of the *Operator's Reference*. The encapsulation type can also be set in the Quick Remote utility for a remote router, as described on page 8-11 in the *User's Guide*. The options have the same descriptions found in the *Operator's Reference*, but have been renamed as follows:

***x*.09.5x & earlier**	***x*.09.60 & later**	
	Configuration Editor Name	**Quick Remote Name**
802.2	802.2	802.2
Ethernet	Ethernet_II	ETHER_II
Novell	802.3 Raw (Novell) [the default]	802.3 [the default]

IPX Ethernet SNAP Encapsulation Added

A.09.60
B.09.60

The Ethernet SNAP frame type is now an option for IPX interfaces. SNAP stands for Subnetwork Access Protocol. This frame type is the fourth IPX encapsulation to be supported on HP routers. To configure SNAP encapsulation using the Configuration Editor, see the section "Configuration Editor Access to IPX Encapsulation Type" on page 69. To configure it for a remote router using Quick Remote, set "SNAP" in column "WAN IPX Encap" or column "LAN IPX Encap."

The Ethernet SNAP frame type is derived from the Ethernet 802.2 frame structure. Most of the fields for the SNAP frame are the same as for the Ethernet 802.2 frame, with the exceptions noted in the list of fields below, and described below that.

- Preamble and Start Frame Delimiter (8 bytes)
- Destination Address (6 bytes)
- Source Address (6 bytes)
- Length (4 bytes)
- Data and Padding (46–1500 bytes)
- LLC 802.2 —different values
  (DSAP, SSAP, and Control fields, 1 byte each)
- Organization Code (3 bytes) —additional field
- Ethernet Type (2 bytes)
- FCS (4 bytes)

DSAP, SSAP, and Control: In Ethernet SNAP frames, the value of the DSAP and SSAP fields denotes the network-layer protocol type of the packet. The value is always AA (hex), which denotes a SNAP format frame. The value of the Control field is always 03 (hex), which denotes the unnumbered format. The unnumbered format indicates that the LLC layer will provide connectionless service. This field is followed by the Organization Code and Ethernet Type fields, described below.

Organization Code This field denotes the organization that assigned the Ethernet Type field to follow. Netware's IPX/SPX packets contain 00-00-00 (hex) in the Organization Code field.

Ethernet Type This field defines the network-layer protocol. Netware's Ethernet Type number is 8137 (hex). Other network protocols use the numbers listed below.

- IP 0800 (hex)
- ARP 0806 (hex)
- Reverse ARP 8035 (hex)
- AppleTalk 809B (hex)
- AppleTalk ARP 80F3 (hex)
- Netware IPX/SPX 8137 (hex)

The minimum Ethernet SNAP frame size (excluding the Preamble and Start Frame Delimiter) is 64 bytes, and the maximum is 1518 bytes.

Configuration Editor Access to SNAP Encapsulation Type

```
11. IPX Routing Service
    2. Network Interface Definitions
```

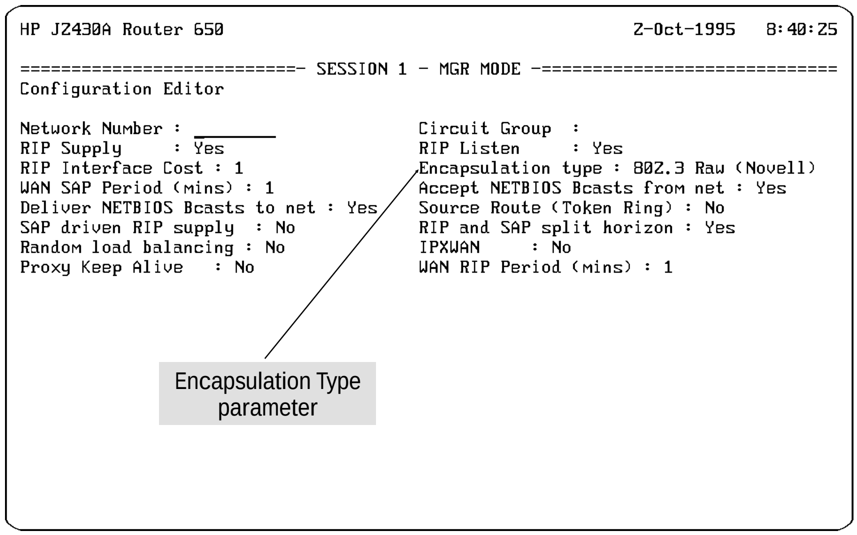


Figure 19. IPX Network Interface Definition Screen for Encapsulation Type

IPX Encapsulation Type Parameter and Options

Encapsulation Type

Selects from four available frame types to be used on IEEE 802.3/Ethernet media.

Default: 802.3 Raw

Note: The default has not changed, it's merely been renamed from "Novell".

Ethernet_SNAP	(new option) The Ethernet Subnetwork Access Protocol (SNAP) frame type. Similar to the 802.2 LLC encapsulation. See the SNAP frame description above on page 67.
802.2	(same as described on page 11-10 of the *Operator's Reference*)
Ethernet_II	(same as described for "Ethernet" on page 11-10 of the *Operator's Reference*)
802.3 Raw	(same as described for "Novell" on page 11-10 of the *Operator's Reference)*

IPX Proxy Keep-Alive

Proxy Keep-Alive can help to reduce the cost of using dial-up links by disabling “Watchdog” (Proxy Keep Alive) traffic between a local file server and a remote client linked by a WAN. (Refer to figure 20.) This feature is effective at the times when the only traffic between the server and client is the Watchdog protocol inquiries generated by the server. When this condition exists, Proxy Keep Alive avoids use of the WAN link by causing the router to do the following:

- Drop the Watchdog (IPX Keep-Alive) protocol inquiries sent by the file server over the specified LAN.
- Send a simulated (“spoofed”) Watchdog (IPX Keep Alive) protocol response back to the local file server to satisfy the server that the client is still active.

When the above occurs, the WAN link is not in use because the router is not transmitting Watchdog inquiries across the WAN, which also means there will be no Watchdog protocol responses returning back across the WAN from the client.

Using the example in figure 20, File Server A sends periodic Watchdog packets to Client B to verify that Client B continues to be available. But if Proxy Keep Alive has been configured for Router A’s link to LAN A, then Router A will not pass on the Watchdog packets to the WAN, but will instead drop them and send a response back to the file server to indicate that Client B is still available. This is termed “watchdog spoofing” and avoids the need to activate (and pay the charges for) a connection solely to transmit the Watchdog traffic across the WAN.

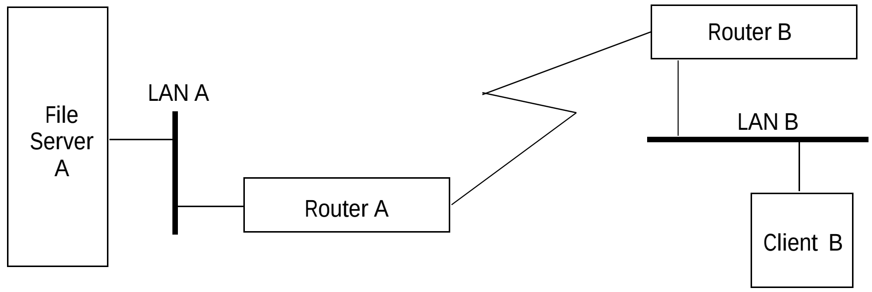


Figure 20. Example of an IPX Network for Watchdog Spoofing

Note If the remote client goes down for any reason while Proxy Keep Alive is enabled, the local server will not detect the failure.

Configuration Editor Access to the Proxy Keep Alive Parameter

```
11. IPX Routing Service
    2. Network Interface Definitions
```

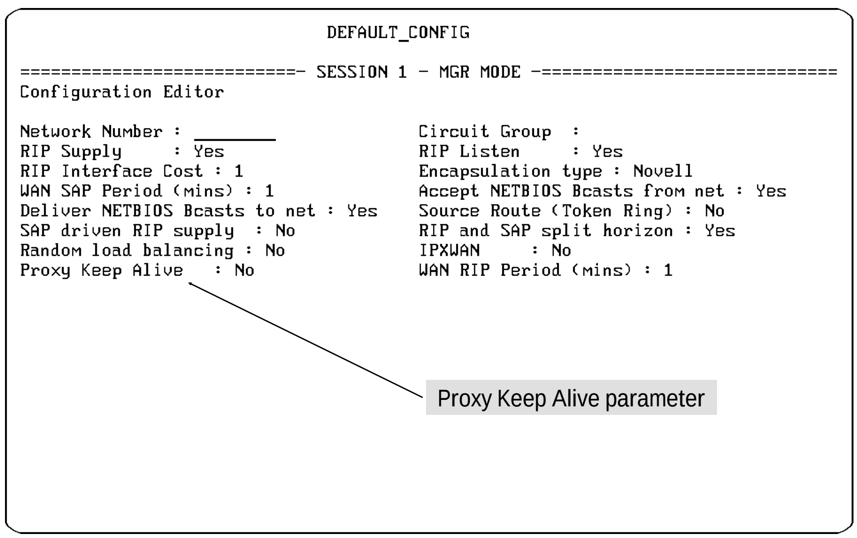


Figure 21. Locating the Proxy Keep Alive Parameter

Parameters and Options

Proxy Keep Alive Enables or disables watchdog spoofing.

Default: No

Yes	Enables watchdog spoofing.
No	Disables watchdog spoofing.

IPX: WAN RIP and SAP Periods

WAN SAP Period

Replace the description on page 11-19 of the *Operator's Reference* with the following description.

Configuration Editor Parameter and Options

WAN SAP Period (mins)

Sets the elapsed time interval between transmissions of SAP advertisements across a WAN link. Use this parameter to control the transmission of unsolicited SAP advertisements (referred to as General Server Responses, or GSRs) across any WAN link, thus reducing the amount of bandwidth consumed by the SAP protocol.

Default: 1 minute
Range: 0 to 9999 minutes

If the circuit group provides a LAN connection (such as IEEE 802.3, token ring, and FDDI), simply press Return. The IPX router always transmits GSRs to such media at one-minute intervals.

If the circuit group provides a point-to-point connection (V.35, T1, E1, etc.), you can control the frequency of GSR transmissions. The default response, 1, specifies standard IPX advertisement (which issues GSRs at one-minute intervals).

To decrease GSR frequency, enter a value (up to a maximum of 9999 minutes).

To disable GSR transmission, enter a value of 0 (zero). You should be careful when disabling GSR transmissions. The loss of a single SAP advertisement can result in unsynchronized binderies at both ends of the link.

Note: If GSR transmissions have been disabled, ''triggered'' WAN SAP updates will continue to occur whenever a new route comes up or an existing route goes down.

Note: When the WAN SAP period is set to anything other than the default value (1 minute), you must ensure that the router at the other end of the link is configured with the identical WAN SAP period.

Also, use a 0 (zero) SAP period carefully. One lost SAP advertisement (due to data packet corruption during transmission, etc.) results in the node binderies getting permanently out of step at each end of a WAN link. If this happens, recovery must be done by explicitly disabling and re-enabling the circuit(s) associated with a 0 (zero) SAP period interface in one of the nodes.

WAN RIP Period

This is a new x.09 configuration parameter for IPX.

Configuration Editor Parameter and Options

WAN RIP Period

Sets the elapsed time interval between transmissions of RIP updates across the WAN link indicated by the associated Network Number and Circuit Group parameters. Use this parameter to control the transmission of unsolicited RIP updates across any WAN link, thus reducing the amount of bandwidth consumed by the RIP protocol.

Default: 1 minute
Range: 0 to 9999 minutes

If the circuit group provides a LAN connection (such as IEEE 802.3, token ring, and FDDI), simply press [Return]. The IPX router always transmits updates to such media at one-minute intervals.)

If the circuit group provides a point-to-point connection (V.35, T1, E1, etc.), you can control the frequency of RIP updates. The default response, 1, specifies standard IPX advertisement (which issues RIP updates at one minute intervals).

To decrease RIP update frequency, enter a value (up to a maximum of 9999 minutes).

To disable RIP updates, enter a value of 0 (zero). You should be careful when disabling RIP updates. The loss of a single RIP update can result in unsynchronized binderies at both ends of the link.

Note: If RIP updates have been disabled, “triggered” WAN RIP updates will continue to occur whenever a new route comes up or an existing route goes down.

Note: When the RIP update period is set to anything other than the default value (1 minute), you must ensure that the router at the other end of the link is configured with the identical WAN RIP Period.

Also, use a 0 (zero) RIP update period carefully. One lost RIP update (due to data packet corruption during transmission, etc.) results in the node binderies getting permanently out of step at each end of a WAN link. If this happens, recovery must be done by explicitly disabling and re-enabling the circuit(s) associated with a 0 (zero) RIP update period interface in one of the nodes.

Traffic Prioritization

For Bridging, IP, IPX, AppleTalk, and DECnet Services

Prioritization provides a tool for managing the movement of traffic through the router. You can use prioritization alone or enhance it by adjusting the link latency and bandwidth reservation features. Bridge prioritization has been modified in release *x*.09. IP, IPX, AppleTalk, and DECnet prioritization is new in release *x*.09.

Prioritization uses criteria similar to those found in filtering to determine the priority level for traffic in bridging and the routing services. Prioritization assigns traffic through the router to one of three levels:

Normal priority. This is the default priority and is automatically assigned to incoming traffic for which no high or low priority level is specified. Traffic assigned Normal priority has second priority for outgoing bridged or routed transmission.

High priority. Incoming traffic assigned High priority has first priority for outgoing bridged or routed transmission.

Low priority. Incoming traffic assigned Low priority has third priority for outgoing bridged or routed transmission.

Note

In release *x*.08, there are two methods for prioritizing bridged traffic:

1. Prioritize all bridged traffic.

   To prioritize all bridged traffic, use the Traffic Priority parameter.

2. Use filtering to prioritize traffic based on its encapsulation type.

   To prioritize on the basis of encapsulation type:
   a. Set Traffic Priority to “Normal” and
   b. Use the “High Priority” and/or “Low Priority” settings for the Action parameter (in the Traffic Filters screen).

In release x.09, the same capabilities exist, but prioritizing bridged traffic on the basis of encapsulation type is done by using a new Traffic Priority menu instead of the Traffic Filters menu.

Priority assignments apply only to traffic being routed through this router. This means that High or Low priority is applied only to traffic received by the router for retransmission to another device on the network. All other traffic is handled at Normal priority. For example, in the network shown in figure 22:

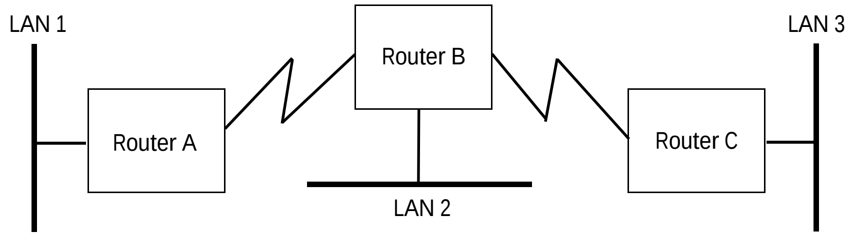


Figure 22. Example Network for Prioritization

- Traffic generated by LAN 1 on Router A and destined for Router C can be prioritized to High or Low while transiting Router B.
- Traffic generated by Router B for transmission to LAN 1 or LAN 3 can have only Normal priority while in Router B, but can be prioritized to High or Low in Routers A and C.
- Traffic generated by Router A and destined only for Router B can have only Normal priority.

To enable prioritization in a routing service, configure the Traffic Priority parameters for that service to assign a High or Low priority to incoming traffic based on the criteria of source, destination, and certain other elements unique to each routing service. (Incoming traffic that does not meet the criteria is left at Normal priority).

Configuration Areas with Packet Prioritization Criteria

	Bridging*	IP	IPX	AppleTalk	DECnet
Source Criteria	MAC source (low) MAC source (high)	Address(es)	Address(es) Node(s) Socket Type	Address(es) Node(s) Socket Type	Area Node
Destination Criteria	MAC dest (low) MAC dest (high)	Address(es)	Address(es) Node(s) Socket Type	Address(es) Node(s) Socket Type	Area Node
Protocol or Other Criteria	DL Format	All, UDP, TCP, Telnet, FTP, SMTP, NFS, DLSw, SNMP, DNS	n/a	n/a	Packet Type
Effect (Correspon-dence)	Ignore Match	Ignore Match Don't Match**	Ignore Match	Ignore Match	Ignore Match

* Applies only to prioritizing bridged traffic on the basis of encapsulation type. To prioritze all bridge traffic regardless of encapsulation type, use the bridge ''Traffic Priority'' parameter instead of the ''Traffic Priority'' menu item.

** ''Don't Match'' is available only when either ''TCP–User Defined'' or ''UDP–User Defined'' is the IP protocol selection.

How Traffic Prioritization Works

Applying "Effect" to the Other Filter Criteria

The "Effect" parameter tells the router how to use the traffic identification criteria (source, destination, or other service-specific data) to make a prioritization decision.

Options and Results for the Effect parameter

"Effect" Setting	Result of "Effect" Setting
Ignore	Ignore the specified packet identification criteria (such as source or destination addresses) and allow any traffic. For example, if Ignore is selected for the ''IP source'' address, then source is not a factor in prioritizing IP traffic.
Match	For the specified packet identification criteria, allow only traffic that exactly matches the selection or range of selections specified by the selection criteria. For example, if Match is selected for the ''IP source'' address, then the source of traffic is a factor, and traffic whose IP source address does not match the source address or range of source addresses specified in the IP traffic priority record will not be prioritized. (That is, such packets will be automatically set to ''Normal'' priority.)
Don't Match	For the specified packet identification criteria, allows only traffic that is outside of the range specified by the selection criteria. **Note:** The option ''Don't Match'' is not available in most cases. For example, if Don't Match is selected for the IP ''UDP/TCP Dest Port'' addresses, then the UDP/TCP destination port is a factor in the selection criteria, and traffic intended for a UDP/TCP destination port or range of ports specified by the ''UDP/TCP Dest Port'' addresses will not be prioritized. (That is, such traffic will be automatically set to ''Normal'' priority.)

Example

In the IP Protocol screen in figure 26 (page 82), the Effect parameter determines whether the criteria will include the IP destination and IP source of traffic as bases for a prioritizing decision. In this example:

- The Protocol parameter is set to "All", meaning traffic from any IP protocol is accepted for prioritizing (unless eliminated by other prioritization elements, such as source or destination constraints).

- The Priority parameter is set to “High”.
- The Effect parameter for “IP dest” (IP destination) is set to “Match”, meaning that the traffic destination must match whatever is specified by the address or range of addresses specified by “IP dest (low)” and “IP dest (high). (To specify a single network address, enter that address for the low value and leave the high value blank. To specify a range of network addresses, enter the bottom of the range for the low value and the top of the range for the high value.)
- The Effect parameter for “IP source” is set to “Ignore”, meaning that packet source is not a prioritizing factor.

```
                              DEFAULT_CONFIG

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

Protocol : All
Priority Action : High
IP dest (low) : 15.100.101.1
IP dest (high) : 15.100.101.3                            Effect : Match
IP source (low) :
IP source (high) :                                       Effect : Ignore
```

Figure 23. Applying "Effect" to Filter Criteria

The above settings mean that High priority is assigned to any IP traffic, from any source address, that is intended for IP destination address 15.100.101.1, 15.100.101.2, and 15.100.101.3. (All IP traffic intended for other destinations are excluded from prioritization and thus will be assigned “Normal” priority.)

Note

Traffic that is not set to High or Low priority is always routed at “Normal” priority.

Configuration Editor Prioritization for Each Service

This section details the Effect parameter in the individual services.

Configuration Editor Access to Prioritization for All Bridge Traffic

Prioritizing all bridge traffic (described in this section) is done in the same way for releases *x*.08 and *x*.09. (Prioritizing bridge traffic based on encapsulation type has changed in release *x*.09 and is described in the next section, starting on page 81.)

```
6. Bridge
    2. Circuit Groups
```

```
                              DEFAULT_CONFIG

===========================- SESSION 1 - MGR MODE -=============================
Configuration Editor
Circuit Group Name :____________
Cost : 100                             STP Priority : 128
LAN ID (Hex) : 1                       Src Rte : No
Max hops : 7                           Block STE : No
Learning Bridge : Yes                  Traffic Priority : Normal
Translational Bridge : No
```

Figure 24. The Bridge Circuit Groups Screen

Parameters and Options

Traffic Priority

Prioritizes all traffic received by the router for bridging, and is an alternative to prioritizing bridge traffic on the basis of *encapsulation type* (described in the next section starting on page 81).

Prioritizes packets received for bridging to other routers via WAN links, and assures that 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.

Default: Normal

High — Incoming packets configured for High priority have first priority for outgoing bridged transmission.

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.

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.

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.

Configuration Editor Access to Encapsulation-Based Bridge Prioritization

```
6. Bridge
    2. Circuit Groups
        2. Traffic Priority
```

```
                              DEFAULT_CONFIG

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

MAC dest (low) : ____________
MAC dest (high) :                                          Effect : Ignore
MAC source (low) :
MAC source (high) :                                        Effect : Ignore
DL Format : MAC Only
Priority Action : High
```

Figure 25. The Bridge Prioritization Screen

Parameters and Options

DL Format — Used in conjunction with the MAC source and MAC dest parameters to determine which bridge traffic will be prioritized (High or Low). Described in chapter 6, ''Bridge Parameters'', in the *Operator's Reference* for your router. This is an element for bridge filtering as well as for traffic prioritization, and operates the same for both functions.

Effect — Determines how to use the corresponding source and destination traffic criteria to make a prioritization decision.

Default: Ignore

Ignore — Allow prioritization of bridge traffic from any source or for any destination (or both).

Match — Allow prioritization of bridge traffic only from source(s) or for destination(s) (or both) specified by the associated source and/or destination parameter settings.

MAC dest (high)
MAC dest (low)
MAC source (high)
MAC source (low)

Source and destination parameters used in conjunction with the DL Format parameter to determine which bridge traffic will be prioritized (High or Low). Described in chapter 6, ‘‘Bridge Parameters’’, in the *Operator's Reference* for your router. These are elements for bridge filtering as well as for traffic prioritization, and operate the same for both functions.

Priority Action

Specifies either High or Low priority for traffic accepted for prioritization.

Default: High

High

Low

Note: Traffic that is excluded from prioritization is automatically set to ‘‘Normal’’ (second) priority.

Configuration Editor Access to IP Protocol Prioritization

```
7. DoD Internet Router
   2. Network Interface Definitions
      2. Traffic Priority
```

```
HP 27288A Router 430           DEFAULT_CONFIG            7-Oct 1995  13:04:44

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

Protocol : UDP - User Defined
Priority Action : High
IP dest (low) :
IP dest (high) :                                         Effect : Ignore
IP source (low) :
IP source (high) :                                       Effect : Ignore

UDP/TCP Dest Port (low) :              (high) :          Effect : Ignore
UDP/TCP Source Port (low) :            (high) :          Effect : Ignore
```

Figure 26. The IP Protocol Prioritization Screen

Parameters and Options

Effect

Determines how to use the corresponding traffic identification criteria to make a prioritization decision.

Default: Ignore

Ignore — Allow prioritization of IP traffic from any source or for any destination (or both).

Match — Allow prioritization of IP traffic only from source(s) or for destination(s) (or both) specified by the associated source and/or destination parameter settings.

IP Dest (high)
IP Dest (low)
IP Source (high)
IP Source (low)

Source and destination parameters used in conjuction with the Protocol parameter to determine which IP traffic will be prioritized (High or Low). Described in chapter 7, Internet Protocol (IP) Parameters, in the *Operator's Reference* for your router. These are elements for IP filtering as well as for traffic prioritization, and operate the same for both functions.

Priority Action

Specifies either High or Low priority for packets accepted for prioritization—destination(s), source(s), and Protocol.

Default: High

High
Low

Note: Traffic that the selection criteria excludes from prioritization is automatically set to ''Normal'' priority.

Protocol

Specifies which IP traffic type to prioritize.

Default: All (specifies all IP traffic for that selection criteria)

All
DLSw
DNS
FTP
NFS
SMTP
SNMP
Telnet

Any of these settings specify the traffic to prioritize.

TCP–User Defined
UDP–User Defined

Either of these settings result in the four parameters listed below to specify the defined port for the traffic to prioritize.

UDP/TCP Dest Port (low), (high)
UDP/TCP Source Port (low), (high)

Low and high source and destination port number parameters appearing when the setting of the Protocol parameter is either "TCP–User Defined" or "UDP–User Defined", to allow you to specify the defined port numbers for the traffic to prioritize. See figure 26 on the previous page.

Configuration Editor Access to DECnet Protocol Prioritization

```
8. DECNET IV Routing Service
   2. Circuit Groups
      2. Traffic Priority
```

```
                              DEFAULT_CONFIG

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

Dest Area (low) : ____________    (high) :                 Effect : Ignore
Dest Node (low) :                 (high) :                 Effect : Ignore
Source Area (low) :               (high) :                 Effect : Ignore
Source Node (low) :               (high) :                 Effect : Ignore
Packet Type (low) :               (high) :                 Effect : Ignore
Priority Action : High
```

Figure 27. The DECnet Prioritization Screen

Parameters and Options

Dest Area (low/high)
Dest Node (low/high)
Packet Type (low/high)
Source Area (low/high)
Source Node (low/high)

Described in chapter 8, DECnet Parameters, in the *Operator's Reference* for your router.

Source and destination parameters used to determine which DECnet traffic will be prioritized. These are elements of the DECnet filtering, and operate the same for both the ''Traffic Filters'' and ''Traffic Priority'' options.

Effect

Determines how to use the corresponding source, destination, and packet type criteria to make a prioritization decision.

Default: Ignore

Ignore — Allow prioritization of DECnet traffic from any source or for any destination, or for any packet type (or all three).

Match — Allow prioritization of DECnet traffic only from source(s) or for destination(s) or for packet types (or all three) specified by the associated source and/or destination and/or packet type parameter settings.

Priority Action Specifies either High or Low priority for traffic accepted by the selection criteria elements (above).

Default: High

High

Low

Note: Traffic that is excluded from prioritization is automatically set to ‘‘Normal’’ (second) priority.

Configuration Editor Access to IPX Protocol Prioritization

```
11. IPX Routing Service
   2. Network Interface Definitions
      5. Traffic Priority
```

```
                              DEFAULT_CONFIG

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

Dest Network (low) : ____________   (high) :               Effect : Ignore
Dest Node (low) :                   (high) :               Effect : Ignore
Dest Socket (low) : NCP                                    Effect : Ignore
Source Network (low) :              (high) :               Effect : Ignore
Source Node (low) :                 (high) :               Effect : Ignore
Source Socket (low) : NCP                                  Effect : Ignore
Priority Action : High
```

Figure 28. The IPX Traffic Prioritization Screen

Parameters and Options

Dest Socket (low)

For prioritization: Specifies the selection criteria for prioritizing IPX packets based on their destination socket type. You can use this parameter either in conjunction with IPX source and destination network and node parameters

For filtering: Operates as described in the *Operator's Reference*.

Default packet type: NCP

Diagnostic	
NCP	(socket number: 0x451 hex)
NetBIOS	(socket number: 0x455 hex)
RIP	(socket number: 0x453 hex)
SAP	(socket number: 0x452 hex)
Serialization	

Source Socket (low)

For prioritization: Specifies the selection criteria for prioritizing IPX packets based on their source socket type. You can use this parameter either in conjunction with IPX source and destination network and node parameters

For filtering: Operates as described in the *Operator's Reference*.

Default: NCP

Diagnostic	
NCP	(socket number: 0x451 hex)
NetBIOS	(socket number: 0x455 hex)
RIP	(socket number: 0x453 hex)
SAP	(socket number: 0x452 hex)
Serialization	

Dest Network (low/high)
Dest Node (low/high)
Source Network (low/high)
Source Node (low/high)

Additional source and destination parameters used to determine which IPX traffic will be prioritized. Described in chapter 11, “IPX Protocol Parameters”, in the *Operator's Reference* for your router. These are elements of the IPX traffic filters, and operate the same for both the ‘‘Traffic Filters’’ and ‘‘Traffic Priority’’ options.

Note: The ‘‘Dest Node’’ and ‘‘Source Node’’ parameters in the IPX Traffic Priority screen operate in the same way as the ‘‘Dest Host’’ and ‘‘Source Host’’ filtering parameters described in the *Operator's Reference*.

Effect

Determines how to use the corresponding source and destination criteria to make a prioritization decision.

Default: Ignore

Ignore — Allow IPX traffic from any source or for any destination and socket type.

Match — Allow IPX traffic only from source(s) or for destination(s) specified by the associated source and/or destination parameter options. Source and destination categories include networks, nodes, and socket types.

Priority Action

Specifies either High or Low priority for packets accepted by the filter elements (above).

Default: High

High

Low

Note: Traffic that is excluded from prioritization is automatically set to ‘‘Normal’’ priority.

Configuration Editor Access to AppleTalk Protocol Prioritization

```
12. AppleTalk Routing Service
    2. Circuit Groups
        2. Traffic Priority
```

```
                              DEFAULT_CONFIG

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

Dest Net (low) : ____________     (high) :                  Effect : Ignore
Dest Node (low) :                 (high) :                  Effect : Ignore
Dest Sock (low) :                 (high) :                  Effect : Ignore
Source Net (low) :                (high) :                  Effect : Ignore
Source Node (low) :               (high) :                  Effect : Ignore
Source Sock (low) :               (high) :                  Effect : Ignore
DDP Type (low) :                  (high) :                  Effect : Ignore
Priority Action : High
```

Figure 29. The AppleTalk Traffic Prioritization Screen

Parameters and Options

DDP Type (high/low)

Used in conjunction with the AppleTalk network, node, and socket parameters to determine which AppleTalk traffic will be prioritized. Described in chapter 12, ‘‘AppleTalk Parameters’’, in the *Operator’s Reference* for your router. These are elements for AppleTalk filtering as well as for traffic prioritization, and operate the same for both functions.

Dest Net (low/high)
Dest Node (low/high)
Dest Sock (low/high)
Source Net (low/high)
Source Node (low/high)
Source Sock (low/high)

Source and destination parameters used in conjuction with the DDP Type parameters to determine which AppleTalk traffic will be prioritized. Described in chapter 12, ‘ ‘AppleTalk Parameters’ ’, in the *Operator’s Reference* for your router. These elements are used for AppleTalk filtering as well as for traffic prioritization, and operate the same for both functions.

Effect

Determines how to use the corresponding source, destination, and DDP Type traffic criteria to make a prioritization decision.

Default: Ignore

Ignore — Allow prioritization of AppleTalk traffic from any source, or for any destination, or for any DDP Type.

Match — Allow prioritization of AppleTalk traffic only from source(s), or for destination(s), or for DDP Type specified by the associated source and/or destination and/or DDP Type parameter settings.

Priority Action

Specifies either High or Low priority for traffic accepted for prioritization.

Default: High

High

Low

Note: Traffic that is excluded from prioritization is automatically set to ‘‘Normal’’ (second) priority.

Managing Outbound, Prioritized Traffic Flow over WAN Links

In the circuit configuration, you can modify bandwidth reservation parameters and the Max Link Latency parameter to better control the access of prioritized traffic to the WAN links in a router.

Configuration Editor Access to Max Link Latency and Bandwidth Reservation

```
4. Circuits
```

Max Link Latency controls the maximum number of milliseconds that any traffic can take to get across a WAN link, by calculating the number of bytes allowed to be queued on the link (as a function of link speed in bits per second).

Bandwidth Reservation parameters prevent any one priority level from taking over the entire bandwidth of a WAN circuit by reserving a percentage of the total available bandwidth for each level of priority. In this way you can "guarantee" bandwidth for packets at each priority level. A parameter for each priority level is available in the menu item below the Circuits parameters, as follows:

```
1. Bandwidth Reservation
```

(The menu item number is other than "1" for some of the WAN circuit types, such as V.25 bis adapter and Frame Relay.)

These parameters are described in chapter 4, "Circuit Parameters", in the *Operator's Reference* for your router.

The following table shows an example of packet queuing at each level for specific bandwidth reservations with a queue length of 128:

Parameter (priority level)	Percent of Bandwidth	Number of Packets
Percent of queue reserved for *high* priority pkts	50	64
Percent of queue reserved for *normal* priority pkts	30	38
Percent of queue reserved for *low* priority pkts	20	26

Effects on Priority Queuing of the Max Link Latency and bandwidth reservation parameters:

Max Link Latency	Bandwidth Reservation	Effects
No (= 0)	No (not configured)	It is possible for higher priority packets to consume all available bandwidth, causing lower priority packets to be dropped.
Yes	No (not configured)	Any packet needing more time than allowed by the link latency will be dropped. It is possible for higher priority packets to consume all available bandwidth, causing lower priority packets to be dropped.
No (= 0)	Yes	Packets of any priority are ‘‘guaranteed’’ to receive their configured percentage of queue bandwidth.
Yes	Yes	Packets of any priority receive their configured percentage of the queue bandwidth if the time they need does not exceed the link latency. Any packet needing more time than allowed by the link latency will be dropped.

Notes

1. When prioritization is active, router throughput decreases because added processing is required for each packet the router receives.

2. To set bandwidth reservation to be *not configured* for the circuit, ensure that the record number following the Bandwidth Reservation menu item is zero, for example:

```
4. Circuits
    1. Bandwidth Reservation (0)
```

   If the record number is other than zero, then bandwidth reservation is set for that circuit. To delete a bandwidth reservation setting from a configuration, display the bandwidth reservation menu item shown above, select it by entering the Bandwidth Reservation menu item number (which is “1” in the above example), and select the Delete action.

Using PPP over Frame Relay

PPP over Frame Relay is a new circuit type that offers the following:

- Allows you to incrementally activate PPP (including compression) on your routers in a Frame Relay network while maintaining interoperability with “regular” Frame Relay peers. The router will use PPP over Frame Relay for peers configured with it, and will fall back to Frame Relay without PPP for peers using Frame Relay without PPP.
- Allows communication with non-HP routers in the same way as is allowed by regular Frame Relay.
- Enables you to use compression for multiprotocol routing in a Frame Relay network.
- Enables negotiation with the remote peer router for the type of compression to use. (Refer to “Using the Predictor Compression Algorithm” on page 96.)
- Allows for interoperating in “mixed” Frame Relay environments where some connections are running with compression on and others are running with compression off. In this environment, the routers negotiate compression and use the default “No Compression” if necessary. That is, transmissions from a router in which compression is “off” will be accepted by a router in which compression is “on”. If the transmitting router has compression “on” and the receiving router has compression “off”, then “No Compression” will be used.
- Allows propagation of ARP frames through Frame Relay (instead of trapping them, as is done in standard PPP configurations).

PPP over Frame Relay normally requires a physical point-to-point WAN connection, such as a leased line, and is not designed for operation in multi-point or multi-access environments. However, when using compression with PPP over Frame Relay, you can use multicast features (provided by the telephone service company) if the Frame Relay network is homogenous (that is, if all routers in the network are running with the same circuit settings). When multicast features are enabled in a homogenous Frame Relay network, each packet is encapsulated in a compressed frame, but the actual data in the packets is not compressed.

Configuration Editor Access to PPP over Frame Relay

```
4. Circuits
```

Then select the circuit to which you want to assign “PPP over Frame Relay” as the circuit type.

```
                               DEFAULT_CONFIG

===========================- SESSION 1 - MGR MODE -=============================
Configuration Editor
Circuit Name : WAN11                   Auto Enable : Yes
Quality of Service : LLC 1 (datagram)  Circuit Type : PPP over Frame Relay
```

For Circuit Type, use ← to select “PPP over Frame Relay”.

Figure 30. Selecting “PPP over Frame Relay”

```
                               DEFAULT_CONFIG

===========================- SESSION 1 - MGR MODE -=============================
Configuration Editor
Circuit Name : WAN11                   Auto Enable : Yes
Quality of Service : LLC 1 (datagram)  Circuit Type : PPP over Frame Relay

                                       Echo Request Time (secs) : 0
Desired Link Quality : 99              Min Frame Spacing : 2
Extended (32-bit) CRC : No             Max Pkt Size : 1578
IP Address :                           LCP Active-Open : Yes
LCP Auto-Restart : Yes                 Max Link Latency (ms) (0=none) : 1000
Use UPAP : No                          Compression : No Compression

1. Frame Relay Parameters (0)
2. Bandwidth Reservation (0)



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

Configure the PPP parameters.

Configure the Frame Relay parameters.

Figure 31. Access to the PPP and Frame Relay Parameters

Parameters and Options

Circuit Type

(Previously existing parameter.) Specifies the circuit type for the circuit identified by the Circuit Name parameter.

PPP over Frame Relay

(New option) Provides a transmission channel for the PPP protocol over a Frame Relay connection to another Frame Relay router or to a Frame Relay network. Results in these additional parameters and menus:

	Echo Request Time
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. Frame Relay Parameters
    1. Permanent Virtual Circuits
    2. Multicast Support
2. Bandwidth Reservation

Note: The corresponding circuit on the peer router must be set to either regular Frame Relay or to PPP over Frame Relay. Also, HP routers can interoperate with other vendors' routers over either Frame Relay or PPP over Frame Relay circuits.

Frame Relay
PPP
etc.

(The previously existing options)

After you set Circuit Type to "PPP over Frame Relay", the PPP parameters appear under the others on the screen. See figure 31 on page 92. You must select an additional menu item to access another screen to configure the Frame Relay parameters (which for the regular circuit type "Frame Relay" appear instead on the same initial circuit screen):

```
1. Frame Relay Parameters
```

Frame Relay Annex A

Two new “Annex A” options have been added to the Management Type parameter to enhance Frame Relay operation, and two other parameters have been added. The additions are described below.

Configuration Editor Access to the Management Type Parameter

Through two possible paths, depending on the Circuit Type setting:

`4. Circuits` *with* `Circuit Type: Frame Relay`

Or:

`4. Circuits` *with* `Circuit Type: PPP over Frame Relay`
`1. Frame Relay Parameters`

Parameters and Options

Management Type

Assigns the interface management mode for the interface between a multiprotocol router and a Frame Relay network. This parameter is described in chapter 4 of the *Operator's Reference*.

Default: LMI (Refer to chapter 4 in the *Operator's Reference* for information on LMI.)

CCITT Annex A

This is a new option that supports CCITT Recommendation Q.933 Annex A. Annex A differs from Annex D in the format of the status message frame. However, the Annex A and Annex D protocol procedures are identical.

Annex A Switch

This is a new option intended to support test/debug environments where two Hewlett-Packard (or Wellfleet) multiprotocol routers are directly connected. In the event of such a configuration, configure one router as a DTE (with ANSI Annex A specified as the Management Type) and the other router as a DCE (with Annex A Switch specified as the Management Type). Selecting Annex A Switch offers you additional parameters:

Provide Update Status	Maximum Poll Interval (seconds)
Monitored Events	Events for Error

‘‘Monitored Events’’ and ‘‘Events for Error’’ are described in chapter 4 of the *Operator's Reference*. ‘‘Maximum Poll Interval’’ and ‘‘Provide Update Status’’ are described below.

LMI
LMI Switch
ANSI Annex D
Annex D Switch
Unsupported

(These are the previously existing options.)

Maximum Poll Interval (seconds)

This parameter appears for a Frame Relay circuit (when the Circuit Type parameter is set to either “Frame Relay” or “PPP over Frame Relay”) when Management Type is set to either ‘‘LMI Switch’’, ‘‘Annex A Switch’’, or ‘‘Annex D Switch’’. It specifies the interval between Status Enq messages received by the Frame Relay network from the router. The status inquiry requests the network to respond with a Link Integrity Verification to verify the status of the DCE/DTE link.

Default: 15 (seconds)
Range: 5-30 seconds

Provide Update Status

This parameter appears for a Frame Relay circuit (when the Circuit Type parameter is set to either “Frame Relay” or “PPP over Frame Relay”) when Management Type for a Frame Relay circuit is set to either ‘‘LMI Switch’’, ‘‘Annex A Switch’,’ or ‘‘Annex D Switch’. It elicits a report from the network on the configuration and status of an existing PVC.

Default: Yes

Yes — Update status.

No — Do not update status.

Enhancements to Compression over PPP Circuit Types

Compression is a method of encoding data so that the resulting file or packet is smaller than the original, and usually results in improved throughput when running on slow WAN links (9.6 to 19.2 Kbits per second). Compressed data sent over a network link needs less bandwidth than the original version would have needed. This enables increased throughput and 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 a circuit, and decompressed. Compression operates over PPP-type WAN circuits and has been enhanced to include the "Predictor" option.

Note

In IPX environments (with all NetWare versions), run compression only when the file server is running the packet burst module, PBURST.NLM 2.02 or greater. Also, the following parameter must be set in the STARTUP.NCF file:

```
set maximum physical receive packet size = 1518
```

Predictor Compression

Predictor compression is significantly faster than the more conventional compression algorithms such as HP PPC. Thus, Predictor compression enables the router to operate more WAN links at higher speeds. This is most significant for the HP Router 650 (which offers 4,8, or 12 WAN ports) and the HP Router 430 (which offers 3 WAN ports). For example, an HP Router 430 using Predictor compression can operate two WAN ports at 56 Kbits per second and the third WAN port at speeds up to 256 Kbits per second. Without using Predictor compression, the 430 can handle a maximum of two 64-Kbits-per-second links.

Predictor compression operates on the following PPP circuit types:

- PPP
- PPP over V.25 bis
- PPP over Frame Relay

The Predictor option is a “type 1” predictor (allowing one packet per frame) and adheres to the following RFCs:

- PPP Compression Control Protocol (CCP) RFC-DRAFT
- PPP Predictor Compression Protocol RFC-DRAFT

WAN Link Planning

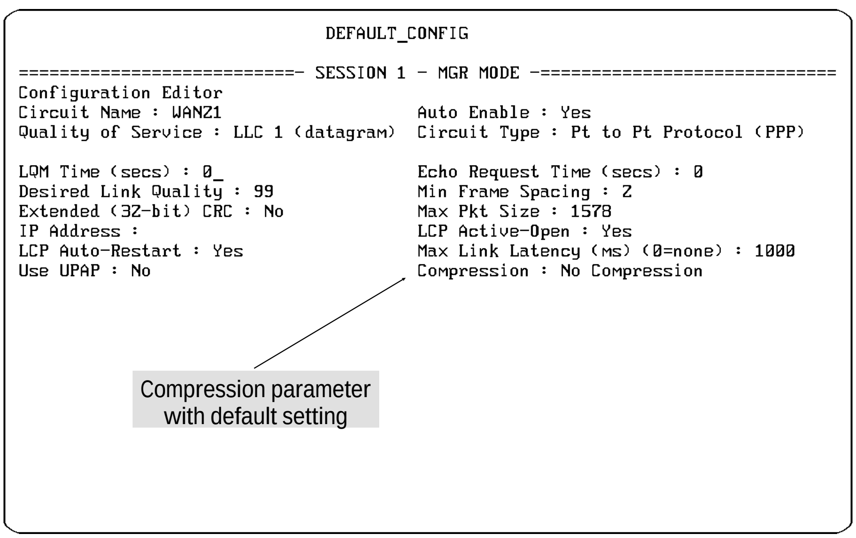
When planning a wide area network, it may be useful to know what link speeds are needed for an estimated WAN utilization level. For example, what link speed should you purchase for running compression if you know you will use approximately 84 Kbits per second of WAN band-width? The following formula provides the estimated speed:

$$\textit{link speed} = \frac{\textit{throughput}}{1.5} \quad \textbf{or} \quad \frac{84\ ^{\text{Kbit}}\!/\!_{\text{s}}}{1.5} = 56\ ^{\text{Kbit}}\!/\!_{\text{s}}$$

For more information, refer to the “Compression” note on the *HP AdvanceStack Routers Documentation and Technical Reference* CD-ROM, included with your documentation package.

Configuration Editor Access to Predictor Compression

```
4. Circuits with Circuit Type: PPP
                               PPP over V.25 bis
                               PPP over Frame Relay
```



```
                              DEFAULT_CONFIG

===========================- SESSION 1 - MGR MODE -============================
Configuration Editor
Circuit Name : WAN21                       Auto Enable : Yes
Quality of Service : LLC 1 (datagram)      Circuit Type : Pt to Pt Protocol (PPP)

LQM Time (secs) : 0_                       Echo Request Time (secs) : 0
Desired Link Quality : 99                  Min Frame Spacing : 2
Extended (32-bit) CRC : No                 Max Pkt Size : 1578
IP Address :                               LCP Active-Open : Yes
LCP Auto-Restart : Yes                     Max Link Latency (ms) (0=none) : 1000
Use UPAP : No                              Compression : No Compression
```


Figure 32. Compression Parameter for Predictor Compression

The following is a revision of the Compression parameter description found on page 4-9 of the *Operator's Reference*.

Compression

Enables or disables packet compression on HP Point-to-Point and PPP-type WAN links connecting two 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 circuit, and decompressed.

Note: To use compression over a given circuit, the same compression type must be configured on both the source and destination routers on that circuit.

Compression operates with the following settings of the Circuit Type parameter:

- Pt to Pt Protocol (PPP)
- PPP over V.25 bis
- PPP over Frame Relay
- HP Point to Point—with the "HP PPC" option only (see options below)

Default: No Compression
Note: This is a change. The default was formerly ''Auto''.

Limitation: On HP routers that are not using Predictor compression, there should be no more than two WAN links operating with compression enabled.

No Compression — Disables packet compression.

Predictor — Available only for WAN circuit types using PPP (listed above). Provides a high-speed, single-packet-per-frame compression (type 1 compression), which is faster than HP PPC compression. Recommended for use in routers having three or more WAN ports operating PPP-type circuits where high-speed compression is desirable, and where the transmission lines are ''clean'' (free of interference that could cause data loss or corruption). Requires that the corresponding port on the peer router also be configured with this option. (If the other port is not also configured for Predictor type 1 compression, then no compression occurs.)

Note: The Predictor option uses more memory than HP PPC compression. When PPP negotiates compression on a link and there is not enough memory for the Predictor option to operate, ''No Compression'' is used. Thus, in situations where multiple routing services are in use, demanding excessive memory, the circuit may revert to operating without compression in order to keep memory usage within acceptable limits. Also, if the PPP link is poor enough to cause the loss of numerous packets, the resulting resynchronizations will slow down PPP operation. Once PPP negotiates a compression setting on a link, that setting tends to remain.

For more information, refer also to the Note following the description of the HP PPC option, below.

HP PPC (Packet-by-Packet)	Enables packet-by-packet compression using a variation of the Lempel-Ziv (LZ) algorithm. This option uses significantly less memory than Predictor compression. It is optimized for running on WAN links that use non-reliable, datagram-oriented services, such as HP Point to Point using LLC1 datagram service. You can also use LLC2 (reliable) service, which provides error detection as well as error recovery by retransmission. However, LLC2 uses more memory in link overhead for acknowledgments and retransmissions, and is not required for HP PPC to run efficiently. **Note:** On the HP Router 650, HP PPC should not be run on WAN links having speeds greater than 256 Kbits per second. The HP PPC algorithm is implemented in software, requiring CPU bandwidth. Thus, throughput is not likely to exceed that of a 256-Kbit/s link, due to the bandwidth needed in the CPU to compress and decompress data. (This factor is true of any LZ-based compression algorithm.) For links having speeds above 256 Kbits per second, use the Predictor option. On fixed-port HP routers such as the HP Router 240 and 430, HP PPC should not be run on WAN links having speeds greater than 64 Kbits per second, due to a CPU-bandwidth limitation similar to that described above. For link speeds above 64 Kbits per second on these routers, use the Predictor option. Also, when using HP PPC on the HP Router 430, which has three WAN ports, no more than two WAN ports should be configured for compression and the third WAN link configured for speeds no higher than 9.6 Kbits per second. As an alternative, consider that the combined maximum—''aggregate norm''—for the Predictor option on fixed-port HP routers is 400 Kbits per second. Thus, for example, using the Predictor option on an HP Router 430 accommodates one WAN port at 256 Kbits per second and the other two at 56 Kbits per second each.
Auto	Available only for the HP Point to Point circuit type. Lets the router automatically sense the compression setting used by the remote device and resets local compression accordingly.

New Statistics Screens

Memory Usage Statistics Screen

The Memory Usage Statistics screen summarizes memory usage as a whole in Series 200 and 400 routers, and usage by slot in Series 600 routers.

```
                              DEFAULT_CONFIG

===========================- SESSION 2 - MGR MODE -============================
                           Memory Usage Statistics

          NAME            LOCAL  Free: byte   seg    GLOBAL  Free: byte   seg
      ---------------     -----      ------   ---    ------      ------   ---
-->      TOTAL           315060        9868     6   2323020     2166392     8











PRESS: 'r' for reset, Down, Up, <- to exit
```

Figure 33. Memory Usage Statistics—Series 200/400 Routers

```
                          DEFAULT_CONFIG

==========================- SESSION 1 - MGR MODE -============================
                        Memory Usage Statistics

         NAME          LOCAL  Free: byte   seg    GLOBAL  Free: byte   seg
      ---------------  -----     ------    ---    ------      ------   ---
--> 1. slot 1        5643168    4971616     24         0           0     0
    2. slot 2         156960      33712      3     26080       19728     1
    3. slot 3        2244960    2082384      2    457696      455888     1
      ---------------  -----     ------    ---    ------      ------   ---
        TOTAL        8045088    7087712     29    483776      475616     2










PRESS: 'r' for reset, Down, Up, <- to exit
```

Figure 34. Memory Usage Statistics—Series 600 Routers

Categories on the Memory Usage Statistics screen are the following:

`NAME` For a Router 650 only, lists individual slots.

`LOCAL` Memory accessed by the CPU.

`GLOBAL` Memory accessed by the CPU and the link device processors.

`Free: byte` Free memory or the amount of memory available for processes in the route to allocate.

`Free: seg` The number of memory segments that have been allocated. (A larger number here indicates increased memory fragmentation.)

Operating System Statistics Screen

The Operating System Statistics screen gives information about router booting, tasks, and CPU.

```
                              DEFAULT_CONFIG

=========================- SESSION 1 - MGR MODE -============================
                         Operating System Statistics

          NAME          Boot Cnt   Tasks   Ready   CPU
       ---------------  --------   -----   -----   ---
--> 1. slot 1                305      39       2     7
    2. slot 2                  1      11       2    12
    3. slot 3                  1      11       2     6
       ---------------  --------   -----   -----   ---
          TOTAL              307      61       6    25









PRESS: 'r' for reset, Down, Up, <- to exit
```

Figure 35. Example of Operating System Statistics Screen—HP 650

Categories on the Operating System Statistics screen include:

`NAME` For a Router 650 only, lists individual slots.

`Boot Cnt` Indicates the number of times that the router has been booted.

`Tasks` Indicates the total number of program entities currently enabled on the operating system of this router. These include the routing and bridging services, utilities, data link services, and the forwarding tasks.

`Ready` Indicates the number of tasks currently ready to run (as opposed to those waiting for the mailbox, waiting for I/O, in the sleep state, and the one task that may be running).

`CPU` Indicates the percentage of CPU utilization.

SNMP Enhancements

Enhancements to SNMP operation include:

- The router now uses the standard SNMP MIB, and conforms to RFC 1213 for MIB II.
- The proprietary SNMP MIB has been removed. For this reason, the information under “snmp: SNMP Information Base” on page 18-90 in the *Operator’s Reference* is now obsolete.
- SNMP now operates much faster than in earlier releases.
- You can use NCL’s Rget commands to examine the MIB of a *local* node without first configuring SNMP. The SNMP descriptions on page 16-40 in the *Operator’s Reference* and page 7-22 in the *User’s Guide* should be updated to indicate this change.
- The Management Priority parameter formerly on the initial screen accessed from the Configuration Editor’s menu item:

  ```
  7. DoD Internet Router
  ```

  is no longer necessary and has been removed.

Note

The “Read/Write” option for the SNMP Session Mode parameter enables reading and writing of MIB data by network management applications.

New and Changed Event Messages

Release x.09 includes the following changes in the Event Log:

dev: Device Event Messages

A.09.60

New and Specific to 100VG

VG attached to hub

Meaning: The router's 100VG port is logged into the 100VG hub.

VG cable failed training

Meaning: The router's VG port failed cable training with the 100VG hub. (For information about 100VG "training", refer to the *100VG-AnyLAN Technology Guide* on the *HP AdvanceStack Routers Documentation and Technical Reference* CD-ROM, included in your documentation package, or to *Planning and Designing High Speed Networks Using 100VG-AnyLAN*, 2nd edition, 1995, by Janis Furtek Costa.)

VG failed to attach

Meaning: The router's 100VG port failed to log into the 100VG hub.

VG port disconnected from hub

Meaning: The router's 100VG port is no longer logged into the 100VG hub.

VG port not connected to hub

Meaning: The router's 100VG port cannot hear tones from the hub, because the cable is not attached, the hub is not powered on, or the cable is faulty.

A.09.60

Similar to Existing Event Messages, for 100VG

100VG circuit assigned to multiple lines

Meaning: One or more line records contains references to the same 100VG circuit.

Action: Modify the lines configuration to make line and circuit records consistent. (See the “Lines Parameters and Options” section for 100VG on page 26.)

CCT *cct#:* 100VG circuit record missing

Meaning: The 100VG circuit with index number *cct#* is not completely configured. There may be some corruption of the configuration file.

Action: To identify the circuit name for that index number, do the NCL command: `get config.cct_table.*`
Find the entry with that index number *cct#*:
`cct_tbl_entry.cct_name[cct#]`
in the list and read the corresponding circuit name beside it. Then reconfigure that 100VG circuit and line.

CCT *cct#:* 100VG line record missing

Meaning: The 100VG line corresponding to the circuit with index number *cct#* is not completely configured. There may be some corruption of the configuration file.

Action: To identify the circuit name for that index number, do the NCL command: `get config.cct_table.*`
Find the entry with that index number *cct#*:
`cct_tbl_entry.cct_name[cct#]`
in the list and read the corresponding circuit name beside it. Then reconfigure that 100VG circuit and line.

CCT *cct#:* Too many lines assigned to the 100VG connector

Meaning: One or more line records contains references to the same Connector VG1 for the same slot. There can be only one line configured per connector.

Action: Modify the lines configuration to ensure that each line has a unique VG connector specified; there is only one Connector VG1 per slot in the router. (See the "Lines Parameters and Options" section for 100VG on page 26.)

DEV CCT *cct#* - XCVR *#* out of range

Meaning: The configuration of circuit with index number *cct#* contains an invalid transceiver number.

Action: To identify the circuit name for that index number, do the NCL command: `get config.cct_table.*`
Find the entry with that index number *cct#*:
`cct_tbl_entry.cct_name[cct#]`
in the list and read the corresponding circuit name beside it. Then reconfigure the lines record. (See the "Lines Parameters and Options" section for 100VG on page 26.)

No 100VG circuits configured

Meaning: This is a possible error condition. No circuits are configured for a router having one or more 100VG ports. None such circuits will be used.

Action: Check your network topology to see if any 100VG circuits should be configured.

Too many 100VG circuits configured

Meaning: The configuration contains an excessive number of VG line records.

Action: Modify the lines configuration to no more than one per 100VG port on the router. (See the "Lines Parameters and Options" section for 100VG on page 26.)

ipx: IPX Router Event Messages

---

ccg:* New Rt to *ipxnet* via *ipx-address

Meaning: Has been changed. It is described at the top of page 17-95 of the *Operator's Reference.* (Here it inaccurately appears with the text "ipx:" in front of it; this text is not part of the message text, but is the managed object that appears in front of all these messages). The IPX routing module generates this event message, no longer whenever it learns a new route or updates an existing route, but now only when the network interface comes up. The "Note" should have the initial words "HP Router 650 Only" removed; the note is valid for all HP routers.

A.09.60
B.09.60

CG *ccg:* Del Srv *server* at *ipx-address*

Has been removed, as of operating code release x.08. It appears on page 17-92 of the *Operator's Reference*.

CG *ccg:* New Srv *server* at *ipx-address*

Has been removed, as of operating code release x.08. It appears on page 17-93 of the *Operator's Reference*.

---

ipx: *ccg:* New Srv *server* at *ipx-address*

Has been removed, as of operating code release x.08. It appears on page 17-95 of the *Operator's Reference*.

pm: Port Module Manager Event Messages

Port Module slot *slot#* state mismatch

Has been removed. It is described on page 17-115 of the *Operator's Reference*. It is replaced by the following event message:

Port Module slot *slot#* removed and not re-installed

This message is described on page 17-114 of the *Operator's Reference*.

tcp: Transmission Control Protocol Event Messages

Connection attempt to *ip-address* failed

Meaning: An attempt to establish a Telnet virtual terminal connection between the router and *ip-address* failed.

Action: Check the event log file for a corresponding TCP event message indicating why the connection attempt failed.

Connection from *ip-address* refused, exceeds limit

Meaning: *ip-address* attempted to establish a Telnet virtual terminal connection into the router, but was refused access because the Telnet connection limit had already been reached.

tftp: TFTP Event Messages

Waiting for FGET to complete

Meaning: The router is attempting a TFTP download of a configuration as a result of a Bootp-initiated configuration request. There will be a short pause in system operation while the appropriate link is activating.

X.25 Event Messages

Switch call - *X* to *Y*

Meaning: Indicates that the X.25 switch received a call from DTE *X* and is switching it to DTE *Y*.

Switched call established.

Meaning: Indicates that the switched call has been accepted.

Switch clear from *X* to *Y*

Meaning: DTE *X* has initiated a clear to DTE *Y*.

Switch cleared - *X* to *Y*

Meaning: The clear initiated by DTE *X* has been confirmed by DTE *Y*.

New Operating Messages

Any of the following messages appearing on the console screen during a TFTP update of the router operating system (initiated by an Fget command) indicate a failure involving the (automatic) download-file compression and probable corruption of the router's operating system (OS) code.

Note In most cases, the OS code can be re-installed with assistance from your Hewlett-Packard support provider, and it should not be necessary to return the router unless the decompression failed due to a hardware problem.

In HP Series 200 or 400 Routers

```
FATAL EXCEPTION: Tftp: decompression failed
```

If this message appears, wait approximately one minue for an automatic boot of the router, then re-execute the Fget command. Contact your Hewlett-Packard support provider for assistance if the command fails again or if you see the following on the screen:

```
router console>
```

In the HP 650 Router

```
router console>
```

If this message appears, contact your Hewlett-Packard support provider for assistance.

Part 3

Changed Features

The following changes were effective as of release x.08, but are repeated here to help ensure that users of earlier releases are aware of them. (Unless otherwise noted, these changes are reflected in the manuals provided with this release.)

- The slot number for the fixed-port routers is now number 1 instead of 2.

  Since the slot number for series 200 and 400 routers never varies, it has little import, but you may have noticed it in the names of some managed MIB objects, such as "buf[2]" and "rok[2]". You would see such objects in the event messages and in the List, Get, and Rget commands. The number 1 will now appear.

  This change was made for consistency among all HP router models, including those in the series 600 with several "slots".

- The industry-standard Point-to-Point Protocol (PPP) has some configuration defaults changed to settings more often required for multivendor interoperability (for example, with 3Com, Cisco, and Proteon routers).

  LQM Time was changed from 3 to 0 seconds. This disables link-quality monitoring, which is not supported by most routers.

  Extended (32-bit) CRC was changed to No. This means that 16-bit error detection is now the default; 32-bit detection is not supported by most routers.

- OSPF configuration (within IP routing) has some parameter defaults changed. AS Boundary now defaults to No. Authentication Type now defaults to No Authentication (not Simple Password). See page 7-8 in the *Operator's Reference*. The change for Authentication Type is *not* reflected there.

- NCL's commands for "Accessing a Remote Management Information Base", Rgetw and Rgetmw, have changed names to Rgethp and Rgetmhp, respectively. Rgethp displays an individual MIB variable from a remote HP router, and Rgetmhp displays values for a whole branch of MIB variables from a remote HP router.

  The commands are described under their old names in the *User's Guide* on page 7-23, and in the *Operator's Reference* on pages 16-48–16-50. They work the same; only the command names have changed.

- The two MIB objects for operating code version have been changed to a single standard SNMP name. (See pages 18-47–18-48 in the *Operator's Reference*.)

  ```
  config.ver_major[0]
  config.ver_minor[0]
  ```

  are now:

  ```
  config.version[0]
  ```

- TFTP (the Trivial File Transfer Protocol) now can be used to either push or pull the operating code or the configuration through the network. This can be done from one centralized facility on the network. For security, each router can be configured with a list of IP addresses from which it will accept these two items.

  In order to push an operating code or configuration to a remote router, the remote router must have IP routing configured (which SmartBoot can accomplish remotely, with the use of Quick Remote's IP address field). The remote router must also have the new IP/TFTP configuration parameter Allow Router to Accept Files set to Yes, and the new Client Address screen following it must include the local (pushing) node's Internet Address. (See the *Operator's Reference*, page 7-8). SmartBoot can accomplish these settings remotely also. Both parameters are set by Quick Remote's TFTP Security field (see page 8-14 in the *User's Guide*).

  Note that the description of NCL's Fput command on pages 16-95–16-96 in the *Operator's Reference* incorrectly states that "You cannot use Fput to put the operating code or configuration on another router." Now you *can* use Fput from one router to another under the conditions described above.

  Also, the description of the TFTP Security field on page 8-14 in the *User's Guide* has errors. The field is "TFTP Security", not "TFTP Client" as stated in the shaded callout on figure 8-5 and in the second sentence of the subsequent paragraph. The column heading on figure 8-5, "TFTP Security IP Address", is correct. The effect of the field is stated incorrectly; the second sentence in the first paragraph should be:

  > That is, if the "TFTP Security IP Address" field contains an address, then the remote router receiving that configuration will subsequently accept a TFTP PUT of a configuration file from that address.

  Step 11 on page 8-11 should state that you enter the IP address of the TFTP server.

Part 4

Notes and Corrections

Unless otherwise noted, these items are *not* shown in other manuals.

- 100VG connector, circuit, and circuit group names are listed incorrectly on page 14 in the *Installation Guide* for the HP J2438A 100VG Port Module.

  In the section "Prepare the router", the final note on configuration at the bottom of the page should be:

  > The connector name for the VG port is "VG1". The default circuit name is "VG#1", and the default circuit group name is "VG#1G", where "#" is the number of the VG port module's slot. Look for these names when you are verifying router initialization and configuration, for example, in the event log.

- The clock speed for internal clocking is limited on lines using an RS-232 WAN cable, as follows:

  In the *Installation Guide* for the series 200 and 400 routers, on page A-3, please note the following for the RS-232/V.24/V.28 cable supplied as an option with the router (part number 28606-63006):

  > The setting of the Clock Speed configuration parameter can be a maximum of 64 Kbit/s when using this HP cable. (Note that this maximum is greater than the default setting of 56 Kbit/s, so the default is also acceptable.)

  In the *Installation Guide* for the series 200 and 400 routers, on page A-12, please note the following for construction of a RS-232/V.24/V.28 cable:

  > The setting of the Clock Speed configuration parameter can be a maximum of 19.2 Kbit/s when using a cable other than the HP 28606-63006 cable.
  >
  > Note that this maximum speed is *less than the default setting* of 56 Kbit/s. If the Clock Source parameter (in the Lines branch of the Configuration Editor) has been changed to the "Internal" setting, then the Clock Speed parameter also must be changed to 19.2 Kbit/s or less. (You can do this in Quick Configuration, by using the hot key [/] [M] to access the Main Configuration menu and then selecting the Lines item.)

  In the *Operator's Reference*, on page 3-4, please note the following for the description of the Clock Speed parameter:

  > The maximum setting is 64 Kbit/s if an HP 28606-63006 5-meter RS-232/V.24/V.28 cable is used, or 19.2 Kbit/s for any other RS-232/V.24/V.28 cable.

- There is an error in the voltage range heading in the specifications in the *Installation Guide* for the series 200 and 400 routers.

  On page C-2, the second column heading under “Power Consumption” should be:

  Maximum current at 100–127 Vac

- A console error message is not included in the router documentation:

  CONFIGURATION INITIALIZATION FAILED

  This message may appear on the console, if one is connected, when booting with a configuration that has a blank record. A blank record can occur when using the Configuration Editor to add or modify a record and pressing Return to navigate through a screen without setting every parameter purposefully. Pressing Return for a field containing a default setting does set that parameter. Pressing Return for a blank field sets nothing for that parameter. Then saving the configuration creates an incomplete record for the screen navigated. When booting, the configuration fails to implement, generating the message shown above. Usually a second line is generated, indicating where the blank record is located:

  Parameter *abc* missing in *xyz* record

  At this point, you are able to return to the Configuration Editor. Delete the unintended record.

  You can avoid this problem by using the action Browse—not Modify or Add—when navigating through screens, until you find parameters you intend to set.

- The wavelength supported on multimode fiber for the FDDI port on the HP Router BR is 1300 nanoseconds. (Single-mode fiber is not supported.) In the *Installation Guide* for the series 200 and 400 routers, this wavelength should be noted with the FDDI Cable definition on page A-19, with the Data Communications Specifications on page C-4, and in appendix D.

- IPX routing restricts the configuration for each port to only one network and one frame type.

- The *User's Guide*, on page 4, states incorrectly that appendix A contains the Parameter Locator. It actually contains “Notes on Configuring From a Bootp Server”, describing the conditions, preparations, and operation for automatic configuration and booting of the router from a server on the network. The Parameter Locator actually is in appendix A of the *Operator's Reference*.

- The help key for editing Quick Configuration fields for empty slots is identified incorrectly in figure 3-23 on page 3-34 of the *User's Guide*.

  The last line of help on the bottom of the screen is actually:

  Press CTRL-E for help with editing this field.

- For the Circuit Type configuration parameter, the option "Manual adapter" is missing from the *Operator's Reference* on page 4-9.

  Manual adapter is used with terminal adapters/modems that either do not have V.25 bis or have it disabled. The terminal adapter on either this router or the other router will be either manually dialed or programmed to dial when DTR is raised.

- The configuration parameter Max Link Latency (for WAN circuit types HP Point-to-Point, Point-to-Point Protocol (PPP), PPP over V.25 bis, and V.25 bis adapter), is defaulted to 1000, not 0 (zero) as shown in the *Operator's Reference* on page 4-19.

- The OSPF configuration parameter Authentication Type defaults to "No Authentication", not "Simple Password" as shown on page 7-8 in the *Operator's Reference*.

- Additional information about the X.25 window size configuration parameter, Pkt Window:

  The Pkt Window parameter on the LAPB (X.25) circuit parameters screen can be set to values from 1 to 7 (referred to as Modulo 8 numbering), and to values from 8 to 127 (Modulo 128 numbering).

  The default (2) and the range (1 to 127) for Pkt Window are shown on page 13-11 of the *Operator's Reference*. A setting of 4 or 5 should be sufficient for most links. To enhance performance on links with high latency or great round-trip propagation time, such as for satellite or cross-continent fiber links, configure Pkt Window to the number of packets that can fill the link. Calculate this as follows:

  $$\frac{1}{linkspeed \times pktsize \times bits/pkt} \times travel\ time$$

  (*travel time* is the time for 1 bit to travel from one unit to another.)

- The syntax of NCL's Disable and Enable commands is incorrect on page 7-8 of the *User's Guide*. Identifiers are not optional. The syntax should appear as follows:

  ```
  disable identifier

  enable identifier
  ```

- The name of the managed object for device drivers is now “dev”, instead of “driver” as shown in the table on page 7-14 in the *User’s Guide*.
- The managed object for Switched Multi-megabit Data Service, “smds”, is omitted from the table on page 7-15 in the *User’s Guide*.
- The string-search feature for NCL’s Log command is included in the *Operator’s Reference*, but not in the *User’s Guide*.

  See the description of Log in the *Operator’s Reference* on pages 16-11–16-12. The additional syntax should appear also in the *User’s Guide* on page 7-8.
- NCL’s Rboot command (for booting a router over the network) appears in the *Operator’s Reference*, but not in the *User’s Guide*.

  See the description of Rboot in the *Operator’s Reference* on page 16-21. Rboot should appear also in the *User’s Guide* on page 7-8.
- The syntax of NCL’s Test command on page 7-8 of the *User’s Guide* should show the station address as a required variable. The syntax should appear as follows:

  ```
  test mac_addr [count] [delay]
  ```
- NCL’s commands for “Accessing a Remote Management Information Base”, Rgethp and Rgetmhp, are described under their old names, Rgetw and Rgetmw, in the *User’s Guide* on page 7-23 and in the *Operator’s Reference* on pages 16-48–16-50. They work the same; only the command names have changed. Rgethp displays an individual MIB variable from a remote HP router, and Rgetmhp displays values for a whole branch of MIB variables from a remote HP router.
- NCL’s Ipmap command (for V.25 bis switched virtual circuits) no longer shows the map state as “connected” while retrying phone numbers. The map state is now “connect wait” while retrying phone numbers. This should be noted in the *Operator’s Reference* on page 16-90.
- Fput and other TFTP PUT errors:

  The description of NCL’s Fput command on page 16-95–16-96 in the *Operator’s Reference* incorrectly states that “You cannot use Fput to put the operating code or configuration on another router.” Fput *can* be used to push (“put” or copy) the operating code or configuration from one router to another. (The operating code on one HP router is not always compatible with another HP router. Refer to the “Software Compatibility Matrix” on page 15 for code compatibility between specific HP routers.) Operating code or configuration can also be pushed onto the router from a centralized file server on the network, using its TFTP utilities.

For security, each router can be configured with a list of IP addresses from which it will accept operating code or a configuration. Otherwise the router will not accept them. Two methods are:

- Set the Allow Router to Accept Files parameter to Yes and configure the subsequent Internet Address parameter to the IP address of the pushing router; this must be done on the router, in the Configuration Editor's TFTP Configuration screen within the DoD Internet Router configuration.
- When SmartBooting the router by using Quick Remote on another router, configure the "TFTP Security" field on the Quick Remote screen.

On page 8-14 in the *User's Guide*, the text "TFTP Security" should appear instead of "TFTP Client" in the shaded callout on figure 8-5 and in the second sentence of the subsequent paragraph. The column heading on figure 8-5, "TFTP Security IP Address", is correct. The effect of the field is stated incorrectly; the second sentence in the first paragraph should be:

> That is, if the "TFTP Security IP Address" field contains an address, then the remote router receiving that configuration will subsequently accept a TFTP PUT of a configuration file from that address.

Also on page 8-14, following that paragraph, add the following:

> This address also specifies that router operating code will be accepted by the remote router from this address.

Step 11 on page 8-11 should state that router operating code as well as a configuration file will be accepted, and should state that you enter the IP address of the "TFTP server" (the pushing router or host), not the "remote device".

The description of TFTP on pages 7-30–7-31 of the *User's Guide* should also describe using NCL's Fput command to copy router operating code or the router's configuration to a file on a remote host. In the Command Syntax and Command/Function sections, the following syntax should be added:

```
fput x.x.x.x operator filename
```

with the function of writing the operating system or configuration file to a remote host, or to another router. From router to router, the operating/configuration files must be compatible; refer to page 15.

- Two error messages for NCL's Ipmap command are missing from the *Operator's Reference* on page 16-91.

  System message failed

  Meaning: The system message used to get information about the associated circuit has failed, so the command cannot be executed.

  Action: Ensure that the circuit is available.

  System out of message buffers

  Meaning: System message buffers ran out, so the Ipmap command could not be executed.

  Action: Wait for load on the router to decline, then try again.

- There should be an illustration of the event log entry in the *User's Guide* on page 5-2 after the second paragraph. You can see this illustration on page 17-2 in the *Operator's Reference*.

- The event message, "Invalid ARP Source", generated by the object "ip", is not included in chapter 17 of the *Operator's Reference*, in the IP section.

  Invalid ARP Source

  Meaning: The IP interface indicated received an ARP request that seemed wrong. It usually indicates an unrecognized subnet address.

  Action: Check for an end node with a misconfigured IP address, or a node configured correctly, but with a subnet different from the one configured for the router IP interface. In the second case, you can configure the parameter Drop Non-local ARP source so that the unrecognized subnet will be ignored.

Appendix A

Application Note: Using Bootstrap Protocols in an Internet Environment

Overview

Bootp and Dynamic Host Configuration Protocol (DHCP) are popular tools that greatly ease a network administrator's work load by providing central administration of IP addresses and configuration files. Originally designed for diskless workstations that would typically be on the same LAN as the server, Bootp has been expanded to support different types of network devices across an enterprise internetwork. The design of Bootp and DHCP require the use of a relay agent to function on an internetwork. The relay agent handles the forwarding of the Bootp or DHCP packets across a router.

Scope

The purpose of this application note is to discuss and clarify the use of HP routers as relay agents in the Bootp and DHCP process. It is not intended to be a complete discussion of the Bootp or DHCP protocols and assumes a knowledge of the IP protocol and IP subnetting.

Definition of Terms

Logical Network Segment A logical network segment here connotes a network segment made up of physical cable segments, hubs, repeaters, and bridges. A router separates logical network segments. Figure 1 shows two logical network segments connected by a router.

IP Subnet An IP subnet is a logical network segment to which an IP subnet address is assigned. It is possible to assign multiple IP subnet addresses to the same logical network segment. This is called multinetting and each IP subnet address creates a different IP subnet.

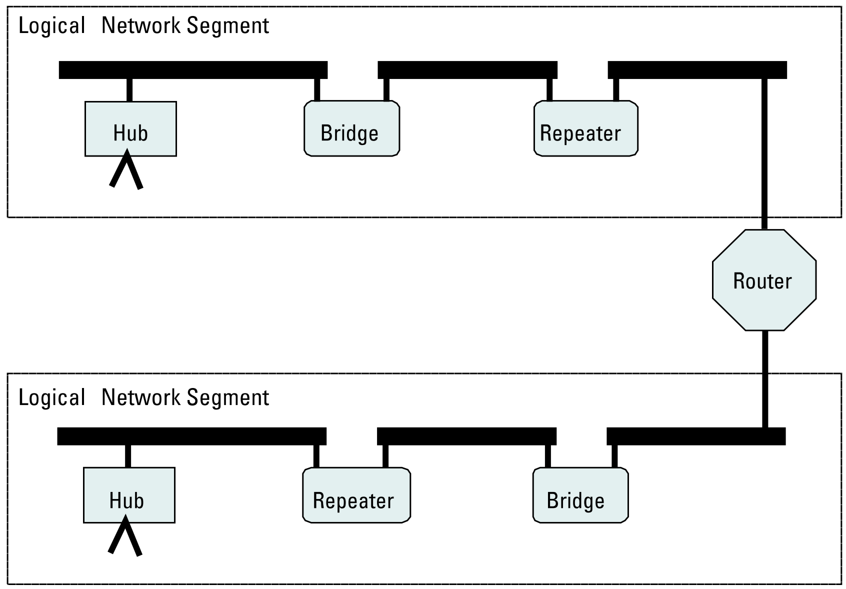


Figure 1. Logical Network Segment

Single Subnet Broadcast The single subnet broadcast uses the assigned network number in the network part of the IP address, the assigned subnet number in the subnet part of the IP address and all ones in the host part of the IP address. For example, assume the class A network 10.0.0.0 is using subnet mask 255.255.255.0 and the particular subnet is 10.140.121.0. The resulting single subnet broadcast would be 10.140.121.255. The single subnet broadcast will be received by all hosts on a particular IP subnet. A router on the subnet will not forward it to any other subnet. If multiple IP subnets are assigned to the same logical network segment (IP multinetting), hosts belonging to one IP subnet will ignore the single subnet broadcasts of any other subnet.

All-subnets Broadcast The all-subnets broadcast uses the assigned network number in the network part of the IP address and has all ones in both the subnet and host parts of the IP address. For example, assume the class A network 10.0.0.0 is using subnet mask 255.255.255.0. The resulting all-subnets broadcast would be 10.255.255.255. A router will not forward an all-subnets broadcast received on any interface, unless the network interface ASB parameter is enabled. If ASB is enabled on the receiving interface, the all-subnets broadcast will be forwarded to another interface only if the interface has ASB enabled and the interface belongs to the specified network or has a route to the specified network.

Local-Wire Broadcast The local-wire broadcast address is 255.255.255.255. It would be tempting to interpret this address as an “all-networks” broadcast that would be forwarded across every subnet on the internetwork. This, however, is not acceptable, so the address 255.255.255.255 is defined to mean all hosts on a logical network segment or “local wire”. It will be received by all the hosts on the local wire, but will not be forwarded by a router to any other subnet. There is a difference between a local-wire broadcast and a single-subnet broadcast when IP multinetting is used. A local-wire broadcast will be received by all hosts on all IP subnets on the logical network segment. A single-subnet broadcast will be received by only those hosts belonging to the particular IP subnet and will be ignored by hosts assigned to different IP subnets on the same logical network segment.

Bootp

Bootp was originally designed to allow a diskless workstation to get its IP address and the name and location of its boot image file from a Bootp server. It was first defined in RFC 951 by Croft and Gilmore in September 1985 and was developed as an improvement over Reverse Address Resolution Protocol (RARP). RARP provides a mechanism to get only an IP address. Bootp has been clarified and enhanced in several succeeding RFCs. As of August 1994, the current RFCs defining Bootp are RFC 951, RFC 1533, RFC 1534, and RFC 1542. Bootp is now used by many different network devices to accomplish the process of booting with varying degrees of limited knowledge. For example:

- A PC with local operating system may need only its IP address, subnet mask and default gateway.
- A print server like JetDirect with local firmware may need the above information plus a configuration file.
- A diskless workstation may need all of the above plus a boot image file.

In general, the Bootp process is a two-step process: the Bootrequest/Bootreply step and the download step. The download step is optional, however, and only required if the client needs to download a boot image or configuration file. TFTP is most often used to download the file in the download step. Bootp uses UDP as the transport layer protocol.

Bootp on a Single IP Subnet

When the client and server are on the same IP subnet, the Bootp process goes as outlined above. The client sends a Bootrequest to the server that responds with a Bootreply. If the download step is required, it uses the information in the Bootreply packet. In detail, the process consists of:

1. The client formats a Bootrequest packet (see “Bootrequest/Bootreply Packet Format” on page 134) with the information it knows at that point in time. Typically, it knows only its own station (MAC) address, which it inserts in the “chaddr” field. The client sends the Bootrequest to UDP port 67 which is the well-known UDP Bootp server port. The source port is 68 which the well-known UDP Bootp client port. The IP header is formatted with the local-wire broadcast as the destination address and 0.0.0.0 as the source address. See figure 2.

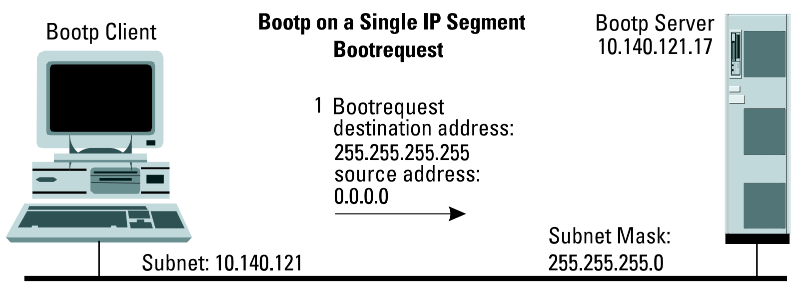


Figure 2. Single Segment Bootrequest

2. The Bootp server, listening on UDP port 67, receives the packet, and uses the client’s station address from the “chaddr” field to find the client’s entry in the Bootp database (/etc/bootptab on a UNIX machine). The server uses the information in the database entry to fill in the appropriate fields in the Bootreply packet. For example, if the client needs to know its IP address, the server’s IP address and the boot/config file name, the servers fills in the “yiaddr” field with the client’s IP address, the “siaddr” field with the server’s IP address, and the file field with the fully qualified name of the boot/config file. In most cases, the server then unicasts the Bootreply packet to UDP port 68 and the client’s IP and station address. Most of today’s IP implementations allow the client to receive this unicast packet without knowing the client’s IP address. In some implementations, however, the client software cannot receive unicast packets until it knows its IP address. In these cases, the client sets the broadcast bit in the Bootrequest flags field and the server broadcasts the Bootreply packet to the client. This step is shown in figure 3.

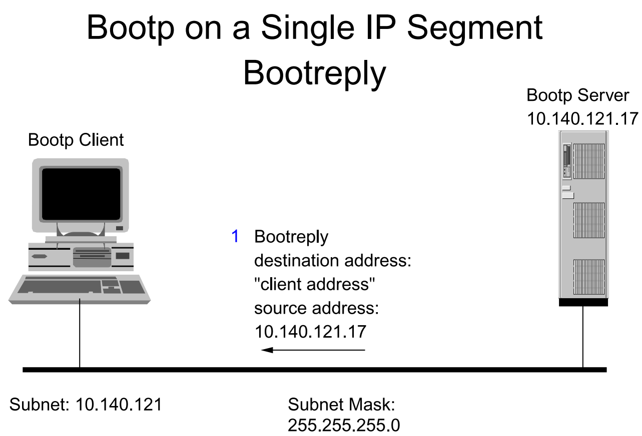


Figure 3. Single Segment Bootreply

3. The client receives the Bootreply packet on UDP port 68 and uses the information in it to initialize its software. If all the client needs is its IP address, the Bootp process is complete. If, however, the client needs to download a boot image or configuration file, it then sets up a TFTP download using the server IP address and file name that was received in the Bootreply packet.

The Bootp Relay Agent

If the Bootp client and server are on different IP subnets, the Bootp server will not receive the Bootrequest because, as mentioned above, the client uses a local-wire broadcast to transmit the Bootrequest, and a router will not forward local-wire broadcasts to any other subnets. A Bootp relay agent is therefore required. It receives a Bootrequest packet on a subnet without a Bootp server and forwards it to a subnet with a Bootp server. In this case, the Bootp process proceeds as follows:

1. The client formats a Bootrequest packet (see "Bootrequest/Bootreply Packet Format" on page 134) with its own station address in the "chaddr" field. The IP header is formatted with the all-hosts broadcast as the destination address and 0.0.0.0 as the source address. The MAC header is formatted with the MAC broadcast as the destination address and the client's station address as the source address. This is just as in the first case.

2. The Bootp relay agent, listening on UDP port 67, receives the Bootrequest packet and places its IP address in the "giaddr" field. (The IP address placed in the "giaddr" field is the address of the interface on which the Bootrequest packet was received.) The relay agent also increments the hops field by one to limit the number of gateways the Bootrequest crosses. The Bootrequest packet is then forwarded to the Bootp server. The method of forwarding the Bootrequest depends on how the relay agent destination is configured. The alternatives are detailed below.

3. The Bootp server, listening on UDP port 67, receives the Bootrequest packet, and uses the client's station address ("chaddr" field) to find the client's entry in the Bootp database (`/etc/bootptab` on a UNIX machine). The server uses the information in the database entry to fill in the appropriate fields in the Bootreply packet. The server knows a relay agent is involved in the process, because the "giaddr" field has been set. The server unicasts the Bootreply packet back to the relay agent using the IP address found in the "giaddr" field. In this step, both the source and destination UDP ports are 67.

4. The relay agent, still listening on UDP port 67, receives the Bootreply packet and unicasts it to UDP port 68 and the client's IP address. (In software versions *x*.09.*xx*, the HP router relay agent has the ability to broadcast the Bootreply to the client if the broadcast bit of the flags field is set.)

5. The client receives the Bootreply packet and uses the information to initialize its software. If all the client needs is its IP address, the Bootp process is complete. If, however, the client needs to download a boot image or configuration file, it sets up a TFTP download using the server IP address and file name received in the Bootreply packet.

Bootp Relay Agent Configuration

The are three alternatives for configuring the relay agent's destination address on HP routers. The configurations differ in how they forward Bootrequest packets from the client to the server and are listed below.

Specific Host Address Destination When a specific host address (the address of the Bootp server) is configured as the relay agent destination, the agent receives the local-wire broadcast Bootrequest and changes the IP destination address to the specific destination host address. The packet is now a normal IP unicast packet that is routed as needed on the internetwork. Therefore, other routers between the relay agent and the server do not need to have the relay agent enabled. The Bootrequest and Bootreply steps using this configuration are shown in figures 4 and 5.

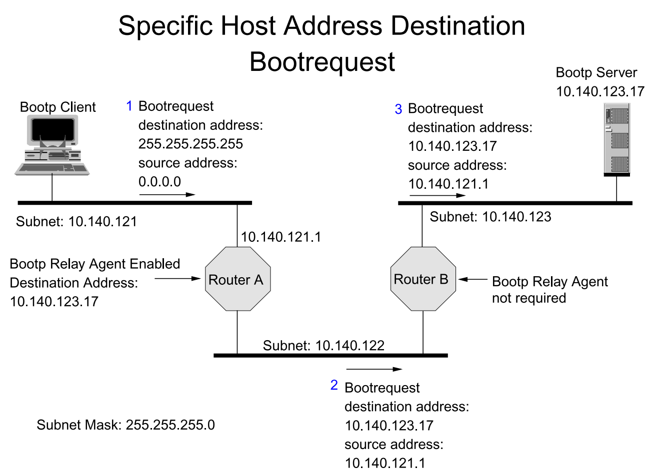


Figure 4. Specific Host Bootrequest

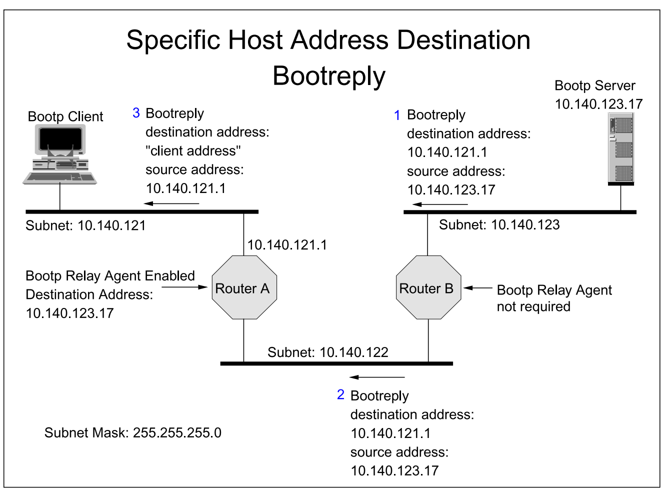


Figure 5. Specific Host Bootreply

Specific IP Subnet Address Destination When a specific subnet address is configured as the relay agent destination, the agent received the Bootrequest as a local-wire broadcast and changes the IP destination address to a single subnet broadcast (for example, 10.140.121.255) to the specified IP subnet. If the specified destination IP subnet is not local to the router, the packet can be routed as needed on the internetwork. Other routers between the relay agent and the server do not need to have the relay agent enabled. The Bootrequest and Bootreply steps using this configuration are shown in figures 6 and 7.

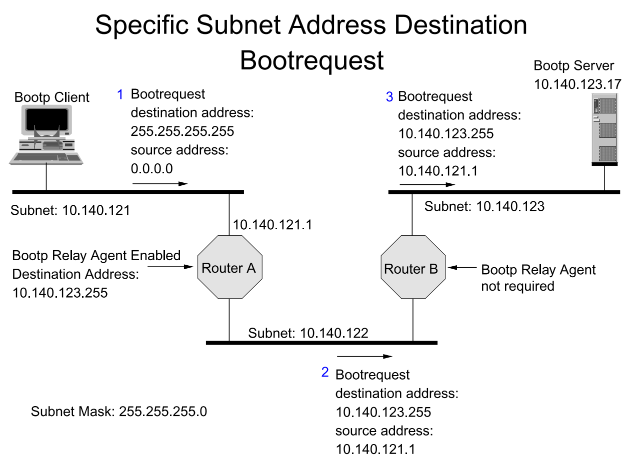


Figure 6. Specific Subnet Bootrequest

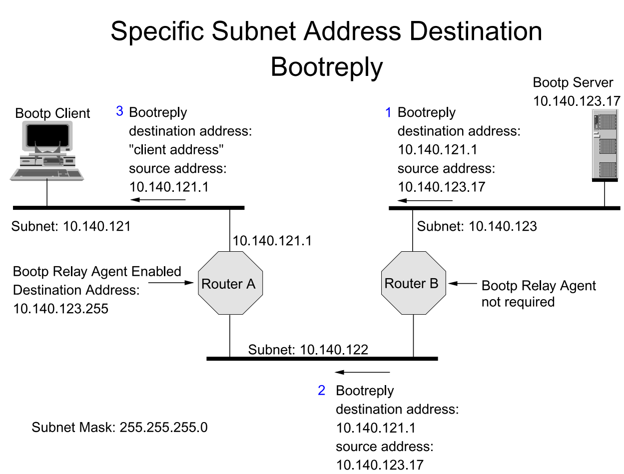


Figure 7. Specific Subnet Bootreply

No Destination, All-Subnets Broadcast, or Local-Wire Broadcast Destination When no relay agent destination, nor destination of the all-subnets broadcast (for example, 10.255.255.255), nor destination of the local-wire broadcast is configured, then the relay agent forwards the Bootrequest packet as a single subnet broadcast (for example, 10.140.121.255). It is broadcast on each IP subnet defined on every interface on the local router. If multiple IP subnets are configured on a single interface (multinetting), the Bootrequest will be transmitted as a single subnet broadcast on each IP subnet. Since the relay agent only forwards the Bootrequest to local IP subnets, if the Bootrequest must cross additional routers to reach the Bootp server, the relay agent must be enabled on each router between the client and the server. The Bootrequest and Bootreply steps using this configuration are shown in figures 8 and 9.

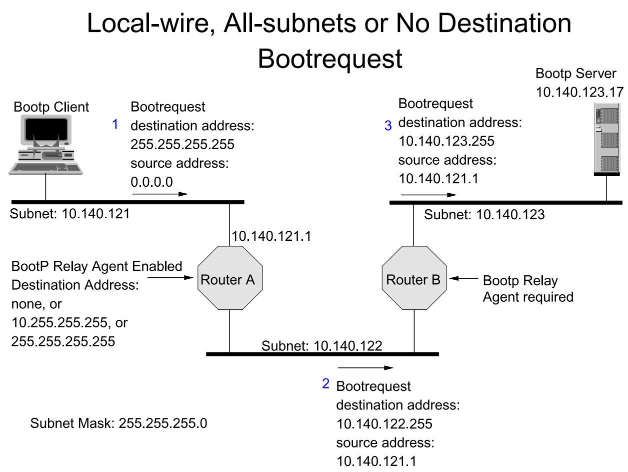


Figure 8. Local-Wire Bootrequest

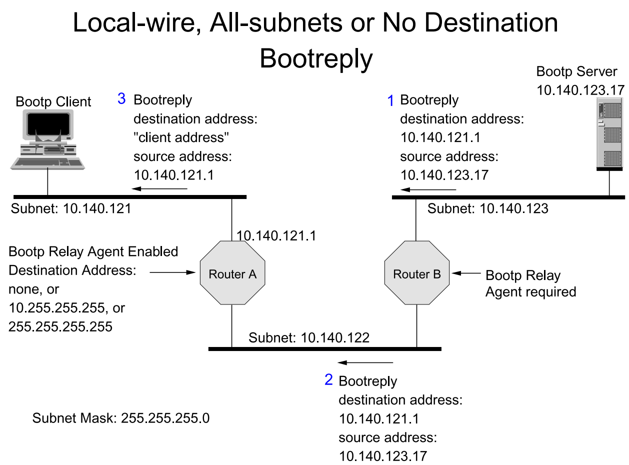


Figure 9. Local-Wire Bootreply

In each case, the Bootreply packet is forward in the same way. The Bootp server sends the Bootreply directly to the relay agent as a normal unicast packet using the address from the “giaddr” field. This packet is routed normally across the internetwork. The relay agent then sends the Bootreply to the client as described above.

DHCP

DHCP is an enhancement to Bootp and has the ability to do automatic and dynamic IP address allocation. Because of these features, DHCP will be even more widely used than Bootp. For example, Microsoft has incorporated DHCP support in both the Windows NT client software (DHCP client) and the Windows NT Advanced Server software (DHCP server). DHCP was defined in RFC 1531 (R. Droms, 10/93) and was designed to be interoperable with Bootp. It uses the same format as Bootp for its Bootrequest and Bootreply packets. This was done specifically to allow Bootp clients to use DHCP servers and to allow Bootp relay agents to forward DHCP Bootrequest/Bootreply packets. The Bootp relay agent handles DHCP Bootrequest and Bootreply packets in the same way it handles Bootp Bootrequest and Bootreply packets. The Bootp relay agent in HP routers has been tested and certified to forward DHCP Bootrequest/Bootreply packets correctly. The relay agent is configured for DHCP in the same way as it is configured for Bootp.

Bootrequest/BootreplyPacket Format

The Bootrequest and the Bootreply packets have the same format and consist of the following fields:

1. ***op*** [1 octet] Opcode: 1=Bootrequest and 2=Bootreply.
2. ***htyp*** [1 octet] Hardware type: specifies media type (for example, 1=Ethernet) and is the same value as the ARP hardware type.
3. ***hlen*** [1 octet] Hardware address length: specifies the length of the hardware address.
4. ***hops*** [1 octet] Set to zero by the client, incremented by each router that the packet crosses. Routers should drop the packet if the hop count exceeds 16.
5. ***xid*** [4 octets] Transaction ID: set to a random number by the client and used to identify the reply.
6. ***secs*** [2 octets] Number of seconds: set by the client in retransmitted Bootrequests to the number of seconds since the first Bootrequest was transmitted.
7. ***flags*** [2 Octets] Bit 0 (MSB) of this field is the broadcast flag. Set by the client if the Bootp server should broadcast its reply.
8. ***ciaddr*** [4 octets] Client IP address: set by the client to its IP address only if it is known at the time the Bootrequest packet is formatted. Otherwise it is set by the client in most implementations to 0.0.0.0.
9. ***yiaddr*** [4 octets] Your IP address: If the Client IP Address field was set to 0.0.0.0 by the client, this field is set by the server to be the IP address of the client.
10. ***siaddr*** [4 octets] Server IP address: set by the server to the IP address of the download server.
11. ***giaddr*** [4 octets] Gateway IP address: set by the first gateway or relay agent to be the IP address of the interface on which the Bootrequest packet was received.
12. ***chaddr*** [16 octets] Client hardware address: set by the client to its station address (hardware address, MAC address).station address
13. ***sname*** [64 octets] Server name: optional server host name; null terminated string.
14. ***file*** [128 octets] Fully qualified directory path boot or config file name; null terminated string.
15. ***vend*** [64 octets] Vendor extensions field: vendor specific field, discussed in RFC 1533.

Appendix B

Case Study: Multi-Vendor Router Networks—Nestec S.A.

Raymond Papaux
Network Consultant
Professional Services Organization
Hewlett-Packard Company (SUISSE) S.A.

Company Overview

Nestec S.A. is a research and administration company providing services for the Nestle group. They are structured in an administration headquarters based in Vevey, Switzerland (hereafter HQ), a generic research center (hereafter CRN) dedicated to fundamental research based in Lausanne, Switzerland, and diverse product specific research sites (hereafter RECOs) in Switzerland and all over the world.

A few years ago, the RECOs and the CRN decided to unify their environment and to start electronic communication within their community. They selected the HP 3000 platform and are using HP's network services and HP DeskManager to provide peer-to-peer communication over X.25 networks. The RECOs and the CRN were also installing and rapidly deploying Ethernet PC LANs built upon Microsoft LAN Manager and TCP/IP.

The Nestle corporation also selected Infonet as the global carrier to provide the basic infrastructure to link all the sites together, on a worldwide basis. Thus, the RECOs and the CRN used X.25 technology for backbone access with HP Model 45 concentrators where appropriate. The HP 3000 provided the gateway functions between the LAN and the WAN.

The HQ is using an IBM mainframe with SNA and Token Ring networks and a host-based E-mail system. It also has directly dependent remote sites spread across the country and internationally. Years ago HQ started the deployment of a Novell network with centralized and decentralized PC servers.

The heterogeneous E-mail systems talk together using an IBM host centralized gateway, located in the USA and managed by Infonet. This gateway links all messaging technologies through a software package from Softswitch, Inc.

Due to the Nestle company structure, all Nestec S.A. entities are autonomous in terms of management and supplier choice, following the corporate guidelines and recommendations.

Business Need

Recent decisions in the company, such as centralization of applications, brought up the need for strengthening the inter-site communication, especially in Switzerland. The Swiss RECOs were asked to interactively access applications residing on the HQ mainframe, and the business required information access to any server in the country.

Furthermore, Nestec S.A. wanted to exchange information with universities and other research companies, and to access data on public servers. Thus, global access to the Internet was another requirement.

Therefore, the above-mentioned needs dictated building an extended LAN, linking all the sites for peer-to-peer connectivity in a multi-protocol environment.

Heterogenous Environments

The HQ had started interconnecting local and remote rings using Wellfleet Communications Inc. routers.

The RECOs and CRN have historically been pleased with HP as an information technology and networking supplier, and as such selected Hewlett-Packard routers to minimize vendors, risks, and support costs.

The third player is a country-based service provider company, called Switch, which supplies commercial and educational Internet access. Switch also provides X.400-to-SMTP (RFC-822) address translation gateway service. As with much of the Internet infrastructure, Switch has built its network using Cisco System Inc. routers.

The above comments and descriptions are meant to help the reader understand the origin and purpose of these three router technologies which caused the multi-vendor data transport network to be a reality at Nestec S.A today.

Network Requirements and Design Criteria

Differences in data flow, traffic volume, and protocols did not allow a straightforward design. Hence, the emphasis was on security, redundancy, and overall network cost optimization (leased lines, equipment, Infonet subscription, support, etc.).

The main data flows are summarized below by traffic groups.

Traffic Group A. Inter-Swiss RECOs (TCP/IP only)

- Interactive access to custom application modules.
- File transfer.
- Sporadic file server connection.
- Electronic mail (HP DeskManager).

Traffic Group B. Swiss RECOs—CRN (TCP/IP only)

- Interactive access to custom application modules.
- File transfer.
- Sporadic file server connection.
- Electronic mail (HP DeskManager).
- General IBM/host spool file distribution.

Traffic Group C. CRN—Headquarters

- Interactive access to custom application modules
- Interactive access to IBM common applications (using TN3270 protocol).
- File transfer with HP 3000, UNIX, and IBM system.
- Moderate connection on NetWare file server.
- IBM/host printer emulation (based on HP-SNA/IMF, IBM3270 emulation).
- IBM/host interactive traffic for non-LAN-based remote users.

Group C traffic requires that TCP/IP, SNA and IPX/SPX traffic be merged over the same line. This telecommun-ication line is further rationalized with TDM multiplexers by integrating router data with voice and X.25 channels.

Traffic group D. RECOs & CRN—Headquarters

- Interactive access to IBM common applications (using TN3270 protocol).
- File transfer with HP 3000, UNIX, and IBM systems.
- Moderate connection on NetWare file server.

Traffic Group E. Swiss RECOs & CRN—Infonet

Infonet access is primarily required for all international traffic. Therefore, X.25 connectivity must be kept for legacy environments such as PAD workgroups, traveling users, and other international RECOs. The extended LAN must therefore provide an entry and connection to the carrier.

Since the major part of the international traffic is electronic-mail batch transfer, a low-cost connection at 9600 bits per second was selected.

Note

Infonet E-mail traffic is divided into two parts:

- An HP DeskManager connection to the other international RECOs (this traffic directly affects the router network connectivity to Infonet)
- An HP DeskManager connection to SoftSwitch gateway traffic which uses SNA/NRJE emulation communication on the HP 3000 E-MAIL gateway machine (ARCOM/X.400, Infonet, and Internet mail).

The resulting SNA traffic is later converted to X.25/QLLC into a HP Model 45 concentrator. This concentrator provides connectivity to TELEPAC (the Swiss PSN X.25 network) for public access, PAD users, and X.400 services.

Interactive application maintenance is also done through Infonet.

Traffic Group F. Swiss RECOs, CRN, and HQ—Internet

This group of traffic covers all the sporadic Internet access by the entire Swiss Nestec S.A. organization.

Design Criteria

One should note here that the scope of this paper is to concentrate on the HP network design part, which covers all the traffic groups described above, along with interconnectivity to other technologies.

The network design criteria were derived with the following objectives in mind:

- Avoid points of failure which would penalize all traffic types.
- Homogenize the type of routers (HP AdvanceStack family).
- Minimize purchase and maintenance costs.
- Optimize interactive performance manageability, security, and redundancy.

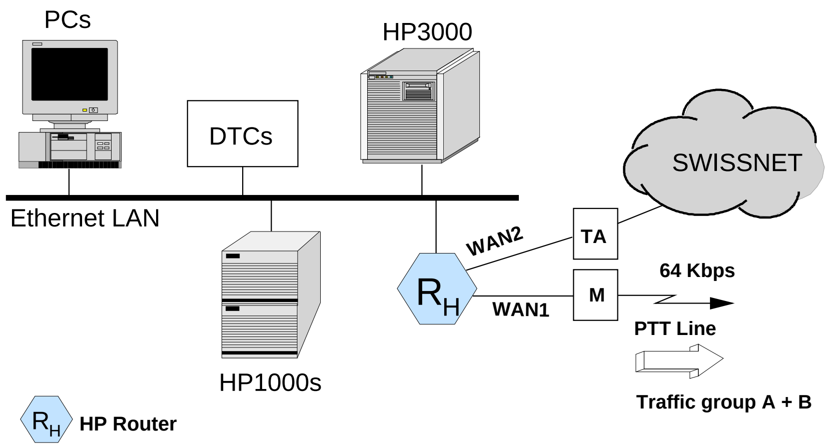
We standardized on the HP Router SR only, with the exception of the HQ which required a HP Router BR for FDDI backbone access. All HP routers are running software version A.07.02.

Network Topology

This paper is not meant to provide all the details of the network, since exhaustive design parameters would produce a document outside the scope of a case study. However, we have concentrated on the driving rationales and other main areas of interest.

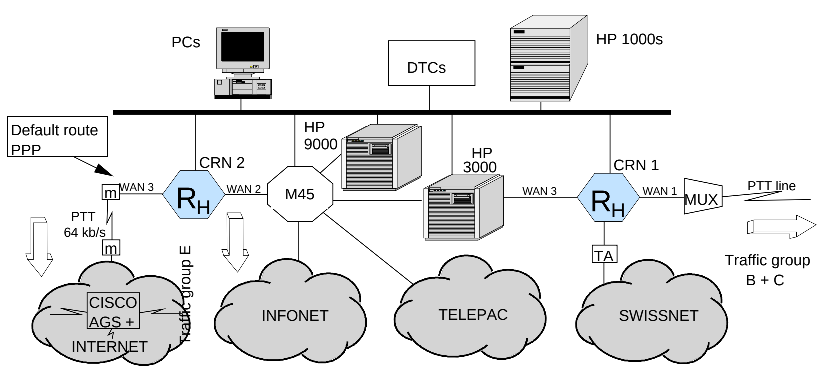
The overall topology is made of point-to-point 64 Kbits-per-second leased lines going from the Swiss RECOs and the CRN toward the HQ in Vevey. This topology design was mainly dictated by traffic group C & D traffic requirements, which are the most sensitive in terms of delay.

Typical RECO Router Design Principles. This part is common and reproducible for most RECOs. It features an HP 3000, a PC LAN, and DTCs on a single Ethernet segment connected to the extended LAN. The port WAN1 of the unique router is linked on the PTT telecommunication line for traffic group A transfer, while the WAN2 port is connected on SWISSNET (Swiss ISDN network) with a V.25 bis dial-up terminal adapter. This link provides a redundant path to HQ for the partial traffic group D, which is mission critical. It is automatically activated by the router when the main telecommunications circuit fails. It is configured as an alternate path for TCP/IP and uses static route configuration, while the main circuits rely on OSPF (discussed later) for getting routing table updates. It is worth mentioning that one should assign a lower preference to static route, so that it is not activated permanently. Figure 1 depicts this basic design.



Case Study Figure 1. Typical Swiss RECO

CRN Router Design Principles. As mentioned earlier, the CRN has more requirements for traffic types, and therefore needs to support more protocols. For cost and convenience reasons, it is also the site chosen for providing the gateway to Infonet and Internet. Therefore, keeping the design criteria in mind, we assigned one router (CRN1 in figure 2) responsible for traffic groups B, C, and part of D, and another (CRN2) to be responsible for traffic groups E and F.



Case Study Figure 2. Research Center (CRN) Network Design

CRN1 basically has the same function as provided for the RECOs, with the exception of SNA encapsulation (synchronous pass-through) capability on WAN3, required for SNA/LU3 printer emulation on an HP 3000. However, in this case the ISDN circuit is configured as a back-up circuit group for providing all redundant services.

Internet and Infonet Access. CRN2 functions as the gateway to the international and outside world. It is not mission-critical in terms of availability. However, special attention is given to it due to the security issues of public network connectivity.

The CRN2 router talks to the Internet gateway router (Cisco System Inc. AGS+/4, OS version 9.1-7) using the PPP protocol configured on the WAN3 port. A default route has been set up for sending all unknown IP Nestec S.A. addresses over this link. As security is a very hot issue while accessing the Internet, an open secured system acting as a firewall has been implemented. It works in conjunction with a filter on CRN2 which lets only a very few well known IP and PORT addresses come in.

Table 1: Protocol Traffic on HQ Routers

Router	Protocols
HQ	IP, IPX
HQ1	IP, IPX, SNA/SPT, ISDN (back-up link)
HQ2	IP, IPX
HQ3	IP, ISDN (alternate back-up route)

On its WAN1 port, CRN2 also talks X.25 to Infonet through an HP Model 45 switch, which concentrates the TELEPAC and Infonet accesses and performs SNA protocol conversion (SDLC X.25/QLLC) for the HP 3000 mail gateway mentioned earlier. Since the remote nodes are mainly HP 3000 MPE/iX systems (European and US RECOs), CRN2 uses RFC-877 IP encapsulation and static routes.

HQ Router Design Principles. This is a great area of interest. It features the logical link between the Wellfleet Communications Inc. and HP router network technologies. The physical link, as shown in figure 3, is made of a dual FDDI ring which is in fact a collapsed backbone (and the OSPF logical backbone), onto which the Wellfleet Communications Inc. Backbone Concentrator Node (OS version 7.71), major NetWare servers, IBM host, and other networking equipment are connected. Again, the design rationale here was security and redundancy. The FDDI backbone also establishes the administration boundary in terms of network operation and responsibilities.

Again, in this case this router configuration responds to the same design criteria and rationale discussed earlier. Protocol traffic is shown by router in table 1.

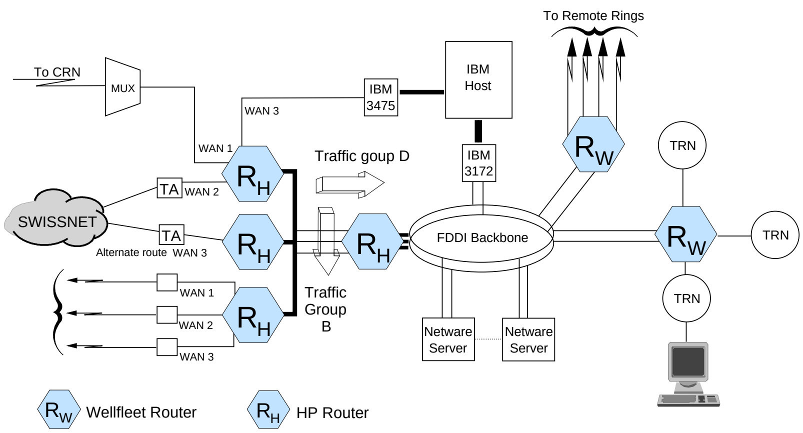
OSPF Areas

We finish this paper with a discussion of routing protocols.

Some “facts of life” led us to choose OSPF. Those criteria are reflected below:

The network is a true heterogeneous multi-vendor transport network, and thus requires a standard routing protocol.

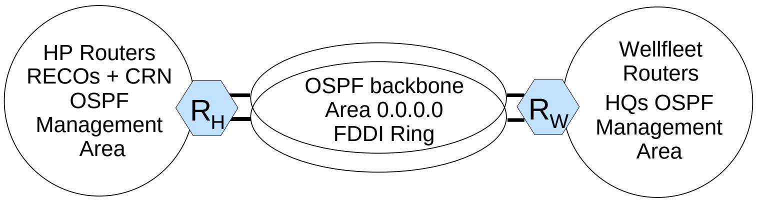
Even though the network is a single autonomous system using a Class B network address, for organizational reasons mentioned earlier, the network is logically divided in two independently manageable areas, for which the boundary is the FDDI ring in HQ (see figure 3).



Case Study Figure 3. HQ Network Design

Due to different LAN topology and history, the Class B address has been subdivided to accommodate different subnet sizes and thus must support a variable subnet mask (the design of the extended LAN network further complicates the situation by introducing a third small point-to-point subnet mask for IP address saving).

Figure 4 shows the autonomous system with the two distinct management areas and the OSPF backbone.



Case Study Figure 4. OSPF Area/Management Boundaries

Any network growth or change in any administered areas can be done independently of each other, assuming that a few basic rules, such as naming and addressing, and OSPF conventions are observed.

Thus, the introduction of OSPF helped us to solve the above issues, and brought us several nice goodies, some of them being fast network reconfiguration and better control of the meshed implementation with alternate redundant links.

Conclusion

Multi-vendor wide-area transport networks are a reality today.

Any conscientious network manager would avoid, for good and pertinent reasons, mixing and matching vendors and technologies when building a brand-new network. However, other factors may force a manager to use different box manufacturers, and allow them to interoperate. Among those factors, buzz words such as “consolidation”, “acquisition”, or simply “functionality” or “economy”, might be good catalysts for this process.

Index

I

K

L

M

N

O

P

Q

R

S

X

Y