Perle P840

Bridge / Router

USER AND SYSTEM
ADMINISTRATION GUIDE

Part number 5500083-15

Federal Communications Commission (FCC)

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Warning: The user is cautioned that modifications to this equipment can void the authority granted by the FCC to operate the equipment.

1.This equipment complies with Part 68 of the FCC rules. On the bottom of this equipment is a label that contains, among other information, the FCC registration number and ringer eqivalence number (REN) for this equipment. If requested, this information must be provided to the telephone company.

2. Applicable USOC jack required: RJ49C

3. If the terminal equipment P840 causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it to be necessary.

4. The telephone company may make changes to its facilities, equipment, pertains or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make the necessary modifications in order to maintain uninterrupted service.

5. The following repairs may be made by the customer: none.

Canadian Emissions Standard ICES-003

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus as set out in the interference-causing equipment standard entitled "Digital Apparatus", ICES-003 of the Department of Communications.

Cet appareil numérique respecte les limites de bruits radioélectriques applicables aux appareils numériques de Classe A prescrites dans la norme sur le matériel brouilleur: "Appareils Numériques", NMB-003 édictée par le ministre des Communications.

Canadian ISDN Approval

The ISDN-S/T interface of this device is intended for direct connection to the S/T jack of an NT-1 unit and therefore does not require Communications Canada certification. The P840 should only be connected to Communications Canada approved NT-1 units.

Statements for ISDN U Module

NOTICE: The Canadian Department of Communications label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operational and safety requirements. The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunication company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alteration made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

CAUTION: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

Using This Manual

This Installation and Applications Guide provides the basic information required to initially set up and configure the P840 router. This guide is organized into the following sections:

"***Installation***" provides instructions for installing the P840.

"***Typical Applications & How to Configure Them***" provides simple configuration examples for typical applications in which the P840 might be used. The applications described in this document are for example only and provide a method of quick configuration of the P840. For more complete information on all of the configuration parameters available, please refer to the P840 PPP Menu Reference Manual on the accompanying CD-ROM.

"***Introduction to Filtering***" provides an introduction to the pattern filtering options of the P840. Several examples of typical pattern filters are also provided.

"***Menu Trees***" provides a graphical tree type overview of the structure of the built-in menu system of the P840. All of the configuration is performed using the options provided in the menu system. The Menu Tree is like an index to the menu options.

"***Configuration Pages***" provides a place to note the current configuration of the P840 for future reference. If a replacement unit is required, the configuration may be quickly modified to be the same as the existing unit.

"***Octet Locations on Ethernet Frames***" provides a graphical representation of the various common Ethernet frames that the P840 will bridge or route. When defining a pattern filter, these frame displays indicate the offset values to use in order to define the pattern filter correctly.

"***Servicing Information***" provides information on opening the case and changing the straps.

Using the Electronic Reference Manual

The P840 Reference Manuals are provided as Adobe Acrobat PDF files on the accompanying CD-ROM. The Menu Reference File is provided individually for ease of configuration reference. The Adobe Acrobat Reader is included on the CD-ROM.

The Adobe Acrobat Reader program is also available for most computer operating platforms from Adobe on the Internet at: www.adobe.com.

The Reference Manual provides the following information:

Introduction to bridging, routing, and P840 features

Pin out references for the link modules

Pin out references for the link modules

List of event and alarm logs

Expanded description of programmable filtering

The P840 PPP Menu Reference Manual provides the following information:

Complete description of the options for the built-in menu system.

Contents

SECTION 1
INSTALLATION

The P840 is an ISDN Ethernet Bridge/Router that provides bridging, IP/IPX routing, and compression over a PPP ISDN connection and support an ISDN BRI interface via an integral ISDN-ST or ISDN-U link module. The ISDN BRI interface supports two 64 Kbps B-channels. Two analog telephone connections are also available when the voice port module is included on a unit with voice support.

The following instructions provide a quick set-up guide for installation of the P840 Router:

Unpack the P840 Router

Rough handling during shipment can damage electronic equipment. As you unpack the bridge/router, carefully check for signs of damage. If damage is suspected, contact the shipper. Save the box and all packing material to protect the bridge/router should it ever need to be moved or returned for service.

Check the packing slip that identifies the components and the LAN connector. The connectors on the rear of the bridge/router provide all external connections to the P840 Router.

Select a Site

Place the bridge/router in a well-ventilated area. The site should maintain normal office temperature and humidity levels. Air vents located on the rear of the bridge/router must have an inch or so of clearance from any object.

Identify the Connectors

Each unit is configured with both straight (MDI) and crossed over (MDI-X) 10BaseT LAN connectors; the P840 will auto-sense between the two. Only one connector may be used at a time.

The RJ-45 ISDN connector has its ISDN interface module factory configured to either ISDN-U or ISDN-ST.

The PHONE connectors are used to connect to regular analog phone devices (phones, fax machines, modems, etc.). The PHONE connectors require the presence of the optional internal voice module.

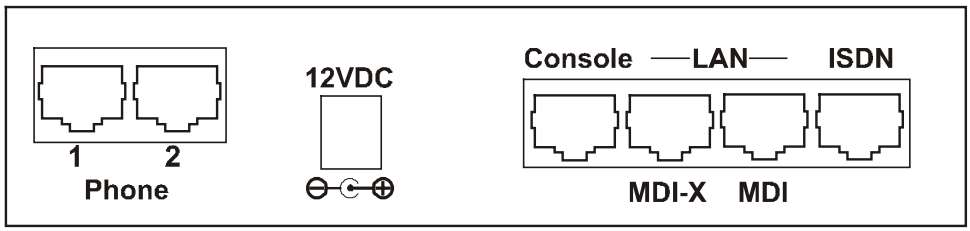


Figure 1-1 Rear View of the P840 Router

Configuring the Router

The P840 configuration may be set up either through the NetWizard Graphical User Interface or through the built in Menus system.

The NetWizard runs on one of the LAN computers. It is designed to lead the user through the basic configurations required to get the Router running.

The menu system operates through a console connection and allows access to all configuration settings available on the Router.

Connect to the Console

Connection to the bridge/router operator's console is made through the RJ-45 connector labeled CONSOLE on the back of the bridge/router. A RJ-45 cable and RJ-45 to DB9 (female) converter are provided for connection to a DB9 (male) connector.

Connect the console port of the P840 Router to a computer running an asynchronous communication package or a standard asynchronous terminal. The bridge/router supports autobaud rates at 1200, 2400, 9600

or 19,200 bps. The bridge/router is managed through the use of "hotkey" Menus.

Appendix D provides the pinout information for the console connector and the DB9 to RJ45 converter.

Make the LAN Connections

Connect the P840 Router to the LAN with the available LAN interface cable.

The Router may be connected directly to a wiring hub or Ethernet switch by using the MDI LAN port and a standard 10BaseT cable.

The Router may be connected directly to a computer network card by using the MDI-X LAN port and a standard 10BaseT cable.

Make the ISDN Link Connection

The ISDN-ST interface of the Router Bridge/Router provides a RJ-45 connector to connect to the RJ-45 connector of the NT1 provided with your ISDN service.

The ISDN-U interface of the Router Bridge/Router provides an integrated NT1 with a RJ-45 connector to connect directly with your ISDN service.

Once the bridge/router has established communications with its partner across the WAN, the "Link" LED(s) will turn green.

Note: Bridge/Router database changes and statistics viewing may be done remotely by establishing Telnet connections to a partner bridge/router across the WAN. This is accomplished by selecting the "Connect" option. The "Connect" option is found under the Telnet Access Menu.

Power Up the Router

Once the LAN and Link connections are made and the console is connected to a terminal, you are ready to power-up the P840 Router. Connect the DC power cord from the supplied power supply to the back of the P840 Router and plug the power supply into the AC wall outlet.

Observe the LEDs as the bridge/router powers up. The LEDs will go through a flashing pattern as the power-up diagnostics are performed. After the power-up diagnostics are finished, the Power LED will go from red to green.

Enter at least one <RETURN> (up to three if necessary) in order for the router to determine the baud rate of the terminal used for the console (i.e., autobaud). The following information will now be seen on the console connected to the router :

```
Terminals supported:
  ansi, avt, ibm3101, qvt109, qvt102, qvt119, tvi925,
  tvi950, vt52, vt100, wyse-50, wyse-vp, teletype
Enter terminal type:
```

Select the terminal type being used if listed and enter its name (in lower case) at the prompt, or choose the terminal type **teletype** if your terminal is not listed. This terminal type operates in scroll mode and may be used successfully until a custom terminal definition is created.

Login and Enter the Required Configuration

At the login screen type a 1 and the default password to enter the menu system of the P840 Router. The default password is "**BRIDGE**" (case sensitive) and should be changed if security is desired.

With the options of the built-in menu system, the Router may be configured to operate within your environment.

Refer to the P840 PPP Menu Reference Manual file for your operating software on the accompanying CD-ROM for a complete description of all the Menu Options.

Mandatory Configuration

The P840 requires a minimum amount of mandatory configuration in order to operate. The following table identifies the configuration parameters that must be defined for proper operation under the operational states shown in the table.

Mandatory Configuration		
Bridge	**IP Router**	**IPX Router**
None	**IP Address**	none
	IP Routing	
	IP Forwarding	
PPP ISDN		
ISDN Switch Type		
Directory Numbers		
Remote Site Profile		

The configuration options required for proper initial operation are described in Section 2: Typical Applications and How to Configure Them.

Refer to Section 2 for details on configuring the P840. Also refer to the P840 PPP Menu Reference Manual file on the accompanying CD-ROM for a complete description of all the Menu Options.

Other options may be changed depending on specific installation configurations. Refer to the menu tree in Appendix A for a reference of the menu structure and options.

Identify the Status LEDs

The meanings of the four 3-color Light Emitting Diodes (LEDs) on the front of the Router are found in the following chart.

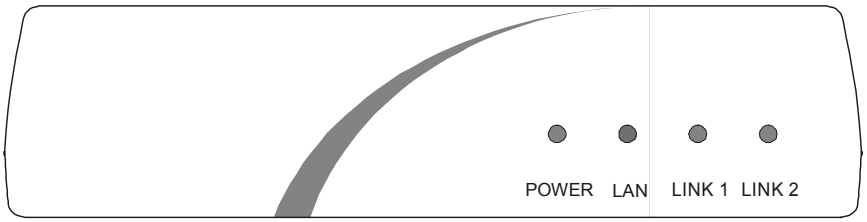


Figure 1-2 Front View of the P840 Router

Green	Bridge/Router is running and has passed power-up diagnostics
Green (flashing)	Bridge/Router is in BOOT mode and is programming the flash
Red	Bridge/Router is powered up but has failed power-up diagnostics
Yellow	Bridge/Router is decompressing the software into the RAM
Yellow (flashing)	Bridge/Router is in BOOT mode
Power	● ○ ○ ○

Green	LAN is connected and forwarding
Red	Bridge/Router is NOT connected to the LAN
Yellow	LAN is connected and NOT forwarding: i.e. Listening, Learning, or Blocking
LAN	○ ● ○ ○

Off	LINK is idle
Green	LINK is up with a data connection
Green (flashing)	Voice call is up
Yellow	LINK is negotiating connection: line answered
Yellow (flashing)	Voice call off hook with dial tone or on hook incoming call ringing
Red	Software failure
LINK 1	○ ○ ● ○

Off	LINK is Disabled or ISDN call is down
Green	LINK is up with a data connection
Green (flashing)	Voice call is up
Yellow	LINK is negotiating connection: line answered
Yellow (flashing)	Voice call off hook with dial tone or on hook incoming call ringing
Red	Software failure
LINK 2	○ ○ ○ ●

The NetWizard Graphical User Interface

The NetWizard router setup assistant comes on the CD-ROM packaged with this router.

The NetWizard is a standalone Java applet that communicates with the Router through the LAN connection.

The NetWizard will run on computer operating systems with Java support. It has been tested on the following platforms: Windows 95, 98 and NT, Mac OS 8, UNIX, and Linux. The minimum recommended PC system is a Pentium 100 MHz CPU, 32 MB of memory and a 256 color VGA monitor; the minimum recommended Macintosh system is a G3.

The network connections and power cord should be properly attached to the router and the router powered up.

Software Installation:

Put the CD in the CD-ROM drive. For systems that support autoplay (Windows 95/98/NT) the CD Introduction page will automatically come up on your browser. For all other systems, use the Internet browser of your choice to open the INDEX.HTM file in the root directory of the CD-ROM. Click on the ***NetWizard Installation*** icon to start the NetWizard installation. A page listing the installer operating platforms available will appear, Choose the installer for your operating system (the "Recommended installer" display bar will show which installation is recommended for your system). Download the Installer to your machine. After the download is complete, go to the location where "install" was saved and start the program (click on the "view instructions" link in the browser to get specific tips on steps required for your operating system).

The ***Install Anywhere*** setup window will appear; select the language you wish to use for the NetWizard, then click on OK and follow the installation steps.

When the NetWizard program is started, the first window that appears is the Launchpad application. This is a small program that searches the local network for any Routers and displays a listing of those found. Select the

one you wish to configure and proceed by clicking on the NetWizard button.

Follow the steps on the NetWizard through the configuration of the router.

Configuration Note:

If the NetWizard is to be installed on a WindowsNT system, the user must log in as "Administrator".

If the NetWizard is to be installed on a Linux system, the user must log in as "root" or an account with superuser privileges.

Note:

If you accidently set the Router to have an incorrect IP address, the NetWizard may not be able to find the Router again. If this occurs, you will have to use the console menu system to reset the router. Please see page 1.2 for how to connect the console and page 2.2 on using the menus.

After logging onto the console, select option ***3 Diagnostics*** from the Main menu, then option ***2 Full Reset*** to clear all settings on the router to their default values.

You may then resume using the NetWizard to set up the router.

SECTION 2
TYPICAL APPLICATIONS & HOW TO CONFIGURE THEM

The P840 is a flexible Ethernet Bridge/Router that supports PPP ISDN circuits. This section will describe how to set up the P840 networking functions.

The P840 may be configured as a simple Ethernet bridge, an Ethernet IP router, an Ethernet IPX router, or a combination of the three. When operating the P840 as a combination bridge/router simply configure each of the components separately.

Note: *The configuration options described within this section are only for initial set up and configuration purposes. For more complete information on all of the configuration parameters available, please refer to the P840 PPP Menus Reference Manual PDF file on the accompanying CD-ROM*

Important: The P840 uses FLASH memory to store the configuration information. Configuration settings are stored to FLASH memory after there has been 30 seconds of idle time. Idle time is when there is no selection or modification of the value in the built-in menu system. If you wish to store a configuration immediately, enter "=" to jump to the main menu, then select option "6" to save the configuration.

Managing the P840
Using the Menus

This section describes the minimum configuration parameters required when setting up the P840. Each of the configuration scenarios requires setting of operational parameters on the P840. The built-in menu system of the P840 is used to configure the unit.

The Router menu system operates on a "hotkey" principle; navigating around the menu system is done by typing the number associated with the desired option; the P840 acts on the choice immediately (no need to hit the "enter" key).

The menu system consists of different menu levels each containing new configuration options. Navigation back out of a nested menu is easily accomplished by pressing the "tab" key. The tab key takes you to the previous menu level. If you wish to move from your current menu location directly to the main menu simply press the equals "=" key.

When choosing menu options that will toggle between values, simply pressing the number associated with that option will cause the options value to change. Each successive selection of the option will cause the option's value to change again.

Some menu options require input from the operator. When selecting an option that requires a value, the menu system will display the range of values acceptable and a prompt symbol ">". Enter the new value at the prompt symbol and press enter. Should you make an error in entering the new value, the <BACKSPACE> key (for most terminals) deletes the most recently entered characters.

Conventions

Throughout this section, P840 menu options are shown that are required for the various configuration choices. The appropriate menu options are shown in each instance in the following format:

Configuration Option Name

Location: Main

↳ Sub-Menu Name

↳ Sub-Menu Name

↳ *Option Name*

The configuration option is shown as well as the options location within the menu system. The ↳ character indicates that a sub-menu level must be chosen. The option name in which a configuration parameter is to be set is shown in italics.

The keyboard graphic in the left margin indicates that this is information that the user will have to enter for configuration.

The note icon is used to indicate information on configuration and set up of the Router.

Configuration Note: *The Configuration Note is used to indicate that there may be a difference in configuration between the various operational modes of the Router.*

The information icon is used to indicate that more information is available on this subject. The information is usually located within another document as specified.

Bridging and Routing

Should You Bridge or Route?

When connecting two Local Area Networks together, the first question to ask is should I bridge or route? The decision to bridge or to route may be decided by how the existing networks have been already set up.

Bridging should be used when the network consists of non-routable protocols or routable protocols using the same network numbers. Some protocols can only be bridged; some of the more well known are NetBEUI (used by Microsoft Windows 3.11, Windows '95, Windows '98, and Windows NT), and LAT (used by Digital Equipment Corp.).

If your IPX or IP network address is the same at both locations, bridging is simpler and requires less configuration. If the locations are to be routed together, the network numbers will have to be different in both cases, this could require extensive reconfiguration.

IPX routing should be used if the two locations are already set up with different IPX network numbers. Routing IPX will minimize the number of SAP and RIP messages being sent across the WAN.

IP routing should be used if the two locations are already set up with different IP network numbers or if you wish to divide your one IP network number into two sub-networks.

In some cases both bridging and routing may be required. Routing may be required for IP information and bridging may be required for NetBEUI.

Bridging

An Ethernet bridge intelligently forwards LAN traffic to remotely connected LANs across the Wide Area Network (WAN).

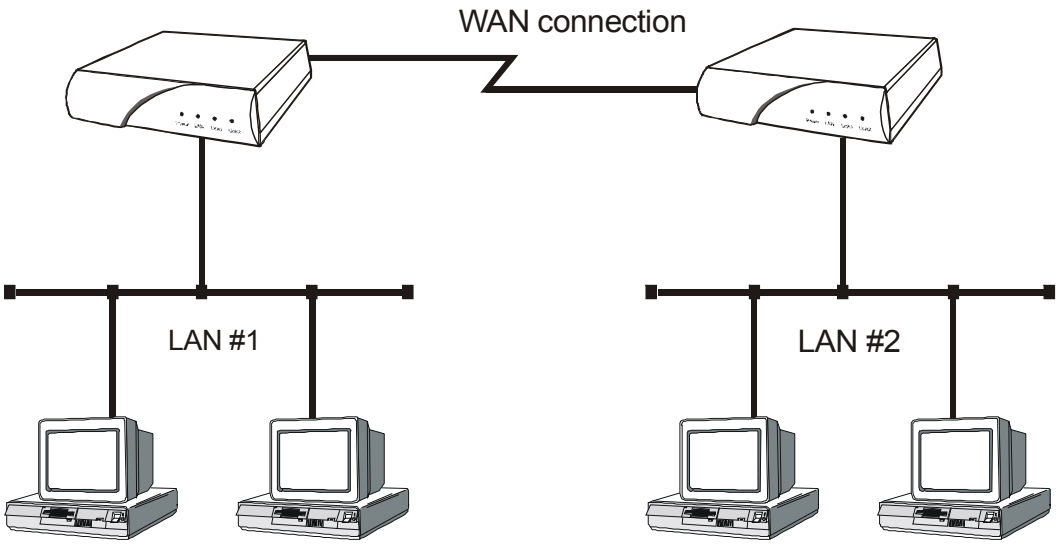


Figure 2-1 Bridged Local Area Networks

Ethernet bridges simply forward information based on Ethernet MAC addresses. If a LAN packet is destined for a device located on a remote LAN, the bridge will forward that packet to the remote LAN. If a LAN packet is destined for a device located on the local LAN, the bridge will ignore the packet.

Ethernet bridges also communicate to each other using what is called the Spanning Tree Protocol (STP). STP is used to prevent loops in a network which cause LAN traffic to be re-broadcast again and again causing network congestion.

The P840 is pre-configured to operate as an Ethernet bridge compatible with the IEEE 802.1d Spanning Tree Protocol definitions. This means that without configuration modifications, the P840 will bridge Ethernet traffic to its partner bridges when the Wide Area Network (WAN) connection has been established (see section 1, page 3 for WAN connection set-up).

The P840 also is pre-configured as an IPX router. This means that if you wish to bridge IPX traffic instead of routing it, you must disable the IPX routing function of the P840. Once IPX routing has been disabled, all IPX traffic will be bridged between partner bridges on the WAN.

To set up a bridge between two LANs:

- Connect each Router to the LAN it will be serving
- Connect the WAN interface of each Router to the equipment supplied by the service provider
- Configure the remote site profile of the partner router if necessary (see section C)
- Establish the WAN connection

IP Routing

An Ethernet IP router is used to intelligently route Internet Protocol (IP) LAN traffic to remotely connected LANs across the WAN.

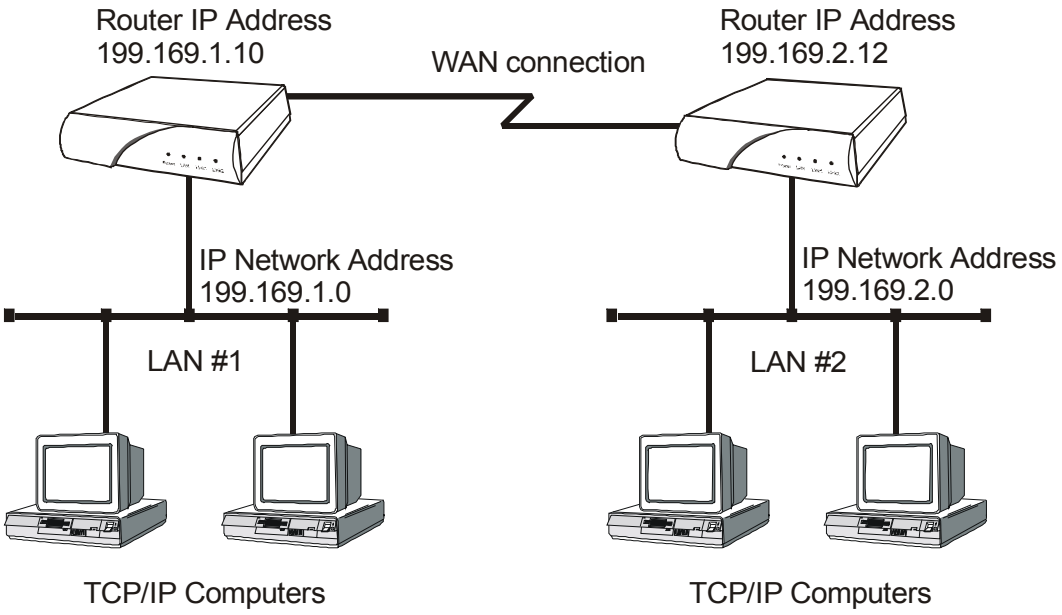


Figure 2-2 IP Routed Local Area Networks

IP routers forward IP frames based upon their IP destination address and an internal routing table. The router maintains the internal routing table with the remote network IP addresses and the remote partner IP routers associated with those networks. When an IP frame is received from the local LAN, the destination IP address is examined and looked up in the routing table. If destination IP network is found in the routing tables, the IP router sends the IP frame to the remote partner Router that is connected to the appropriate remote IP network. If no explicit route entry is found in the routing table, the IP frame is sent to the Default Gateway.

IP Addressing

Devices on an IP network are located by their IP addresses, which is a 32 bit number divided into four 8 bit fields. The IP address identifies both the network and the host device (also known as a node) on that network. The address is usually written as the four decimal values for the fields (between 0 and 255) separated by decimal points; for example 196.65.43.21.

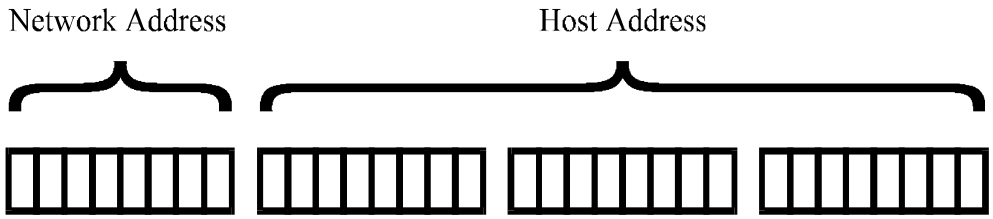
The high order field defines the IP class of the address. There are three commonly used classes of IP address:

A: 1 to 127

B: 128 to 191

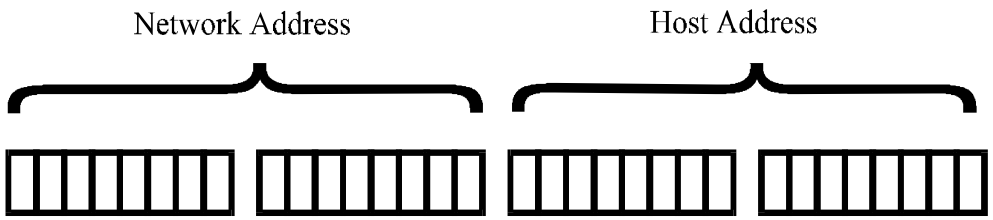
C: 192 to 223

For class A addresses, only the first 7 bits of the high order field represents the network address, so there can be 127 networks. The remaining three fields are the host portion of the address there can be over 16 million (2^{24}) host devices on each class A network.



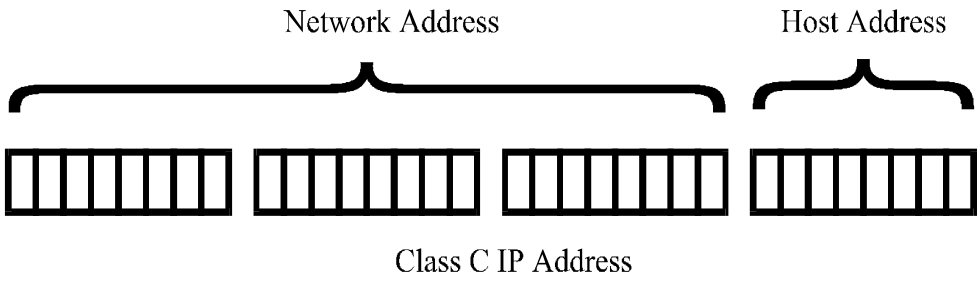
Class A IP Address

Class B uses the first two fields for network addresses and can address approximately 16,000 networks. The two low order fields allow approximately 65,000 host addresses (2^{16}) for each network.



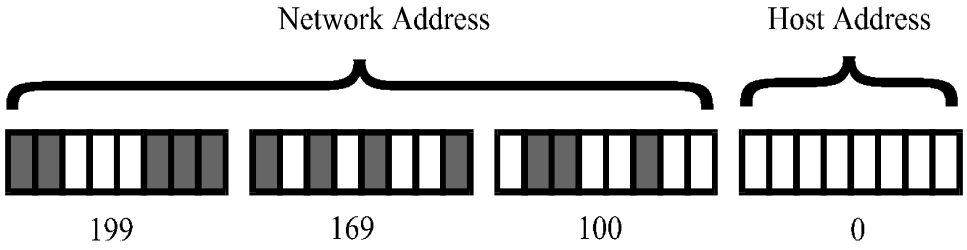
Class B IP Address

Class C Uses three high order fields to address over 2 million networks, the low order field is used to address up to 254 hosts.



IP addresses within a private network may be assigned arbitrarily, however, if that network is to interconnect with the global Internet, it is necessary to obtain a registered IP address.

For example, a small company is connected to the Internet; they are assigned a single class C IP network address (199.169.100.0). This network address allows the company to define up to 255 host addresses within their network.



Masks

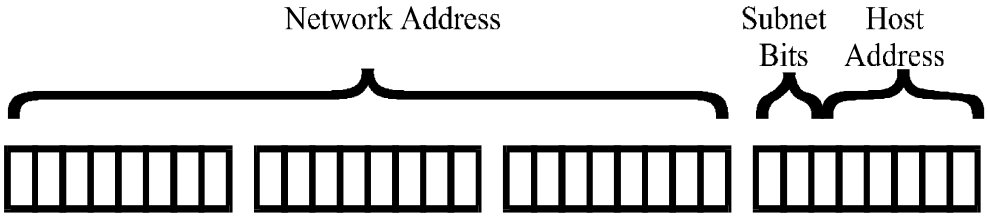
The portion of the IP address to use as the network address is specified by using a mask; a mask is the contiguous number of bits to be used for the network address all set to 1. When the mask is logically ANDed with an IP address, the result is the network address. The mask is specified by entering the mask size as the number of bits in the mask. For the standard Class A, B and C Internet addresses, the mask sizes would be 8, 16 and 24 respectively.

Networks are not restricted to the above standard sizes; the mask (and hence the network address it specifies) may be any number of bits from 8 to 32. This gives much more flexibility to match the size of the two fields of the IP address to the number of networks and hosts to be serviced.

IP Subnets

An IP network may be divided into smaller networks by a process called sub-netting. A subnet is specified using some of the high order bits of the host field of the IP address for sub-network addressing. The portion of the IP address to be used as the subnet address is defined by using a subnet mask.

If the company in the example above (Class C IP address 199.169.100.0) decides to split their network into two LANs to reduce the load on their network, the original IP network address may be sub-netted into two or more smaller IP networks consisting of a smaller number of host addresses in LAN. This allows each of the sites to be a smaller IP network and to be routed together to allow inter-network communication.



Subnet Addressing

The subnet mask size is the number of bits in the subnet mask. In the above figure the subnet mask size would be 26 (24 bits for the class C network address and 2 subnet bits). The subnet size is the number of subnet bits - in the above figure, the subnet size would be 2. The subnet mask size for the above example networks will be 26 and the resulting mask is 255.255.255.192:

In this example, specifying a subnet mask size of 26 will produce a subnet size of 2 bits. Two bits gives 4 possible sub-network addresses from the original IP network address. Two of the resulting sub-networks will have either all zeros or all ones as the subnet address; under standard subnets, these addresses are reserved for network functions and hence are invalid addresses. So setting a subnet mask size of 26 will generate two sub-networks with up to 62 host addresses each (64 potential addresses minus

the all zero and all one addresses). The new IP sub-network addresses will be: 199.169.100.64 and 199.169.100.128.

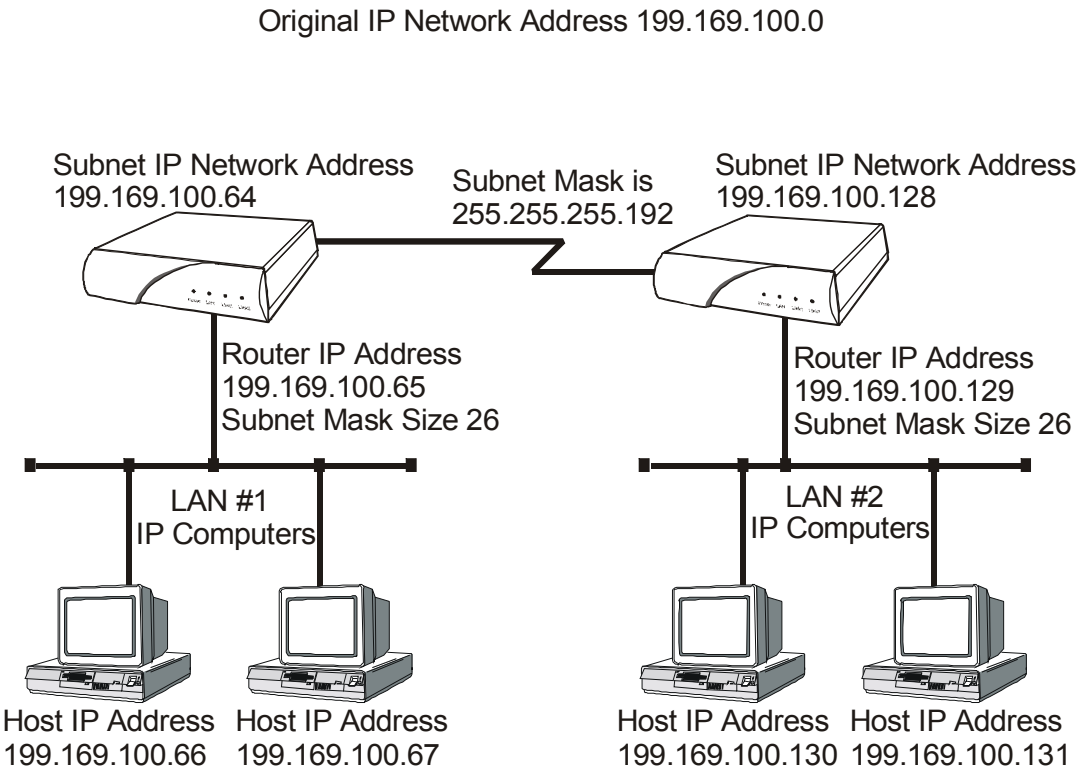


Figure 2-3 Defining an IP Subnet Mask

Devices on LAN#1 will have addresses from 199.169.100.65 to 199.169.100.126, devices on LAN#2 will have addresses from 199.169.100.129 to 199.169.100.254.

To configure the P840 to route between the newly created sub-networks, the following parameters must be defined on each router.

1. IP Address

Location: Main
- Configuration
  - LAN Set up
    - LAN IP Set up
      - *IP Address / Mask*
        199.169.100.64 / 26 for Route#1
        199.169.100.128 / 26 for Route#2

IP Default Gateway

An IP default gateway is an IP router that is resident on the local IP network that this Router is connected to and is used to route IP frames for destination networks that do not exist in the routing table. When an IP frame is received that is destined for a network that is not listed in the routing table of the Router, the Router will send the IP frame to the default gateway. If the device originating the IP frame is on the same LAN as the Router, the Router will then send an ICMP redirect message to the originating device. Any future IP frames for that destination network will then be sent directly to the default gateway instead of the Router.

A default gateway may be configured if there are a large number of routes that will pass through another router to a larger network. An example of this would be a router that is used to connect to the Internet. All of the routers on the LAN would have the Internet access router as the default gateway.

IP Static Route

With its default settings, the P840 will automatically learn the routes to other devices on the network through RIP messages. In some instances it may be desirable to have a predetermined or static route that will always be used to reach certain devices, such as when one specific router is to be used to reach a remote site network. The static route will have precedence over all learned RIP routes even if the cost of the RIP learned routes is lower.

Edit Static Route

Location: Main
- Configuration
  - IP Routing Set up
    - IP Routes
      - Edit Route
        - *Route IP Address*
        - *Next Hop*
        - *Cost*
        - *Add*

Each static IP route is defined in the Edit Route menu. The destination network IP address is specified when you first

enter the menu and then the IP address of the next hop route and the cost may be defined.

Once static IP routes are defined, they may be viewed with the *Show Static Routes* command from the IP Routes menu.

Configuration Note: *When the IP routing protocol is set to none, static routes will be used to route traffic. The subnet mask size must also be defined when creating a static route entry. The subnet mask is required to allow a static route to be created to a different IP network address. See the previous section for an explanation of subnet masks.*

IPX Routing

The P840 is pre-configured to operate as an IPX router when installed in an IPX network. The Router will learn the IPX network numbers from the local LAN and when the WAN connections are established, the Router will route the IPX frames to the appropriate destination IPX network.

The IPX routing scenario may consist of one of the two following configurations. The first configuration consists of Novell servers located on each of the LAN segments to be connected. The second configuration consists of Novell servers located on only one of the LAN segments to be connected. The Router will need to be configured differently in the second configuration with Novell servers located on only one of the LAN segments.

Novell Servers in Both Locations

An Ethernet IPX router is used to intelligently route Novell IPX LAN traffic to remotely connected LANs across the WAN.

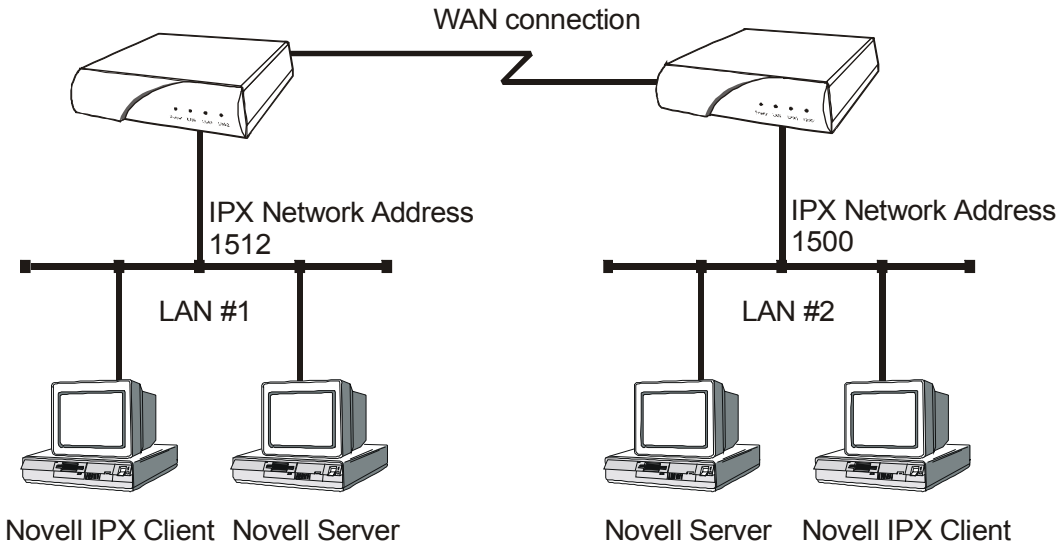


Figure 2-4 IPX Routed Local Area Networks (Servers on both sides)

IPX routers forward IPX frames based upon their IPX destination address and an internal routing table. The router maintains the internal routing table with the remote network IPX addresses and the remote partner IPX routers associated with those networks. When an IPX frame is received from the local LAN, the destination IPX address is examined and looked up in the routing tables. Once the destination IPX address is found in the routing tables, the IPX router sends the IPX frame to the remote partner Router that is connected to the appropriate remote IPX network.

To configure the P840 to be an IPX router when both LAN segments contain Novell servers, the IPX network numbers are learned automatically from the routing information and service announcements sent by the servers. The Router will automatically assign the IPX network numbers and proceed to route the IPX frames to the appropriate destination network.

When two IPX LAN segments with Novell servers on each segment are to be connected together with IPX routers, you must ensure that the IPX network numbers on each of the Novell servers is ***unique****. If the IPX network numbers are the same, the IPX routers will not operate.*

Once the WAN connections have been established to the remote partner Routers, the IPX router portion of the Routers will begin to build their routing tables according to the IPX frames they receive from the network. Manual entries may be made in the routing tables by adding static IPX routes.

Novell Servers in One Location Only

Some Novell LAN installations require that a remote LAN that consists of only Novell IPX clients be connected to a central LAN that contains the Novell servers and some more clients. In this configuration, the Router located at the remote site must be configured with the appropriate IPX network numbers. The IPX network number must be configured manually because there is no Novell server at the remote site. The Router must act as a Novell server to supply the proper IPX network number to the clients on the remote site LAN.

In the following diagram, the Router connected to LAN #2 must be configured with IPX network number 1500 using the appropriate frame type. The clients connected to LAN #2 must also be running with the same frame type as defined on the Router. After the Routers have established the WAN connection, the IPX routing procedures will cause the names of the services located on LAN #1 to be stored in the services table on the Router on LAN #2. When one of the clients on LAN #2 starts up, it will look for a server on the local LAN and the Router will respond with the list of servers that are located on the central LAN.

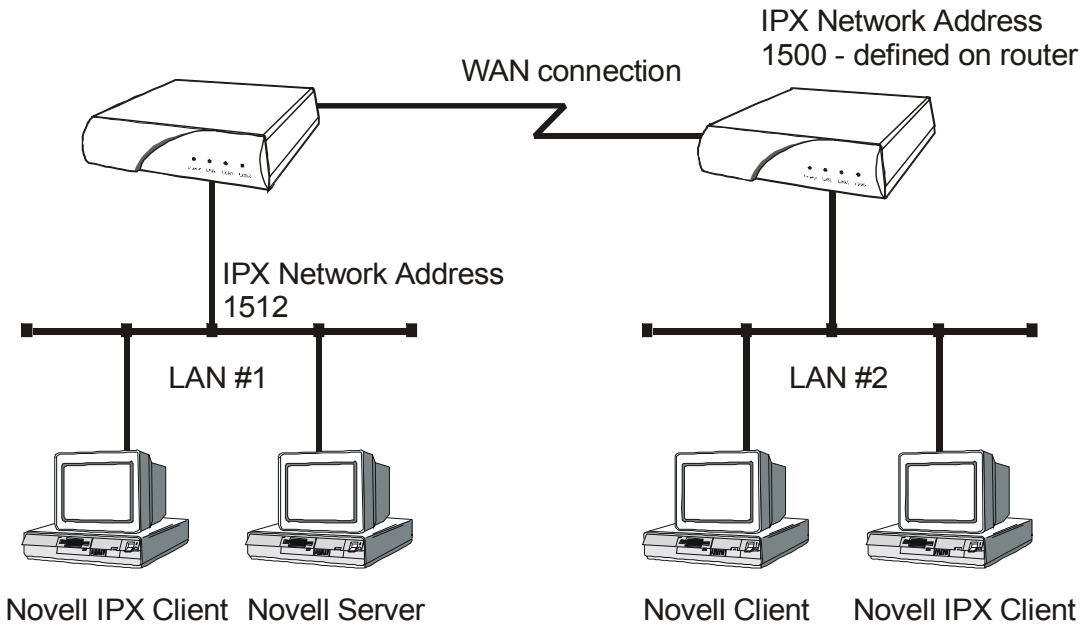


Figure 2-5 IPX Routed Local Area Networks

(Servers on one side)

The following steps must be performed on the Router connected to LAN #2.

IPX Routing Disabled

Location: Main

↳ Configuration

↳ IPX Routing Set up

↳ *IPX Routing*

Disabling IPX routing allows the IPX frame types to be modified.

Configuration Note: *IPX Routing does not need to be disabled in order to change the defined network numbers on a PPP Router.*

IPX Frame Types

Location: Main

- Configuration
  - IPX Routing Set up
    - Configure LAN Networks
      - *Ethernet-II Frames*
      - *RAW 802.3 Frames*
      - *IEEE 802.2 Frames*
      - *802.2 SNAP Frames*

Define the appropriate IPX network number for the appropriate frame type. Note that IPX network numbers must be unique. If more than one frame type is to be used, each frame type must have a unique IPX network number. There must be no duplicate IPX network numbers within your entire IPX routed network, they must all be unique. The IPX network numbers may be any value from 0 to FFFFFFFF HEX.

IPX Routing Enabled

Location: Main

- Configuration
  - IPX Routing Set up
    - *IPX Routing*

IPX routing must be re-enabled to allow the Router to operate as an IPX router with the newly defined IPX network numbers.

All Router routers connected to the same WAN must have IPX routing enabled for IPX routing to take place between the LANs. When a number of Router routers are connected on the same WAN and one of the Routers has IPX routing disabled, all of the Routers will become bridges only for IPX frames.

IPX Forwarding Enabled

Location: Main

↳ Configuration

↳ IPX Routing Set up

↳ *IPX Forwarding*

IPX forwarding must be re-enabled to allow the Router to forward IPX frames onto the WAN to the partner IPX Router routers.

Configuration Note: *The IPX Forwarding function enables or disables the forwarding of IPX traffic when IPX routing is enabled. When IPX forwarding is disabled, all IPX traffic across the WAN links will be blocked. While IPX forwarding is disabled, the Router will still operate as an IPX router and maintain its routing and server tables.*

The configuration options described here are only for initial set up and configuration purposes. For more complete information on all of the configuration parameters available please refer to the P840 PPP Menu Reference Manual file on the accompanying CD-ROM.

PPP Overview

Point to Point Protocol (PPP) is a connection protocol that allows control over the set-up and monitoring of network communications. It is used in procedures for user authentication (name and password), connection management (spoofing, bandwidth on demand, multilink), and compression.

PPP Link Configuration

A PPP connection between two routers may use a number of Network Control Protocols for communication. An IP router connection will use the Internet Protocol Control Protocol (IPCP) for all IP communications. An IPX router connection will use the Internet Packet Exchange Control Protocol (IPXCP) for all IPX communications.

In order to establish an IPCP or IPXCP link connection between two PPP routers, either a numbered link or an unnumbered link connection must be established. The two types of link connections are available to allow for greater flexibility between vendors products.

Numbered Links

A numbered link assigns a network address (either IP or IPX) to both ends of the WAN connection. In a numbered link configuration, the WAN connection may be viewed as another LAN network with the two PPP routers simply routing information between their local LANs and the common connected WAN network.

Because the WAN is considered to be a separate network, each of the stations on that network must be assigned a network address. If a numbered IP link is to be established, then each WAN interface must be assigned an IP address on a unique IP network. The WAN IP network address must be different from the two existing networks that are being connected together with the PPP routers.

If a numbered IPX link is to be established, then each WAN interface must be assigned an IPX node address on a unique IPX network number. The WAN IPX network address must be different from the two existing networks that are being connected together with the PPP routers.

The IP address of the local WAN link is defined as the **Local IP Address** within the remote site profile settings and the direct dial portion of the Quick Start menu. The IP address of the WAN link of the remote PPP router is defined as the **Peer IP Address** within the remote site profile settings and the direct dial portion of the Quick Start menu. The WAN IP network number is defined by defining a subnet mask size to

use when defining the local IP address. The size of the subnet mask will determine the IP network number used.

The IPX node address of the local WAN link is defined as the **Local IPX Node** within the remote site profile settings. The IPX address of the WAN link of the remote PPP router is defined as the **Peer IPX Node** within the remote site profile settings. The WAN IPX network number is defined with the **IPX Net** option in the remote site profile settings.

Configuration Note: *When making a direct dial connection within the Quick Start menu, only IP numbered and IPX unnumbered links are allowed. For different types of connections, a remote site profile should be configured with the appropriate IPCP and IPXCP settings defined.*

Unnumbered Links

An unnumbered link does not use network addressing on the WAN link. The WAN connection is roughly equivalent to an internal connection with each of the two end point routers operating as half of a complete router that is connected between the two endpoint LANs.

When an IPCP link is set to unnumbered, the only configuration option applicable is **Peer IP Address**. The peer IP address in this case is the IP address of the remote PPP router, that is the IP address of its LAN connection. If the peer IP address is not specified, the Router will attempt to determine it when negotiating the IPCP connection.

When an IPXCP link is set to unnumbered, no addressing configuration is required. All of the IPX settings are negotiated during the IPXCP connection.

Configuration Note: *When making a direct dial connection within the Quick Start menu, only IP numbered and IPX unnumbered links are allowed. For different types of connections, a remote site profile should be configured with the appropriate IPCP and IPXCP settings defined.*

Location: Main
- Configuration
  - WAN Set up
    - Remote Site Set up
      - Edit Remote Site
        - Protocol Set up
          - IP Parameters
            - *Peer IP address*

Multilink Operation

Multilink operation defines the use of more than one link to connect between two PPP routers. The **MultiLink Operation** option of the remote site profile for a connection is enabled by default.

When a multilink connection is established, the multilink (MP) options within the PPP Set up and Advanced PPP Set up menus will determine the operation of the multilink connection.

Configure Remote Site Profiles

Remote Site Profiles allow the Router to have different sets of configuration parameters for each of the remote site routers that may be called or that may call this Router. This allows complete control over the configuration of each possible connection.

Each remote site profile is assigned an identification number when it is created, whether it is created manually by the user editing the remote site profile or automatically under frame relay auto-learning. The remote site is also named with an alias, which provides a more descriptive identifier for the remote site profile. For example, a remote site profile may be created with a name that describes the location of the remote router or a user name on an incoming connection. The alias may be up to 16 characters long and must begin with an alphabetic character (blanks and the character "!" are not allowed).

There can be up to 40 remote site profiles. The ID numbers are assigned automatically in ascending order as the site profiles are created.

ID numbers 41, 42 and 43 are templates for creating remote site profiles with ISDN, Frame Relay or Leased Line connections respectively. A template may have its parameters set to match common network configurations and then be used to quickly set up a number of similar new sites. In addition to the reserved templates, you can use any remote site as a template to create a new site.

The remote site profile allows the definition of various connection parameters: Circuit set-up, Bridge and Routing protocol configurations, activation criteria and security.

The following steps must be performed on the P840 in order to define a new remote site profile.

Remote Site Profile ID & Alias

Location: Main

↳ Configuration

↳ WAN Set up

↳ Remote Site Set up

↳ Edit Remote Site

The remote site alias must be entered. The remote site profile is then created, an ID number is automatically assigned to it and the remote site profile is opened for editing. If a remote site profile already exists, either

the ID number or the alias may be provided to access the site profile for editing.

Now that the remote site profile is created, a link number must be assigned as the primary link number. The primary link number is the link interface that the Router will use to attempt to establish a connection to the remote site PPP router.

Primary Link Number

Location: Main
Configuration
WAN Set up
Remote Site Set up
Edit Remote Site
Connection Set up
Primary Link Number

ISDN Connection Remote Site Profiles

The ISDN call parameters for each of the remote sites that may be called from this router must be defined. The Router must know what ISDN phone number to dial when a connection to this remote site is required and what security parameters to use when establishing a connection.

When this Router receives an ISDN connection it will prompt the calling device for a user name and password (PPP access security); when the name and password have been authenticated, the user name is used to search the remote site profile entries to find a match. Once a match is found, the configuration parameters defined within that remote site profile are used to finish establishing the PPP connection.

Configuration Note: *The remote site profile alias, user name of the security entry, and the user name defined on the partner PPP router must all be the same for a connection to be established.*

Remote Site ISDN Phone Number

Location: Main
↳ Configuration
↳ WAN Set up
↳ Remote Site Set up
↳ Edit Remote Site
↳ Connection Set up
↳ ISDN Call Set up
↳ *ISDN Number*

The ISDN number defined here is the ISDN phone number of the remote site ISDN PPP router. This is the ISDN phone number that will be dialed to establish a connection to this remote site profile.

Frame Relay Remote Site Profiles

When frame relay is activated on the P840 it is set by default to automatically query the frame relay service to auto-learn the required parameters and automatically set up remote site profiles for each connection. See Frame Relay Configuration in the following section for more details.

Digital Leased Remote Site Profiles

As a leased line provides a dedicated line directly to a single remote site, the default settings will likely be all that is necessary to connect to this site.

If necessary, the Bridge, IP, IPX and Compression settings may need to be configured within their parameter menus to match the partner router.

Configure Remote Site Profiles for PPPoE

Remote Site Profiles allow for the router to be configured to support PPP over Ethernet (PPPoE) client on the router. The PPPoE feature on the Perle routers provide a PPPoE client support on Ethernet interfaces to a bridging DSL modem to the Internet. This feature will create a PPP tunnel to an ISP located somewhere on the ATM network side of the xDSL modem. This feature eliminates the hassle and potential error of running a PPPoE client on each LAN workstation that requires Internet access.

The following steps must be performed in order for the router to be configured for PPPoE connection. The remote site set-up for the PPPoE should refer to the section for Configure Remote Site Profiles for Leased Line PPP as the initial guideline for setting up a remote site configuration for PPP. Afterwards the following steps transform the PPP remote site connection to a unique PPPoE remote site configuration.

Location: Main

- Configuration
  - WAN Set-Up
    - Remote Site Set-up
      - Edit Remote Site
        - Connection Set-up
          - Primary Link
          - *LAN*

The Auto-Call field will be automatically setup to be enabled when a LAN interface is selected as the primary link. This will allow the PPPoE connection to be established automatically upon boot-up of the router.

To verify that PPPoE is enabled for this remote connection, view the read-only parameter

Location: Main

Configuration
WAN Set-UP
Remote Site Set-Up
Edit Remote Site
Protocol Set-Up
PPPoE
enabled

When setting up your PPPoE link with your ISP provider, one global IP addresses will be provided that should be used for the PPPoE remote site configuration. By enabled the NAT feature on the remote site configuration allows you to maintain only one global IP addresses for all PC workstation on your internal LAN.

Location: Main

Configuration
WAN Set-up
Remote Site Set-Up
Edit Remote Site
Protocol Set-Up
IP Set-up
NAT enabled
enabled

Access to some web pages is a common problem experienced when running a PPPoE client on a router. By design, PPPoE packets can support a maximum MTU of up 1492 bytes. Normally when a connection is established over common PPP, the TCP protocol negotiates its maximum data size using the mss option (default 1460). By default, most Windows PCs have their TCP mss option set to 1460 bytes. Since PPPoE requires an additional 8 bytes of header data, the TCP mss option should decrease to 1452 bytes. Therefore when configuring the router for PPPoE, the remote site NAT configuration automatically

adjust its TCP mss option to 1452 to accommodate this requirement. To verify this value has been adjusted:

Location: Main

- Configuration
  - WAN Set-Up
    - Remote Site Set-up
      - Protocol Set-Up
        - IP Parameters
          - NAT Advanced Set-up
            - TCP mss
              - *enabled*
            - TCP mss value
              - *1452*

Normally your ISP provider will provide you with an outgoing username and password and to authenticate with their services. The PPPoE remote site configuration needs to have the security section configured with this ISP parameters to authenticate the PPPoE connection.

Location: Main

- Configuration
  - WAN Set-Up
    - Remote Site Set-Up
      - Security Set-Up
        - Outgoing Username
          - *ISP provided username*
        - Outgoing PAP password
          - *ISP provided password*
        - Outgoing CHAP password (if required by ISP)
          - *ISP chap password*

To ensure that network traffic is routed to the PPPoE connection, the router must be configured to have the default IP gateway setup to your newly created PPPoE remote site connection.

Location: Main

↳Configuration

↳IP Routing Set-up

↳Gateway

↳*PPPoE remote site alias*

Basic Configurations

The P840 may be configured to handle the two BRI B-channels as both switched circuit ISDN links, as both Digital-Leased links (Digital-Leased is also known as Super-digital, ADSL-lite or monopole) or as one of each type. In addition, each Digital-Leased link may be set for either Frame Relay or PPP operation. The types of service available should be dicussed with your service provider.

Connection

The software controls used to determine when to attempt a connection to a remote site may be any one of the following methods:

IP Address Connect: Defining a remote site profile within the IP Address connect table and enabling IP Address Connect will cause a call to be made when a packet for this IP address is routed. This is the most common connection method.

Location: Main
- Configuration
  - WAN Set up
    - IP Address Connect
      - Edit IP Address Entry
        - *ID # for this entry*
        - *IP address of remote site*
        - *Remote site ID or alias*

Location: Main
- Configuration
  - WAN Set up
    - IP Address Connect
      - IP Address Connect
        - *enabled*

Manual Call: The system operator may use the Manual Call option of the Remote Site Set up menu to initiate a connection attempt.

Location: Main
- Configuration
  - WAN Set up
    - Remote Site Set up
      - Manual Call
        - *Remote site ID or alias to call*

Auto Call: Enabling the Auto-Call option within the Edit Remote Site menu of this remote site profile causes the Router to attempt to establish a connection to this remote site profile each time the Router starts up.

Location: Main
- Configuration
  - WAN Set up
    - Remote Site Set up
      - Edit Remote Site
        - Connection Set up
          - Auto call
            enabled

Basic ISDN Connections

The default settings of the P840 configure it for ISDN routing (rather than Digital_Leased). It may establish WAN connections to other bridge/routers via ISDN (Integrated Services Digital Network) connections. Either 1 or 2 ISDN B-channels (2 B-channels per ISDN BRI interface) may be used.

Before the P840 can establish an ISDN connection to another router, the ISDN information must be defined. The ISDN switch type must be defined for the ISDN interface, and the phone numbers must be defined. The following diagram shows three routers connected together, with two ISDN B-channels being configured on one unit and one channel on the other units.

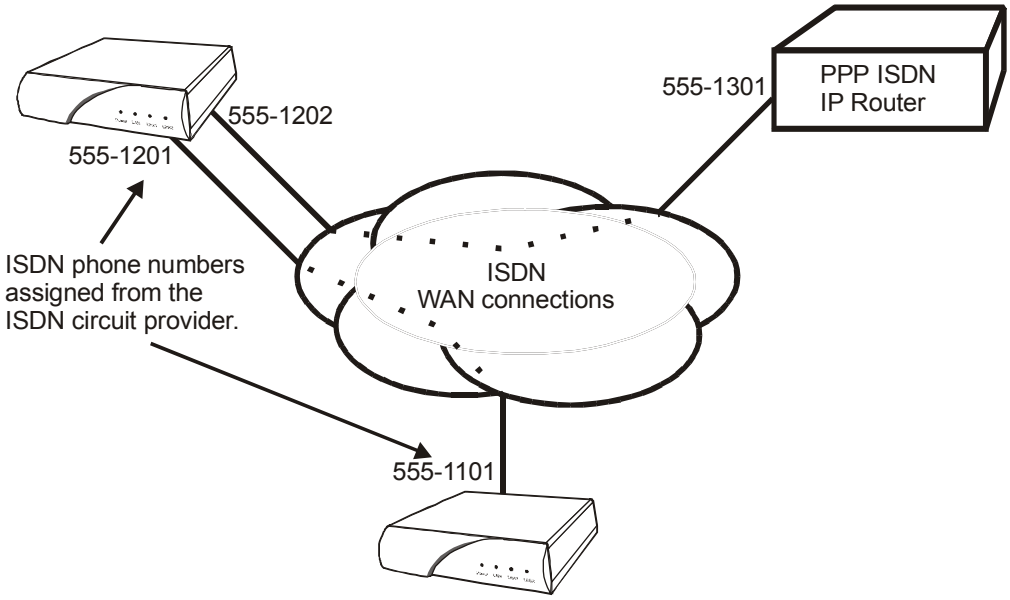


Figure 2-6 Basic ISDN Configuration

The following steps must be performed to configure the P840 for switched ISDN operation:

Switch Type

Location: Main

↳ Configuration

↳ WAN Set up

↳ *Switch Type*

Ten ISDN switch types are available: net3, ni-1, ni-2, dms-100, 5ess-pp, 5ess-mp, tph1962, kdd, sweden, or ntt. Note that if your routers are located within different ISDN jurisdictions, the ISDN switch type may be different on each of the units.

Directory Numbers & SPIDs

Location: Main

- Configuration
  - WAN Set up
    - Link Set up
      - ISDN Set up
        - *Directory Number 1*
        - *SPID 1*
        - *Directory Number 2*
        - *SPID 2*

The directory number(s) will be the ISDN phone numbers used to establish a call between the routers. The SPIDs are used to register the ISDN interface with the central switch.

Configuration Note: *For most European installations, the switch type will be NET3 which only requires one directory number. The Router will operate without putting in the directory number for a NET3 switch, but it is recommended that it be entered,*

Most North American installations use the switch type NI-1 and must have the two directory numbers entered, as well as two SPID (Service Profile Identifiers) values. For an NI-1 switch type, enter only the local portion of the directory number unless the area code is required for local calls. The SPID must be set to the exact number given by the ISDN service provider.

Once the ISDN switch type and directory numbers have been configured, the Router must be reset for the new values to take effect and for the ISDN BRI interface to register with the central switch.

Soft Reset

Location: Main
↳ Diagnostics
↳ *Soft Reset*

Once the Router has restarted it is ready to establish ISDN connections.

With the ISDN numbers and switch type defined, an ISDN call may be placed to another properly configured bridge/router. The calls may be placed manually or automatically. The automatic call features available are Auto-Call or IP Address Connect. An Auto-Call connection is established each time the Router starts up. An IP Address Connect call is established to a specifically configured remote Router when certain IP traffic is received from the local LAN.

"Quick Start" PPP ISDN Connections

The PPP P840 provides a "Quick Start" menu option that allows you to enter the basic configuration parameters required to establish a manual direct dial ISDN connection to another PPP IP/IPX router. Once the connection is established and is working properly, the Router **should be configured** with a **remote site profile** entry for that router. Once the remote site profile is created, ISDN calls may be placed automatically each time the Router starts up (Auto-Call) or automatically depending upon the time of day activation schedule or upon receiving IP frames from the local LAN destined for the IP network connected to that particular PPP router.

When establishing a direct dial connection from the "Quick Start" menu, the Bridging, IP and IPX configuration is partially predetermined. The IP connection requires the configuration of the local IP address of this Router. The IPX connection is an unnumbered connection that does not require any configuration. Each of the IP or IPX functions may also be disabled before the manual dial ISDN call is made.

The first step to a direct dial connection is to define the switch type and numbers as shown on the previous two pages (basic ISDN configuration). Once the ISDN configuration has been entered and the Router has been reset, a direct dial may be made to a remote site Bridge or IP/IPX PPP router.

If security is required for the direct dial connection refer to the Configure PPP Security section for information on setting the security passwords and user names for PPP.

IPX Router Connection

To establish an IPX PPP direct dial connection, enter the ISDN phone number of the remote site PPP router in the manual dial option. Refer to the Configure as an Ethernet IPX Router, section 2.1.3 for more information on IPX configuration required.

Manual Dial

Location: Main

↳ Quick Start

↳ Direct Dial

↳ *ISDN number*

Enter the ISDN phone number of the remote site IPX PPP router and an ISDN call will be placed.

IP Router Connection

To establish an IP PPP direct dial connection, the IP addresses must be supplied for this device before the ISDN call may be placed. Refer to the Configure as an Ethernet IP Router, section 2.1.2 for more information on the IP configuration required.

IP Address

Location: Main

↳ Quick Start

↳ Direct Dial

↳ *IP Address*

This is the IP address and subnet mask size for the link of this Router in the numbered IP connection.

Manual Dial

Location: Main

↳ Quick Start

↳ Direct Dial

↳ *ISDN number*

Enter the ISDN phone number of the remote site IP PPP router and an ISDN call will be placed.

Basic Frame Relay Configuration

The P840 may be configured to route frame relay packets over Digital Leased service (also known as Super-digital, ADSL-lite or monopole) on one or both BRI channels.

If a link on the P840 is configured for frame relay, it will communicate over WAN connections to other frame relay units via Frame Relay Permanent Virtual Circuits (PVC). From 1 to 40 PVC's may be defined to connect to other frame relay units. Before the P840 can establish a PVC connection to another frame relay router, at least one PVC must be defined. The P840 is pre-configured to query the frame relay service to auto-learn the required parameters; they may also be set manually.

The DLCI (Data Link Connection Identifier) number for the PVC is assigned by the frame relay service provider. The PVC must be defined on the physical link on the P840. The following diagram shows three P840 units connected together with a PVC being configured on each unit. The configuration of the PVCs within the frame relay cloud is controlled by the frame relay service provider.

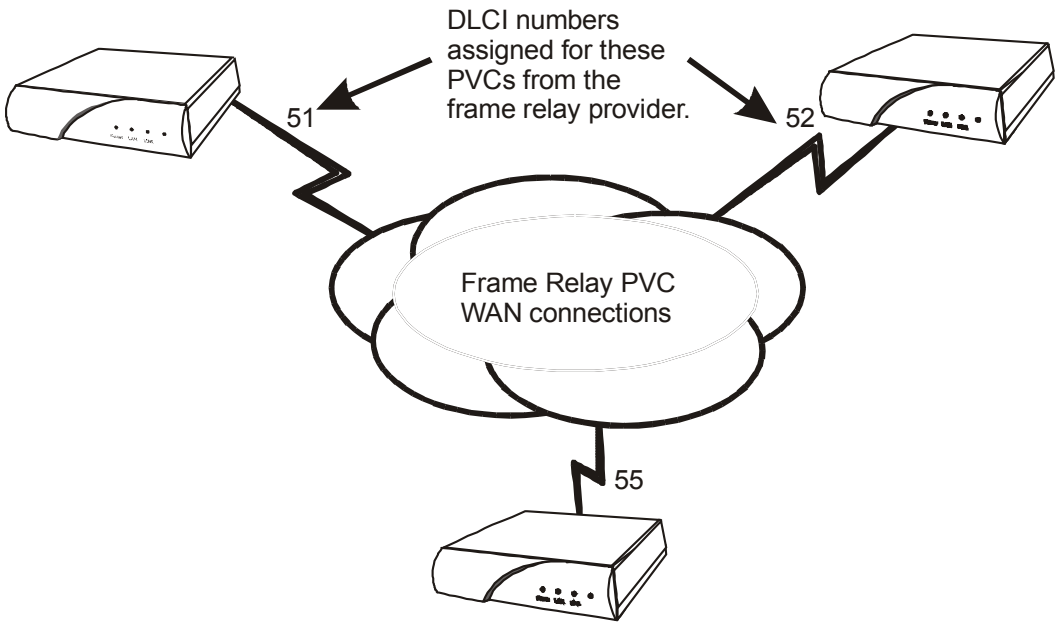


Figure 2 - 8 Frame Relay configuration

The link must be set to operate in Digital-Leased mode:

Set link to Digital-Leased

Location: Main
↳ Configuration
↳ WAN Set up
↳ Link Set up
↳ Logical ISDN type
Digital-Leased

Frame Relay must then be enabled:

Frame Relay enable

Location: Main
↳ Configuration
↳ WAN Set up
↳ Link Set up
↳ Frame Relay
enabled

The router will request confirmation of the change, enter "yes".

Auto Learning the Frame Relay Configuration

Under the default frame relay settings, the P840 is configured to query the frame relay service to auto-learn the LMI type and the PVC DLCI numbers. This auto-learn function allows the P840 to be plugged into the frame relay service and auto-learn the PVC configuration to become operational without further configuration. (Manual configuration is also allowed by modifying the options within each Remote Site Profile and the individual link configuration menus. Please see the P840 PPP Menus Manual on the accompanying CD-ROM for information on manual configuration).

When the P840 first starts up it will query the frame relay service to determine the LMI type. Once the LMI type is determined, the PVC configurations will be known from the full status enquiry messages. If the DLCI numbers of the PVC's on your service are determined during this learning process, the P840 will automatically create a remote site profile for each PVC. The automatically created remote site profiles will be named "LinkxDLCIyyy" where x is the physical link number the PVC is on and yyy is the DLCI of the PVC.

If during this learning process the maximum number of remote sites (40) has been reached, the P840 will prompt you that there are no remote sites available. A new remote site cannot be auto-created unless one of the existing remote sites is manually deleted.

Within each of the remote site profiles automatically created, Bridging, IP routing, and IPX routing are all set to "enabled". Because each of these options are enabled by default and the automatically created remote site profiles will establish a PVC connection to the remote site routers, the P840 will bridge and IPX route data without any user configuration. Because an IP router requires an IP address, the P840 must be configured with an IP address before IP routing is fully operational.

To configure an IP address for the P840, use the IP address option.

IP Address

Location: Main
- Configuration
  - LAN Set-up
    - LAN IP Set-up
      - *IP Address / Subnet mask size*

If security is required for the PVC connection refer to the Configure PPP Security section for information on setting the security passwords and user names for PPP.

By default, PPP is disabled for each of the newly created remote site profiles. If PPP encapsulation is desired, for example to use security, the PPP encapsulation option should be set to "enabled". By default, when PPP encapsulation is enabled multilink is also enabled.

PPP Encapsulation

Location: Main

↳ Configuration
↳ WAN Set-Up
↳ Remote Site Set-Up
↳ Edit Remote Site
↳Connection Set-up
↳ *PPP*
enable

The configuration options described here are only for initial set up and configuration purposes. For more complete information on all of the configuration parameters available please refer to the P840 PPP Menus Reference Manual file on the accompanying CD-ROM.

Basic Leased Line Configuration

The P840 may be configured to route PPP packets over Digital-Leased service (also known as Super-digital, ADSL-lite or monopole) on one or both BRI channels. The P840 in Digital-Leased mode will operate as a PPP leased line bridge/router if the frame relay function is disabled. The leased line P840 establishes PPP (Point to Point Protocol) WAN connections to other PPP leased line P840s or to other vendor's PPP leased line routers via direct leased line connections.

The following diagram that shows a P840 and another vendor's unit connected together with a direct leased line connection.

Figure 2 - 9 Basic PPP Leased Line Configuration

The link must be set to operate in Digital-Leased mode:

Set link to Digital-Leased

Location: Main
↳ Configuration
↳ WAN Set up
↳ Link Set up
↳ Logical ISDN type
Digital-Leased

To run PPP leased line, frame relay must be disabled:

Frame Relay disable

Location: Main
↳ Configuration
↳ WAN Set up
↳ Link Set up
↳ Frame Relay
↳ *disabled*

The router will request confirmation of the change, enter "yes".

Bridge Connection.

As soon as the above configuration is set, the P840 will attempt to establish the link connection to the remote site PPP router.

The Bridge connection does not require any configuration for operation.

IP Router Connection.

If IP traffic is to be routed, the IP address of the P840 must be set.

Local IP Address

Location: Main
↳ Configuration
↳ LAN Set-up
↳ LAN IP Set-up
↳ *IP Address / Subnet mask size*

Once the local IP address has been configured, the P840 will attempt to establish the link connection to the remote site PPP router.

The IP connection is an unnumbered connection that requires only the configuration of the IP address of this P840.

IPX Router Connection

As soon as the above configuration is set, the P840 router will attempt to establish the link connection to the remote site PPP router.

The IPX connection is an unnumbered connection that does not require any configuration.

If security is required for the connection, refer to the Configure PPP Security section for information on setting the security passwords and user names for PPP.

The configuration options described here are only for initial set up and configuration purposes. For more complete information on all of the configuration parameters available please refer to the P840 PPP Menus Reference Manual file on the accompanying CD-ROM.

ADVANCED FEATURES

Dynamic Host Configuration Protocol

The P840 uses Dynamic Host Configuration Protocol (DHCP) to allow users in a small office environment to be added and removed from a network with all of the network information (i.e. IP address, DNS, subnet mask, etc.) being configured automatically. DHCP configures devices (DHCP clients) from a central DHCP server. It is designed to allocate network addresses to a number of hosts on the Router's LAN and supply the minimal configuration needed to allow hosts to operate in an IP network.

The following steps must be performed on the P840 to configure it as a DHCP server.

DHCP Services

Location: Main

Configuration

Applications Set up

DHCP Set up

DHCP Services

Server

DHCP Services options which are available are none, relay and server. Set to server to enable this device as a DHCP Server.

IP Address Pool

Location: Main

Configuration

Applications Set up

DHCP Set up

Server IP address pool

IP address pool

First IP Address/
number of addresses

The IP address pool option requires setting the first IP address in the range that is to be used for the devices attached to the DHCP Server. The number of addresses to be assigned must also be specified, to a maximum of 253.

With the DHCP Services and IP Address Pool defined, devices may be attached to the network (up to the maximum specified) and they will be automatically configured.

Configuration Note: *When setting up a router as a DHCP server that will have both a DNS server on the internal network and a remote connection to another DNS server (for example, through an ISP), then the local DNS server should be set as the primary DNS and the external DNS server as the secondary DNS.*

DNS Set-Up

Location: Main

- Configuration
  - Applications Set up
    - DHCP Set up
      - DNS set-up
        - Primary DNS
          -IP address local DNS server
        - Secondary DNS
          -IP address external DNS server

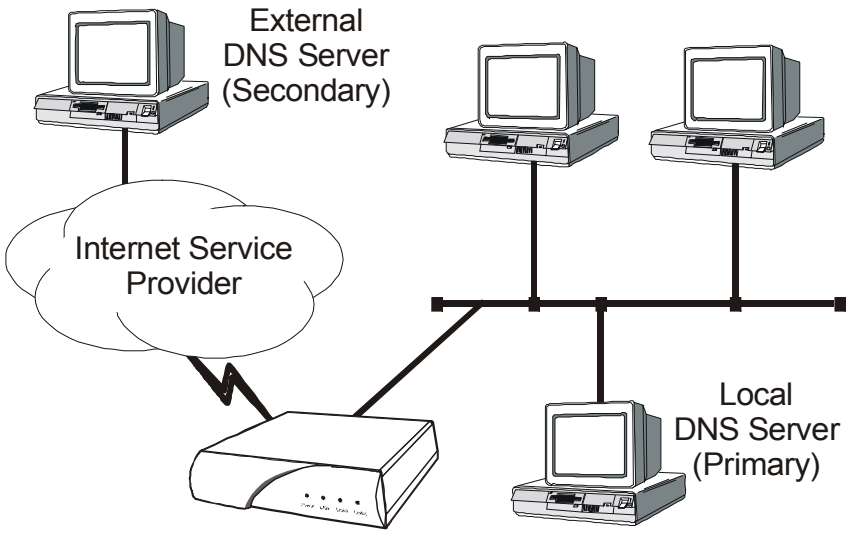


Figure 2-10 Local + External DNS Server Configuration

The configuration options described here are only for initial set up and configuration purposes. For more complete information on all of the configuration parameters available please refer to the P840 PPP Menu Reference Manual on the accompanying CD-ROM.

Network Address Translation and Port Translation

The P840 provides support for Network Address Translation (NAT). Network Address Translation is a technique that translates private IP address on a private network to valid global IP addresses for access to the Internet. Network Address Port Translation (NAPT) translates both the IP address and the port number. The advantage of port translation is that more than one private IP address can be translated to the same global IP address. Port translation allows data exchanges initiated from hosts with private IP addresses to be sent to the Internet via the Router using a single global IP address. A global IP address must be assigned to the WAN link upon which NAPT is enabled for port translation to work. The global IP address will be assigned by the ISP.

To use NAPT, the private network addresses of the services that will be available globally must be assigned:

NAT Exports

Location: Main
- Configuration
  - Applications Set up
    - NAT Exports
      - Edit Services
        - *enter the private network IP address of each service offered*

Applications

Then NAT (Network Address Translation) is enabled:

NAT Enable

Location: Main

Configuration

WAN Set up

Remote Site Set up

Edit Remote Site

Protocol Set up

IP Parameters

NAT Enabled

Enabled

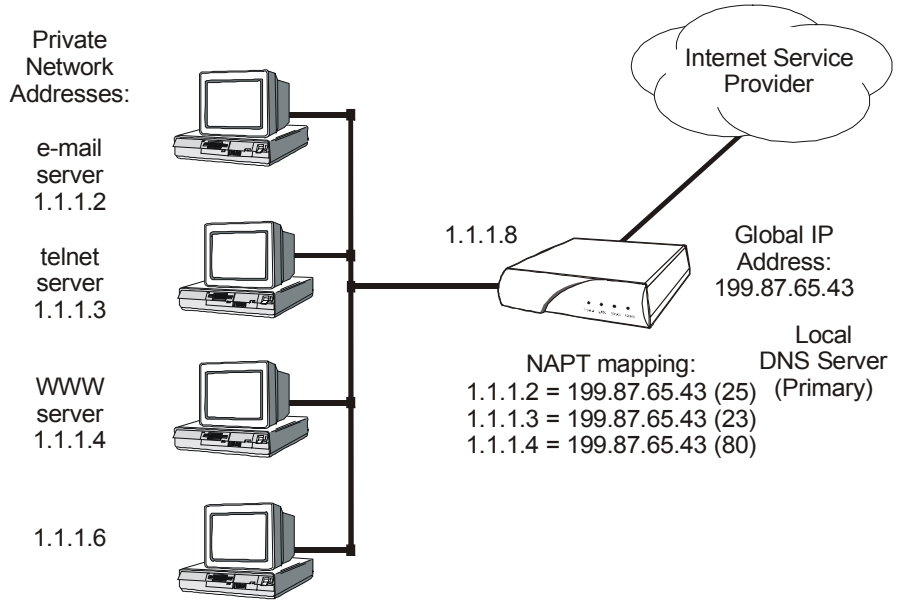


Figure 2-11 NAPT Configuration

Security

The Router provides a number of means of providing security on incoming and outgoing traffic on a network. These methods include access authentication, firewall limiting access to only designated device addresses, private network address translation (NAT) and filtering for both incoming and outgoing traffic.

Configure PPP Security

The PPP P840 provides support for both PAP and CHAP security access authentication. An outgoing user name, PAP password , and CHAP secret are defined that the Router will use when responding to an authentication request from a remote site PPP router.

The security option in the "Quick Start" menu allows you to quickly define the security level to be used for PPP authentication.

Security

Location: Main

Quick Start

Security level

When choosing the security option you may choose none, PAP or CHAP.

The cold start defaults for the security user name and passwords are as follows. These defaults will exist when the Router is first started before any configuration is entered, and after a Full Reset has been performed. These default values are also set when the Router is placed in TFTP Network load mode for upgrading the operating software via TFTP transfers. Care should be taken when upgrading a group of Routers that have security levels set.
Default outgoing user name for each remote site when it is defined is the same as the default device name. Default PAP password and CHAP secret are both set to "BRIDGE".

The complete security configuration for both incoming and outgoing calls is defined within the Security menu of the WAN Set up section.

⌨ *Security Level*

Location: Main

↳ Configuration
↳ WAN Set up
↳ Security Set up
↳ *Security Level*

The security level defines the type of security that this Router will request when a remote site PPP router attempts to establish a PPP connection. The security may defined as none, PAP, or CHAP.

When a security level is defined on this Router, an entry for each remote site PPP router that may be connected to this Router **must** be placed in the security database. The security database is used to store the user names and passwords of the remote site PPP routers.

⌨ *Remote Site Security Parameters Entry*

Location: Main

↳ Configuration
↳ WAN Set up
↳Edit Remote Site
↳ Security Parameters
↳ Outgoing *User Name*
↳ Incoming *PAP Password*
↳ Outgoing *PAP Password*

or

↳ Incoming *CHAP Secret*
↳ Outgoing *CHAP Secret*

The outgoing entries in the security database define the user names and passwords/secrets that this Router will send in response to an authentication request is sent from the remote partner router. The incoming entries define the passwords/secrets that this Router expects to receive from the remote partner in response to authentication requests.

For a pair of partner routers with security enabled, the outgoing user name in the security parameters entry of one router must match the remote site alias in the partner router's remote sites table.

The configuration options described here are only for initial set up and configuration purposes. For more complete information on all of the configuration parameters available, please refer to the PPP ISDN Menus Reference Manual file on the accompanying CD-ROM.

Configure Firewall

The P840 provides Firewall security for restricting access between any two networks connected through the router. Firewalls are set up on a per connection basis for the LAN and remote sites. The direction of filtering is from the perspective of the Router; incoming traffic is from the network in question to the Router, outgoing is from the Router to the network. The direction of filtering may be set to incoming, outgoing, both or none. Once the direction of filtering for a connection has been set, holes may be created in the firewall to allow specified traffic through. Normally, the LAN firewall is used for restricting intranet traffic (connections within the corporate network) and remote site firewalls are used to limit access from less trusted sources, such as the Internet or dial-up ISDN links.

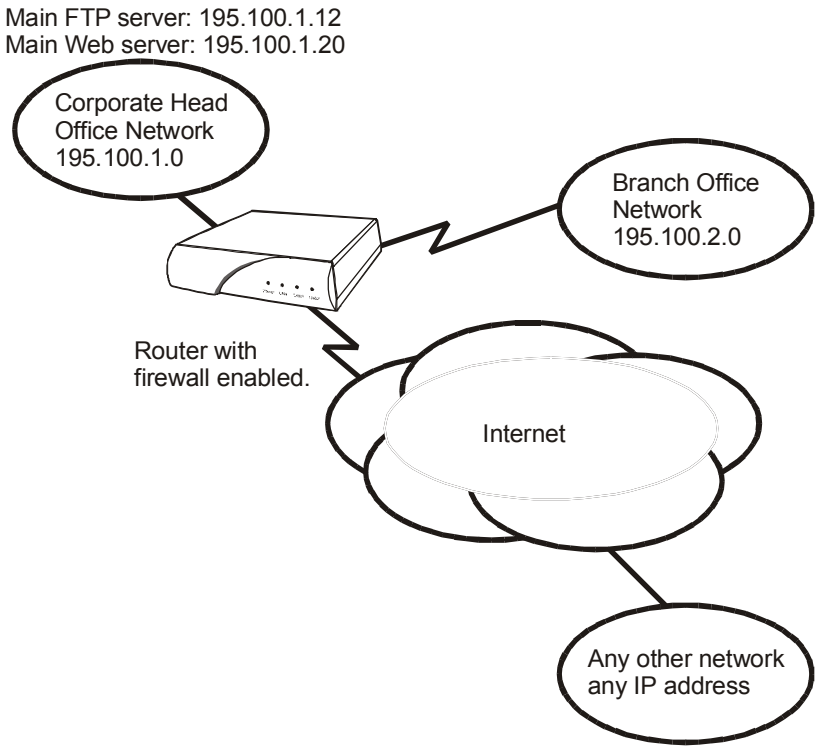


Figure 2-12 Sample Firewall Application

The above diagram shows a corporate head office network, which is connected to the Internet with a P840. There is also a branch office at a remote site connected with a Digital Leased link. The administrator at the corporate head office wishes to set up an IP firewall to allow everyone on the Internet to have access to the corporate FTP and Web servers and nothing else. The administrator also wishes to allow all of the TCP traffic from the branch office network to have access to the head office. Anyone in the corporation may have unrestricted access to the Internet.

The following steps must be performed on the P840 to set up the firewall support as desired.

First the firewall on the ISP connection (remote site 1) of the WAN is set up. The firewall option is set to "inbound" to have this WAN firewall filter traffic from the ISP to the Router while allowing unrestricted access out to the Internet.

Firewall WAN Remote Site Filter direction

Location: Main
- Configuration
  - Applications Set up
    - Firewall Set up
      - WAN Firewall Set up
        - *enter ID# 1 for ISP remote site*
        - Firewall
          - *inbound*

The firewall on the Internet connection is set up to protect the entire corporate network, including the branch office, from unauthorized traffic.

Then the entries are made in the "Designated Servers" menu to allow Internet access to the FTP and Web servers on the corporate network.

FTP & WWW Designated Servers

Location: Main
- Configuration
  - Applications Set up
    - Firewall Set up
      - WAN Firewall Set up
        - *ID# 1 for ISP remote site*
        - Designated Servers
          - *FTP Server*
          - 195.100.1.12
          - *WWW (HTTP) Server*
          - 195.100.1.20

When defining a designated server you will be prompted for the IP address of that device. Adding an entry to the designated servers list allows you to quickly setup a firewall entry without having to figure out TCP port values.

Next, the LAN firewall is set up to restrict access to the LAN. The firewall option is set to "outbound" to have the LAN firewall filter traffic from the Router.

⌨ *Firewall LAN Filter Direction*

Location: Main
- Configuration
  - Applications Set up
    - Firewall Set up
      - LAN Firewall Set up
        - Firewall
          - *Outbound*

Then an entry is placed in the firewall table to allow devices in the branch office remote site to have unlimited TCP access to devices in the head office.

⌨ *Firewall Table Entry*

Location: Main
- Configuration
  - Applications Set up
    - Firewall Set up
      - LAN Firewall Set up
      - Edit Firewall Entry
        - *filter ID # 1*
        - *Dest IP Address*
          — 195.100.1.0
        - *Destination Mask*
          — 255.255.255.0
        - *Source IP Address*
          — 195.100.2.0
        - *Source Mask*
          — 255.255.255.0
        - *Protocol Type*
          — TCP
        - *entry direction*
          —outbound

Finally, holes are provided in the LAN firewall to allow Internet access to the FTP and WWW servers.

Firewall

Location: Main

- Configuration
  - Applications Set up
    - Firewall Set up
      - LAN Firewall Set up
        - Designated Servers
          - *FTP Server*
            - 195.100.1.12
          - *WWW (HTTP) Server*
            - 195.100.1.20

The configuration options described here are only for initial set up and configuration purposes. For more information on all of the configuration parameters available please refer to the Menu Reference Manual file on the accompanying CD-ROM.

Network Address Translation

Using private addresses on a network and NAT/NAPT for interactions over a WAN connection hides the internal address from the rest of the world. Access is restricted to only those services that are specifically designated to be available.

Filters

The programmable filtering functions available on the P840 provide a very powerful means of controlling traffic flow to and from a network. Please see section 3 ***Introduction to Filtering*** for details on how to set up various filtering operations.

Compression

Compressing data allows data throughput rate considerably greater than the physical line rate. The actual rate achieved will depend on how compressible the specific data is. Generally, graphics and databases compress up to 600%, text 400 to 500%, binary codes about 200%.

Enable compression

Location: Main

- Configuration
  - WAN Set up
    - Remote Site Set up
      - Edit Remote Site
        - Protocol Set up
          - CCP parameters
            - Compression
            - *Enabled*

Bandwidth On Demand

The Router may be set to activate its secondary link when the load on the primary link exceeds a user-defined threshold.

Set the traffic loads for enabling and disabling the secondary circuit

Location: Main

- Configuration
  - WAN Set up
    - Remote Site Set up
      - Edit Remote Site
        - Threshold
          - *up threshold*
          - *up stability timer*
        - *down threshold*
          - *down stability timer*

The up and down stability timers are the delay times that the primary link must be above the threshold before the secondary is activated or below threshold before it is brought down. This prevents activation or deactivation of the secondary link due to momentary peaks or drops in traffic.

Bandwidth Allocation Control Protocol (BACP) may be used to negotiate the link activation between partner routers (BACP must be used if the partner router is not another Router).

Enable BACP

Location: Main

- Configuration
  - WAN Set up
    - Remote Site Set up
      - Edit Remote Site
        - Protocol Set up
          - BACP Set up
            - BACP
              - *enable*
              - call mode
                - *local* or *partner*

Call mode determines which router originates the call to bring up the second link.

If BACP is not used, the partner Routers will use proprietary negotiations to determine which router is to activate the second link.

QOS - Priority Queuing

Priority Queuing (PQ) allows the users to configure the router to allow specific traffic bound for an outgoing interface to be prioritized into high, medium, normal and low queues. Packets sent to the high priority queue are serviced first, followed by the packets on the medium queue and so on. The router can configure outbound traffic to specific queues based upon protocol, addresses and incoming interfaces.

To enable Priority Queuing you must configure a Priority list which contains the criteria items for the outbound packets. Each packet will be compared to item #1 in the Priority List and then progress down the list of items in order until a match is found. When a match is found, the comparison search will stop and the packet will be given the priority configured for that item. Thus more specific priority criteria should be defined at the beginning of the list.

To define item criteria within a Priority List:

Location: Main
↳Configuration
↳QOS Setup
↳Priority Queuing
↳Edit Priority List
↳Edit Items

Once the Priority List is defined, the Priority List can be assigned to a Remote Site interface or the LAN interface.

To assign a Priority List to a LAN interface

Location: Main
Configuration
Lan Set-up
QOS Setup
Queuing Strategy
Priority
Priority List Number

To assign a Priority List to a Remote Site Connection

Location: Main
Configuration
Wan Set-up
Remote Site Set-up
Edit Remote Site
Protocol Set-up
QOS Setup
Queuing Strategy
Priority
Priority List Number

Simple Network Time Protocol (SNTP)

The Simple Network Time Protocol (SNTP) feature on the Perle Routers support the client side of the protocol as described in RFC 2030. The router will be able to obtain its time from a NTP or SNTP server and then can be synchronized amongst other network devices. Additionally, the router can also be configured to support various time variations features such as local time zone and adjustments for daylight savings time.

When the Perle router has SNTP enabled it will periodically send NTP packets to the NTP/SNTP server which will respond with the network time. The router will synchronize its internal clock with the response from the NTP/SNTP server. The method in which the router sends or receives the NTP packets from the NTP/SNTP server is configurable in three modes: unicast, multicast and anycast.

In unicast mode, the router will have to be configured with the IP Address of the NTP server and will periodically send a request packet to the NTP server. The NTP server will then respond directly to this request with the current time. The Perle router supports a primary and a secondary IP Address for NTP servers.

In multicast mode, the router does not initiate the request packets but waits to receive the periodic broadcasts from the NTP server with the current time. Once the router receives an NTP packet from the server, it will then synchronize its internal clock with the current time.

In anycast mode, the router will send out a request packet as a broadcast on the LAN to get a response from any NTP server. When the first response is received from an NTP server, the internal clock of the router is synchronized. The router will learn the IP Address of the NTP server that responded and then operate in unicast mode.

The Perle router supports time variation feature of local time zones and daylight savings time regardless if the internal clock is synchronized with an NTP server. The local time zone feature allows the router to offset the internal clock by a configurable time from the UTC time. The configurable time zone off set can be specified in hours (0 to 23) and minutes (0 to 59) and can also be specified by a specific name up to 4 characters.

Adjustments to the internal clock for daylight saving time (Summer-time) can be enabled and specified for one time within the year or recurring year after year. Configuration parameters allow the router to enable

Summer-time each year by specifying the month, week, day and hour for the begin and end Summer-time.

To enable SNTP on the router and setup for unicast mode to directly obtain the time from a specific NTP server implement the following steps.

Location:

- Configuration
  - Application Set-up
    - SNTP Set-up
      - SNTP Client
        - *enable*
      - Mode
        - *unicast*
      - Primary IP Address
        - *IP Address (XXX.XXX.XXX.XXX)*
      - Secondary IP Address
        - *IP Address (XXX.XXX.XXX.XXX)*
      - Version
        - *3*

The time zone and daylight savings time configuration is setup within the device setup menu. To configure for Eastern Standard Time (EST) and have daylight saving time implemented for this year only, implement the following steps:

Location:

- Configuration
  - Access Set-up
    - Device Set-up
      - Time Zone Setup
        - Hours Offset
          - *5*
        - Minutes Offset
          - *0*
        - Name

- *EST*
- Summer Time Setup
  - Summer Time
    - *enabled*
  - Summer Time Mode
    - *date*
  - Summer Time Start
    - *Year*
    - *Month*
    - *Date*
    - *Time*
  - Summer Time End
    - *Year*
    - *Month*
    - *Date*
    - *Time*
  - Offset
    - 60

SECTION 3
INTRODUCTION TO FILTERING

The P840 provides programmable filtering which gives you the ability to control under what conditions Ethernet frames are forwarded to remote networks. There are many reasons why this might need to be accomplished, some of which are security, protocol discrimination, bandwidth conservation, and general restrictions.

Filtering may be accomplished by using two different methods. The first method is to filter or forward frames based solely on their source or destination MAC address. This method of filtering is useful when bridging between LANs and for providing remote access security in any type of network. The Ethernet MAC (Media Access Control) address is checked against the addresses in the filtering list and the frame is filtered or forwarded accordingly.

The second method of filtering is pattern filtering where each frame is checked against a filter pattern. The filter pattern may be defined to perform a check of any portion of the Ethernet frame. Separate filter patterns may be defined for bridged frames, IP routed frames, and IPX routed frames.

For more information on filtering, please refer to the Programmable Filtering section of the P840 reference manual file. The PDF file is located on the accompanying CD-ROM.

MAC Address Filtering

MAC address filtering is provided by three built-in functions.

The first function is "Filter if Source"; the second is "Filter if Destination." The third function allows you to change the filter operation from "positive" to "negative." The positive filter operation causes frames with the specified MAC addresses to be filtered. The negative filter operation causes frames with the specified MAC addresses to be forwarded.

You may easily prevent any station on one segment from accessing a specific resource on the other segment; for this, "positive" filtering and the use of "Filter if Destination" would be appropriate. If you want to

disallow a specific station from accessing any service, "Filter if Source" could be used.

You may easily prevent stations on one segment from accessing all but a specific resource on the other segment; for this, "negative" filtering and the use of "Forward if Destination" would be appropriate. If you want to disallow all but one specific station from accessing any service on the other segment, the use of "Forward if Source" could be used.

Pattern Filtering

Pattern filtering is provided in three separate sections: Bridge Pattern Filters, IP Router Pattern Filters, and IPX Router Pattern Filters. When the Router is operating as an IP/IPX Bridge/Router, each of the frames received from the local LAN is passed on to the appropriate internal section of the Router. The IPX frames are passed on to the IPX router, the IP frames are passed on to the IP router, and all other frames are passed on to the bridge. Different pattern filters may be defined in each of these sections to provide very extensive pattern filtering on LAN traffic being sent to remote LANs.

Pattern filters are created by defining an offset value and a pattern match value. The offset value determines the starting position for the pattern checking. An offset of 0 indicates that the pattern checking starts at the beginning of the data frame. An offset of 12 indicates that the pattern checking starts at the 12th octet of the data frame. When a data frame is examined in its HEX format, an octet is a pair of HEX values with offset location 0 starting at the beginning of the frame. Please refer to *Appendix C - Octet Locations on Ethernet Frames* for more information on octet locations in data frames.

The pattern match value is defined as a HEX string that is used to match against the data frame. If the HEX data at the appropriate offset location in the data frame matches the HEX string of the filter pattern, there is a positive filter match. The data frame will be filtered according to the filter operators being used in the filter pattern.

The following operators are used in creating Pattern filters.

- offset Used in pattern filters to determine the starting position to start the pattern checking.

  Example: 12-80 This filter pattern will match if the packet information starting at the 12th octet equals the 80 of the filter pattern.

| OR Used in combination filters when one **or** the other conditions must be met.

  Example: 10-20|12-80 This filter pattern will match if the packet information starting at the 10th octet equals the 20 of the filter pattern or if the packet information starting at the 12th octet equals the 80 of the filter pattern.

& AND Used in combination filters when one **and** the other conditions must be met.

  Example: 10-20&12-80 This filter pattern will match if the packet information starting at the 10th octet equals the 20 of the filter pattern and the packet information starting at the 12th octet equals the 80 of the filter pattern.

~ NOT Used in pattern filters to indicate that all packets **not** matching the defined pattern will be filtered.

  Example: ~12-80 This filter pattern will match if the packet information starting at the 12th octet does not equal the 80 of the filter pattern.

( ) brackets Used in pattern filters to separate portions of filter patterns for specific operators.

Example: 12-80&(14-24|14-32) This filter pattern will be checked in two operations. First the section in brackets will be checked and then the results of the first check will be used in the second check using the first portion of the filter pattern. If the packet information starting at the 14th octet equals 24 or 32, and the information at the 12th octet equals 80, the filter pattern will match.

Popular Filters

Some of the more commonly used pattern filters are shown here.

Bridge

Bridge pattern filters are applied to Ethernet frames that are bridged only. When the Router is operating as a router, all routed frames will be unaffected by the bridge pattern filters.

IP & Related Traffic

IP & Related Traffic	
Forward only	~(12-0800|12-0806)
Filter	(12-0800|12-0806)

Novell IPX Frames

Novell IPX Frames	
EthernetII	(12-8137)
802.3 RAW	(14-FFFF)
802.2	(14-E0E0)
802.2 LLC	(14-AAAA&20-8137)

NetBIOS &NetBEUI (Microsoft Windows)

NetBIOS & NetBEUI (Microsoft Windows)	
Filter	(14-F0F0)
Forward only	~(14-F0F0)

Banyan

Banyan
(12-0BAD)
(12-80C4)
(12-80C5)

IP Router

IP router pattern filters are applied to IP Ethernet frames that are being routed. When the Router is operating as an IP router, all IP routed frames will be checked against the defined IP router pattern filters. IP routed frames are unaffected by the bridge pattern filters and the IPX router pattern filters.

NetBIOS over TCP

NetBIOS over TCP	
NETBIOS Name Service	(22-0089)
NETBIOS Datagram Service	(22-008A)
NETBIOS Session Service	(22-008B)

Note: Uses the TCP Destination Port location

Other interesting TCP Ports

Other interesting TCP Ports		
Decimal	Hex	Usage
21	15	FTP
23	17	Telnet
25	19	SMTP
69	45	TFTP
109	6D	POP2
110	6E	POP3

APPENDIX A
MENU TREES

The menu trees on the next few facing pages are a graphical representation of the hierarchy of the built-in menu system of the P840. The menus are shown with the options of the menus being displayed below the specific menu name.

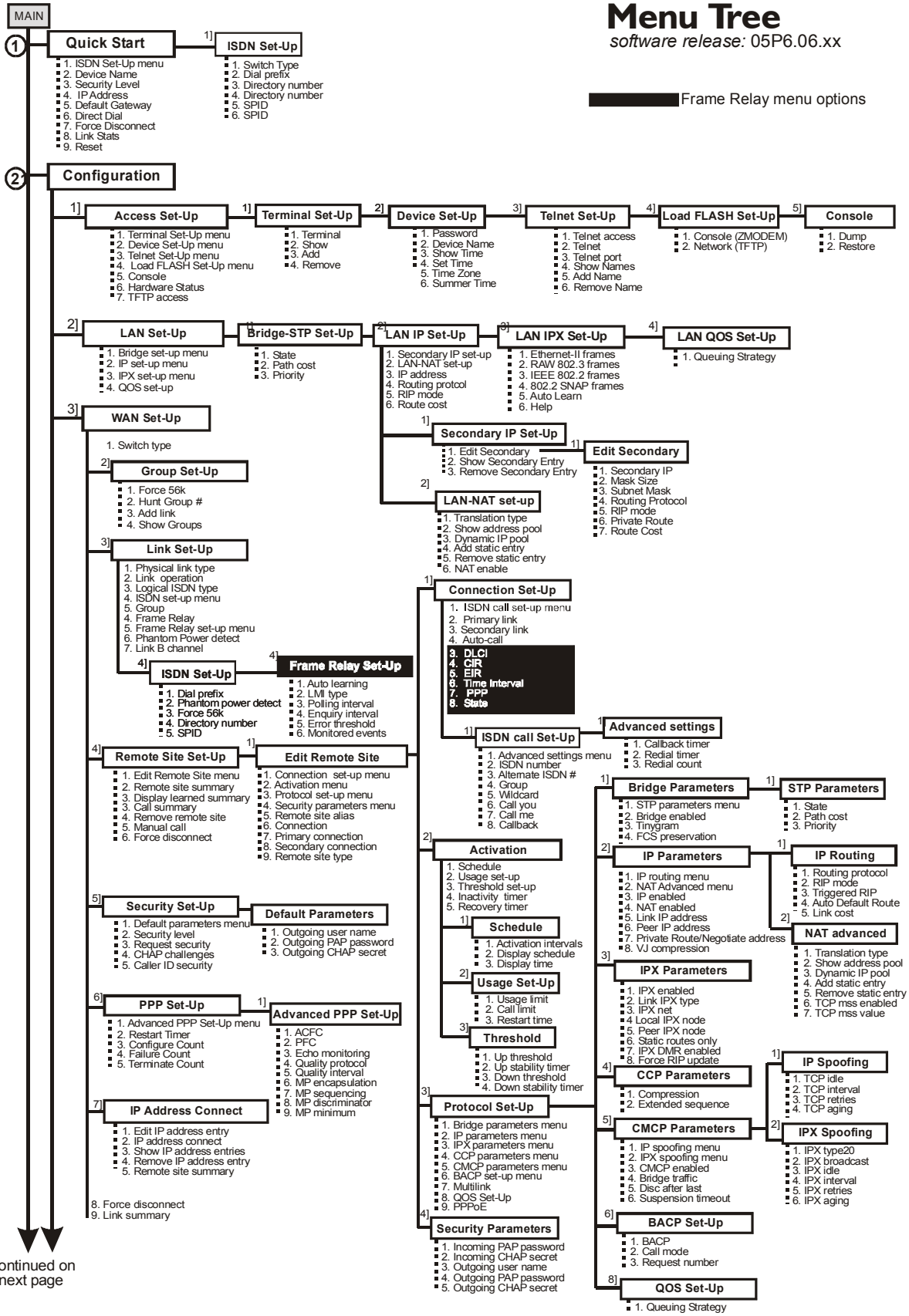
Each of the menu options shown in the menu tree is explained in the accompanying P840 menu reference files. The PDF files are located on the accompanying CD-ROM.

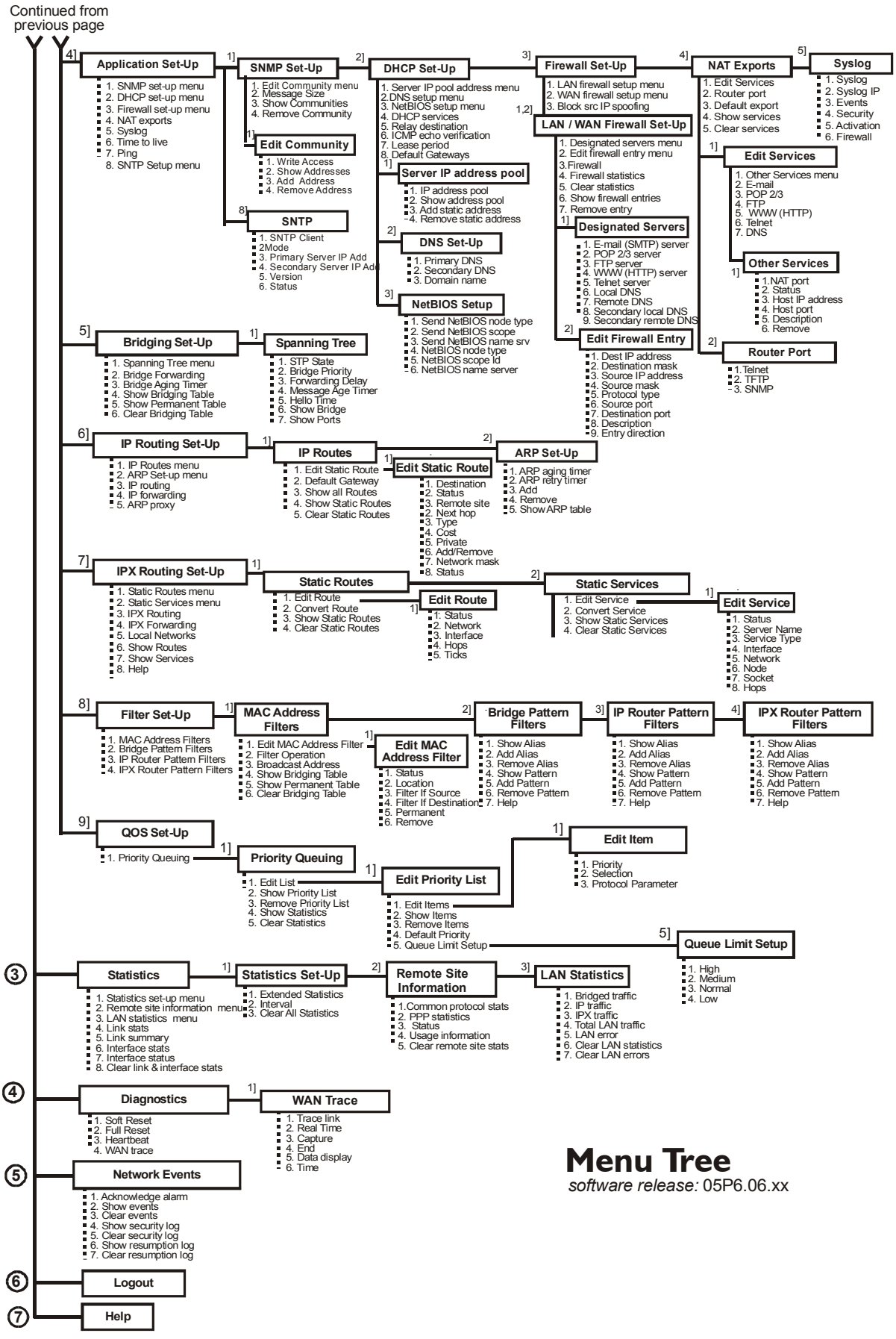
Menu names are displayed in boxes. The numbers on the left side of the boxes indicate the menu option from the parent menu that this menu corresponds to. All menu options are listed with numbers indicating their actual position within the menu system.

Menu Tree

software release: 05P6.06.xx

Frame Relay menu options




Continued from previous page
4] Application Set-Up
1. SNMP set-up menu
2. DHCP set-up menu
3. Firewall set-up menu
4. NAT exports
5. Syslog
6. Time to live
7. Ping
8. SNTP Setup menu
1] SNMP Set-Up
1. Edit Community menu
2. Message Size
3. Show Communities
4. Remove Community
1] Edit Community
1. Write Access
2. Show Addresses
3. Add Address
4. Remove Address
8] SNTP
1. SNTP Client
2Mode
3. Primary Server IP Add
4. Secondary Server IP Add
5. Version
6. Status
2] DHCP Set-Up
1. Server IP pool address menu
2.DNS setup menu
3. NetBIOS setup menu
4. DHCP services
5. Relay destination
6. ICMP echo verification
7. Lease period
8. Default Gateways
1] Server IP address pool
1. IP address pool
2. Show address pool
3. Add static address
4. Remove static address
2] DNS Set-Up
1. Primary DNS
2. Secondary DNS
3. Domain name
3] NetBIOS Setup
1. Send NetBIOS node type
2. Send NetBIOS scope
3. Send NetBIOS name srv
4. NetBIOS node type
5. NetBIOS scope Id
6. NetBIOS name server
3] Firewall Set-Up
1. LAN firewall setup menu
2. WAN firewall setup menu
3. Block src IP spoofing
1,2] LAN / WAN Firewall Set-Up
1. Designated servers menu
2. Edit firewall entry menu
3.Firewall
4. Firewall statistics
5. Clear statistics
6. Show firewall entries
7. Remove entry
1] Designated Servers
1. E-mail (SMTP) server
2. POP 2/3 server
3. FTP server
4. WWW (HTTP) server
5. Telnet server
6. Local DNS
7. Remote DNS
8. Secondary local DNS
9. Secondary remote DNS
2] Edit Firewall Entry
1. Dest IP address
2. Destination mask
3. Source IP address
4. Source mask
5. Protocol type
6. Source port
7. Destination port
8. Description
9. Entry direction
4] NAT Exports
1. Edit Services
2. Router port
3. Default export
4. Show services
5. Clear services
1] Edit Services
1. Other Services menu
2. E-mail
3. POP 2/3
4. FTP
5. WWW (HTTP)
6. Telnet
7. DNS
1] Other Services
1.NAT port
2. Status
3. Host IP address
4. Host port
5. Description
6. Remove
2] Router Port
1.Telnet
2. TFTP
3. SNMP
5] Syslog
1. Syslog
2. Syslog IP
3. Events
4. Security
5. Activation
6. Firewall
5] Bridging Set-Up
1. Spanning Tree menu
2. Bridge Forwarding
3. Bridge Aging Timer
4. Show Bridging Table
5. Show Permanent Table
6. Clear Bridging Table
1] Spanning Tree
1. STP State
2. Bridge Priority
3. Forwarding Delay
4. Message Age Timer
5. Hello Time
6. Show Bridge
7. Show Ports
6] IP Routing Set-Up
1. IP Routes menu
2. ARP Set-up menu
3. IP routing
4. IP forwarding
5. ARP proxy
1] IP Routes
1. Edit Static Route
2. Default Gateway
3. Show all Routes
4. Show Static Routes
5. Clear Static Routes
1] Edit Static Route
1. Destination
2. Status
3. Remote site
2. Next hop
3. Type
4. Cost
5. Private
6. Add/Remove
7. Network mask
8. Status
2] ARP Set-Up
1. ARP aging timer
2. ARP retry timer
3. Add
4. Remove
5. Show ARP table
7] IPX Routing Set-Up
1. Static Routes menu
2. Static Services menu
3. IPX Routing
4. IPX Forwarding
5. Local Networks
6. Show Routes
7. Show Services
8. Help
1] Static Routes
1. Edit Route
2. Convert Route
3. Show Static Routes
4. Clear Static Routes
1] Edit Route
1. Status
2. Network
3. Interface
4. Hops
5. Ticks
2] Static Services
1. Edit Service
2. Convert Service
3. Show Static Services
4. Clear Static Services
1] Edit Service
1. Status
2. Server Name
3. Service Type
4. Interface
5. Network
6. Node
7. Socket
8. Hops
8] Filter Set-Up
1. MAC Address Filters
2. Bridge Pattern Filters
3. IP Router Pattern Filters
4. IPX Router Pattern Filters
1] MAC Address Filters
1. Edit MAC Address Filter
2. Filter Operation
3. Broadcast Address
4. Show Bridging Table
5. Show Permanent Table
6. Clear Bridging Table
1] Edit MAC Address Filter
1. Status
2. Location
3. Filter If Source
4. Filter If Destination
5. Permanent
6. Remove
2] Bridge Pattern Filters
1. Show Alias
2. Add Alias
3. Remove Alias
4. Show Pattern
5. Add Pattern
6. Remove Pattern
7. Help
3] IP Router Pattern Filters
1. Show Alias
2. Add Alias
3. Remove Alias
4. Show Pattern
5. Add Pattern
6. Remove Pattern
7. Help
4] IPX Router Pattern Filters
1. Show Alias
2. Add Alias
3. Remove Alias
4. Show Pattern
5. Add Pattern
6. Remove Pattern
7. Help
9] QOS Set-Up
1. Priority Queuing
1] Priority Queuing
1. Edit List
2. Show Priority List
3. Remove Priority List
4. Show Statistics
5. Clear Statistics
1] Edit Priority List
1. Edit Items
2. Show Items
3. Remove Items
4. Default Priority
5. Queue Limit Setup
1] Edit Item
1. Priority
2. Selection
3. Protocol Parameter
5] Queue Limit Setup
1. High
2. Medium
3. Normal
4. Low
③ Statistics
1. Statistics set-up menu
2. Remote site information menu
3. LAN statistics menu
4. Link stats
5. Link summary
6. Interface stats
7. Interface status
8. Clear link & interface stats
1] Statistics Set-Up
1. Extended Statistics
2. Interval
3. Clear All Statistics
2] Remote Site Information
1.Common protocol stats
2. PPP statistics
3. Status
4. Usage information
5. Clear remote site stats
3] LAN Statistics
1. Bridged traffic
2. IP traffic
3. IPX traffic
4. Total LAN traffic
5. LAN error
6. Clear LAN statistics
7. Clear LAN errors
④ Diagnostics
1. Soft Reset
2. Full Reset
3. Heartbeat
4. WAN trace
1] WAN Trace
1. Trace link
2. Real Time
3. Capture
4. End
5. Data display
6. Time
⑤ Network Events
1. Acknowledge alarm
2. Show events
3. Clear events
4. Show security log
5. Clear security log
6. Show resumption log
7. Clear resumption log
⑥ Logout
⑦ Help
Menu Tree
software release: 05P6.06.xx

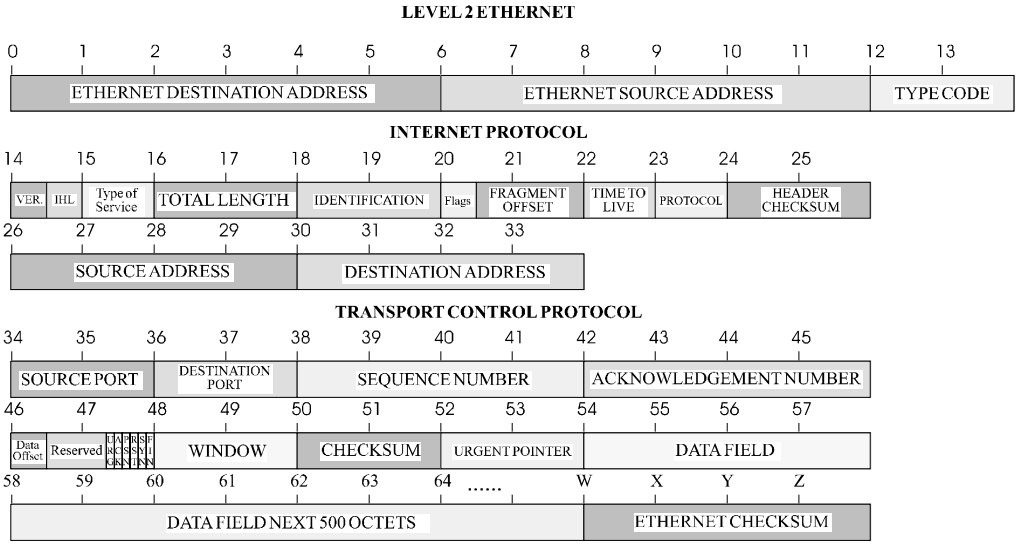
APPENDIX B
OCTET LOCATIONS ON ETHERNET FRAMES

This appendix provides octet locations for the various portions of three of the common Ethernet frames. When creating pattern filters these diagrams will assist in the correct definition of the patterns. The offset numbers are indicated by the numbers above the frame representations.

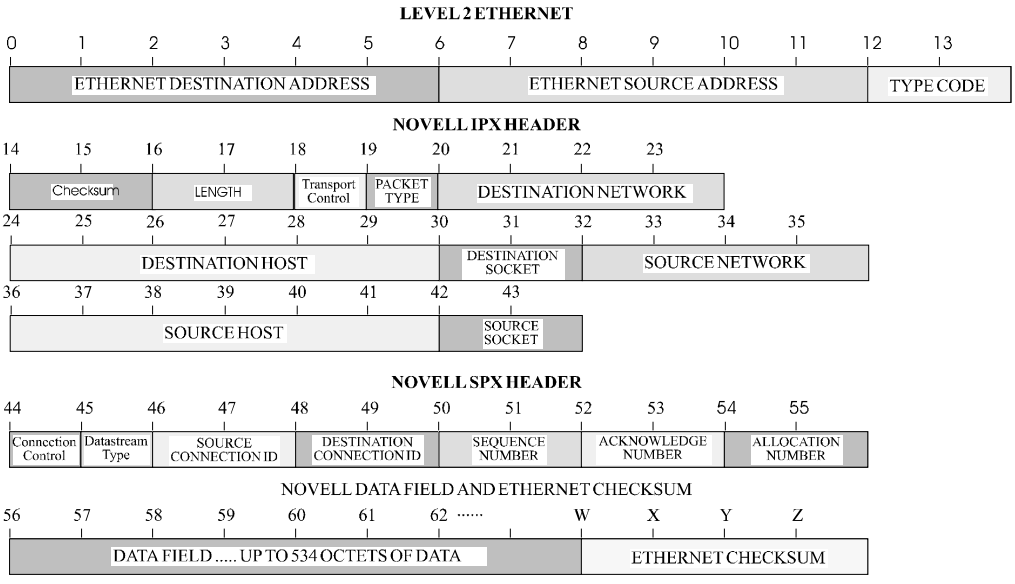
Note the differences in the TCP/IP and Novell frames when bridging and when routing. When routing, the TCP/IP and Novell frames are examined after the Level 2 Ethernet portion of the frame has been stripped from the whole data frame. This means that the offset numbers now start from 0 at the beginning of the routed frame and not the bridged frame.

Some of the common Ethernet type codes are also shown here. The Ethernet type codes are located at offset 12 of the bridged Ethernet frame.

Octet Locations on a Bridged TCP/IP Frame



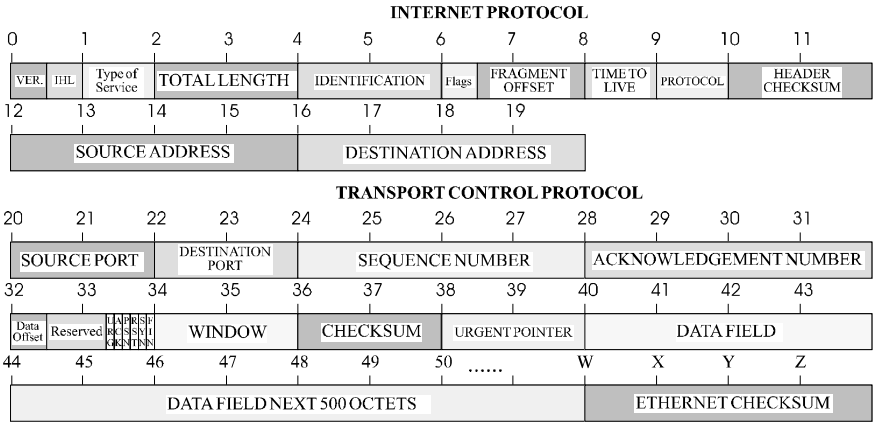
Octet Locations on a Bridged Novell Netware Frame



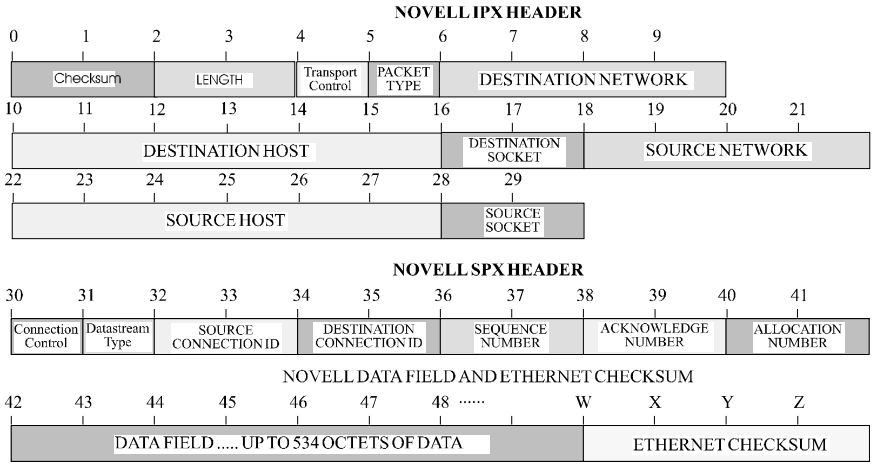
ETHERNET Type Codes

Type Code	Description
0800	DOD IP
0801	X.75 Internet
0804	Chaosnet
0805	X.25 Level 3
0806	ARP
0807	XNS Compatibility
6001	DEC MOP Dump/Load
6002	DEC MOP Remote Console
6003	DEC DECNET Phase IV Route
6004	DEC LAT
6005	DEC Diagnostic Protocol
6006	DEC Customer Protocol
6007	DEC LAVC, SCA
8035	Reverse ARP
803D	DEC Ethernet Encryption
803F	DEC LAN Traffic Monitor
809B	Appletalk
80D5	IBM SNA Service on Ether
80F3	AppleTalk AARP (Kinetics)
8137-8138	Novell, Inc.
814C	SNMP

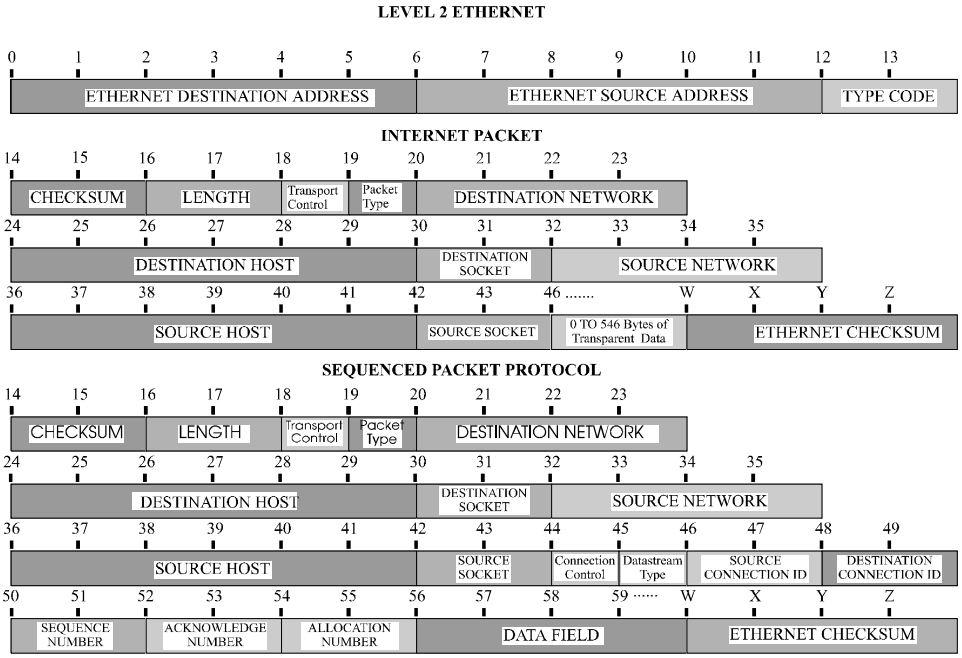
Octet Locations on an IP Routed TCP/IP Frame



Octet Locations on an IPX Routed Novell Netware Frame



Octet Locations on a Bridged XNS Frame



APPENDIX C
SERVICING INFORMATION

Opening of the case is only to be performed by qualified service personnel.

WARNING !

Before servicing ensure that appliance coupler is disconnected.

Always disconnect the power cord from the rear panel of the router.

Geraetesteckvorrichtung trennen vor den Wartung.

Opening the case

1) Remove power from the router and remove the other cabling.
2) Turn the router over and place it on a flat, cushioned surface.
3) Remove the two Phillips head screws that fasten the case together.
4) Hold the two halves of the case together and turn the router right side up.
5) Lift off the top half of the case.

Identifying the Internal Components

The major components of concern and the jumper strap positions are shown in the following illustration.

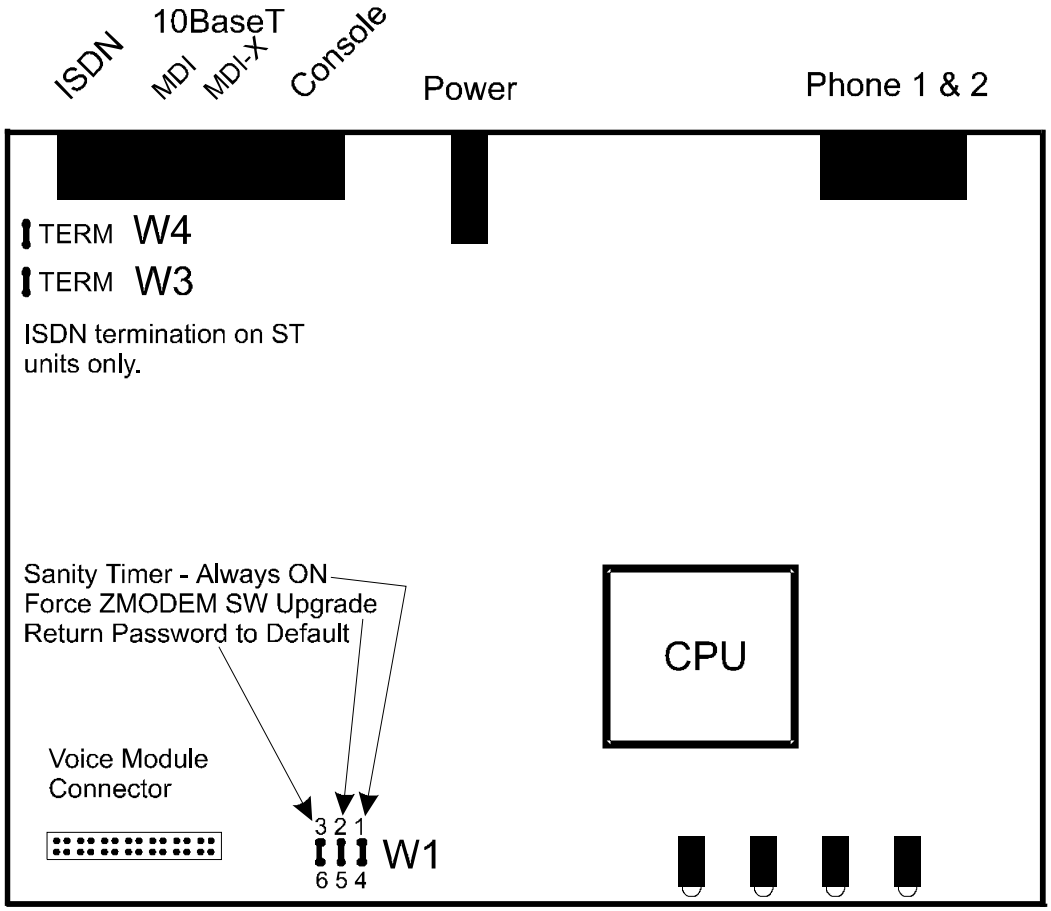


Figure C-1 Top Internal View of the Router Router

Connecting to the ISDN-U Link Module

The connection to the central office is made with the RJ45 ISDN connector on the rear panel. Pins 4 and 5 are used for the connection. These pins are polarity insensitive.

To Clear a "Lost" Password

1) Remove power from the router.
2) Remove the case cover.
3) Remove the jumper strap on pins 3-6 of W1.
4) Re-attach the power to the router and wait for Power LED to go green.
5) Remove power from the router.
6) Re-install the jumper strap on pins 3-6 of W1.
7) Install the case cover
8) Power up the router.
9) Log into the router using the default password "BRIDGE" and change the password as desired.

Changing the Termination Straps on the ISDN Interface

The ISDN ST interface module has two configurable straps that control whether the ISDN connector is set to terminated or unterminated.

Straps W3 and W4 are set to the TERM position by default. The TERM position is used when the router is the only ISDN device connected to the ISDN circuit.

Setting W3 and W4 to be open (unterminated) allows this router to be part of a daisy-chain connection to the ISDN circuit.

Connecting to the Console Connector

The console connector on the P840 is a DCE interface on a RJ45 pinout. The supplied DB9 to RJ45 converter should be used to connect to the DB9 connector of a DTE terminal. This connection will then provide access to the built-in menu system.

If the console interface is to be connected to a modem or other DCE device, a standard RS-232 crossover converter should be used.

The following table illustrates the console pinouts.

RJ45 connector on unit (DCE)	DB9 connector on converter (DCE)	RS-232 signal name
2	6	CTS
3	4	DTR
4	5	GND
5	2	RxD
6	3	TxD
7	8	DSR
8	1	CD

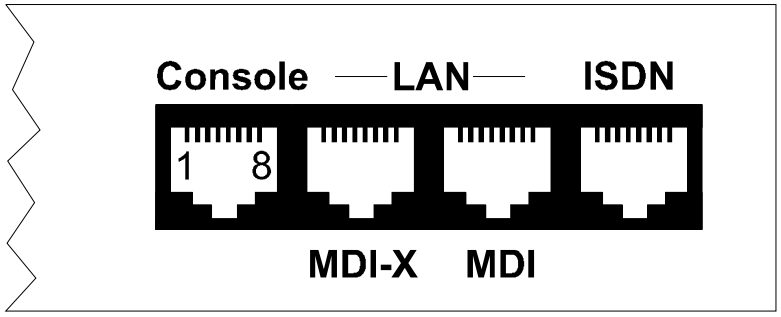


Figure C-2 Rear View of the Console Connector

APPENDIX D
SOFTWARE UPGRADES

Procedures for performing a Console ZMODEM Flash Load to upgrade the operating software of the router:

1) Save the current configuration of the router (Main menu: option 6).

2) Execute the Console (ZMODEM) command from the Load FLASH Set-Up menu.

3) Confirmation is required. Enter "yes" to proceed.

4) After the router restarts, the router will be in receive ZMODEM mode. The router will display the following messages on the console port:

```
System                                                  startup
Receiving                    ZMODEM                        ...
**B0100000023be50
```

5) Start the ZMODEM transfer and send the file "###.all" from the Operational/Boot Code directory on the CD-ROM.

6) Once the ZMODEM transfer is complete, the router will verify the file "###.all" in memory, program and verify the FLASH, clear the configuration to default values (except the password), and then reset. After the reset, the router will operate normally using the newly upgraded software. A byte status message will be displayed on the console port during the programming of the FLASH.

On the rare occasion that during the programming of the FLASH something happens to the router (power hit or hardware reset), causing the FLASH to become corrupted, the router will restart in ZMODEM receive mode only. If the router does not start in ZMODEM receive mode, refer to Appendix D: Servicing Information for recovery procedure.

The ZMODEM Load Flash operation may be aborted by aborting the ZMODEM transfer and then entering 5 control-X characters "^X" from the console keyboard. After the control-X characters are sent, the router will display a limited menu system. Choose the Abort Load option from the Load FLASH Set-Up menu. This will cause the router to reset and return to normal operations operating from the existing software.

If the ZMODEM transfer operation needs to be restarted after it has been canceled or after loading the first file, simply choose the Console (ZMODEM) option from the Load FLASH Set-Up menu once again.

Considerations:

When the router is placed in Console load BOOT mode, the LAN interface and the WAN interface will be disabled. The router will only accept information from the console management port.

The BOOT code of the Router may be upgraded by performing a load of the "###.all" file from the Operational/Boot Code directory on the CD-ROM.

Procedures for performing a TFTP Flash Load to upgrade the operating software of the router:

1) Execute the Network (TFTP) command from the Load FLASH Set-Up menu.

2) Enter "none" to connect locally or enter the remote site ID number or alias to connect to a remote site.

3) Start the TFTP application to be used for transfers to the router. The IP address of the router may be found in the Internet Set-Up menu.).

4) Put the file "###.all" for this router from the Operational/Boot Code directory on the CD-ROM to the router. (Any router not in Network Load BOOT mode will respond with an access violation error.)

5) The router will verify the file "###.all" in memory, program and verify the FLASH, clear the configuration to default values (except: IP Address, IP Routing state, IP Forwarding state, WAN Environment, Link 1 & 2 State, Password and connection data for the remote site, if applicable), and then reset. After the reset, the router will operate normally using the newly upgraded software.

The router may take up to two (2) minutes to program and verify the FLASH. The console will not respond during this time.

To check on the router's current state during this process, get the file "status.txt" from the router. This file will report the router's state: both the mode and version if no errors have occurred, or an error message.

On the rare occasion that during the programming of the FLASH something happens to the router (power hit or hardware reset), causing the FLASH to become corrupted, the router will restart in ZMODEM receive mode only. If the router does not start in ZMODEM receive mode, refer to Appendix D: Servicing Information.

The TFTP Load Flash operation may be aborted by re-connecting to the console of the router and choosing the Abort Load option from the Load FLASH Set-Up menu. This will cause the router to

reset and return to normal operations operating from the existing software.

In the following diagram of a cluster of routers, when upgrading the three Router routers in the diagram, the upgrade order should be Router C, then Router B, and finally Router A.

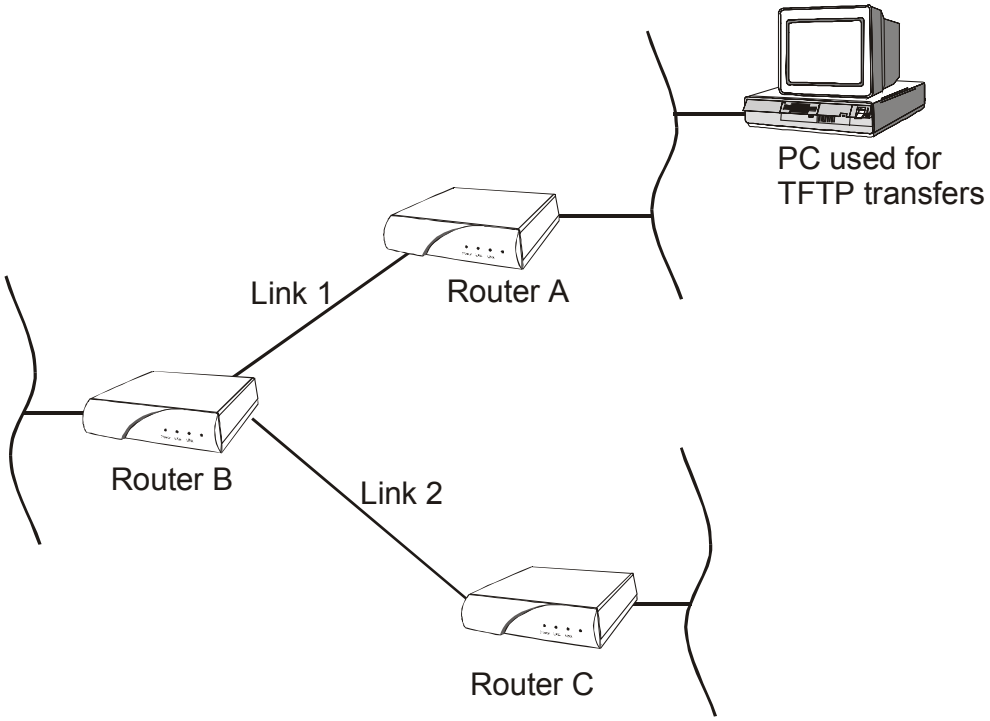
A TFTP software load to Router C would be performed as follows:

- Using TFTP, get config.txt from each router and save.
- Telnet to Router C. Enter the ID or alias of Router B in the Network (TFTP) option to put Router C in Network Load mode. When Router C restarts in Network Load mode, the connection to "Router B" will be re-established only if autocall is enabled on router B.

The TFTP transfer of the upgrade code may now be performed from the PC to Router C. Once Router C has completed programming the flash and has restarted in operational mode, the connection to Router B will be re-established only if autocall is enabled on router B.

Once router C is operating with the new software, the PC may be used to reload the config.txt file back to Router C.

Repeat for Router B, then again for Router A. Perform the Router B upgrade using the ID or alias of Router A. Router A upgrades would not require a remote site ID as the PC used for TFTP transfers is located on the same LAN as Router A.


PC used for
TFTP transfers
Router A
Link 1
Router B
Link 2
Router C