Perle P850

Bridge / Router

USER AND SYSTEM
ADMINISTRATION GUIDE

Part number 5500086-15

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 equivalence 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 P850 router 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. If trouble is experienced with this equipment, P850, please contact TriNexus Communications at 1-888-668-7711 for repair and warranty information. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

6. 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.

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 P850 router. This guide is organized into the following sections:

"***Installation***" provides instructions for installing the P850 router.

"***Typical Applications & How to Configure Them***" provides simple configuration examples for typical applications in which the P850 router might be used. The applications described in this document are for example only and provide a method of quick configuration of the P850 router. For more complete information on all of the configuration parameters available, please refer to the PPP Menu Reference Manual on the accompanying CD-ROM.

"***Introduction to Filtering***" provides an introduction to the pattern filtering options of the P850 router. 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 P850 router. 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 P850 router 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 P850 router 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 P850 router Reference Manuals are provided as Adobe Acrobat PDF files on the accompanying CD-ROM. The PPP Menus Reference File is provided individually for ease of configuration reference.

The Adobe Acrobat Reader program is included on the CD-ROM. It 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 P850 features
- Pin out references for the link modules
- List of event and alarm logs
- Expanded description of programmable filtering

The P850 PPP Menus Reference Manual provides the following information:

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

Contents

I - INSTALLATION

The P850 is an Ethernet Bridge/Router that provides bridging, IP/IPX routing, and compression over a frame relay permanent virtual circuit or a PPP leased line circuit..

The following instructions provide a quick set-up guide for installation of the P850 router

Unpack the P850

Rough handling during shipment can damage electronic equipment. As you unpack the router, carefully check for signs of damage. If damage is suspected, contact the shipper. Save the box and all packing material to protect the 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 router provide all external connections to the P850 router.

Select a Site

Place the router in a well-ventilated area. The site should maintain normal office temperature and humidity levels. Air vents located on the rear of the router must have an inch or so of clearance from any object. Units should not be stacked.

Identify the Connectors

Each unit is configured with both straight (MDI) and crossed over (MDI-X) 10BaseT LAN connectors; the P850 will auto-sense between the two. Only one connector may be used at a time.

The P850 router is produced with four different WAN interface modules: V.35, CSU-DSU, Universal WAN or T1/E1. The type of module in a unit may be determined by looking at the label over the WAN connector on the back panel.

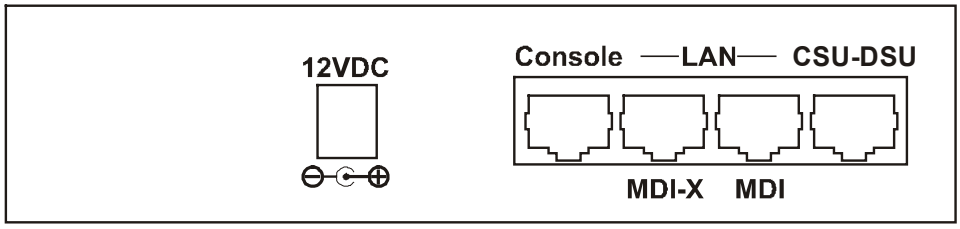


Figure 1 - 1 Rear View of the CSU-DSU P850 router

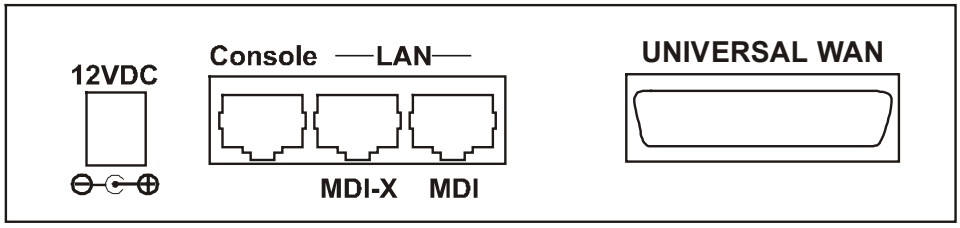


Figure 1 - 2 Rear View of the Universal WAN P850

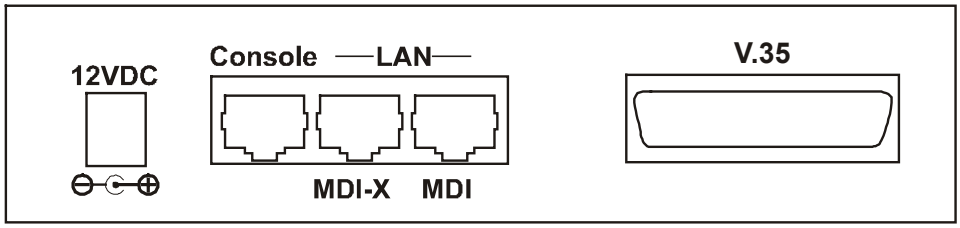


Figure 1 - 3 Rear View of the V.35 P850 router

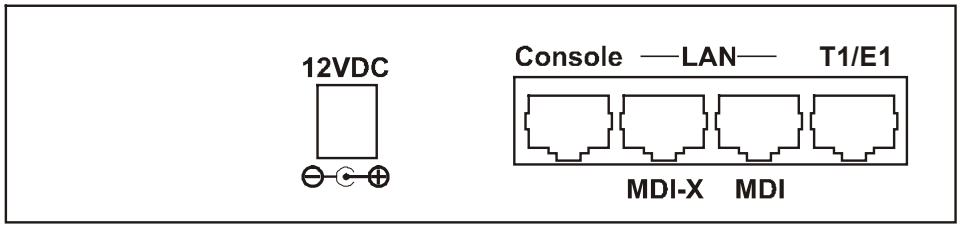


Figure 1 - 4 Rear View of the T1/E1 P850 router

Connect to the Console

Connection to the router operator's console is made through the RJ-45 connector labeled CONSOLE on the back of the 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 P850 router to a computer running an asynchronous communication package or a standard asynchronous terminal. The router supports autobaud rates at 1200, 2400, 9600 or 19,200 bps. The router is managed through the use of "hotkey" Menus.

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

Make the LAN Connections

Connect the P850 router to the LAN with the available LAN interface cable.

The P850 may be connected directly to a wiring hub or Ethernet switch by using the MDI LAN port and a standard 10BaseT cable.

The P850 may be connected directly to a computer network card by using the MDI-X LAN port and a standard 10BaseT cable.

Make the WAN Link Connection

The Universal WAN module may be selected to operate as a V.11, V.35, RS232, or EIA530 interface. The Universal WAN interface module uses a DB25 connector. Be sure to secure the cable connector to the router and the communications equipment with connector screws to prevent accidental disconnection.

WARNING: ensure that the connector cable used with the Universal interface module has the correct pinouts for the operational mode selected for the interface (V.11, V.35, RS232, or EIA530). Using the incorrect cable connector for the operational mode selected may cause permanent damage to the interface module. Please see Appendix D for pinout assignments.

Note: When the P850 router is initially powered up, the Universal WAN will have the default type of "none". Before the link can be

used, it must be configured to the type of connection service that will be used; please see the following section for this procedure.

The V.35 module and Universal WAN module in V.35 mode require interface converters that convert from a DB25 connector to a male 34 pin (V.35) connector used for the V.35 service interface. Be sure to secure the cable connector to the router and the communications equipment with connector screws to prevent accidental disconnection.

The T1/E1 and LX411 CSU-DSU interfaces connect with a standard RJ-45 (RJ-48C specification for T1/E1, RJ-48S specification for CSU/DSU) connector

After the P850 is powered up and the router has established communications with its partner across the WAN, the "Tx" LED will turn green.

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 P850 router. Connect the DC power cord from the supplied power supply to the back of the P850 router and plug the power supply into the AC wall outlet.

Observe the LEDs as the 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.

The console will also display testing and initialization messages as it performs these tasks (if this is the first time the router has been powered up on this console, the display may be unreadable until the next step is performed).

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 P850 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 P850 may be configured to operate within your environment.

Refer to the P850 PPP Menus Reference Manual file on the accompanying CD-ROM for a complete description of all the Menu Options.

Mandatory Configuration

The P850 router 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	

Frame Relay	**PPP Leased Line**	
None	**Frame Relay Disabled**	
	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 P850 router. Also refer to the Menu Reference Manual file on the accompanying CD-ROM for a complete description of all the Menu Options.

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

Setting the Link Interface Type

(Universal WAN only)

The Universal WAN Interface must be configured to match the service to which it will be connected.

WARNING: ensure that the connector cable used with the Universal interface module has the correct pinouts for the operational mode selected for the interface (V.11/X.21, V.35, RS232/V.24, or RS530/RS422). Using the incorrect cable connector for the operational mode selected may cause permanent damage to the interface module. Please see Appendix D for pinout assignments.

Set Link Interface Type:

Location: Main
↳ Configuration
↳ WAN Set Up
↳ Link Set Up
↳ *Link Interface Type*

Select the Service type to which this P850 router will be connected.

Note: If the module is being changed from one type of service to another, you must first select "none" before a new selection may be chosen. Also the link must be toggled through a disable/enable cycle before the change is brought into effect.

Setting the T1/E1 Parameters

(T1/E1 WAN only)

The parameters requred for a T1 or E1 connection may be obtained from your service provider. These may then be entered via the T1/E1 set-up menu to configure the router for that service.

T1/E1 Selection:

Location: Main

↳ Configuration

↳ WAN Set Up

↳ Link Set Up ↳ T1/E1 Set Up

↳ Link mode

T1 or E1

Set the service mode to which this P850 router will be connected.

Service parameters:

Location: Main

↳ Configuration

↳ WAN Set Up

↳ Link Set Up ↳ T1/E1 Set Up

↳ Speed/Channel rate

56/64 kbps

↳ T1/E1framing

framed/unframed/SF/ESF

↳ Line encoding

AMI/INV_AMI/

B8ZS/HDB3

Select the service channel speed, framing format, and encoding as designated by the service provider.

T1 service requires the specification of a Line Build Out factor. This parameter modifies the transmitted signal to compensate for degradation due to line losses between the transmitter and receiver. A number of different options are available to meet standards for T1 long haul (direct connection to service providers central office facility), T1 short haul (connection through a local PBX), AT&T TR64211 specification long haul and AT&T TR64211 short haul. Your service

provider will tell you which specification their service requires. Short haul LBOs are listed as the length of the cable run (in feet) between the router and the local exchange.

E1 service does not require line build out selection.

Set Link Interface Type:
Location: Main
↳ Configuration
↳ WAN Set Up
↳ Link Set Up ↳ T1/E1 Set Up
↳ LBO
as specifed

T1 long-haul LBOs: L0db, L7.5db, L15db, L22.5db

Short haul LBOs: S0to110ft, S110to220ft, S220to330ft, S330to440ft, S440to550ft, S550to660ft

AT&T standard TR64211long-haul connection: TL0db

AT&T standard TR64211 short-haul connection: TS0to110ft, TS110to220ft, TS220to330ft, TS330to440ft, TS440to550ft, TS550to660ft

If fractional T1/E1 service is being provided, you will need to specify the channels/timeslots to be used.

Set Link Interface Type:
Location: Main
↳ Configuration
↳ WAN Set Up
↳ Link Set Up ↳ T1/E1 Set Up
↳ Slot/Channel Set Up
↳ Start
first channel
↳ Number
number of channels

Some E1 service providers reserve timeslot 16 for network management use. If your service specifies that timeslot 16 is for their use, toggle this option to *reserved*

Set Link Interface Type:

Location: Main

↳ Configuration

↳ WAN Set Up

↳ Link Set Up ↳ T1/E1 Set Up

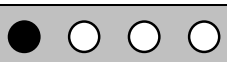
↳ Slot/Channel Set Up

↳ E1 Timeslot 16

reserved

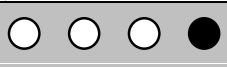
Identify the Status LEDs

The meanings of the four 3-colour Light Emitting Diodes (LEDs) on the front of the P850 router are found in the following chart:

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

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

Green	LINK is up, idle
Green (flashing)	LINK is up transmitting data traffic
Yellow	LINK negotiating - control signals asserted on link
Red	LINK is down (no control signals present)
Tx	

Green	LINK is up, idle
Green (flashing)	LINK is up receiving data traffic
Yellow	LINK negotiating - control signals received from link
Red	LINK is down (no control signals present)
Rx	

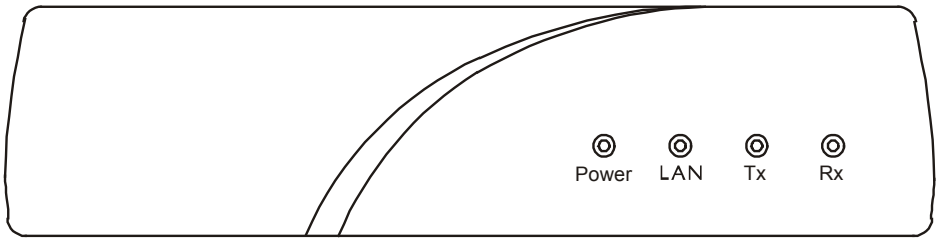


Figure 1-4 Front View of the P850 router

2 - TYPICAL APPLICATIONS & HOW TO CONFIGURE THEM

The P850 is an Ethernet Bridge/Router that supports frame relay RAW 1490 permanent virtual circuits, frame relay encapsulated PPP permanent virtual circuits and PPP leased lines. This section will describe how to set up the P850 using each of its networking functions.

The P850 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 P850 as a combination bridge/router simply configures each of the components separately.

The configuration options described within this section are only for initial set up and configuration purposes. For more information on all of the configuration parameters available, please refer to the P850 PPP Menus Reference Manual file on the accompanying CD-ROM.

Important: The P850 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 values in the built-in menu system. If you wish to save the configuration immediately, enter "=" to jump to the main menu, then select option "6" to save the configuration.

Managing the P850 Using Menus

This section describes the minimum configuration parameters required when setting up the P850. Each of the configuration scenarios requires setting of operational parameters on the P850. The built-in menu system of the P850 is used to configure the unit.

When navigating around the menu system, a new menu or an option may be chosen by simply typing the number associated with the option that you wish to choose. The menu system operates on a "hotkey" principal. Each menu option may be chosen by simply typing the number associated with that option. The P850 will accept the choice and act on it immediately.

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 options value to change.

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 ">". Simply 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, P850 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 is finally 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 provide miscellaneous information on the configuration and set up of the P850.

Configuration: *The Configuration Note is used to indicate that there may be another configuration item that is effected by changing this option.*

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.

The caution icon indicates that caution should be taken when performing this task.

Basic Frame Relay Configuration

North American P850s are configured to have frame relay enabled as the default setting. With frame relay enabled, the router 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 P850 can establish a PVC connection to another frame relay router, at least one PVC must be defined. The P850 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 P850. Refer to the following diagram that shows three P850 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.

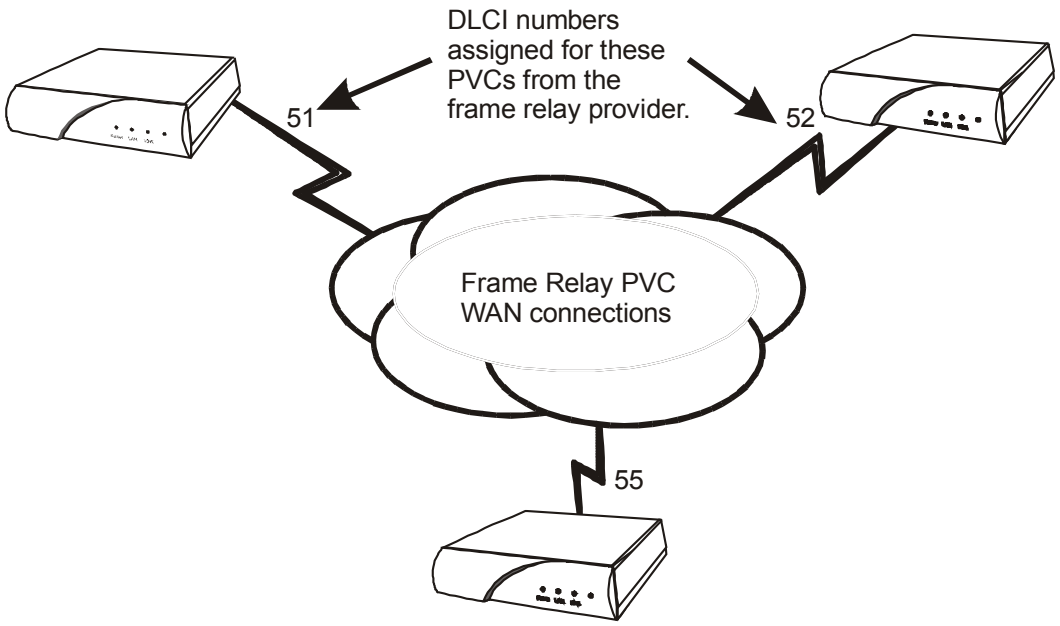


Figure 2 - 1 Frame Relay configuration

Configuration: The default configuration for P850s shipped outside North American is to have frame relay disabled. To run frame relay on these routers, it must first 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".

For an P850 with a CSU-DSU interface, the default clock speed that the P850 will expect to receive from the DCE link is 64Kbps. If the DCE link is 56 Kbps, then the Link Speed value must be reset to 56 here.

Link Speed

Location: Main
↳ Configuration
↳ WAN Set up
↳ Link Set up
↳ *Link Speed*
56

Auto Learning the Frame Relay Configuration

The P850 is pre-configured to query the frame relay service to auto-learn the LMI type and the PVC DLCI numbers. This auto-learn function allows the P850 to be plugged into the frame relay service and auto-learn the PVC configuration to become operational without further manual configuration.

Manual configuration is also allowed by modifying the options within each Remote Site Profile and the individual link configuration menus.

When the P850 first starts up it will query the frame relay service to try 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 P850 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 P850 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.

Manual Configuration - LMI Type

The LMI Type option allows you to manually specify the type of Link Management Interface in use by the Frame Relay service provider for the Frame Relay service.

When the LMI type is set to none, the P850 simply creates frame relay packets and sends them on the defined PVC's. The links are not checked for errors. There is no congestion control checking. The link is only monitored for control signals.

To manually configure the LMI type the Auto-Learning option must be disabled.

Auto-Learning

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

LMI Type

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

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 P850 PPP Menus Reference Manual file on the accompanying CD-ROM.

"Quick Start" Frame Relay

Since the P850 auto-learns the frame relay configuration, only a couple of parameters need to be configured before the unit is fully operational as an IP router for frame relay.

Upon initial start up, the P850 is pre-configured to query the frame relay service to auto-learn the LMI type and the PVC DLCI numbers. The P850 will then automatically create a remote site profile for each PVC.

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 P850 will bridge and IPX route data without any user configuration. Because an IP router requires an IP address, the P850 must be configured with an IP address before IP routing is fully operational.

To configure an IP address for the P850, 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 P850 PPP Menus Reference Manual file on the accompanying CD-ROM.

Basic Leased Line Configuration

P850s shipped outside North America are configured to have a default setting as a leased line router. The P850 will operate as a PPP leased line bridge/router if the frame relay function is disabled. The Leased Line P850 establishes PPP (Point to Point Protocol) WAN connections to other PPP Leased Line P850 units or to other vendors PPP leased line routers via direct leased line connections.

Configuration: *The default configuration for North American P850 is to have frame relay enabled. 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".

"Quick Start" PPP Leased Line Connections

The PPP Leased Line P850 requires only a few configuration parameters to establish a direct connection to another PPP IP router.

Once the connection is established and is working properly, the P850 **should be configured** with a **remote site profile** entry for that vendors router.

Before the P850 can establish a link connection to another PPP router, the link speed information must be defined. Refer to the following diagram that shows an P850 unit and another vendors unit connected together with a direct leased line connection.

Figure 2 - 2 Basic PPP Leased Line Configuration

The following steps must be performed on the P850 unit.

Link Speed

Location: Main
↳ Configuration
↳ WAN Set up
↳ Link Set up
↳ *Link Speed*

The clock speed that the P850 will expect to receive from the DCE link device must be defined.

Local IP Address

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

This is the IP address and subnet mask for the link of this P850 in the unnumbered IP connection.

Bridge Connection.

Once the link speeds have been configured, the P850 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.

Once the link speeds and local IP address have been configured, the P850 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 the P850.

IPX Router Connection

Once the link speeds have been configured, the P850 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 P850 PPP Menus Reference Manual file on the accompanying CD-ROM.

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 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.

Configure as an Ethernet Bridge

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

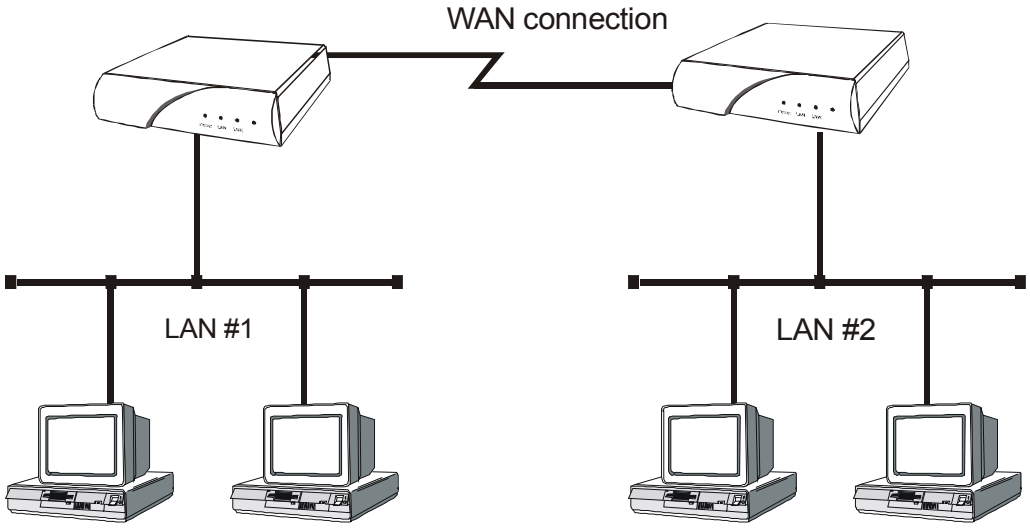


Figure 2 - 3 Bridged Local Area Networks

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 P850 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 P850 will bridge Ethernet traffic to its partner bridges when the Wide Area Network (WAN) connection has been established.

The P850 router 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 P850 router. Once IPX routing has been disabled, all IPX traffic will be bridged between partner bridges on the WAN.

The two Local Area Networks may be bridged together with minimal configuration required. Simply connect the P850s to each of the LANs and connect the interface module to the supplied equipment from the service provider. The WAN set up must be configured appropriately in order for the links to operate. Once the WAN connection has been established to the remote partner P850, the P850 will proceed to bridge the LAN traffic between the two locations.

If SNMP or Telnet management is required for the P850, an IP address must be defined for each P850. The IP address allows network management stations to use SNMP to configure and monitor the P850 remotely. The IP address also allows Telnet stations to connect to the P850 and view the built-in menu system without having to physically connect to the device.

IP Address

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

The IP address consists of four 8-bit numbers and is represented by 4 fields separated by periods ("**.**"), where each field is specified by a decimal number (e.g. 199.169.1.10). Each decimal number must be less than or equal to 255 (the maximum value of an 8-bit field).

The IP address is first specified and then you will be prompted to enter the size of the subnet mask.

The size of the subnet mask. defines the subnet mask by using the specified number to reserve a series of contiguous bit locations from the start of the entire IP address. These reserved bit locations are then used as the network portion of the IP address.

For example, with a class C IP address, a subnet mask size of 26 will mask the 24 network address bits plus 2 host bits for the subnet address, resulting in 4 subnet addresses being created. (Note that depending on whether or not nonstandard subnets are allowed, not all of these addresses may be valid; see the sections on defining masks).

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 P850 PPP Menus Reference Manual file on the accompanying CD-ROM.

Configure as an Ethernet IP Router

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

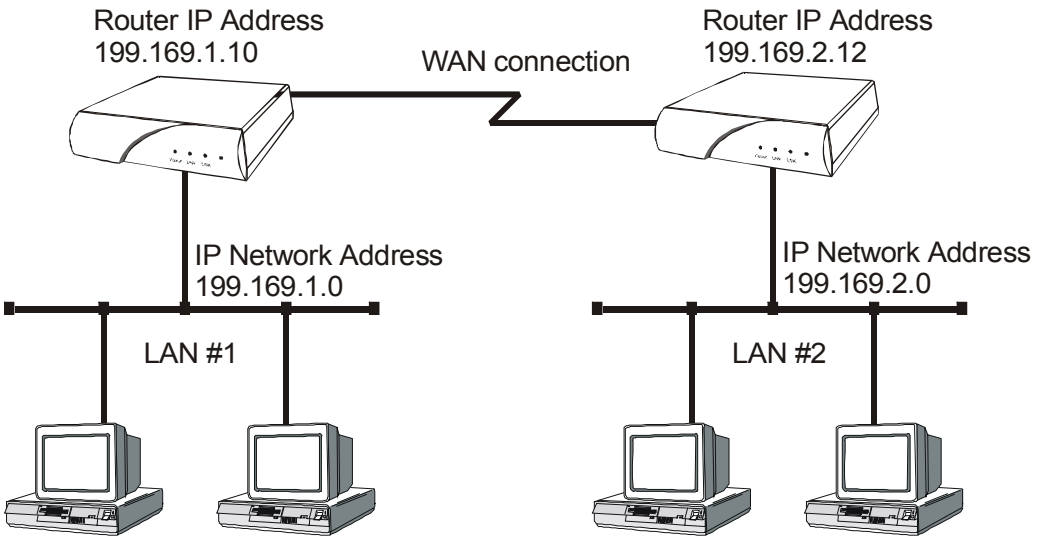


Figure 2 - 4 IP Routed Local Area Networks

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 tables. Once the destination IP network is found in the routing tables, the IP router sends the IP frame to the remote partner P850 that is connected to the appropriate remote IP network. If no explicit route entry is found in the routing tables, the IP frame is sent to the Default Gateway.

To configure the P850 to be an IP router, the following parameters must be defined in the built-in menu system.

IP Address

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

The IP address consists of four 8-bit numbers and is represented by 4 fields separated by periods ("**.**"), where each field is specified by a decimal number (e.g. 199.169.1.10). Each decimal number must be less than or equal to 255 (the maximum value of an 8-bit binary number).

The IP address is first specified and then you will be prompted to enter the Subnet mask size.

The Subnet mask size defines the subnet mask by using the specified number to reserve a series of contiguous bit locations from the start of the entire IP address. These reserved bit locations are then used as the network portion of the IP address for the subnet.

For example, with a class C IP address, a subnet mask size of 26 will mask the 24 network address bits plus 2 host bits for the subnet address, resulting in 4 subnet addresses being created. (Note that depending on whether or not nonstandard subnets are allowed, not all of these addresses may be valid; see the sections on defining masks).

The *default gateway* parameter only needs to be defined when there is another IP router connected to the LAN that is the default gateway for this IP network.

Once the WAN connections have been established to the remote partner P850s, the IP router portion of the P850s will begin to build their routing tables according to the IP frames they receive from the network. Manual entries may be made in the routing tables by adding *static IP routes*.

Define an IP Default Gateway

An IP default gateway is an IP router that is resident on the local IP network that this P850 is connected to and is used to route IP frames for destination networks that do not exist in the routing tables. When an IP frame is received that is destined for a network that is not listed in the routing tables of the P850, the P850 will send the IP frame to the default gateway. If the device originating the IP frame is on the same local LAN as the P850, the P850 will then send an ICMP redirect message to the originating device. Any future IP frames for that destination network will then be sent to the default gateway instead of the P850.

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 P850s on the local LAN would have the Internet access router as the default gateway. The P850s would route information within the internal network and any IP frames that are destined for the Internet would be routed to the default gateway.

Default Gateway

Location: Main
↳ Configuration
↳ Application Set up
↳ DHCP Set up
↳ *Default Gateway*

The IP address of the default gateway consists of 4 octets and is represented by 4 fields separated by periods ("**.**"), where each field is specified by a decimal number (e.g. 199.169.1.10). Each decimal number must be less than or equal to 255, that is the maximum value of each 8-bit field.

A configured Default Gateway will override a default route learned from RIP.

Configuration: *The Default Gateway may be located across the WAN connection.*

Define an IP Static Route

Static IP routes may be defined when one specific router is to be used to reach a destination IP 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
        - Edit Static Route
          - *Remote Site*
          - *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 all of the static IP routes are defined they may be viewed with the *Show Static Routes* command from the IP Routes menu.

Configuration: *When the IP routing protocol is set to none, 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.*

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 P850 PPP Menus Reference Manual file on the accompanying CD-ROM.

Define an IP Subnet Mask

An IP network may be divided into smaller portions by a process called sub-netting. A subnet is specified using high end bits of the host field of the IP address for network addressing. This is done with a subnet mask. Thus, the size of the subnet (i.e. The number of bits available for subnet addressing) is the size of the subnet mask minus the length of the network field of the IP address for that class (8, 16 or 24 bits for classes A, B and C respectively). 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. Their network will be attached to the Internet with an IP router.

If this company 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.

The P850 allows masks from 8 to 32 bits. The mask size determines how many bits of the host field of the original IP network address will be used for the creation of subnets. In this example, a subnet mask size of 26 will produce a subnet size of 2 bits (24 bits from the class C network address field plus 2 bits from the host address field). 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 mask of 26 will generate two resulting sub-networks with up to 62 host addresses each (64 potential addresses minus the all zero and all one addresses). The new IP network addresses will be: 199.169.100.64 and 199.169.100.128. The subnet mask for the newly created networks will be 255.255.255.192..

Configuration: *The mask size entered defines the size of the subnet mask from the* ***start*** *of the entire IP address. This allows subnet sizes from 0 to 24 bits. A subnet mask size of 8 in a class A address represents a subnet size of 0 or no subnetting performed.*

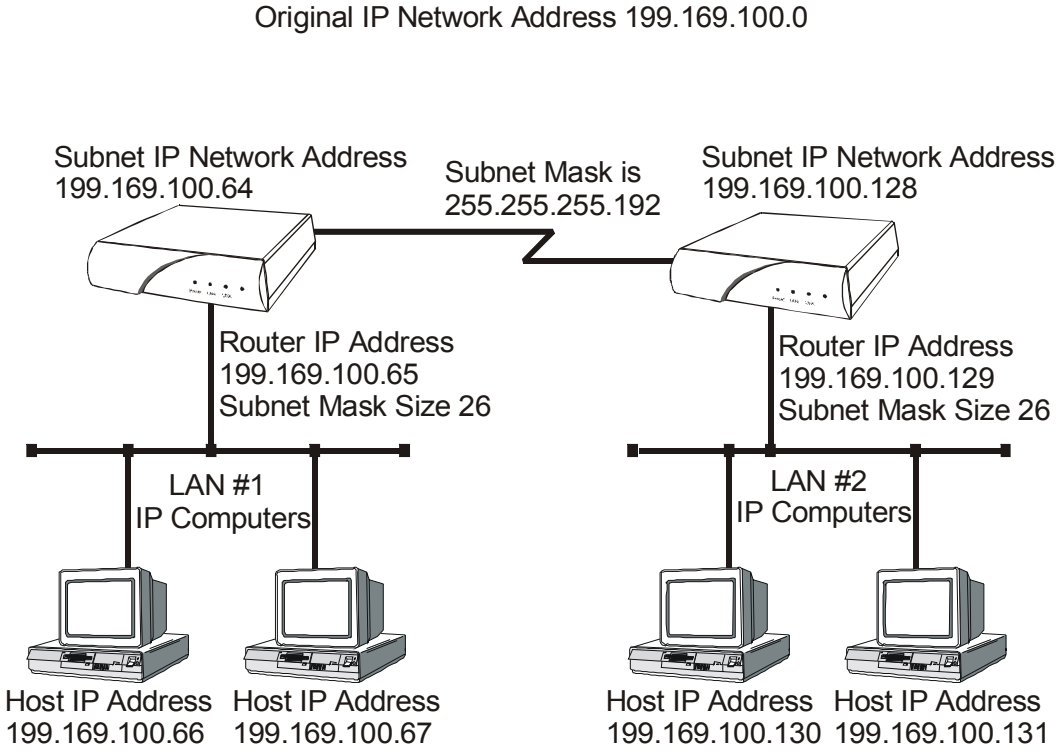


Figure 2 - 5 Defining an IP Subnet Mask

To configure the P850 routers to route between the newly created sub-networks, the following parameters must be defined in the built-in menu system.

IP Address & Subnet Size

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

The IP address consists of 4 octets and is represented by 4 fields separated by periods ("**.**"), where each field is specified by a decimal number (e.g. 199.169.1.10). Each decimal number must be

less than or equal to 255, that is the maximum value of each 8-bit field.

The IP address is first specified and then you will be prompted to enter the mask size.

The mask size defines the subnet mask by using the specified number to reserve a series of contiguous bit locations from the start of the entire IP address. These reserved bit locations are then used as part of the network portion of the IP address.

For example, with a class C IP address, a subnet size of 26 will provide 2 host bits for the subnet address resulting in 4 possible subnets. The addresses for two of these are all ones or all zeros and are not valid under standard subnets, leaving two subnets available.

Configuration: *The subnet mask size entered defines the size of the subnet mask from the* ***start*** *of the entire IP address.*

The configuration of the sub-netted class C IP network is now completed. Remember that each of the 2 sub-networks created may only have 62 host IP addresses defined.

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 P850 PPP Menus Reference Manual file on the accompanying CD-ROM.

Configure as an Ethernet IPX Router

The P850 is preconfigured to operate as an IPX router when installed in an IPX network. The P850 router will learn the IPX network numbers from the local LAN and when the WAN connections are established, the P850 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 P850 IPX 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.

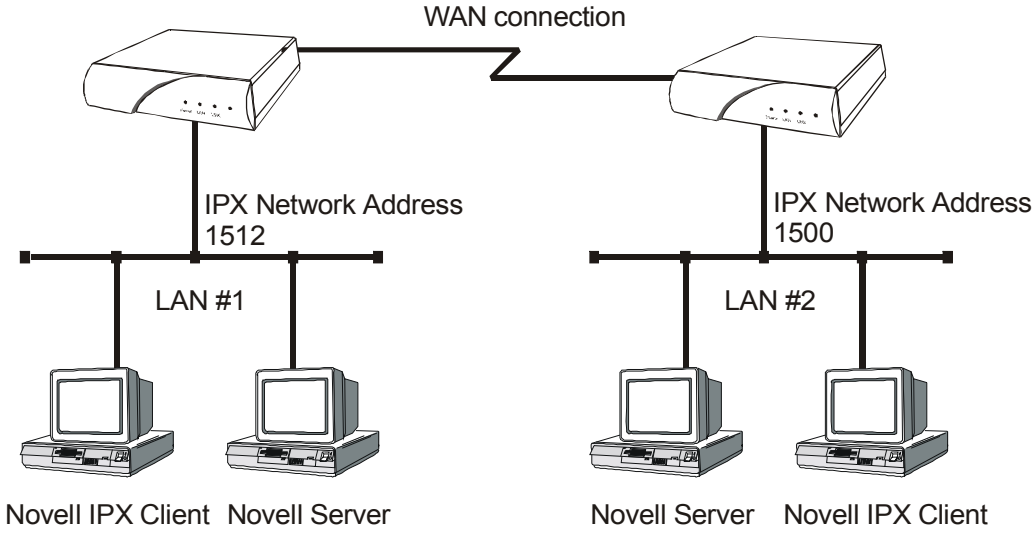


Figure 2 - 7 IPX Routed Local Area Networks (Servers on both sides)

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 P850 router that is connected to the appropriate remote IPX network.

To configure the P850 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 P850 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 P850 routers, the IPX router portion of the P850 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*.

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 P850 PPP Menus Reference Manual file on the accompanying CD-ROM.

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 P850 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 P850 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 P850 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 P850. After the P850s 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 P850 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 P850 will respond with the list of servers that are located on the central LAN.

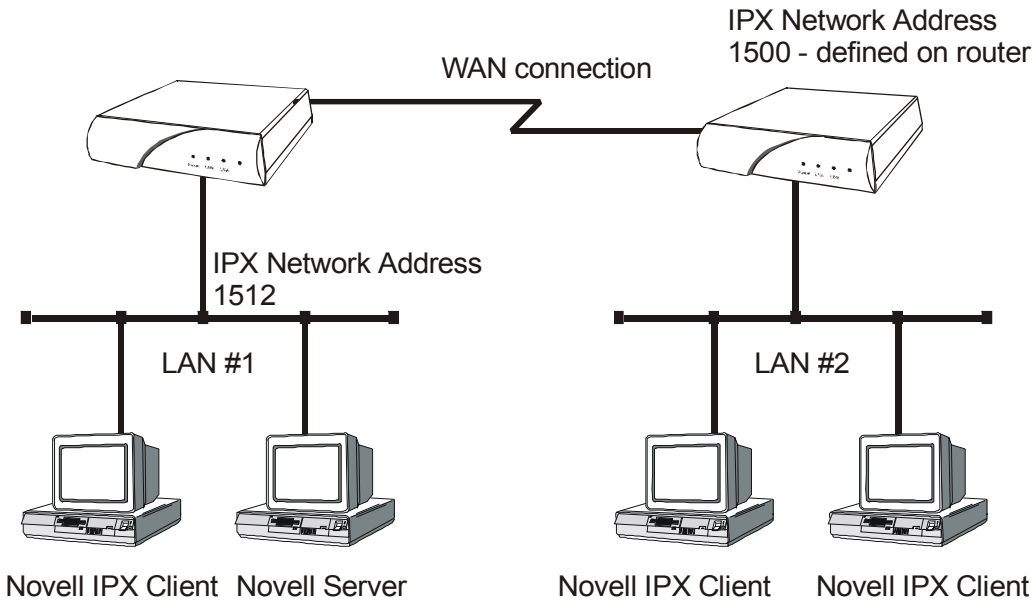


Figure 2 - 8 IPX Routed Local Area Networks (Servers on one side)

The following steps must be performed on the P850 router connected to LAN #2.

IPX Frame Types

Location: Main
- Configuration
  - IPX Routing Set up
    - Configure LAN Nets
      - *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.

Configuration: *Since there is not a server on LAN 2 in this example, the IPX network number may be manually configured and the P850 router will proceed to route between the two networks. When manually configuring an IPX network number for a frame type that has already learned a network number, IPX routing must be disabled before the new network number is assigned.*

PPP Link Configuration Overview

A PPP (Point to Point Protocol) connection between two routers may use a number of Network Control Protocols (NCP) for communication. An IP router connection will use the Internet Protocol Control Protocol (IPCP) NCP for all IP communications. An IPX router connection will use the Internet Packet Exchange Control Protocol (IPXCP) NCP 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 than 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 than 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. 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. The WAN IP network number is defined by defining a subnet size to use when defining the local IP address. The size of the subnet 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 IP 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.

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 P850 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.

Configure Dynamic Host Configuration Protocol

The P850 uses Dynamic Host Configuration Protocol (DHCP) to allow users in a small office environment to simply enable DHCP clients on their workstations and power them up to get their proper initialization. You would then be able to use TCP/IP applications (such as connecting to the Internet). DHCP allows configuration of devices (DHCP clients) to be handled from a central DHCP server. This allows devices 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. It is designed to allocate network addresses to a number of hosts on the P850's LAN and supply minimal configuration needed to allow hosts to operate in an IP network.

The following steps must be performed on the P850 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 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
↳ *IP Address / number of addresses*

The IP address pool option requires having the first IP address in the range that is wanted for the devices attached to the DHCP Server to be set. 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.

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
↳ Application Set up
↳DHCP set-up
↳DNS set-up
↳Primary DNS
-IP address local DNS server
↳Secondary DNS
-IP addr external DNS server

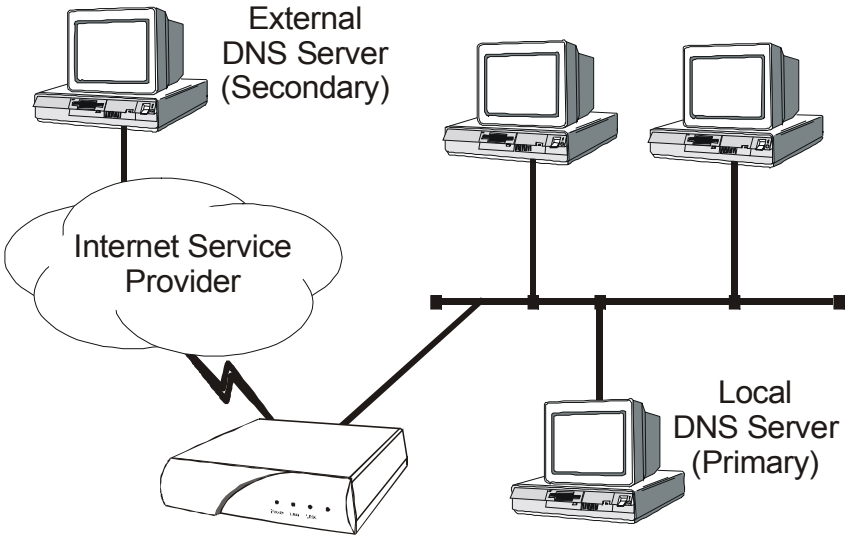


Figure 2 - 9 Local + External DNS Server Configuration

Configure Network Address Translation (NAT)

Support is provided for Network Address Translation (NAT). Network Address Translation is a technique which translates private IP addresses on a private network to valid global IP addresses for access to the Internet. Port translation (NAPT) allows more than one private IP address to 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 NAPT 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.*

The NAT enabled option allows you to enable Network Address Translation.

NAT Enabled

Location: Main
- Configuration
  - WAN Set up
    - Remote Site Set up
      - Edit Remote Site
        - Protocol Set up
          - IP Parameters
            - NAT Enabled
              - *Enabled*

The Translation Type option allows you to use Network Address Port Translation.

Translation type

Location: Main

↳ Configuration
↳ WAN Set up
↳ Remote Site Set up
↳ Edit Remote Site
↳ Protocol Set up
↳ IP Parameters
↳ NAT Advanced
↳ Translation type
↳ *Port*

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 P850 PPP Menus Reference Manual file on the accompanying CD-ROM.

Configure PPP Security

The P850 provides support for both PAP and CHAP PPP security authentication. An outgoing user name, PAP password , and CHAP secret are defined that the P850 will use when responding to an authentication request from a remote site PPP router.

The cold start defaults for the security user name and passwords are as follows. These defaults will exist when the P850 is first started before and configuration is entered, and after a Full Reset has been performed. These default values are also set when the P850 is placed in TFTP Network load mode for upgrading the operating software via TFTP transfers. Care should be taken when upgrading a group of P850s that have security levels set.

Default user name is the same as the default device name.

Default PAP password and CHAP secret are both set to "none".

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 P850 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 P850, an entry for each remote site PPP router that may be connected to this P850 **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.

Security Database Entry

Location: Main

↳ Configuration

↳ WAN Set up

↳ Edit Remote Site

↳ Security Parameters ↳ Incoming *PAP Password* ↳ Incoming *CHAP Secret*

↳ Outgoing *User Name*

↳ Outgoing *PAP Password*

↳ Outgoing *CHAP Secret*

The security entries in the security database define the user names and passwords that remote site PPP routers will provide when an authentication request is sent from this P850.

When defining the user names for the PPP routers that will be connecting together, you should remember that the remote site PPP router user name that is authenticated by the P850 is used to match to the configured remote site profiles.

If a match to a configured remote site profile exists, the incoming call will use the configuration defined within that remote site profile. This also allows easier viewing of the remote site statistics.

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 P850 PPP Menus Reference Manual file on the accompanying CD-ROM.

Configure Firewall

The P850 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 P850; incoming traffic is from the network in question to the P850, outgoing is from the P850 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 links.

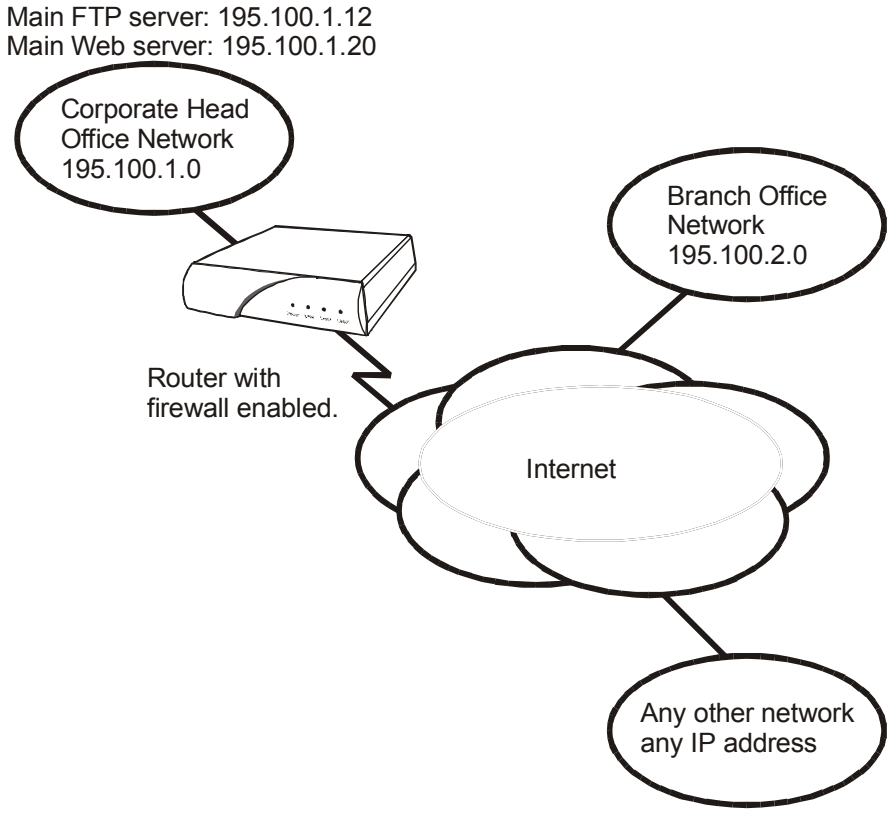


Figure 2-10 Sample Firewall Application

The above diagram shows a corporate head office network, which is connected, to the Internet with an P850. 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 P850 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 P850 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 P850.

⌨ *Firewall LAN Filter Direction*

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

An entry is made in the firewall table to allow the devices in the branch office 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

Applications

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 P850 PPP Menus Reference Manual file on the accompanying CD-ROM.

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*

Applications

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*

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 Set-up
      - Queuing Strategy
        - *Priority*
        - *Priority List Number*

To assign a Priority List to a Remote Site Configuration

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

3 - INTRODUCTION TO FILTERING

The P850 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 P850 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 P850 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 P850. 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 P850 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 P850 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

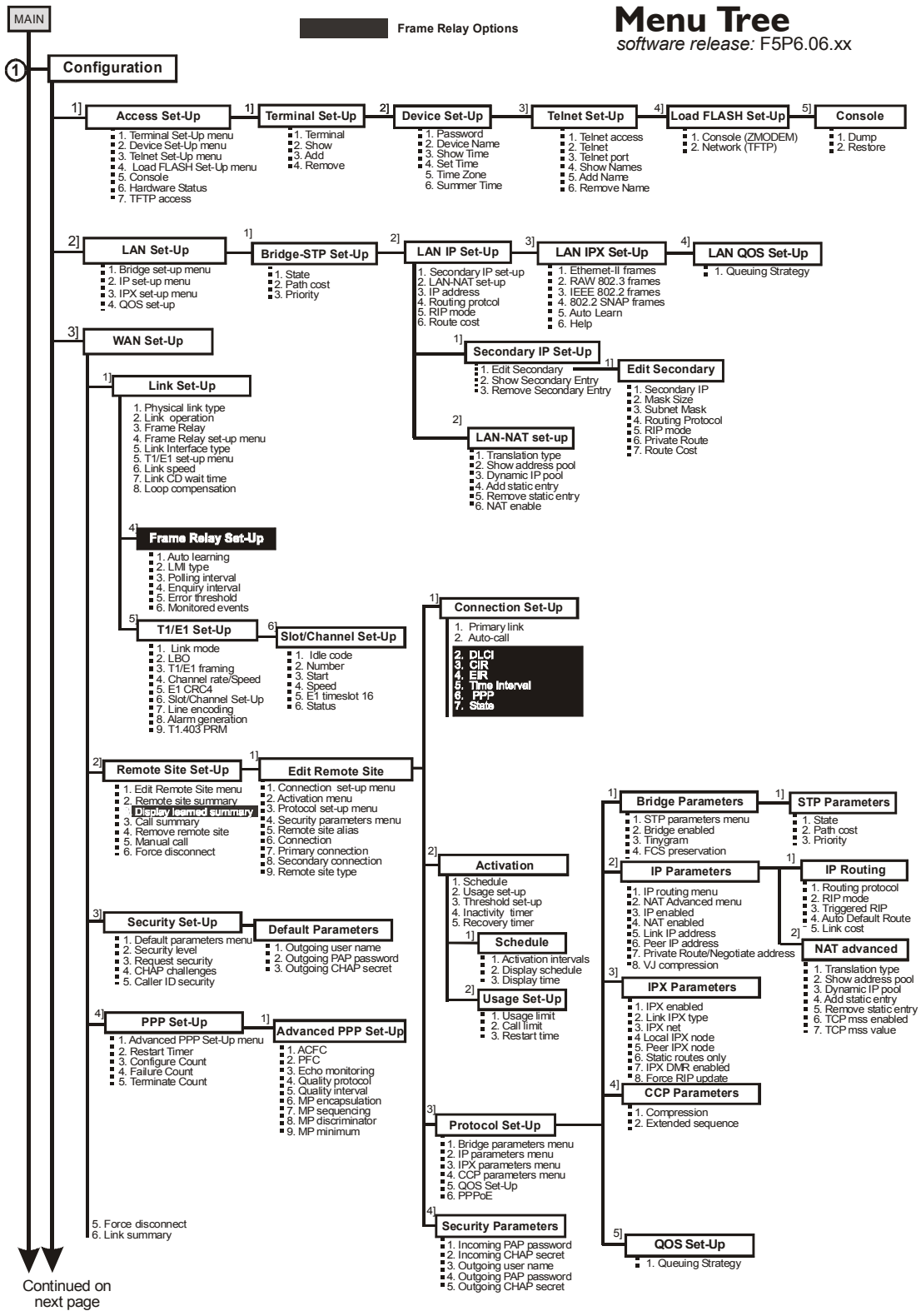
Other interesting TCP Ports		
Decimal	Hex	Usage
21	15	FTP
23	17	Telnet
25	19	SMTP
69	45	TFTP
109	6D	POP2
110	6E	POP3

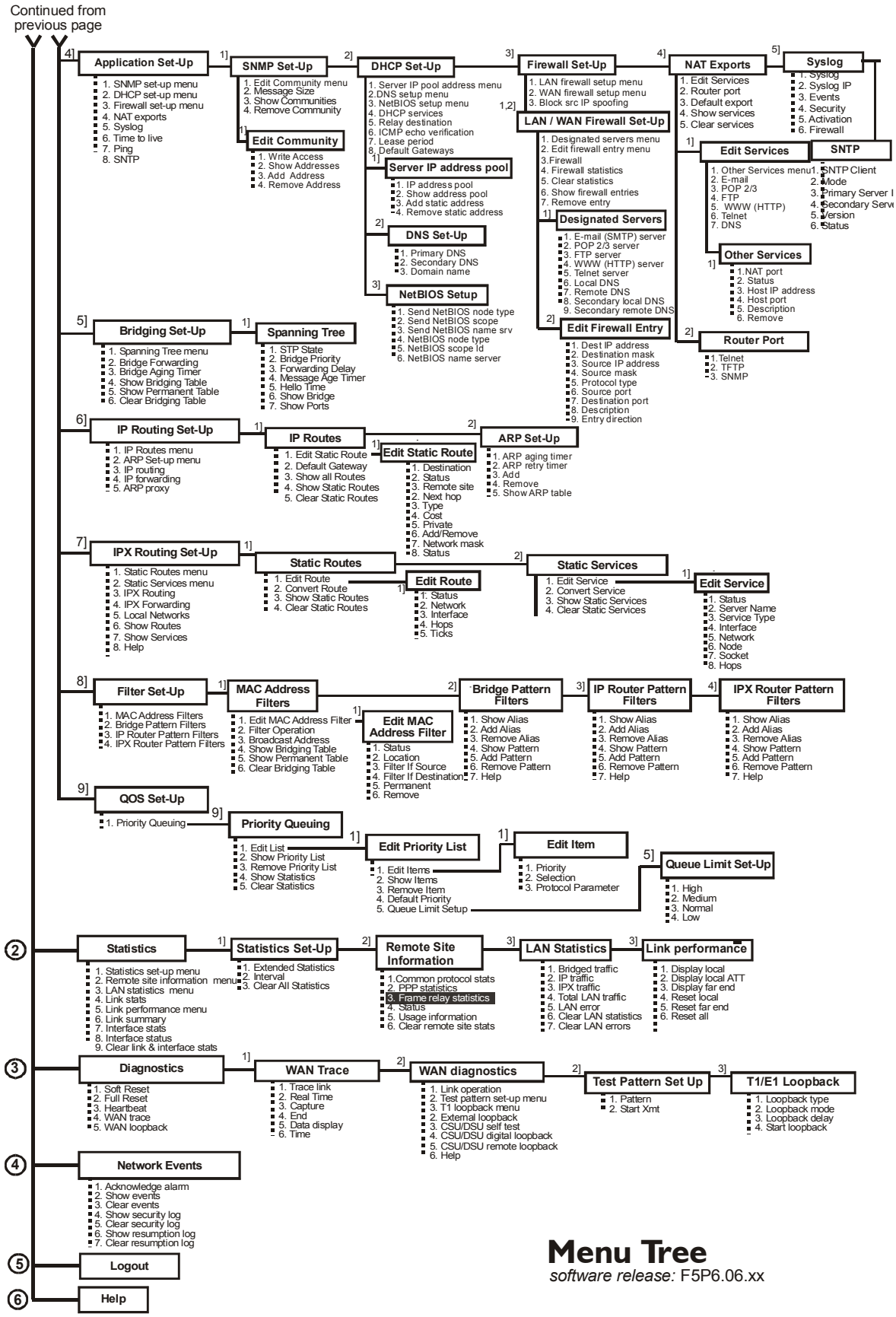
APPENDIX A
MENU TREES

The menu trees on the next few facing pages are a graphical representation of the hierarchy of the built-in menu system of the P850. 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 P850 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.


MAIN
Frame Relay Options
Menu Tree
software release: F5P6.06.xx
1 Configuration
1] Access Set-Up
1. Terminal Set-Up menu
2. Device Set-Up menu
3. Telnet Set-Up menu
4. Load FLASH Set-Up menu
5. Console
6. Hardware Status
7. TFTP access
1] Terminal Set-Up
1. Terminal
2. Show
3. Add
4. Remove
2] Device Set-Up
1. Password
2. Device Name
3. Show Time
4. Set Time
5. Time Zone
6. Summer Time
3] Telnet Set-Up
1. Telnet access
2. Telnet
3. Telnet port
4. Show Names
5. Add Name
6. Remove Name
4] Load FLASH Set-Up
1. Console (ZMODEM)
2. Network (TFTP)
5] Console
1. Dump
2. Restore
2] LAN Set-Up
1. Bridge set-up menu
2. IP set-up menu
3. IPX set-up menu
4. QOS set-up
1] Bridge-STP Set-Up
1. State
2. Path cost
3. Priority
2] LAN IP Set-Up
1. Secondary IP set-up
2. LAN-NAT set-up
3. IP address
4. Routing protocol
5. RIP mode
6. Route cost
3] LAN IPX Set-Up
1. Ethernet-II frames
2. RAW 802.3 frames
3. IEEE 802.2 frames
4. 802.2 SNAP frames
5. Auto Learn
6. Help
4] LAN QOS Set-Up
1. Queuing Strategy
1] Secondary IP Set-Up
1. Edit Secondary
2. Show Secondary Entry
3. Remove Secondary Entry
1] Edit Secondary
1. Secondary IP
2. Mask Size
3. Subnet Mask
4. Routing Protocol
5. RIP mode
6. Private Route
7. Route Cost
2] LAN-NAT set-up
1. Translation type
2. Show address pool
3. Dynamic IP pool
4. Add static entry
5. Remove static entry
6. NAT enable
3] WAN Set-Up
1] Link Set-Up
1. Physical link type
2. Link operation
3. Frame Relay
4. Frame Relay set-up menu
5. Link Interface type
5. T1/E1 set-up menu
6. Link speed
7. Link CD wait time
8. Loop compensation
4] Frame Relay Set-Up
1. Auto learning
2. LMI type
3. Polling interval
4. Enquiry interval
5. Error threshold
6. Monitored events
5] T1/E1 Set-Up
1. Link mode
2. LBO
3. T1/E1 framing
4. Channel rate/Speed
5. E1 CRC4
6. Slot/Channel Set-Up
7. Line encoding
8. Alarm generation
9. T1.403 PRM
6] Slot/Channel Set-Up
1. Idle code
2. Number
3. Start
4. Speed
5. E1 timeslot 16
6. Status
2] Remote Site Set-Up
1. Edit Remote Site menu
2. Remote site summary
Display learned summary
3. Call summary
4. Remove remote site
5. Manual call
6. Force disconnect
1] Edit Remote Site
1. Connection set-up menu
2. Activation menu
3. Protocol set-up menu
4. Security parameters menu
5. Remote site alias
6. Connection
7. Primary connection
8. Secondary connection
9. Remote site type
3] Security Set-Up
1. Default parameters menu
2. Security level
3. Request security
4. CHAP challenges
5. Caller ID security
Default Parameters
1. Outgoing user name
2. Outgoing PAP password
3. Outgoing CHAP secret
4] PPP Set-Up
1. Advanced PPP Set-Up menu
2. Restart Timer
3. Configure Count
4. Failure Count
5. Terminate Count
1] Advanced PPP Set-Up
1. ACFC
2. PFC
3. Echo monitoring
4. Quality protocol
5. Quality interval
6. MP encapsulation
7. MP sequencing
8. MP discriminator
9. MP minimum
5. Force disconnect
6. Link summary
1] Connection Set-Up
1. Primary link
2. Auto-call
2. DLCI
3. CIR
4. EIR
5. Time Interval
6. PPP
7. State
2] Activation
1. Schedule
2. Usage set-up
3. Threshold set-up
4. Inactivity timer
5. Recovery timer
1] Schedule
1. Activation intervals
2. Display schedule
3. Display time
2] Usage Set-Up
1. Usage limit
2. Call limit
3. Restart time
3] Protocol Set-Up
1. Bridge parameters menu
2. IP parameters menu
3. IPX parameters menu
4. CCP parameters menu
5. QOS Set-Up
6. PPPoE
4] Security Parameters
1. Incoming PAP password
2. Incoming CHAP secret
3. Outgoing user name
4. Outgoing PAP password
5. Outgoing CHAP secret
1] Bridge Parameters
1. STP parameters menu
2. Bridge enabled
3. Tinygram
4. FCS preservation
1] STP Parameters
1. State
2. Path cost
3. Priority
2] IP Parameters
1. IP routing menu
2. NAT Advanced menu
3. IP enabled
4. NAT enabled
5. Link IP address
6. Peer IP address
7. Private Route/Negotiate address
8. VJ compression
1] IP Routing
1. Routing protocol
2. RIP mode
3. Triggered RIP
4. Auto Default Route
5. Link cost
2] NAT advanced
1. Translation type
2. Show address pool
3. Dynamic IP pool
4. Add static entry
5. Remove static entry
6. TCP mss enabled
7. TCP mss value
3] IPX Parameters
1. IPX enabled
2. Link IPX type
3. IPX net
4 Local IPX node
5. Peer IPX node
6. Static routes only
7. IPX DMR enabled
8. Force RIP update
4] CCP Parameters
1. Compression
2. Extended sequence
5] QOS Set-Up
1. Queuing Strategy
Continued on next page


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
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
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
SNTP
1. SNTP Client
2. Mode
3. Primary Server I
4. Secondary Serve
5. Version
6. Status
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
9] 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 Item
4. Default Priority
5. Queue Limit Setup
1] Edit Item
1. Priority
2. Selection
3. Protocol Parameter
5] Queue Limit Set-Up
1. High
2. Medium
3. Normal
4. Low
2 Statistics
1. Statistics set-up menu
2. Remote site information menu
3. LAN statistics menu
4. Link stats
5. Link performance menu
6. Link summary
7. Interface stats
8. Interface status
9. 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. Frame relay statistics
4. Status
5. Usage information
6. 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
3] Link performance
1. Display local
2. Display local ATT
3. Display far end
4. Reset local
5. Reset far end
6. Reset all
3 Diagnostics
1. Soft Reset
2. Full Reset
3. Heartbeat
4. WAN trace
5. WAN loopback
1] WAN Trace
1. Trace link
2. Real Time
3. Capture
4. End
5. Data display
6. Time
2] WAN diagnostics
1. Link operation
2. Test pattern set-up menu
3. T1 loopback menu
2. External loopback
3. CSU/DSU self test
4. CSU/DSU digital loopback
5. CSU/DSU remote loopback
6. Help
2] Test Pattern Set Up
1. Pattern
2. Start Xmt
3] T1/E1 Loopback
1. Loopback type
2. Loopback mode
3. Loopback delay
4. Start loopback
4 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
5 Logout
6 Help
Menu Tree
software release: F5P6.06.xx

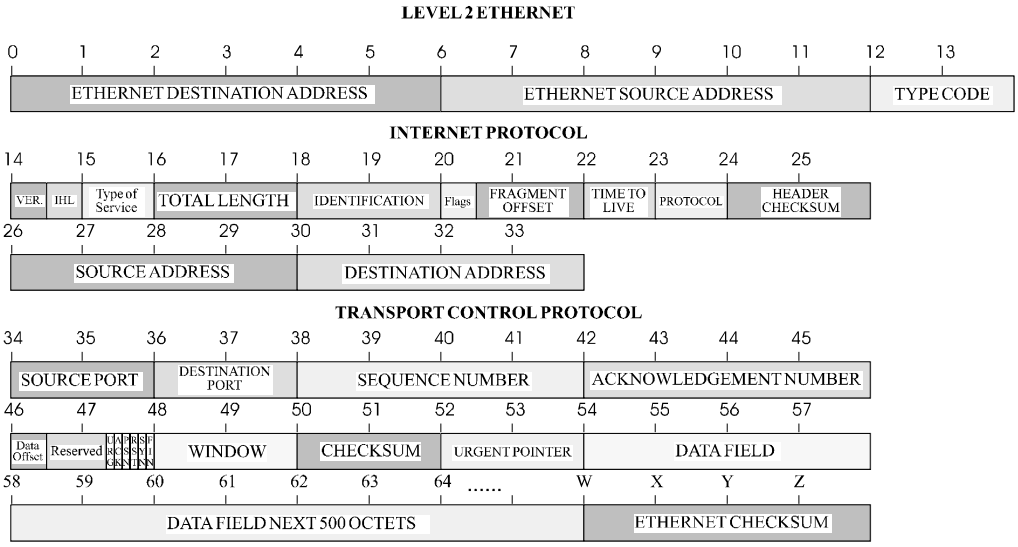
APPENDIX B
OCTET LOCATIONS ON ETHERNET FRAMES

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.

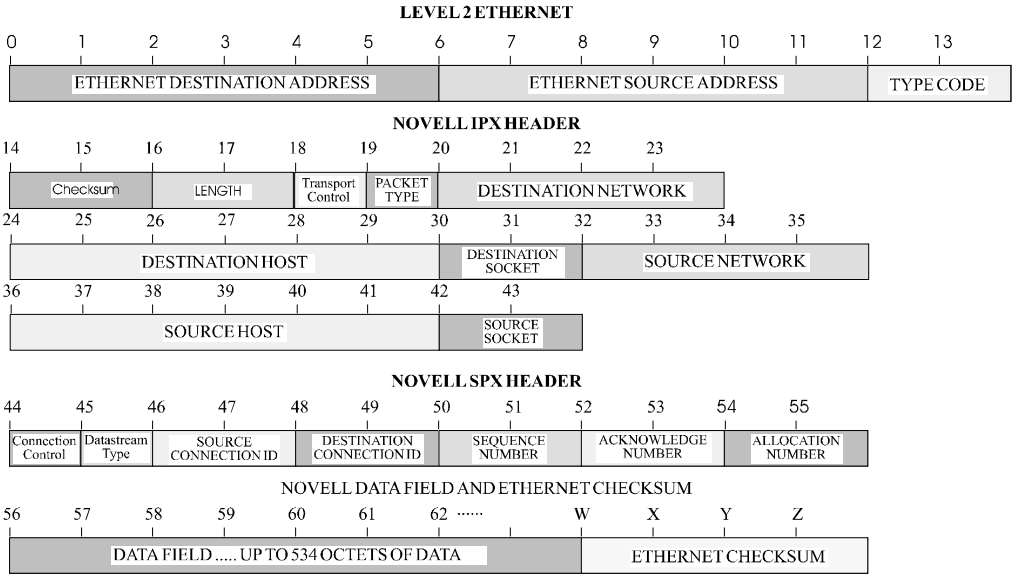
Note the differences in the TCP/IP and Novell frames when bridging and when routing. When routing, the TCP/IP and Novell frames are examined after the Level 2 Ethernet portion of the frame has been stripped from the whole data frame. This means that the offset numbers now start from 0 at the beginning 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



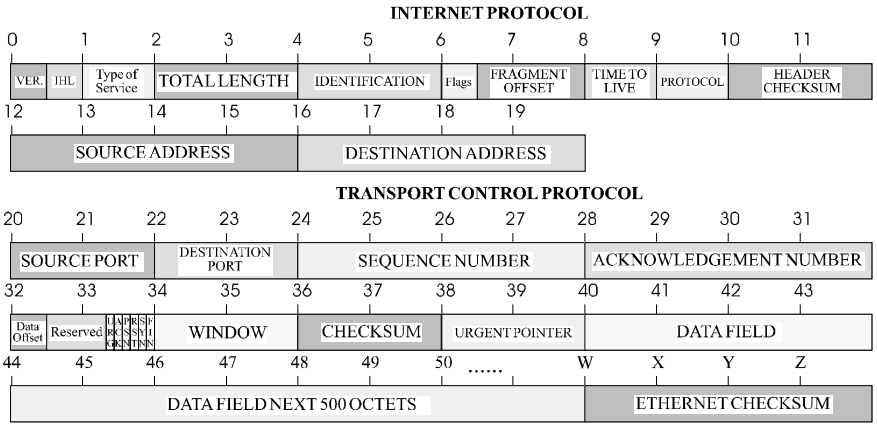
Octet Locations on a Bridged Novell Netware Frame



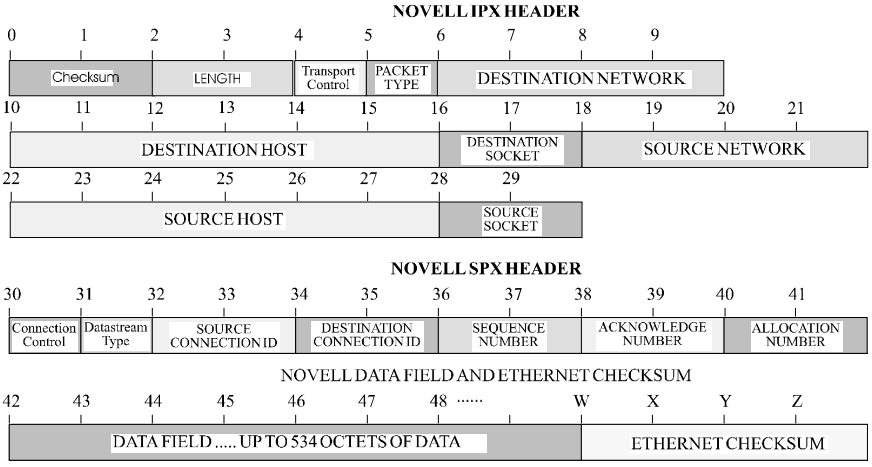
ETHERNET Type Codes

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

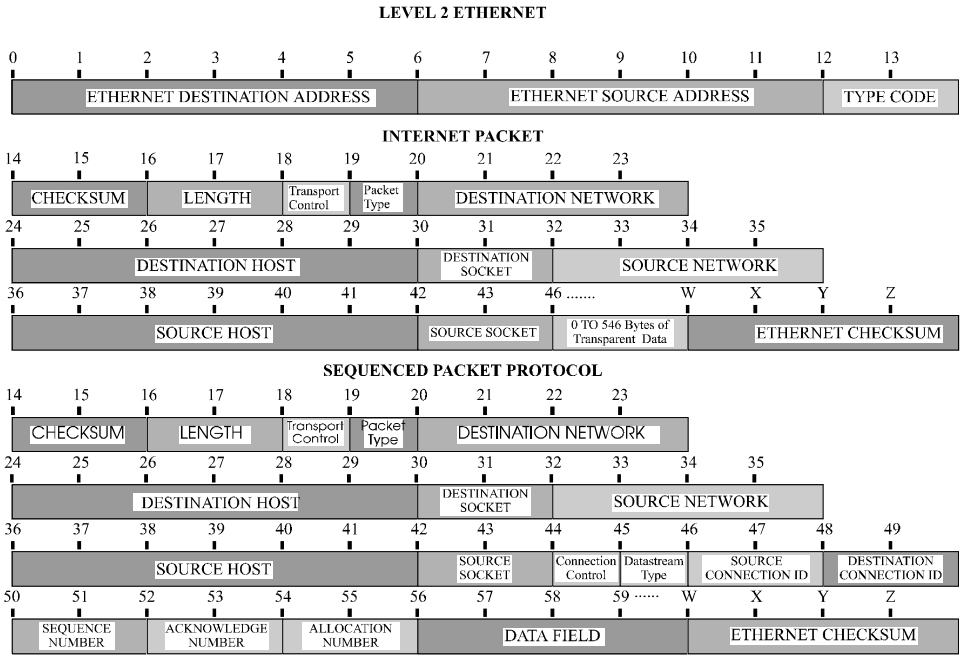
Octet Locations on an IP Routed TCP/IP Frame



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 bridge/router.

Geraetesteckvorrichtung trennen vor den Wartung.

Opening the case

1) Remove power from the bridge/router and remove the other cabling.
2) Turn the bridge/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 bridge/router right side up.
5) Lift off the top half of the case.

Identifying the Internal Components

The major components and the jumper strap positions are shown:

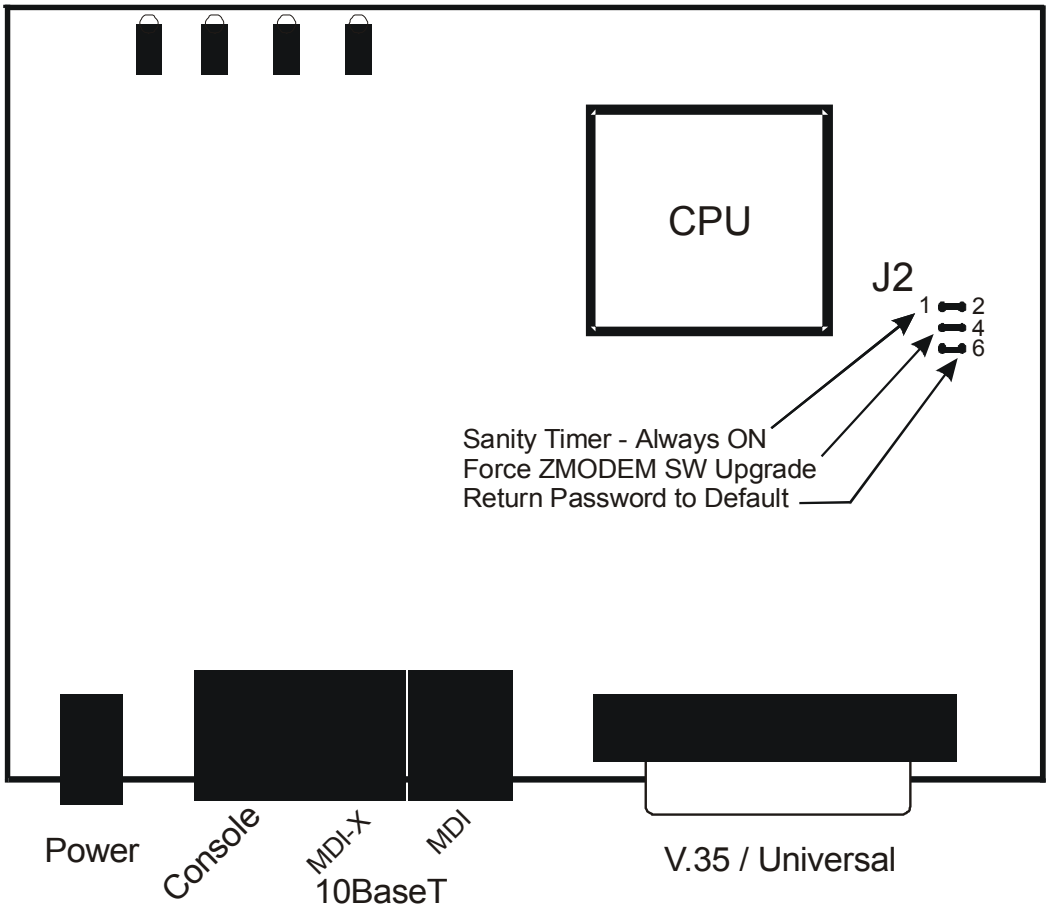


Figure C-1 Top Internal View of the P850 router V.35 or Universal WAN interface

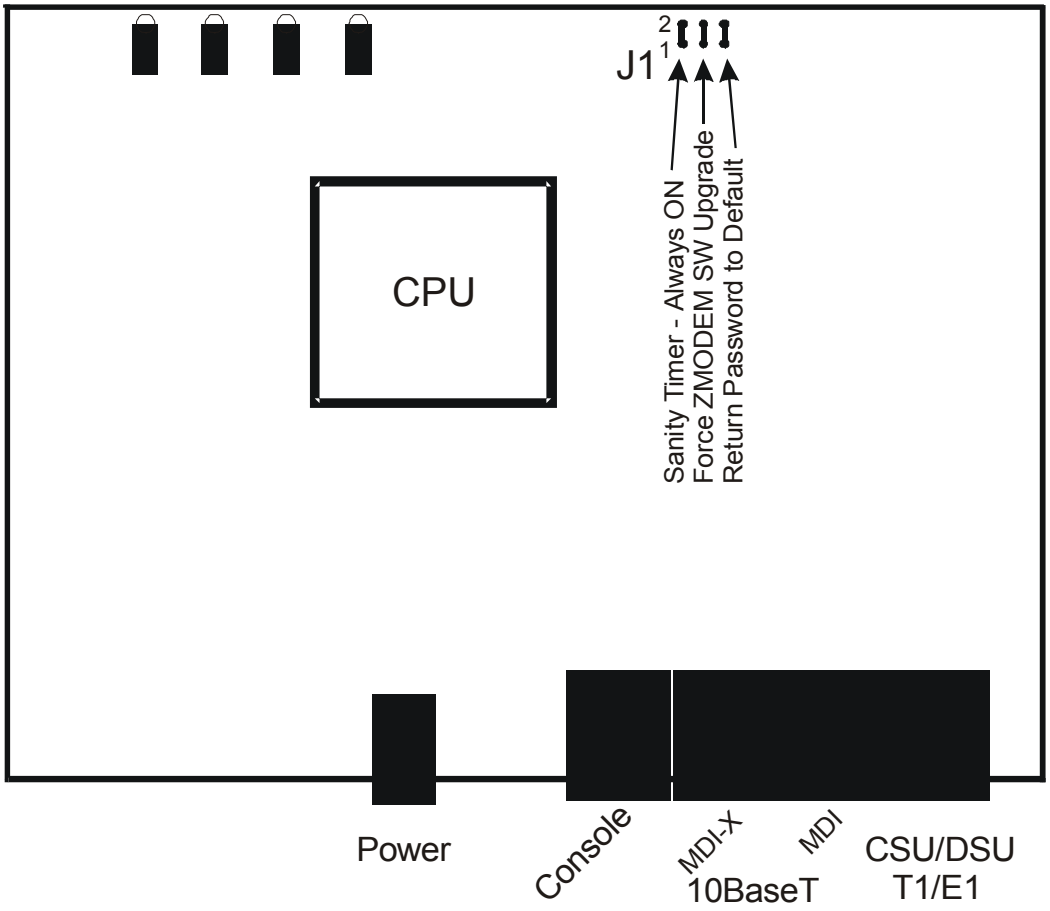


Figure C-2 Top Internal View of the P850 CSU-DSU or T1/E1

Sanity Timer

Do not remove this strap – pins 1-2.

Force ZMODEM Software Load

On the rare occasion that during the programming of the FLASH something happens to the bridge/router (power hit or hardware reset), causing the FLASH to become corrupted, the bridge/router will restart in ZMODEM receive mode only. If the bridge/router does not start in ZMODEM receive mode, perform the following steps:

1) power down the bridge/router,
2) open the case,
3) remove the strap from the center set of pins: 3-4,
4) power up the bridge/router. The bridge/router should now restart and be in ZMODEM receive mode.
5) Re-install the strap and replace the cover.

Please refer to Appendix E or the Menus Reference Manual for information on how to do software upgrades.

To Clear a "Lost" Password

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

Connecting to the Console Connector

The console connector on the P850 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

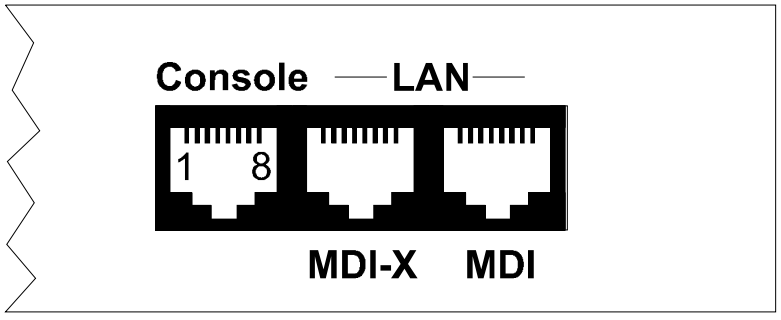


Figure C-3 Rear View of the Console and LAN Connectors

WAN Interface Connection

Pinout Information

The P850 router is manufactured with three different WAN link modules: V.35, LXT411 CSU/DSU or Universal WAN. The type installed may be determined from the label above the WAN link output connector on the back of the router.

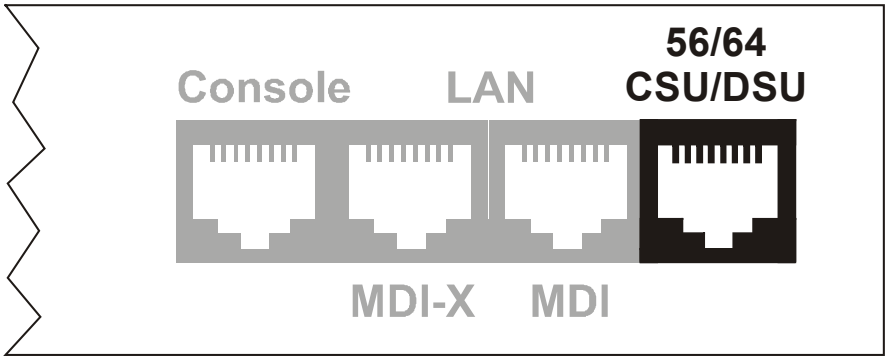
V.35 Module:

The V.35 link interface is provided as a DB25 connector on the back of the bridge/router, so an interface converter is needed to convert to the standard V.35 connectors.

When connecting two bridge/routers back-to-back without modems, a null-modem cable is required to crossover the pins on the links. Crossing over the pins allows two bridge/routers both configured as DTE interfaces to be connected together. With this configuration, both bridge/routers will provide clocking for the links, and each bridge/router must have a link speed defined.

CSU/DSU Module:

P850 routers with an LXT411 CSU/DSU interface module use a



standard RJ45 service connector, pinout specification RJ48S.

Figure C-4 Rear View of the CSU-DSU Connector

The LXT411 CSU/DSU link connection is set to operate at 64 Kbps by default. The link may be set to 56 Kbps via the software menus if required.

When two CSU/DSU link routers are to be connected via a leased line in a back to back set-up, the unit must be set to 56 Kbps link speed and a null-modem crossover cable used for the connection.

A DSU/CSU crossover cable would be constructed as follows:

1 --> 7
2 --> 8
7 --> 1
8 --> 2

T1/E1 Module:

P850 routers with a T1/E1 interface module use a standard RJ45 service connector, pinout specification RJ48C.

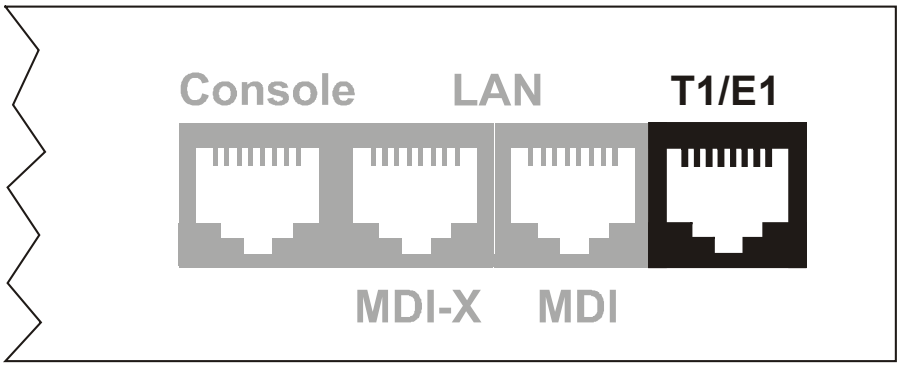


Figure C-5 Rear View of the T1/E1 Connector

When two T1/E1 routers are to be connected in a back to back set-up, a null-modem crossover cable used for the connection.

A T1/E1 crossover cable would be constructed as follows:

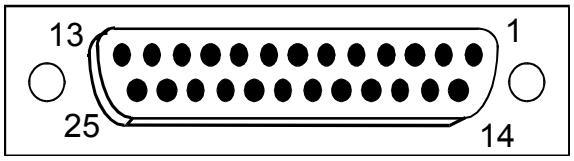
1 --> 4
2 --> 5
5 --> 2
4 --> 1

Pins 1 and 2 are receive (1 = ring, 2= tip)

Pins 4 and 5 are transmit (4 = ring, 5= tip)

UNIVERSAL WAN Module:

The Universal WAN Interface module in this router may be configured to operate in one of four modes: V.11/X.21, V.35, RS232/V.24, or RS530/RS422. The interface connector for all types is a standard DB25 pin female connector.



WARNING: ensure that the connector cable used with the Universal WAN interface module has the correct pinouts for the operational mode selected for the interface (V.11X.21, V.35, RS232/V.24, or RS530/RS422). Using the incorrect cable connector for the operational mode selected may cause permanent damage to the interface module.

Pinouts for each mode of operation are listed on the pages following.

V.35 Link Pinouts

DB25 Contact No.	M.34 Contact No.	Circuit Name	Direction To DCE	Direction From DCE
1	A	Protective Ground	NA	
2	P	Transmitted Data (A)	X	
3	R	Received Data (A)		X
4	C	Request to Send	X	
5	D	Clear to send		X
6	E	Data Set Ready		X
7	B	Signal Ground	NA	
8	F	Data Channel Received Line Signal Detector		X
9	X	Receiver Signal Element Timing (B)		X
10		----------		
11	W	Terminal Signal Element Timing (B)	X	
12	AA	Send Signal Element Timing (B)		X
13		----------		
14	S	Send Data (B)	X	
15	Y	Send Signal Element Timing (A)		X
16	T	Received Data (B)		X
17	V	Received Signal Element Timing (A)		X
18	L	Local Loopback	X	
19		----------		
20	H	Data Terminal Ready	X	
21	N	Remote Loopback		
22		----------		
23		----------		
24	U	Terminal Signal Element Timing (A)	X	
25	NN	Test Mode	X	

Figure C - 6 V.35 Link Pin Outs

The connecting cable must be a shielded cable.

Circuits which are paired (contain an (A) and (B) reference) should be connected to twisted pairs within the connecting cable.

NOTE For U.K. Approval:

The connecting cable may be any length between 0 and 5M. One end must be terminated in a male 34 pin X.21 bis connector as defined in ISO-2593 1984. The other end must be terminated in a male 25 pin X.21 bis connector as defined in ISO-2110 1989

RS232C / V.24 Link Pinouts

Contact No.	Circuit	Circuit Name	Direction To DCE	Direction From DCE
1	AA	Protective Ground	NA	
2	BA	Transmitted Data	X	
3	BB	Received Data		X
4	CA	Request to Send	X	
5		----------		
6	CC	Data Set Ready		X
7	AB	Signal Ground	NA	
8	CF	Received Line Signal Detector (CD)		X
9		----------		
10		----------		
11		----------		
12		----------		
13		----------		
14		----------		
15	DB	Transmit Signal Element Timing (DCE Source)		X
16		----------		
17	DD	Receive Signal Element Timing (DCE Source)		X
18		Local Loopback	X	
19		----------		
20	CD	Data Terminal Ready	X	
21		----------		
22	CE	Ring Indicator		X
23		----------		
24	DA	Transmit Signal Element Timing (DTE Source)	X	
25		----------		

Figure C-7 RS232 / V.24 Link Pinouts

The connecting cable must be a shielded cable.

NOTE For U.K. Approval:

The connecting cable may be any length between 0 and 5M. Each end must be terminated in a male 25 pin X.21 bis connector as defined in ISO-2110 1989.

RS530 / RS422 Link Pinouts

Contact Number	Circuit	Circuit Name	Direction To DCE	Direction From DCE
1	Shield	Protective Ground	NA	
2	BA (A)	Transmitted Data	X	
3	BB (A)	Received Data		X
4	CA (A)	Request to Send	X	
5	CB (A)	Clear to Send		X
6	CC (A)	Data Set Ready		X
7	AB	Signal Ground	NA	
8	CF (A)	Received Line Signal Detector		X
9	DD (B)	Receive Signal Element Timing (DCE Source)		X
10	CF (B)	Received Line Signal Detector		X
11	DA (B)	Transmit Signal Element Timing (DTE Source)	X	
12	DB (B)	Transmit Signal Element Timing (DCE Source)		X
13	CB (B)	Clear to Send		X
14	BA (B)	Transmitted Data	X	
15	DB (A)	Transmit Signal Element Timing (DCE Source)		X
16	BB (B)	Received Data		X
17	DD (A)	Receive Signal Element Timing (DCE Source)		X
18	LL	Local Loopback	X	
19	CA (B)	Request to Send	X	
20	CD (A)	Data Terminal Ready	X	
21	RL	Remote Loopback	X	
22	CC (B)	Data Set Ready		X
23	CD (B)	Data Terminal Ready	X	
24	DA (A)	Transmit Signal Element Timing (DTE Source)	X	
25		----------		

Figure C-8 RS530 / RS422 Link Pinouts

The connecting cable must be a shielded cable.

Circuits which are paired (contain an (A) and (B) reference) should be connected to twisted pairs within the connecting cable.

V.11 / X.21 Link Pinouts

Contact No.	X.21 Circuits Ref.	Circuit Name	Direction To DCE	Direction From DCE
1		Protective Ground	NA	
2	T (A)	Transmitted Data (A)	X	
3	C (A)	Control (A)	X	
4	R (A)	Received Data (A)		X
5	I (A)	Indication (A)		X
6	S (A)	Signal Element Timing (A)		X
7		----------		
8	Ground	Signal Ground	NA	
9	T (B)	Transmitted Data (B)	X	
10	C (B)	Control (B)	X	
11	R (B)	Received Data (B)		X
12	I (B)	Indication (B)		X
13	S (B)	Signal Element Timing (B)		X
14		----------		
15		----------		

Figure C-9 V.11 / X.21 Link Pinouts

The connecting cable must be a shielded cable.

Circuits which are paired (contain an (A) and (B) reference) should be connected to twisted pairs within the connecting cable.

NOTE For U.K. Approval:

The connecting cable may be any length between 0 and 5M.

V.11 / X.21 DB25 to DB15 Connector Cable

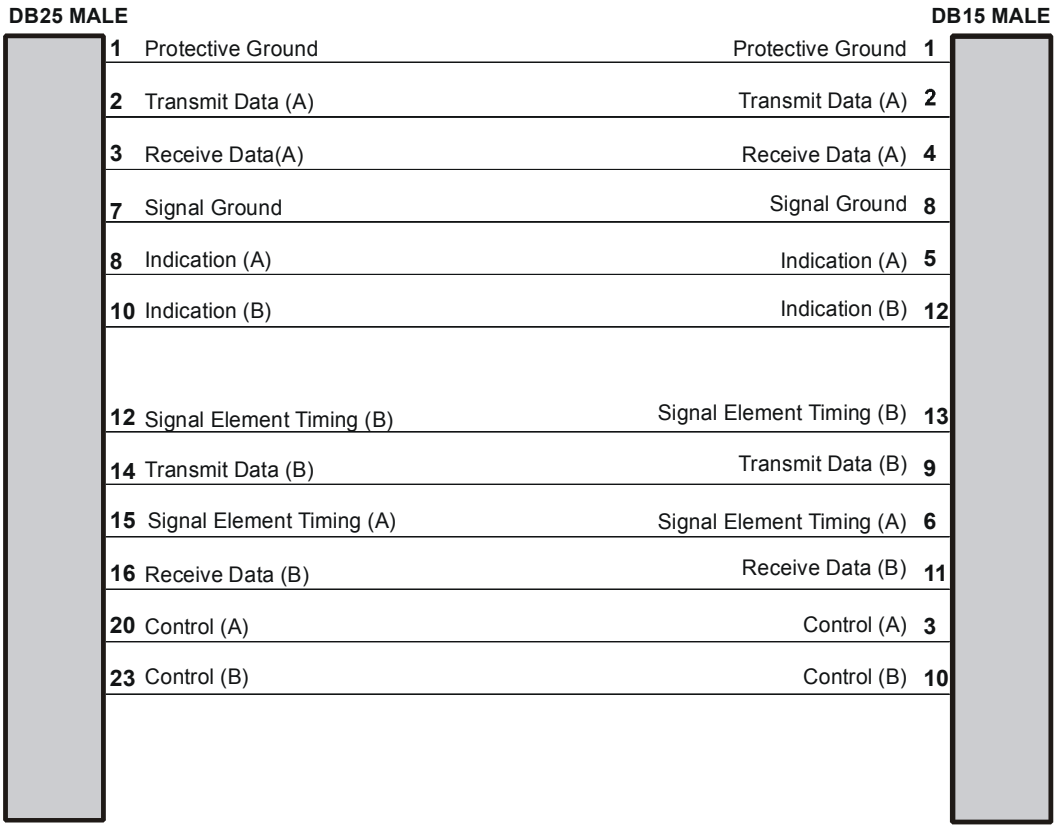


Figure C-10 V.11 / X.21 DB25 to DB15 Connector Cable

NOTE For U.K. Approval:

The connecting cable may be any length between 0 and 5M.

V.35 Null-Modem Cable Configuration

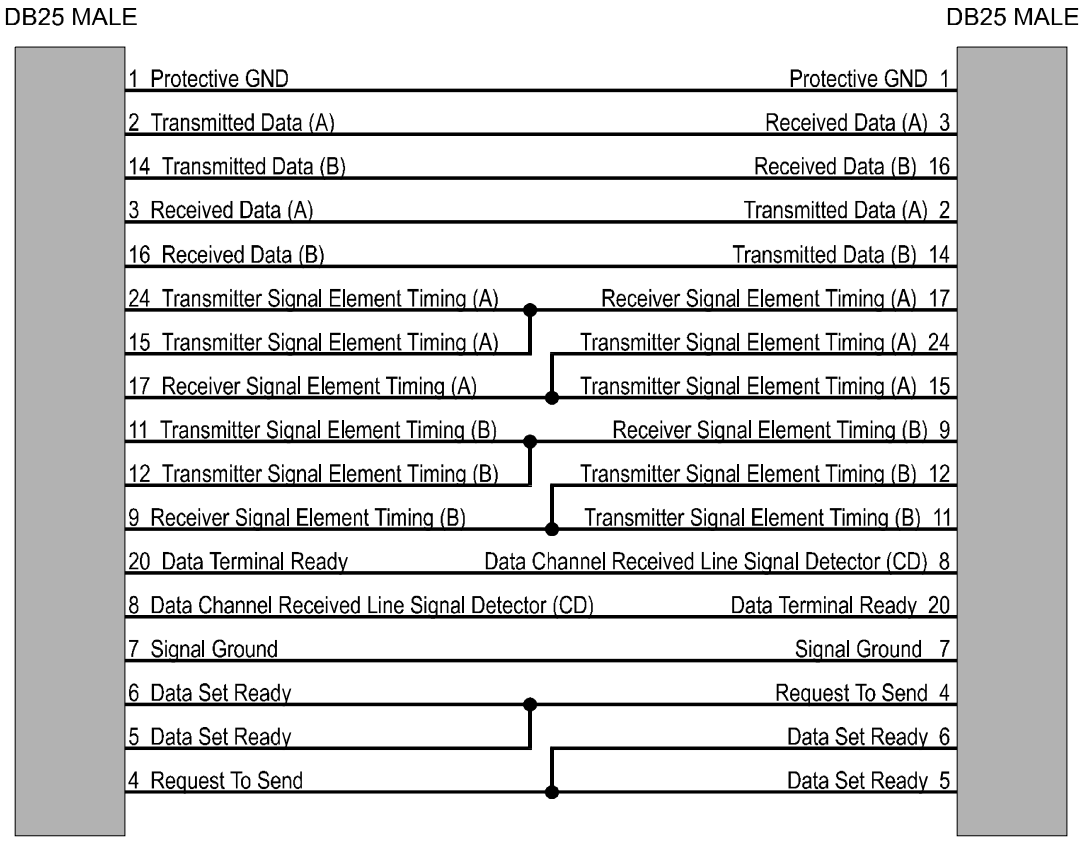


Figure C - 11 V.35 Null-Modem Cable

The connecting cable must be a shielded cable.

Circuits which are paired (contain an (A) and (B) reference) should be connected to twisted pairs within the connecting cable.

This cable is needed when it is necessary to connect two units back-to-back and a set of modems is not available. Note that this cable specifies DB25 connectors on each end to allow direct connection to the link interface connector on each unit.

The link speed must be defined for each of the two units.

RS232 / V.24 Null-Modem Cable

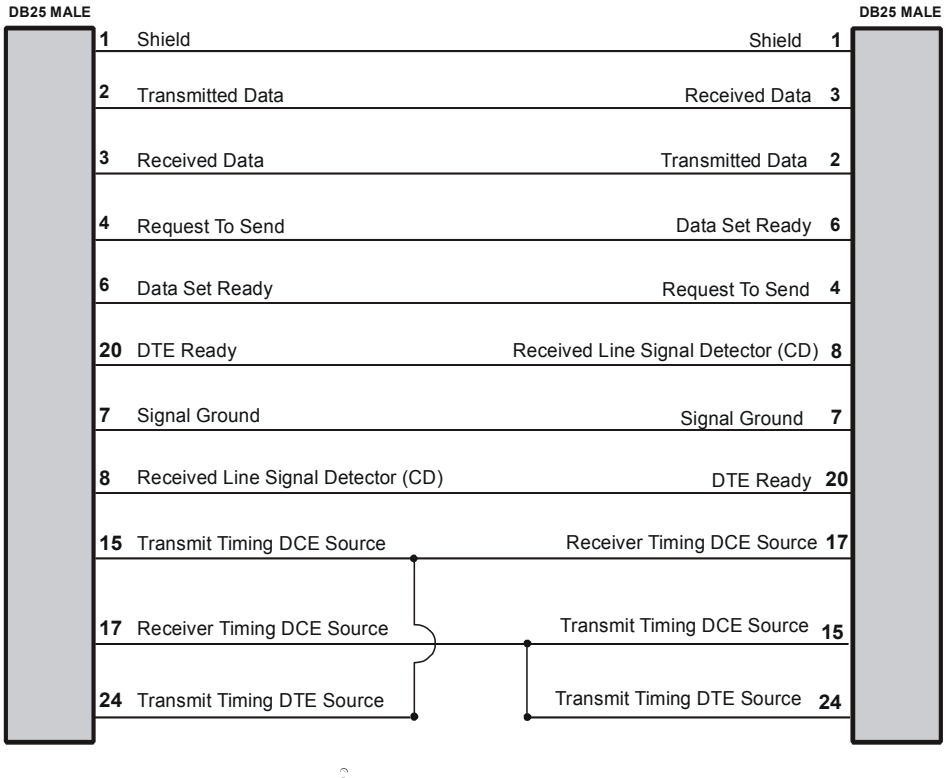


Figure C-12 RS232 / V.24 Null-Modem Cable

The connecting cable must be a shielded cable.

This cable is needed when it is necessary to connect two units back-to-back and a set of modems is not available. Note that this cable specifies DB25 connectors on each end to allow direct connection to the link interface connector on each unit. The link speed must be defined for each of the two units.

RS530 / RS422 Null-Modem Cable

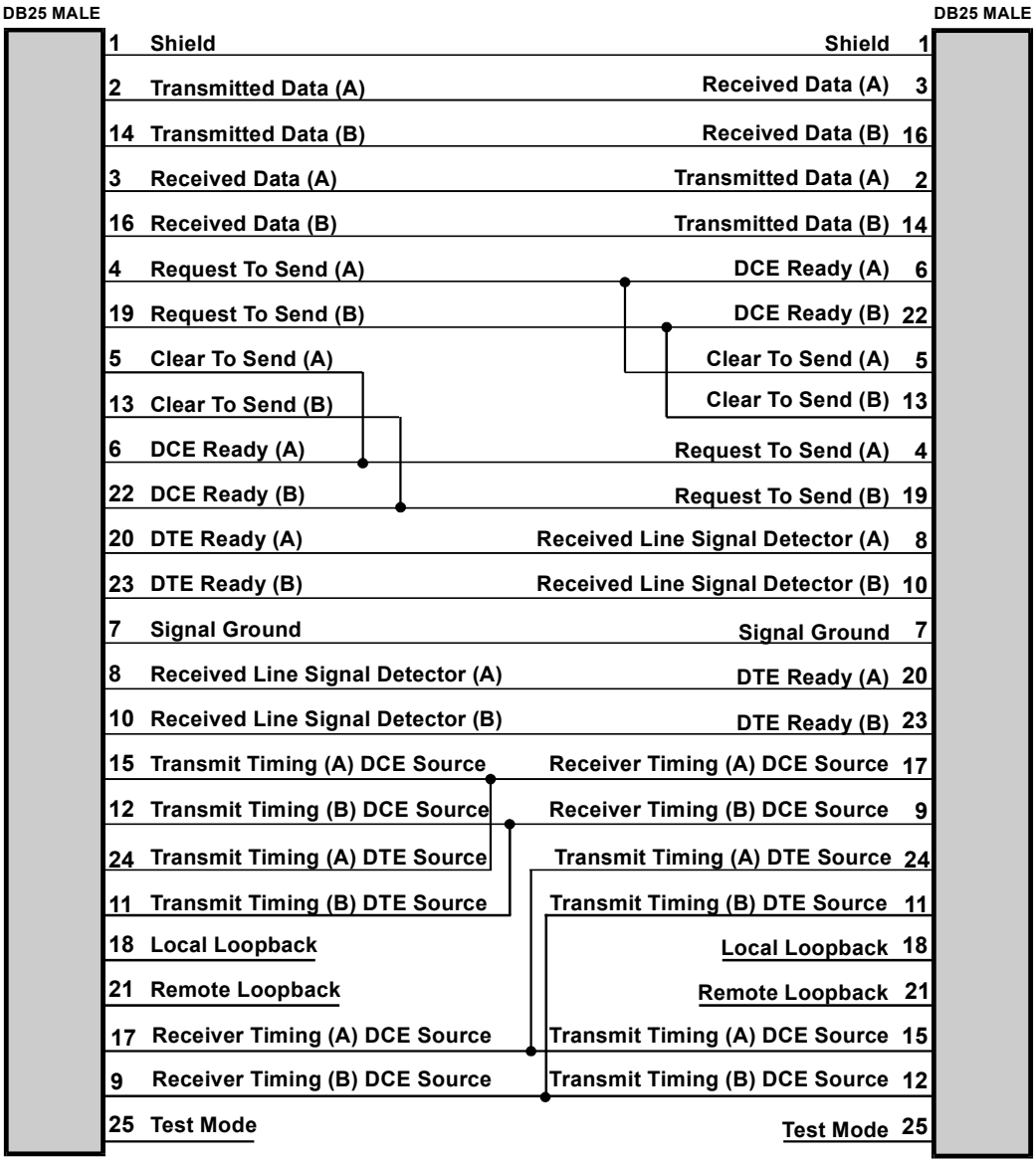


Figure C-13 RS530 / RS422 Null-Modem Cable

The connecting cable must be a shielded cable.

Circuits which are paired (contain an (A) and (B) reference) should be connected to twisted pairs within the connecting cable.

This cable is needed when it is necessary to connect two units back-to-back and a set of modems is not available. Note that this cable specifies DB25 connectors on each end to allow direct connection to the link interface connector on each unit. The link speed must be defined for each of the two units.

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. A byte status message will be displayed on the console port during the programming of the FLASH. After the reset, the remote sites information will have to be re-entered, either from a saved configuration file (recommended) or by manually reentering the information for each site.

On the rare occasion that during the programming of the FLASH something happens to the bridge/router (power hit or hardware reset), causing the FLASH to become corrupted, the bridge/router will restart in ZMODEM receive mode only. If

the bridge/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 P850 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 remote sites information will have to be re-entered, either from a saved configuration file (recommended) or by manually reentering the information for each site.

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 bridge/router (power hit or hardware reset), causing the FLASH to become corrupted, the bridge/router will restart in ZMODEM receive mode only. If

the bridge/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 P850 routers in the diagram, the upgrade order should be Router C, then Router B, and finally Router A.

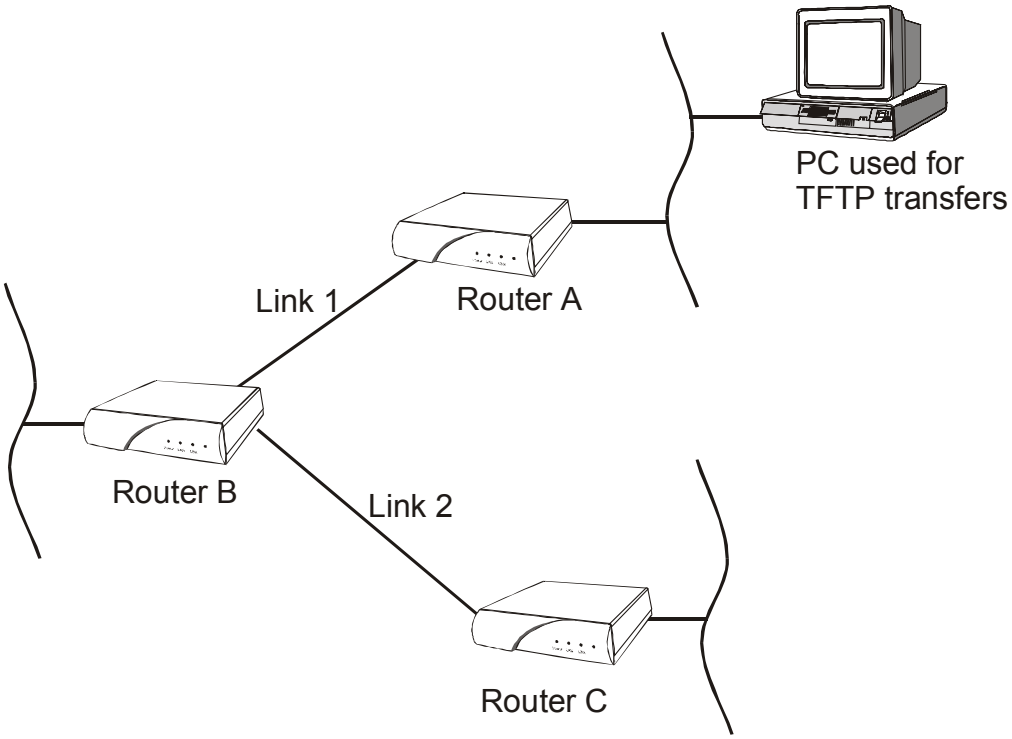
A TFTP software load to Router C would be performed as follows:

- 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