# Perle P840
# Bridge/Router
# VPN Menu Reference

Part number 5500065-17

Throughout this manual, information that is presented by the router and entered into the router will be shown in a bordered box, as shown here.

```
Screen information being displayed or entered.
```

## Initial Router & Management Console Power-Up

The following screen information will be seen on the console connected to the router when it is first powered on:

```
Terminals supported:

 teletype ansi, avt, ibm3101, qvt109, qvt102, qvt119, tvi925, tvi950,
 vt52,vt100, wyse-50, wyse-vp

Enter terminal type:
```

As the terminal type is not yet defined at the very first power-up, this screen may be slightly mixed up. Enter at least one <RETURN> (up to three if necessary) on the Network Console in order for the router to determine the baud rate of the terminal used for the console (i.e. auto-baud) and then proceed.

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

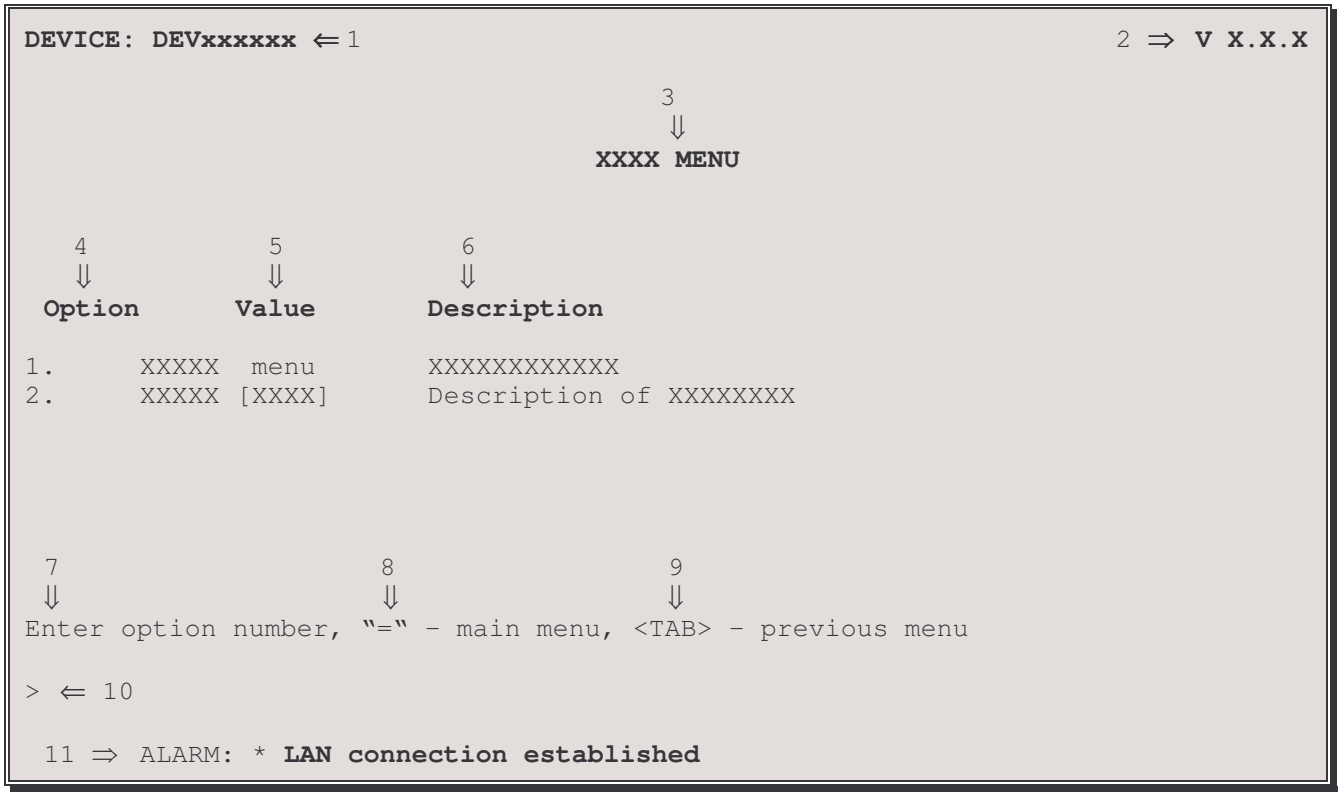
## Menu Command Entry

Once the terminal type is specified, the MAIN (LOGIN) MENU will be displayed.

The P840 router uses a "hotkey " Menu. A menu option is chosen by selection of the desired option number.

Entry of parameters is from the "**>**" prompt. When a parameter is required, enter the necessary string and end it with a <Return>. If the entry is not accepted, an error message will be reported and the parameter will have to be re-entered. Should you make an error, the <BACKSPACE> key (for most terminals) deletes the most recently entered characters.

## Menu Structure




The Menu Screens are structured with 11 primary elements:

1. Device Name
2. Software Version
3. Menu Name
4. Option Number and Option Name
5. Option Value
6. Option Description
7. Choosing an Option
8. Returning to the Main Menu
9. Returning to the Previous Menu
10. Command Prompt
11. ALARM display for a just-happened alarm event

## Elements of the Menu Screens:

1. **Device Name**
   A default Device Name in the format DEVxx-xx-xx is supplied by the system for each router. (xxxxxx are the last 6 digits of the MAC address of the router). The Device Name may be changed in the Device Set-Up Menu.

2. **Software Version**
   The version of the software currently installed in the router is shown in the upper right-hand corner of each menu display.

3. **Menu Name**
   Each MENU is named to indicate its grouped Options.

4. **Option Number and Option Name**
   Choosing the number for the Option makes the selection. If you prefer a command-style interface, typing the first few unique letters of the desired Option is enough to identify the Option. Enter the selection with a <Return>.

5. **Option Value**
   The Value of an Option may indicate several parameters—for example:

| | |
|---|---|
| State | [enabled], [disabled], [present], [not_present], ... |
| Setting | [5 sec.], [5 min.], ... |
| Path | "menu" indicates a sub-menu |
| Name | [vt100], [Bridge_5], [none] |

6. **Option Description**
   This is a single-line description of the Option.

7. **Choosing an Option**
   Select the Option by entering its number or unique first letters at the prompt.

8. **Returning to the Main Menu**
   The equals ("=") sign returns you to the Main Menu. (All major menu paths start at the Main Menu. If you want to switch to the Main Menu, enter " = ").

9. **Returning to the Previous Menu**
   To go back to the previous higher level menu, enter a <TAB>.

10. **Command Prompt >**
    All data entry is made at the Command Prompt.

11. **ALARM display for an occurring event**
    The display of an ALARM notifies a viewing router manager that an event of significance has occurred. Since not every ALARM can be viewed as it occurs, the latest 199 ALARMs are recorded and can be viewed from the Network Events Menu.

**Note:** Depending on the configuration setting of this device, some options are not always displayed and some menus will have different options. Display lines with these options are in italics in this manual. If the option may appear on the menu screen with various numbers, the possible numbers are listed in the write up for the option, for example:

**3/4 ISDN Set-Up.**

## Login Menu

```
                                LOGIN MENU

    Option            Description
 1. Login           - Initiate operator session
 2. Help            - Read menu introduction









Enter option number


>
```

This is the **LOGIN MENU** seen when powering up a console connected to the router.

**1 - Login**

The Login option allows entry of the password for the router. The default password is "BRIDGE"; change it if security is desired. See the Installation & Applications Guide for information on restoring the default password to the router.

**Action to Take:**

Choose the Login Option and use the default password "BRIDGE." The characters will not be echoed on the screen. Once the password is accepted, you will be given the expanded MAIN MENU for full access to router management features.

**2 - Help**

The Help option provides a brief description of menu format and usage.

## Main Menu

```
                                MAIN MENU

    Option                Value          Description

 1. Quick start            menu
 2. Configuration          menu         - Define operating parameters
 3. Statistics             menu         - Device LAN and WAN statistics
 4. Diagnostics            menu         - Access troubleshooting tools
 5. Network events         menu         - View network event history
 6. Save configuration                  - Save configuration immediately
 7. Logout                              - End operator session
 8. Help                                - Read menu introduction


Enter option number

>
```

The **MAIN MENU** is a starting and ending point for management of the router. This menu allows access to menus and provides the Logout Option. Options 1-4 are major paths. To switch major paths, return to the MAIN MENU by entering "=".

**1 - Quick Start**

The Quick Start option takes you to the Quick Start Menu, where a directly dialed ISDN call may be placed without having to configure a large number of parameters. The configuration parameters required to establish a direct dial ISDN call are definable within the Quick Start menu.

**2 - Configuration**

The Configuration option takes you to the Configuration Menu, where all the various router parameters are defined. Take this path to define the operating parameters of the terminal used for the router console.

**3 - Statistics**

The Statistics option takes you to the Statistics Menu, where statistics can be examined to evaluate router, LAN, and link performance.

**4 - Diagnostics**

The Diagnostics option takes you to the Diagnostics Menu, where special diagnostic functions can be used to analyze LAN, link, and router problems.

**5 - Network Events**

The Network Events option takes you to the Network Events Menu, where the 199 latest Alarms can be examined.

**6 – Save Configuration**

The settings of any configuration options that have been changed from their default values are saved.

**7 - Logout**

The Logout option terminates your session and secures the router. The next user must log in and enter the correct password to view or change the router configuration.

**8 - Help**

The Help option provides a brief, one-screen description of menu format and usage.

## Quick Start Menu

```
                          QUICK START MENU

    Option              Value          Description
 1. ISDN set-up         menu         - Configure ISDN
 2. Device name         "DEV050607"  - Name this device
 3. Security level      [none]       - Set security protocol
 4. IP address          [none]       - Define IP address and mask
 5. Default gateway     [none]       - Define default gateway
 6. Direct dial                      - Make a manual ISDN call
 7. Force disconnect                 - Disconnect a call
 8. Link status                      - View status of link
 9. Soft reset                       - Reset device (retain configuration)



Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **QUICK START MENU** provides configuration options to make an ISDN direct dial connection.

**1 - ISDN set-up**

The ISDN set-up option takes you to a menu where the switch type, dial prefix number and directory number(s) may be set. Depending on the switch type selected, Service Profile ID(s) may also be entered.

**2 - Device name**

The Device Name option allows you to name (or rename) this device for identification purposes. The router name will be displayed in both the Value column of this option and in the upper left-hand corner of all menu screens. If the router has not been named, the device name defaults to a prefix of "DEV" followed by the last six digits of the LAN port MAC address (eg. DEV050607).

**3 - Security level**

The Security Level option allows you to choose the type of security authentication to request from remote site PPP routers. The choices are none, PAP or CHAP.

**Default:** [none]

```
Enter :
    none, PAP, CHAP

>
```

**4 - IP Address**

The IP Address option allows the definition of an Internet Protocol (IP) address and corresponding subnet size for the router. The router requires an IP address.

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. 92.3.1.10). Each decimal number must be less than or equal to 255, that is the maximum value of each 8-bit field.

The size of subnet mask variable defines the number of bits in an IP address to be used for network and subnetwork addressing (the remainder being used for host addressing). Subnetting allows multiple logical networks within a single standard IP network address.

**Default:** [none]

```
Enter :
    none, internet address (up to 15 characters)
>

Enter :
    size of subnet mask (from 8 to 32)
>
```

**5 - Default gateway**

The Default Gateway option allows the identification of a default gateway (i.e. *router*). Messages destined for hosts not on this (sub-)network are forwarded to the default gateway. The default gateway may be located on the local LAN or may be one of the remote site peer IP routers.

If the IP address of the remote site peer IP router is not known, the default gateway may be defined as the remote site ID. This will cause the default gateway to become whatever device is currently connected at that remote site.

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

If more than one default gateway is defined within the routing table, the default gateway with the lowest cost will be used and displayed in this option.

**Default:** [none]

```
Enter :
    none, gateway IP address, remote site ID or alias (up to 18 characters)
>
```

**6 – Direct Dial**

The Direct Dial option allows the entry of an ISDN number which will then be called immediately by this P840.

**7 - Force Disconnect**

The Force Disconnect option will cause the chosen link to be disconnected.

```
Enter :
     Link to disconnect (1 or 2), all
>
```

**8 - Link Status**

The Link Status option displays the status of the links, either individually (more statistics), or together (provides overview).

Please refer to the Link Status displays for more detailed information.

**9 - Soft Reset**

Selecting the Soft Reset option resets the router software and restarts the router. The current configuration is retained.

## Configuration Menu

```
                          CONFIGURATION MENU

   Option                 Value          Description
 1. Access set-up         menu         - Establish access parameters
 2. Interfaces set-up     menu         - Define interface parameters
 3. Connections set-up    menu         - Configure connection operation
 4. Packet Services set-up menu        - Define packet services
 5. Applications set-up   menu         - Configure Internet applications




Enter option number, "=" - main menu, <TAB> - previous menu


>
```

The **CONFIGURATION MENU** provides paths to menus for configuration of this router.

**1 - Access Set-Up**

The Access Set-up option takes you to the Access Set-Up Menu, where passwords, names, dates, and times are set and viewed. From this menu, you can save or restore the router configuration and connect to another router in the network of routers.

**2 - Interfaces Set-Up**

The Interfaces Set-up option takes you to the Interfaces Set-up Menu where controls for the LAN, WAN link(s) and the console terminal are set.

**3 - Connections Set-Up**

The Connections Set-up option takes you to the Connections Set-up Menu, where WAN connections to each remote site location are configured, login security is set, PPP parameters entered and IP address connection tables set.

**4 – Packet Services Set-Up**

The Packet Services Set-up option takes you to the Packet Services Set-up Menu, where data packet bridging, routing, IP security and filtering and QOS parameters are set.

**5 - Applications Set-Up**

The Applications Set-up option takes you to the Applications Set-up Menu, where the internet connection management applications for SNMP, DHCP, Firewalls, Network Address Translation and Syslog may be accessed.

## Access Set-Up Menu

```
                          ACCESS SET-UP MENU

    Option               Value          Description
 1. Device set-up        menu        - Set security/time/names
 2. Telnet set-up        menu        - Set up remote communications
 2. Upgrade device       menu        - Perform feature upgrade
 4. Load FLASH set-up    menu        - Prepare for software update
 5. Console              menu        - Dump/restore configuration from console
 6. Hardware status                  - Display hardware information
 7. TFTP access         [disabled]   - Allow TFTP configuration saves/loads



Enter option number, "=" - main menu, <TAB> - previous menu


>
```

The **ACCESS SET-UP MENU** provides options for saving and restoring the router configuration as well as paths to menus for terminal, device, and remote access configuration.

**1 - Device Set-Up**

The Device Set-up option takes you to the Device Set-Up Menu, where the device name, password, dates, and times are set and viewed.

**2 - Telnet Set-up**

The Telnet Set-up option takes you to the Telnet Access Menu, where you can connect to another router in the network of routers.

**3 – Upgrade Device**

The Upgrade Device option takes you to the Upgrade Device Menu where an upgrade key may be entered to enable optional features on this router.

**4 - Load FLASH Set-Up**

The Load FLASH Set-up option takes you to the Load FLASH Set-Up Menu, where you can update the software in this device using TFTP or console Z-modem transfers.

**Note:** this operation cannot be performed from a secondary IP address.

**5 - Console**

The Console option takes you to the Console Menu, where the present configuration may be dumped to the console computer for storage or a stored configuration uploaded from the console computer.

**6 - Hardware Status**

The Hardware Status option displays the status of the router hardware.

```
                        Hardware Status


Boot Code version    : 51B1.4.1.4          System Code revision : 7a0
Boot Code revision   : 0                   Service reference    : 0/0
RAM size             : 8  MB               ROM size             : 2 MB
MAC check code       : b9876d23
LAN interface type   : 10BaseT        MAC address          : 02-03-04-05-06-07
Module types         : (1) BRI ST  (2) BRI ST
CPU type             : 68EH360
CPU speed            : 25 Mhz
Compression          : enabled
Voice interface       : installed revision xxx
```

**Boot Code version** The software boot code version currently installed in this P840. This is the number that is displayed in the upper right of the menu screens when in console load mode.

**Boot Code revision** The software boot code revision number currently installed in this P840. A control number for tracking minor software revisions.

**System Code revision** The system code software revision number currently installed in this P840.

**Service Reference** Internal factory reference number.

**MAC Address** The MAC Address of the LAN port for this router.

**MAC Check Code** Check code used for feature upgrades.

**RAM size** The amount of RAM in this router.

**ROM size** Indicates the size of the FLASH EEPROM installed.

| | |
|---|---|
| **LAN Interface Type** | The type of LAN interface that is configured on this router. |
| **Module Type** | The type of link interface of this router installed |
| **Compression** | Indicates whether data compression is enabled or disabled. |
| **Voice interface** | Indicates whether or not a voice interface is installed and the revision number. |

**7 - TFTP Access**

The TFTP Access option determines whether a remote LAN device will be allowed to make a TFTP connection to this router to dump (get) or restore (put) the configuration.

The TFTP application must be in "netascii" or "ascii" mode for configuration transfers.

**Default:** [disabled]

**Procedures for performing a Configuration Dump using TFTP:**

1) 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.)

2) Get the file "config.txt" from the router.

3) Use a text editor to check the configuration file saved to the PC disk to confirm that the information is still in order. If minor errors occurred, they may be corrected with the text editor. If errors were major, get the configuration file again.

**Procedures for performing a Configuration Load using TFTP:**

1) 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.)

2) Put the file "config.txt" to the router.

3) When the transfer is complete, the configuration will have been restored to the router.

.

## Device Set-Up Menu

```
                              DEVICE SET-UP MENU

    Option              Value          Description
 1. Password                         - Change login password
 2. Device name       "DEV050607"    - Name this device
 3. Show time                        - Display current date and time
 4. Set time                         - Set date and time
 5. Time zone set-up   menu          - Set time zone
 6. Summer time set-up menu          - Set summer time









Enter option number, "=" - main menu, <TAB> - previous menu



>
```

The **DEVICE SET-UP MENU** allows the definition of the Device name, and a password to control local/remote access to the router management console. You can also set the real-time clock and date. Note that the clock is a 24-hour real-time clock.

**1 - Password**

The Password option allows you to change the router's login password. (The characters will **not** be echoed on the screen.) (If you have no need for a password, enter <NONE> in CAPS, and the entry of a password will be bypassed.) The password is case sensitive and must be entered precisely. An example is given below:

```
Enter:
 new password (1 to 8 characters)
> brooklyN

Enter:
 verification of new password (1 to 8 characters)
> brooklyN
New password installed
```

**2 - Device Name**

The Device Name option allows you to name (or re-name) this device for identification purposes. The router name will be displayed both in the Value column of this option and in the upper left-hand corner of all menu screens. If the router has not been named, the device name in the upper left-hand corner of the screen and the information in the Value column will show a prefix of DEV followed by the last six characters of the LAN port MAC address (e.g. DEV006045).

```
Enter:
 Device name string (up to 16 characters)
> Router5
```

**3 - Show Time**

The Show Time option displays the current day of the week, date and time.

```
Wednesday 1998-08-05 15:16:16
```

**4 - Set Time**

Use the Set Time option to set the date and 24-hour Time Clock. Note that if your network uses features of the P840 router which are controlled by activation times (such as Bandwidth-On-Demand or backup recovery) across different time zones, you must standardize on one time zone for all routers that use this feature.

```
Enter:
 Date in format yyyy-mm-dd, no_change
1998-09-27

Enter:
 Time in format hh:mm:ss
14: 25: 00
```

**5- Time zone set-up**

The Time zone Set-up option takes you to the Time Zone Set-Up Menu, where the router time zone offset in hours and minutes are set as well as the name of the time zone.

**6- Summer time set-up**

The Summer time Set-up option takes you to the Summer Time Set-Up Menu, where the daylight savings time can be enabled on a specific date or recurring by specifying the date and time for the start and end of summer time.

## Time Zone Set-Up Menu

```
                              TIME ZONE SET-UP MENU

    Option            Value          Description
 1. Offset direction  [+]         - Direction of offset from UTC
 2. Offset hours      [0]         - Hours offset from UTC
 3. Offset minutes    [0]         - Minutes offset from UTC
 4. Name              [none]      - Time zone name




Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **TIME ZONE SET_UP MENU** allows the router to be configured for a specific time zone

**1 – Offset Direction**

The Offset Direction option allows the internal clock to be adjusted forward (+) or behind (-) UTC.

**Default:** [+]
**Options:** **+, -**

**2 – Offset hours**

The Offset hours option allows the internal clock to be adjusted to deviate from UTC a specific number of hours.

**Default:** [0]
**Range:** 23 or lower

**3 – Offset Minutes**

The Offset Minutes option allows the internal clock to be adjusted to deviate from UTC a specific number of minutes.

**Default:** [0]
**Range:** 59 or lower

**4 – Name**

The Name option allows time zone to be classified up to 4 characters in length. This name will be seen whenever the time is displayed to the user.

**Default:** [none]
**Maximum:** up to 4 characters

## Summer Time Set-Up Menu

```
                          SUMMER TIME SET-UP MENU

    Option              Value          Description
 1. Summer time         [enabled]      - Enable/Disable Summer time
 2. Summer time mode    [date]         - Set summer time mode
 3. Summer time start   menu           - Set summer time start
 4. Summer time end     menu           - Set summer time end
 5. Offset              [60]           - Offset for summer time
 6. Name                [none]         - Name of the time zone




Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **SUMMER TIME SET_UP MENU** allows the router to be configured for daylight savings time

**1 – Summer Time**

The Summer Time option enables/disables summer time which accommodates configuration for daylight savings time.

**Default:** [disabled]
**Options:** disabled, enabled

**2 – Summer Time Mode**

The Summer Time Mode option allows the router to adjust for daylights saving time once or recurring each year. *Date* option indicates the daylight saving time adjust will occur once and allow you to configure the summer time start and summer end time (year, month, time). *Recurring* option specifies the daylights savings time will be adjusted each year based upon the rules configured within the summer time start and summer time end (year, month, week, day and time).

**Default:** [date]
**Options:** date, recurring

**3- Summer Time start**

The Summer Time Start option takes you to the Summer Time start Menu, where the summer begin time specifics are configured.

**4- Summer Time end**

The Summer Time End option takes you to the Summer Time End Menu, where the summer end time specifics are configured.

**4- Offset**

The Offset option specifies the amount of minutes to adjust the internal clock by when the summer time begin and re-adjusts the internal clock when summer time ends.

**Default:** [60]
**Range:** 1 - 180

**4 – Name**

The Name option specifies the name of the time zone to be displayed to be classified up to 4 characters in length. This name will be seen whenever the time is displayed to the user.

**Default:** [none]
**Maximum:** up to 4 characters

## Summer Time Start/End Menu (date mode)

```
                          SUMMER TIME START MENU

   Option              Value          Description
 1. Year               [2003]         - Start year
 2. Month              [April]        - Start month of the year
 3. Date               [1]            - Start day of the month
 4. Time               ["02:00"]      - Start time of day.




Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **SUMMER TIME START MENU (date mode)**specifies the summer time start/end time parameters for daylights savings time to begin with date mode configured.

**1 – Year**

The Year option specifies the year in which summer time will begin/end. The Year option is only available for *date* mode and will not be shown for *recurring* mode

**Default:** [2003]
**Range:** 2003- 2035

**2 – Month**

The Month option specifies the month of the year in which daylight savings time will start/end. The month option is available for both *date* and *recurring* mode.

**Default:** [January]
**Options:** January, February, March, April, May, June, July, August, September, October, November, December

**3- Date**

The Date option specifies the day of the month to start summer time.

**Default:** [1]
**Range:** 1 to 31

**4- Time**

The Time option specifies the time of day to begin summer time. The time is entered in the hh:mm (hh – hours, mm minutes) format.

**Default:** ["1:00"]
**Format:** hh:mm format

## Summer Time Start/End Menu (recurring mode)

```
                          SUMMER TIME START MENU
```

```
   Option              Value          Description
 1. Month              [April]        - Start month of the year
 2. Week               [1]            - Start week of the month
 3. Day                [Sunday]       - Start day of the week
 4. Time               ["02:00"]      - Start time of day.




Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **SUMMER TIME START MENU (recurring mode)** specifies the summer time start time parameters for daylights savings time to begin with recurring mode configured.

**1 – Month**

The Month option specifies the month of the year in which daylight savings time will start/end.

**Default:** [January]
**Options:** January, February, March, April, May, June, July, August, September, October, November, December

**2 – Week**

The Week option specifies the week of the month n which summer time will start/end.

**Default:** [1]
**Range**: 1 to 5 or last

**3- Day**

The Day option specifies the day of the week to start/end summer time.

**Default:** [Sunday]
**Options:** Sunday, Monday, Tuesday,Wednesday, Thursday, Friday,Saturday

**4- Time**

The Time option specifies the time of day to begin/end summer time. The time is entered in the hh:mm (hh – hours, mm minutes) format.

**Default:** ["1:00"]
**Format:** hh:mm format

**4- Offset**

The Offset option specifies the amount of minutes to adjust the internal clock by when the summer time begin and re-adjusts the internal clock when summer time ends.

**Default:** [60]
**Range:** 1 - 180

**4 – Name**

The Name option specifies the name of the time zone to be displayed to be classified up to 4 characters in length. This name will be seen whenever the time is displayed to the user.

**Default:** [none]
**Maximum:** up to 4 characters

## Telnet Set-Up Menu

```
                              TELNET SET-UP MENU

    Option          Value          Description
 1. Telnet access [enabled]     - Allow incoming Telnet connection
 2. Telnet                      - Connect to a remote device
 3. Telnet port   [default}     - Alternate remote device port
 4. Show names                  - Display known device names
 5. Add name                    - Add a remote device name
 6. Remove name                 - Delete remote device name




Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **TELNET SET_UP MENU** allows telnet connections to be made to other routers in the network.

**1 - Telnet Access**

The Telnet Access option allows LAN/WAN network devices to make Telnet connections to this router for management. Once the connection is established, the network device will be presented with the menu interface for configuration management and statistics viewing.

**Default:** [enabled]

**Considerations:**

When a Telnet connection is made to a router, ensure that the Telnet session is in character mode, and carriage return padding (or translation) is set to NULL (or no translation). The extra character sent when carriage return padding is on will cause some displays to behave erratically.

**Note:** A Telnet connection from another IP address is allowed three attempts to login with the correct password. After three failures, that IP address will be rejected for the following ten minutes if any further attempts are made and the following alarm message is logged and displayed on the console:

```
Alarm: Possible intruder 192.168.89.65 exceeded password attempts limit
```

**2 - Telnet**

Choosing the Telnet option, and specifying the name or IP address of the router you wish to connect to, connects to the other router for configuration purposes and viewing of statistics.

The Device name at the top left of each Menu identifies the router being controlled.

If there is no data transmitted or received for a period of 5 minutes, the Telnet session will be disconnected. This time limit cannot be modified.

To disconnect from the router being controlled, enter Control-C ( **^C** ).

**Considerations:**

If the Internet Address of a remotely connected router is changed, immediately disconnect from the remote router by entering a Control-C ( **^C** ) and re-establish a new Telnet connection using the new Internet Address of the remote router.

**3 - Telnet Port**

The Telnet port option allows you to choose an alternate port number that a remote device can use for Telnet access to this router. This is necessary when Telnet is one of the exported services offered under Network Address Translation (NAT), as the well known port number will be used for the network Telnet server. An alternate port number must be supplied to Telnet to this router.

**4 - Show Names**

The Show Names option displays a listing of device names, their IP addresses and a user entered note of up to 75 characters.

```
Device Name            IP Address        Notes
----------------       ---------------   -----------------
Tokyo                  92.0.0.1          current device
Kyoto                  92.0.0.2          on link 1
Amsterdam              92.0.0.5          on link 2


Type: [s] to redraw, [=] main menu, any other key to end.
```

**note:** the [s] to redraw is case sensitive; it must be lower case.

**5 - Add Name**

Use the Add Name option to add a device name, IP address and any desired notes. Note that when a note is added, if spaces are desired within the note, you must enclose the note in quotations (“). Ensure that the note is not more than 75 characters in length.

```
Enter:
 Device name (up to 16 characters)
>

Enter:
 IP address
>

Enter:
 Notes
>
```

**6 - Remove Name**

The Remove Name option allows you to remove a selected name. Note that the removal of a name also automatically removes the IP address and any notes associated with the name.

```
Enter:
 all, Device name
>
```

## Upgrade Device Menu

```
                          UPGRADE DEVICE MENU

    Option                    Description
 1. VPN      - Upgrade to support VPN




Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **Upgrade Device Menu** may be used to enter a feature key code to enable VPN support on this router. Please contact your equipment supplier for information about obtaining this upgrade.

## Load FLASH Set-Up Menu

```
                          LOAD FLASH SET-UP MENU

   Option                   Description
 1. Console (ZMODEM)      - Load through serial port
 2. Network (TFTP)        - Load through IP network









Enter option number, "=" - main menu, <TAB> - previous menu


>
```

From the **LOAD FLASH SET-UP MENU,** the software in the router may be updated to the latest version. The download file, referred to in this section as "###.all", will be found in the directory with the new software release number ### (e.g. 05P.04.03.02).

**Considerations:**

When installing a new version of operating software in a router, ensure that the current configuration is backed up before the installation process is started (see Access Setup Menu: Dump and Restore options).

**Note:** this operation cannot be performed from a secondary IP address.

**1 - Console (ZMODEM)**

Resets the router and places it in Console load mode. Once the router is in Console load mode, the "###.all" file may be sent using the ZMODEM transfer protocol. The Console load mode may only be used with a direct connection to the serial management port of the router.

The ZMODEM application **must** be in 32 bit CRC mode for software upgrade transfers.
This option must be confirmed before operation by typing "yes" when prompted.

**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.

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

4) Start the ZMODEM transfer and send the file "###.all" from the Boot/Operational Code directory on the CD-ROM.
5) Once the ZMODEM transfer is complete, the router will verify the file "###.all" in memory, program and verify the FLASH, clear the configuration to default values (except the password), and then reset. After the reset, the router will operate normally using the newly upgraded software. A byte status message will be displayed on the console port during the programming of the FLASH.

   On the rare occasion that during the programming of the FLASH something happens to the 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: power down the bridge/router, remove the case cover, remove the jumper on pins 2-5 of strap W1, power up the bridge/router, power down the bridge/router, re-install jumper on w1 pins 2-5, replace the case cover and power up the bridge/router. The bridge/router should now restart and be in ZMODEM receive mode. Please refer to the Servicing Information section of the Installation & Applications Guide for information on removing the case and changing the strap settings.

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 and WAN interfaces will be disabled. The router will only accept information from the console management port.

The BOOT code of the P840 may be upgraded by performing a load of the "###.all" file from the BOOT/Operational Code directory on the CD-ROM.

Maximum connection speed for ZMODEM transfer on a P840 is 9600 Bps.

**2 - Network (TFTP)**

Resets the router and places it in Network Load mode. Once the router is in Network Load mode, a TFTP connection may be made to the router to upgrade to a new version of software. Make sure to disconnect any telnet sessions to the router before starting the TFTP transfer

The TFTP application must be in "octet" or "binary" mode for software upgrade transfers.

**Procedures for performing a 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. Login when connected.

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" to the router from the Boot/Operational Code dierectory on the CD-ROM.
(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, the Switch Type, Directory Numbers, SPIDs, Password and connection data for the remote site, if applicable), and then reset. After the reset, the router will operate normally using the newly upgraded software. In some upgrade situations the Directory Numbers and SPIDs may be corrupted after the upgrade and will need to be re-entered.

   - 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: power down the bridge/router, remove the case cover, remove the jumper on pins 2-5 of strap W1, power up the bridge/router, power down the bridge/router, re-install jumper on W1 pins 2-5, replace the case cover and power up the bridge/router. The bridge/router should now restart and be in ZMODEM receive mode. Please refer to the Servicing Information section of the Installation & Applications Guide for information on removing the case and changing the strap settings.

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.

**Considerations:**

When the router is placed in Network (TFTP) load mode, the router will restart and then remain idle.

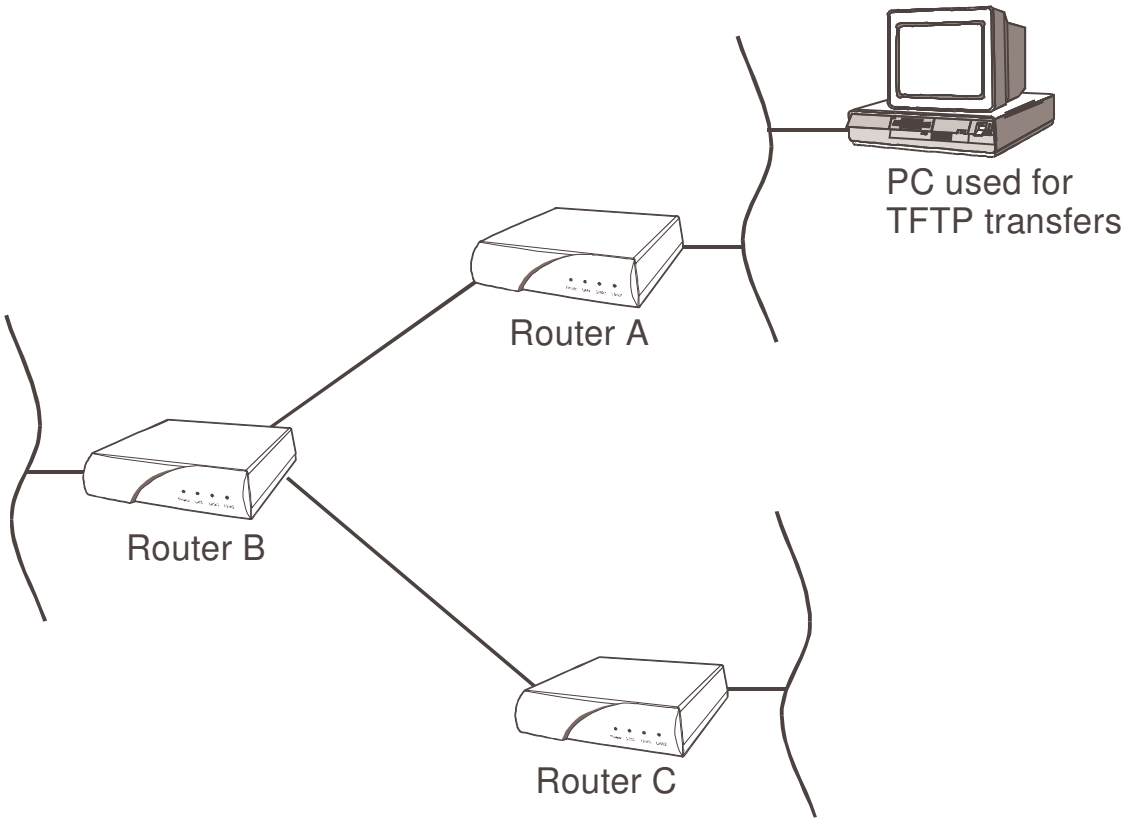
In the following diagram of a cluster of routers, when upgrading the three P840 routers in the diagram, the upgrade order should be Router C, then Router B, and finally Router A.

A TFTP software load to router 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.




.

## Console Menu

```
                          CONSOLE MENU

    Option          Description
 1. Dump          - Back-up configuration from console
 2. Restore       - Load configuration from console









Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The options in the **Console Menu** allow the current configuration settings of this router to be dumped to a backup device or for a saved configuration to be uploaded to restore the router to a previous configuration.

**Note:** Dump and Restore may not be performed over a telnet connection.

**1 - Dump**

Lists the configuration changes from the default settings to the console so it may be stored on a PC running a terminal-emulation package. It is recommended that after configuration of the bridge/router, the configuration changes be saved so that the device may be restored to these settings if required.

The Dump option should not be used during a connection to another bridge/router.

Note that only changes from the default settings are saved, not the entire configuration.

Two kinds of settings are not considered part of the configuration, and therefore are not included in the dump: trace settings and the password.

**Procedures for performing a Configuration Dump:**

1) Prepare the emulation package so that it is ready to accept the transfer of the configuration file.

2) Send the file (dump) to the PC disk using the Dump command.

3) Use a text editor to check the configuration file saved to the PC disk to confirm that information is still in order. If minor errors occurred, they may be corrected with the text editor. If errors were major, check the emulation package settings and dump the configuration again.

**2 - Restore**

Restores a configuration to the bridge/router that was previously saved to a disk file with the Dump command.

Note that the Restore will only restore those configuration settings that were changed from the default settings at the time the Dump was performed; Restore does not overwrite the entire configuration. Any changes made since the Dump was performed will not be overwritten and will thus remain in effect after the restore. It is strongly recommended that you do a full reset (under the Diagnostics menu) before performing a Restore to be certain that the system is restored to the state it was in at the time of the Dump. After a full reset, the IP address of the router must be re-entered.

**Considerations:**

The terminal-emulation package selected should have the capability to pace the loading of commands into the bridge/router. This may be done through the setting of a delay timer (character or line pacing) or a wait for the echo of the character before transmitting the next character.

The pacing function is commonly available, although pacing procedures will vary with each emulation package.

The Load option should not be used during a connection to another bridge/router.

**Procedures for performing a Configuration Load:**

1) Prepare the PC to transfer the configuration file.
2) Execute the Load command.
   Confirmation is required. Enter "yes" to proceed.
3) Send the file from the PC to the router.
4) When the transfer is complete, the configuration will have been restored to the bridge/router.

## Interfaces Set Up Menu

```
                          INTERFACES SET-UP MENU

   Option              Value         Description
 Device: DEV80e90e                                          V 05V4.6.2.8
                          INTERFACES SET-UP MENU

   Option              Value         Description
 1. LAN set-up         menu        - Define LAN environment
 2. WAN set-up         menu        - Configure WAN operation
 3. Terminal set-up    menu        - Define operator's console
 4. Voice set-up       menu        - Configure voice interface




Enter option number, "=" - main menu, <TAB> - previous menu
```

The **INTERFACES SET-UP MENU** contains

**1 - LAN Set-Up**

The LAN Set-up option takes you to the LAN Set-Up Menu, where the parameters for the Local Area Network configuration are configured.

**2 - WAN Set-Up**

The WAN Set-up option takes you to the WAN Set-Up Menu, where the Wide Area Network links are configured and controlled.

**3 - Terminal Set-Up**

The Terminal Set-up option takes you to the Terminal Set-Up Menu, where the terminal parameters used for the router console are selected.

**4 - VOICE Set-Up**

The Voice Set-up option takes you to the Voice Set-Up Menu, where the parameters for the Voice interfaces on this device are configured.

This menu option is not available when the voice module hardware is not installed in this P840.

## LAN Set-Up Menu

```
                          LAN SET-UP MENU

    Option                 Value          Description
 1. Bridge set-up          menu         - Define LAN port STP options
 2. IP set-up              menu         - Define IP parameters
 3. QOS set-up             menu         - Define Quality of Service for Interface




Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **LAN SET-UP MENU** contains options used to enable the router to be recognized as a device on the Local Area Network(s). This will enable it to bridge and route data, to connect to other routers across the LAN, and allow SNMP Network Management Stations to be able to access the router's SNMP agent.

If this is a model 5200 router that has a second LAN module installed, you will be requested to select for which LAN you wish to set the parameters, 1 or 2.

```
Enter :
    Set Reference LAN interface (1 or 2)
```

Once this is done, the options below are enabled.

**1. Bridge Set-Up**

The Bridge set-up option directs you to the LAN Bridge-STP Menu where STP Port parameters are set.

**2. IP Set-Up**

The IP set-up option takes you to the LAN IP Set-Up Menu where LAN IP routing parameters may be set for this LAN.

**3. QOS Set-Up**

The QOS Set-up option allows you to assign a QOS feature to this interface.

Note: This option is not displayed for a P1705 model

## LAN Bridge-STP Menu

```
                              LAN BRIDGE-STP MENU

    Option        Value          Description
 1. State        [enabled]     - Enable/disable port
 2. Path cost    [100]         - Define network cost for port
 3. Priority     [128]         - Set port priority









Enter option number, "=" - main menu, <TAB> - previous menu


>
```

The **LAN Bridge-STP MENU** allows the management of the LAN bridging state, path cost, and priority.

**1 - State**

The State option toggles between Enabling and Disabling of the Spanning Tree Protocol for the LAN port.

**Considerations:**

When the port is [enabled] the states are reported as Listen(ing), Learn(ing), Forward(ing) or Block(ing). If the port is disconnected, "Disabled" is shown in the Show Ports display (even if the state is enabled).

When the port is [disabled], it does not participate in frame relay or the learning process. Also, when [disabled] the port is not included in the STP topology calculations and will not be activated by the STP should it be needed to take over from a failed bridge.

**2 - Path Cost**

The Path Cost option allows the setting of the contributing path cost to the Root for this port.

**Contribution of Path Cost to Root Path Cost:**

The path cost to the Root Bridge is added to those path costs of other bridges along the same stream to the Root Bridge. The result is the Root Path Cost.

Once the Root Bridge is selected, a determination of which bridge(s) will become blocked where necessary is made. This determination is made by comparing the sum of the path costs (i.e. the Root Path Cost) to the Root Bridge. Where redundant paths exist, the bridge with the lowest Root Path Cost to the Root Bridge will become the *Designated Bridge* for the LAN. If all contending bridges' ports have the same Root Path Costs, then first their Bridge IDs (Priority/MAC address) and second their Port IDs (Port Priority) will be used as tiebreakers.

**Default:** [100]

**Range:** 1 to 65535

**Considerations:**

Increasing this value increases the total cost of the path to the Root Bridge. This may (depending on the topology) cause a bridge along the path to the Root bridge to be taken out of service and a blocked bridge to come into service.

Decreasing the value may have the opposite effect.

**3 - Priority**

The Priority option allows the setting of the port priority. This value is entered in decimal format and appears in hex format in the Port ID/Designated Port identifier (as applicable) of the Port Status display.

**Default:** [128] (decimal)

**Range:** 0 - 255

**Considerations:**

Increasing this value lowers the probability of this port becoming the Root port to the Root bridge. Decreasing this value increases the probability.

## LAN IP Set-Up Menu

```
                          LAN IP SET-UP MENU

    Option                 Value                Description
 1. Secondary IP set-up    menu               - Configure Secondary IP
 2. LAN - NAT set-up       menu               - LAN specific NAT setup
 3. IP address            "198.2.2.2" [24]    - Define IP address
 4. MTU size              [1500]              - MTU size at IP layer on LAN
 5. Routing protocol      [rip1_compatible]   - Define routing protocol
 6. RIP mode              [both]              - Define RIP send/receive mode
 7. Route cost            [0]                 - Cost added to learned routes




Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **LAN IP SET-UP MENU** contains options used to enable the router to be recognized as an Internet Protocol device on the network, to negotiate IP routes and to route IP data packets on the LAN.

**1 – Secondary IP Set-Up**

The Secondary IP Set-up option takes you to the Secondary IP set-up Menu, where this LAN may be configured to use secondary IP addresses on the local network for local routing.

**2 – LAN – NAT Set-Up**

The LAN-NAT set-up option takes you to the LAN-NAT set-up Menu, where Network Address Translation parameters for the primary LAN may be assigned. This option would be used when NAT is to be used between the primary LAN and the secondary LAN(s).

**3 – IP Address**

The IP Address option defines an Internet Protocol (IP) address and corresponding subnet size for the LAN. The LAN requires an IP address.

The P840 router supports SNMP that uses UDP for message transmission, and UDP runs on top of IP. An IP address is also required to connect to other routers across the LAN by using Telnet (for example, from a remote router to a local bridge).

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. 92.3.1.10). Each decimal number must be less than or equal to 255, that is the maximum value of each 8-bit field.

The size of subnet mask variable defines the number of bits in an IP address to be used for network and subnetwork addressing (the remainder being used for host addressing). Subnetting allows multiple logical networks within a single standard IP network address.

**Note:** after changing the IP address of this LAN, a soft reset must be performed to bring the change into effect.

**Default:** [none]

```
Enter :
    none, internet address (up to 15 characters)
>

Enter :
    size of subnet mask (from 8 to 32)
>
```

**4. MTU size**

The Maximum Transmission Unit – the largest size, in bytes, of the data packet (including headers) transmitted. Data packets above this size will be fragmented. The standard MTU sizes for ethernet and PPP are 1500 bytes. As IPSec processing increases the size of the IP packet, there is an increased chance of fragmentation. If there is a path segment that has a smaller MTU, it is generally better to fragment packets at the origin (this router) using this option than assuming they will be fragmented en route (if the path segment cannot do fragmentation, the packet will not be transmitted). Packet fragmentation can be tuned with the Ping option (8) in the Applications menu.

**Default:** [1500]

**5 - Routing Protocol**

The Routing Protocol option defines the type of IP routing protocol to be used on this Local Area Network. The P840 may be set up to use different types of IP routing protocols on each of its LANs and WAN links.

When the routing protocol is defined as none, the P840 will operate as an IP router but will NOT participate in the exchange of RIP messages between the other IP routers in the network. All IP routing is accomplished by using the static routes table. All routes within the network must be manually entered in the static routing table.

When the routing protocol is defined as rip1, the P840 will operate as a RIP1 IP router. All routing information will be sent and received via broadcast RIP packets.

When the routing protocol is defined as rip1_compatible, the P840 will operate as a RIP2 IP router in broadcast mode. All routing information will be sent via broadcast RIP2 packets. Routing information may be received as broadcast RIP1, broadcast RIP2, or multicast RIP2.

When the routing protocol is defined as rip2, the P840 will operate as a RIP2 IP router. All routing information will be sent via multicast RIP2 packets. Routing information may be received as broadcast RIP2 or multicast RIP2.

Partner routers connected on the network do not need to have their IP routing protocols set to the same values. An IP router at a central site may have it's routing protocol set to RIP so that it may continue to listen to RIP messages and adapt to the changes of the local network, while the remote locations, with their default routes back to the main router, cannot propagate any incorrect routing information that might be present on the remote segments. Each of the routers at the remote sites would have their routing protocol set to none.

**Default:** [rip1_compatible]

**Choices:** none, rip1, rip1_compatible, rip2

**5 - RIP Mode**

The RIP Mode option defines how this P840 will participate in RIP IP routing message exchange for this subnet.

When the RIP mode is set to both, the P840 will send and receive RIP routing messages.
When the RIP mode is set to send_only, the P840 will only send RIP routing messages.
When the RIP mode is set to receive_only, the P840 will only receive RIP routing messages.

**Default:** [both]

**Choices:** both, send_only, receive_only

**7 - Route Cost**

The Route Cost option defines the amount of extra routing cost to add to routes that are learned from this LAN. This added cost may be useful in forcing learned routes to have a higher cost when they are across a slower LAN connection.

**Default:** [0]

## Secondary IP Set-up Menu

```
                          SECONDARY SET-UP MENU

   Option                    Value          Description
 1. Edit secondary entry     menu         - Modify/add Secondary IP entry
 2. Show secondary entries                - Display secondary IP entries
 3. Remove secondary entry                - Delete secondary IP entry


Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The Secondary IP Set-Up Menu contains options to configure secondary Local Area Networks or subnetworks on this network. This provides the ability to set up a number of independently addressed virtual networks or subnetworks on the same physical local area network (also known as Secondary IP Addressing). Up to 16 secondary IP networks may be defined on this router.

**1 - Edit Secondary Entry**

The Edit Secondary Entry option takes you to the Edit Secondary Entry Menu, where the parameters for the secondary IP networks are defined.

**2 - Show Secondary Entries**

The Show Secondary Entries option displays a listing of the entries in the Secondary local network table.

```
                Secondary              Subnet              Secondary IP
 ID    Alias    IP Address          Size / Mask            Subnet/Network
 --   -------   ---------------   ---------------------   ----------------
  1   LAN.1     199.65.43.21       24   255.255.255.0     199.65.43.0
  2   LAN.2     198.123.45.67      28   255.255.225.240   198.123.45.64
 12   LAN.12    199.76.54.32       14   255.252.0.0       199.76.0.0
```

**ID:** the identification numbers between 1 and 16 entered for the secondary local networks

**Alias:** the alias names assigned (automatically) to the secondary local networks; set as LAN.id#

**Secondary IP Address:** the IP addresses of each of the secondary local networks

**Subnet Mask Size:** the number of bits set in the subnet mask for each of the secondary IP networks

**Subnet mask:** the four decimal number representation of the bits set for the subnet mask.

**Secondary IP Subnet / Network:** the network or subnet IP address of the secondary subnet or network as defined by the Secondary IP Address and subnet mask.

**3 - Remove Secondary Entry**

The Remove Secondary Entry option allows you to delete a selected entry from the secondary local network table, or to clear all entries.

## Edit Secondary Entry Menu

```
                          EDIT SECONDARY ENTRY MENU

    Option              Value          Description
 1. Secondary IP      *[        ]   - Secondary IP address
 2. Mask size         *[        ]   - Secondary subnet mask size
 3. Subnet mask       *[        ]   - Secondary subnet mask
 4. Routing protocol   [        ]   - Define routing protocol
 5. RIP mode           [        ]   - Define RIP send/receive mode
 6. Private route      [        ]   - Do not advertise this route
 7. Route cost         [        ]   - Cost added to learned routes




Enter :
    Set the entry ID (from 1 to 16)


>
```

The Edit Secondary Entry Menu provides options for entering parameters for routing to secondary networks or subnetworks through this router.

When an ID number for a secondary network is entered for the first time, you will be prompted to enter the defining IP address and mask size for the network. Once the secondary network is defined, the IP address and mask cannot be edited with this menu; the entry must be removed and re-entered to change these parameters.

**1 - Secondary IP**

The Secondary IP Address for this router on the secondary network or subnet with the new ID number is entered here the first time the ID number for this secondary network is entered.

The secondary IP address is used to access the secondary subnet or network through this router.

The IP address consists of 4 eight-bit fields separated by periods ("**.**"), where each field is specified by a decimal number (e.g. 92.3.1.10). Each decimal number must be less than or equal to 255 (the maximum value of an 8-bit binary number).

* Display only. This address is set when the entry is defined for the first time and may not be changed here; to make a change, the entry must be removed from the secondary address table and re-entered.

**2 - Mask Size**

The Mask Size defines the number of contiguous bit locations from the start of the IP address to be used for the subnet mask for this secondary network. The Subnet Mask when applied to the secondary IP address defines this Secondary IP subnet or network.

* Display only. This number is set when the entry is defined for the first time and may not be changed here; to make a change, the entry must be removed from the secondary address table and re-entered.

**3 - Subnet Mask**

The Subnet Mask option displays the subnet mask defined by the subnet mask size in option 2.

* Display only. This mask is set when the mask size entry is defined for the first time and may not be changed here; to make a change, the entry must be removed from the secondary address table and re-entered.

**4 - Routing Protocol**

The Routing Protocol option defines the type of IP routing protocol to be used on this secondary network.

When the routing protocol is defined as none, the P840 will NOT participate in the exchange of RIP messages for this secondary network with the other networks. Routing on this secondary network is accomplished by using static routes. All routes within this secondary network must be manually entered as the static routes. Host devices and other routers on this network must be statically configured (they will not receive RIP messages). Routes with next hops on this network must be statically configured on this router. In addition to the static routes entered, this router will use routing information learned from other interfaces and networks

When the routing protocol is defined as rip1, the P840 will use RIP1 IP protocol for this secondary network. All routing information will be sent and received via broadcast RIP packets.

When the routing protocol is defined as rip1_compatible, the P840 will use RIP2 IP protocol in broadcast mode for this secondary network. All routing information will be sent via broadcast RIP2 packets. Routing information may be received as broadcast RIP1, broadcast RIP2, or multicast RIP2.

When the routing protocol is defined as rip2, the P840 will use RIP2 IP protocol for this secondary network. All routing information will be sent via multicast RIP2 packets. Routing information may be received as broadcast RIP2 or multicast RIP2.

Networks on this router do not need to use the same IP routing protocols. For example, one secondary network may be set as RIP_compatible to learn and advertise changes to the network, while another may be set to none and must use static routes.

**Default:** [rip1_compatible]

**Choices:** none, rip1, rip1_compatible, rip2

**5 - RIP Mode**

The RIP Mode option defines how this P840 will participate in RIP IP routing message exchange for this subnet.

When the RIP mode is set to both, the P840 will send and receive RIP routing messages.

When the RIP mode is set to send_only, the P840 will only send RIP routing messages.

When the RIP mode is set to receive_only, the P840 will only receive RIP routing messages.

**Default:** [both]

**Choices:** both, send_only, receive_only

**6 - Private Route**

Setting this secondary network IP address to be a private route causes the IP address and network to not be advertised in the RIP information.

**Default:** [disabled]

**7 - Route Cost**

The Route Cost option defines the amount of extra routing cost (in hops) to add to routes that are learned from this Secondary network. This can be used in the case of multiple routes to artificially increase the cost of a less preferred route so that it will be used only if the preferred route is not available. The cost will not be added (and thus not appear in the route statistics) until a connection is made.

**Default:** [0]

## LAN – NAT Menu

```
                              LAN - NAT MENU

   Option                 Value          Description
 1. Translation type      [port]       - Define translation method
 2. Dynamic IP pool       [none]       - Dynamically assigned mappings
 3. Show address pool                  - Display IP mappings
 4. Add static entry                   - Specify IP-IP mapping
 5. Remove static entry                - Remove static IP mapping
 6. NAT enabled           [disabled]   - Enable address translation



Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The LAN - NAT Menu sets parameters for the NAT address pool for the primary LAN. Network Address Translation (NAT) is a technique that translates private IP addresses on a private network to valid global IP addresses for access to another network. Network Address Port Translation (NAPT) translates both the IP address and the port. The advantage of port translation is that more than one private IP address can be translated to the same single global IP address. NAPT allows data exchanges initiated from hosts with private IP addresses to be sent to other networks via the P840 using a single global IP address. Port translation can also be used from one private network to another private network if the two networks have conflicting IP addresses.

**1 - Translation Type**

This option sets the address translation method to be used for NAT. The address may be translated as either a port or an internal IP address. With IP address translation, each internal IP address is mapped to one global IP address; with port translation, several internal IP addresses may be mapped to a single global IP address.

**Default:** [port]

**2 - Dynamic IP Pool**

The Dynamic IP Address Pool option defines the block of global IP addresses that may be used to map to internal addresses. The router will assign a global IP address from this pool to the internal address of a device on the network.

The first address in the range must be specified followed by the number of addresses in the pool. The pool size may be up to 253 addresses.

**Note:** The pool may not have a pool size assigned such that the pool would contain an address that is a broadcast address (all binary 1s in the host portion of the IP address) for standard A, B or C class networks. If a pool size is entered which causes this condition, the following warning will be displayed:

```
Pool can not have that many addresses with the start address specified, Enter:
```

Enter a smaller size for the pool or assign a different starting address.

**3 - Show Address Pool**

This option displays the IP address pool for this remote site.

```
                          NAT ADDRESS POOL

Pool Address        Type    Actual Address                Status
------------        -----   --------------                ---------
12.34.5.6           Static  196.23.45.6                   In use
12.34.5.12          Static  196.23.45.24                  Reserved
23.45.6.10          Dynamic 123.45.67.8                   In use
23.45.6.11          Dynamic None assigned                 Available
23.45.6.12          Dynamic None assigned                 Available
23.45.6.13          Dynamic None assigned                 Available
```

The Pool Address is the internal address to be used on this network; the Actual Address is the global IP address to which the internal address is assigned.

When the last dynamically assigned address in the address pool is reached, the router will automatically use port translation with that address in order to allow as many connections as possible. If there are zero or one address specified for the pool, then port translation will be used for all connections. If zero, the address assigned by the remote router IPCP or the address specified in the "Peer IP address" option will be used. If one address is specified, that address will be used.

**4 - Add Static Entry**

The Add Static Address option assigns a specific internal IP address of a device to a specific global IP address. When this option is selected, first enter the internal IP address to be assigned then the global IP address.

**5 - Remove Static Address**

The Remove Static Address option removes the static address assignment from the address pool. Addresses may be removed individually by entering the global IP address to be taken off, or the entire list of static address assignments may be cleared by entering "all".

**6 - NAT Enabled**

The NAT enable option enables or disables Network Address Translation on the LAN.

When NAT is enabled this router will not send RIP messages out. The router will be able to receive RIP requests. IP pattern filters and Firewall use the non-translated IP address. (i.e. the private IP address that is used on the private network).

**Default:** [disabled]

## LAN QOS Set-up Menu

```
                          LAN QOS SET-UP MENU

    Option                 Value           Description
 1. Queueing strategy     [priority] [1] - Define type of queueing strategy



Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The LAN QOS SET-UP MENU allows you to specify a Priority List to the interface. A Priority List contains items which defined packet parameters which can be assigned to a high, medium, normal or low priority queue.

**1. Queueing Strategy**

The Queueing Strategy option define the type of QOS method and the Priority List ID to be assigned to the LAN interface.

The first parameter of the Queueing strategy defines the type of Quality of Service applied to the LAN interface

**Default**: [none]
**Choices**: none, priority

The second parameter of the Queueing strategy assigns the QOS priority list to be assigned to the LAN interface. The QOS Priority List is defined by numbers and only one can be assigned to the LAN interface.

**Default**: [no default value]
**Range**: 1 to 16

Note:
This parameter only appears if the first parameter has been set to priority.

## WAN Set-Up Menu

```
                              WAN SET-UP MENU

    Option                 Value          Description
 1. Switch type           [NI-1]        - Set switch type
 2. Link set-up            menu         - Configure link parameters




Enter option number, "=" - main menu, <TAB> - previous menu


>
```

The **WAN SET-UP MENU** allows the definition of link operation for the router.

**1 - Switch Type**

Choosing the Switch Type option defines the ISDN switch (signaling) type that this router is connected to.

When the Switch Type is changed, a **Soft Reset** must be performed for this to take effect. This allows the router to initiate operation with the new switch type.

**Default:** If S/T module is installed: [NET3]
If U module is installed: [NI-1]

**Choices:** DMS-100, NI-1, NI-2, 5ESS-PP, 5ESS-MP, NET3, TPH1962, KDD, SWEDEN, and NTT

**Considerations:**

The 5ESS switch types are split into two versions: 5ESS-PP (point to point) and 5ESS-MP (multipoint). In ISDN, point to point means that both B channel links in an ISDN BRI are used for a connection between a pair of devices. Multipoint means that one link of the BRI may be used to connect to one device, the other link may be used to connect to a different device.

**3 - Link Set-Up**

The Link Set-up option takes you to the Link Set-Up Menu, where the link interfaces are configured. Directory numbers and Service Profile Identifiers are defined for the ISDN B-channels.

## Group Set-Up Menu

```
                              GROUP SET-UP MENU

    Option                  Value         Description

 1. Force 56k       [disabled]    - Force 56k rate adaptation
 2. Hunt group #    [none]        - Set common telephone number
 3. Add link                      - Add a specific link to this group
 4. Show groups




Enter:
    group number (1 or 2)

> 1
```

The above display is the first level of the **GROUP SET-UP MENU**. Once the group number is entered, the group number specified is added to the menu title bar and the Options are as shown below:

```
                            GROUP SET-UP 1 MENU

    Option                  Value         Description

 1. Force 56k       [disabled]    - Force 56k rate adaptation
 2. Hunt group #    [none]        - Set common telephone number
 3. Add link                      - Add a specific link to this group
 4. Show groups



Enter:

>
```

The **GROUP SETUP MENU** provides for grouping sets of ISDN B-channels together. These sets may be hunt groups or callback groups.

A hunt group phone number is defined by the ISDN service provider. This method of grouping the B-channels allows one ISDN phone number to be used to establish connections from remote site devices to multiple B-channels on the central site device. A group of single link protocol remote site devices may all dial in to the same ISDN phone number at the central site and contend for a link connection. This greatly simplifies the configuration process.

**Consideration:** If this P840 is configured with remote site callback enabled, (this router will place a return call when it receives a prompting call from a remote site), then a callback group should be set up. A callback group is a grouping of one (the primary ISDN call number) or two (primary and alternate) ISDN numbers that a remote site router may dial to trigger the callback from this P840. If a callback group is not set up, the callback would come from the first available ISDN link; if this was not be the primary or alternate number used by the remote site router, the callback would be rejected by the remote site.

.

By default, all B-channel links are initially configured to be in group 1. Group 1 is defined with multilink operation disabled.

.

**Note:** this menu will only be displayed if the Logical ISDN Type set to ISDN.

**1 - Force 56K**

This option forces the B-channels in this group to use V.110 rate adaptation for all incoming and outgoing calls.

If the path to a destination number passes through a 56 Kbps digital circuit or the destination itself is a 56 K switched digital service, V.110 rate adaptation must be performed to allow the data to be sent at 56 K on the 64 K ISDN lines. When an ISDN call is placed, the local ISDN service must be informed that V.110 rate adaptation is required to fully complete this connection. Adding a percent symbol "%" before the ISDN number will cause the P840 to send a message to the local ISDN service requesting V.110 rate adaptation.

**Note:** The link must be disconnected for this operation to take effect.

**Default:** [disabled]

**2 - Hunt Group #**

Enter the Hunt Group ISDN phone number assigned to this group of B-channels by the ISDN circuit provider. This Hunt Group number is used by this P840 to inform the remote site partner devices which ISDN number to call when performing a "suspend" or "resume" of a connection managed circuit. This means that the remote site device will call the Hunt Group number when attempting to re-establish the ISDN call.

**Note:** Hunt Groups are a service from ISDN service providers and must be requested from them. If you have not subscribed for Hunt Group service, select "none" as the entry for this option. If a Hunt Group number is not defined, the ISDN number of the B-channel used to establish the call will be used for connection management negotiations.

When adding entries to the Stored Number table on remote partner ISDN P840 routers, this Hunt Group Number should be entered in the ISDN Number section in the table on the remote P840.

**Default:** [none]

```
Enter :
    none, Directory number (up to 35 characters)

>
```

**3 - Add Link**

Use this option to add a B-channel link to this group. Each link must always belong to only one group, so adding a link to a group will remove it from the previous group.

```
Enter :
    link number (1 or 2)

> 1
```

**4 - Show Groups**

Choosing this option displays an overview of the group configurations.

```
                          Groups Configuration

 Group Force Directory                Links
   #    56K   number                 1   2
   1          9876543                *
   2     Y    12345678                   *
```

## Link Set-Up Menu

```
                              LINK SET-UP MENU

    Option                  Value          Description
 1. Physical link type  *[         ]




Enter:
    link number (1 or 2)

> 1
```

The above display is the first level of the **LINK SET-UP MENU**. Once the WAN link number is entered, the link number specified is added to the menu title bar and one of the menus shown on the following pages will appear. The menu displayed will depend on whether an ISDN or a leased line interface module is installed for that link.

## Link Set-Up Menu - ISDN

If the link has an **ISDN BRI** interface module and the logical ISDN type is **ISDN**, the menu will be:

```
                              LINK SET-UP 1 MENU

    Option                    Value          Description
 1. Physical link type      *"BRI"
 2. Link operation           [enabled]     - Enable/disable link
 3. Link IP MTU size         [1500]        - MTU size at IP layer on link
 4. Logical ISDN type        [ISDN]
 5. ISDN set-up               menu         - Configure ISDN operation
 5. Group                    [1]




Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **LINK SET-UP MENU** allows the configuration the link connections on this P840. The options displayed for this menu will vary depending on what interface modules are installed on this router.

**1 - Physical link type**

The Physical Link Type option displays the type of interface module installed for this link. This is a display-only item and may not be changed.

**Values:** BRI

**2 - Link Operation**

The Link Operation option toggles between [enabled] and [disabled] to allow this link to be used for connections.

**Default:** [enabled]

**3. Link IP MTU size**

The Maximum Transmission Unit – the largest size, in bytes, of the data packet (including headers) transmitted. Data packets above this size will be fragmented. The standard MTU sizes for ethernet and PPP are 1500 bytes. As IPSec processing increases the size of the IP packet, there is an increased chance of fragmentation. If there is a path segment that has a smaller MTU, it is generally better to fragment packets at the origin (this router) using this option than assuming they will be fragmented en route (if the path segment cannot do fragmentation, the packet will not be transmitted). Packet fragmentation can be tested with the Ping option (8) in the Applications menu.

**Default:** [1500]

**4 - Logical ISDN Type** (if BRI module installed on this link)

The Logical ISDN Type option allows you to select between a switched (dial up) ISDN circuit or a digital leased circuit to configure the router to match the type of service connected to this interface module.

The ISDN option is used when a switched (dial up) ISDN service is connected to the BRI module.

The Digital_Leased option is used when a permanent leased ISDN circuit is available from your ISDN service provider and is connected to the BRI module; please see the Link Set-up menu on following pages for a description of this option.

When this link is set to use digital leased circuits instead of switching circuits, the ISDN call establishing functions are not displayed on the menu.

**Default:** [ISDN]

**Values: ISDN, Digital_Leased**

**Considerations:**

The state of the Logical ISDN type option is saved when performing a software upgrade. This means that when the P840 restarts, it will return to the operation state that was enabled before the upgrade was performed.

**5 - ISDN Set-Up**

The ISDN Set-Up option takes you to the ISDN Set-up menu where ISDN switch types and other ISDN parameters may be set.

**Note:** this option appears only if the router has an ISDN BRI module installed on this link and Logical ISDN Type is set to ISDN.

**5 - Group**

The identifying number of the Group to which this link is to belong is set here.

**Default:** [1]

**Choices:** 1 or 2

**Note:** Groups may also be set under the Group Set-up Menu. Links set in that menu need not be set here.

## Link Set-Up Menu – Digital Leased

If the link has an **ISDN BRI** interface module and the logical ISDN type is **Digital_Leased**, the menu will be:

```
                          LINK SET-UP 1 MENU

   Option                  Value         Description
 1. Physical link type    *"BRI"
 2. Link operation         [enabled]          - Enable/disable link
 3. Link IP MTU size       [1500]             - MTU size at IP layer on link
 4. Logical ISDN type      [Digital_Leased]
 5. Frame Relay            [enabled]          - Enable/disable frame relay
 6. Frame relay set-up      menu              - Configure Frame relay
 7. Phantom power detect   [disabled]         - Detect phantom power
 8. Link B channel        *[B1]               - Assign B channel




Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **LINK SET-UP MENU** configures the link connections on this P840. The options displayed for this menu will vary depending on what interface modules are installed on this router.

**1 - Physical link type**

The Physical Link Type option displays the type of interface module installed for this link. This is a display-only item and may not be changed.

**Values:** BRI

**2 - Link Operation**

The Link Operation option toggles between [enabled] and [disabled] to allow this link to be used for connections.

**Default:** [enabled]

**3. Link IP MTU size**

The Maximum Transmission Unit – the largest size, in bytes, of the data packet (including headers) transmitted. Data packets above this size will be fragmented. The standard MTU sizes for ethernet and PPP are 1500 bytes. As IPSec processing increases the size of the IP packet, there is an increased chance of fragmentation. If there is a path segment that has a smaller MTU, it is generally better to fragment packets at the origin (this router) using this option than assuming they will be fragmented en route (if the path segment cannot do fragmentation, the packet will not be transmitted). Packet fragmentation can be tuned with the Ping option (8) in the Applications menu.

**Default:** [1500]

**4 - Logical ISDN Type** (if BRI module installed on this link)

The Logical ISDN Type option allows you to select between a switched (dial up) ISDN circuit or a digital leased circuit to configure the router to match the type of service connected to this interface module.

The ISDN option is used when a switched (dial up) ISDN service is connected to the BRI module; please see previous Link Set-up Menu for a description of this option.

The Digital_Leased option is used when a permanent leased ISDN circuit is available from your ISDN service provider and is connected to the BRI module. A digital leased circuit is permanently established by your service provider and does not require ISDN phone numbers or dialing functionality. When a digital leased circuit is established, the P840 will treat it as if it were a normal 64 Kbps leased line connection for each assigned B-channel.

When this link is set to use digital leased circuits instead of switching circuits, the ISDN call establishing functions are not displayed on the menu.

**Default:** [ISDN]

**Values:** ISDN, Digital_Leased

**Considerations:**

The state of the Logical ISDN type option is saved when performing a software upgrade. This means that when the P840 restarts, it will return to the operation state that was enabled before the upgrade was performed.

**The following options appear if an ISDN module is present and Logical ISDN Type is set to Digital_Leased:**

**5 – Frame Relay**

The Frame Relay option allows you to select between a frame relay circuit or a PPP leased circuit to configure the router to match the type of service connected to this interface module.

When this link is set to use Leased instead of Frame Relay, the Frame Relay options are not displayed on the menu.

**Default:** If International software loaded: [disabled] – router is in Leased Line mode.
If North American software loaded: [enabled] – router is in FrameRelay mode.

The router will request confirmation of the change when this menu item is selected, enter "yes"

**Considerations:**
The state of the Logical Leased type option is saved when performing a software upgrade. This means that when the P840 restarts, it will return to the operation state that was enabled before the upgrade was performed.

**6 – Frame Relay Set-Up**

The Frame Relay Set-up option takes you to the Frame Relay Set-up menu where auto-learning may be disabled and LMI parameters set.

**Note:** this option appears only if the ISDN Type is set to Digital Leased and FrameRelay is enabled.

**6/7 - Phantom Power Detect**

Most NT-1s provide a signal to the connected ISDN device to indicate that the NT-1 is powered up and functioning correctly. This signal is generally called phantom power. Some NT-1s do not support phantom power. This option should be disabled if the NT-1 connected to the ISDN link module does not support phantom power.

If the P840 is having difficulty obtaining a connection to the NT-1, this option should be disabled.

**Default:** [disabled]

**Considerations:** This option will not appear when the WAN module is an ISDN type U interface.

**7/8 - Link B Channel**

When the digital leased circuit option is configured on an ISDN BRI link, the ISDN B-channels must be assigned to link numbers for normal operation. When a B-channel on the BRI is assigned to a link number, the P840 then treats the ISDN B-channel as a 64 Kbps leased line connection. If only one B channel is set to digital leased and the other is set to ISDN, then the B channel is automatically assigned and is not changeable (B1 for even link numbers, B2 for odd links). If both B channels on the BRI are set to digital leased, the B channels may be assigned as follows:

Link 1 may be assigned B-channel 1, B-channel 2 or both.

If link 1 is assigned B-channel 1, the other channel is available to service link 2 on the ISDN module; if link 1 is assigned B-channel 2, the other channel is not available.

This option is available only when the Digital Leased Circuit option is enabled.

```
Enter :
    B1, B2, B1–B2

>
```

If B-channel 2 has not previously been assigned to the odd numbered link on this ISDN module, the even numbered link may be assigned B-channel 2 or none.

If link 2 is assigned none, it is not available for user data connection. It may still be used as the second channel for 128 Kbps communication or for voice (if enabled).

This option is available only when the Digital Leased Circuit option is enabled.

```
Enter :
  B2, none

>
```

**Considerations:**

If B-channel 2 is already claimed by link 1 and you wish to reassign it to link 2, you must first reassign B1 to link 1 (select "B1"); otherwise, the following error display will appear:

```
Error: B2 is currently allocated to first link
```

## ISDN Set-Up Menu

```
                              ISDN SET-UP MENU

    Option                    Value          Description
 1. Dial prefix               [none]       - Set dial prefix
 2. Phantom power detect      [disabled]   - Detect phantom power
 3. Force 56k                 [disabled]   - Force 56k rate adaptation
 4. Directory number          [none]       - Set directory number
 5. SPID                      [none]       - Link service profile identifier


Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **ISDN SET-UP MENU** provides for stored ISDN number set-up.

**Note:** this menu appears only if this router has an ISDN module installed and Logical ISDN type is set to ISDN (not Digital Leased).

**1 - Dial Prefix**

The Dial Prefix option is used when the ISDN P840 is attached to an ISDN PBX. If a dialing prefix is required before an outside line is obtained, the dialing prefix must be entered here.

**Default:** [none]

**2 - Phantom Power Detect**

Most NT-1s provide a signal to the connected ISDN device to indicate that the NT-1 is powered up and functioning correctly. This signal is generally called phantom power. Some NT-1s do not support phantom power. This option should be disabled if the NT-1 connected to the ISDN link module does not support phantom power.

If the P840 is having difficulty obtaining a connection to the NT-1, this option should be disabled.

**Default:** [disabled]

**Considerations:** This option is not available when the link module is an ISDN type U interface.

**3 - Force 56K**

This option forces both B-channels on this P840 router to use V.110 rate adaption for incoming and outgoing calls.

If the path to a destination number passes through a 56 Kbps digital circuit or the destination itself is a 56 K switched digital service, V.110 rate adaption must be performed to allow the data to be sent at 56 K on the 64 K ISDN lines. When an ISDN call is placed, the local ISDN service must be informed that V.110 rate adaption is required to fully complete this connection.

**Note:** Adding a percent symbol "%" in the ISDN number will cause the P840 to send a message to the local ISDN service requesting V.110 rate adaption.

**Default:** [disabled]

**4 - Directory Number**

Enter the ISDN number of the B-channel (up to 15 characters). The ISDN number is available from the ISDN circuit provider. For a type NI-1 switch, enter only the local portion of the directory number, unless the area code is required for local calls.

When the Directory Number is changed, a **Soft Reset** must be performed for this to take effect. The router will be reset and begin operation with the new directory number.

**Default:** [none]

**Note:** in Net3 ISDN environments with BACP enabled, directory numbers must be configured for BACP to function.

**The following option appears when an ISDN switch type is set to NI-1, NI-2, DMS-100 or 5ESS-MP:**

**5 - SPID**

Enter the ISDN Service Profile Identifier (SPID) number assigned to this B-channel. The SPID number is available from the ISDN circuit provider.

When the SPID is changed, a **Soft Reset** must be performed for this to take effect. The router will be reset and begin operation with the new SPID.

## Frame Relay Set-Up Menu

```
                    LINK SET-UP 1 FRAME RELAY SET-UP MENU

 Option               Value          Description

 1. Auto-learning     [disabled]   - Enable/disable LMI and DLCI learning
 2. LMI type          [ansi]       - Network interface
 3. Polling interval  [10 sec]     - Request network status
 4. Enquiry interval  [6]          - Full status enquiry
 5. Error threshold   [3]          - Enquiry failure tolerance
 6. Monitored events  [4]          - Error count interval



Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **FRAME RELAY SET-UP MENU** allows the configuration of the frame relay parameters for the link. The options displayed in this menu will depend on the Auto-Learning setting selected

**Note:** this menu will be displayed if this link has Frame Relay enabled in the Link Set-UP Menu.

**1 - Auto-Learning**

The Auto-Learning option toggles between [enabled] and [disabled] to allow this frame relay router to try to auto-learn the LMI type as well as the configured DLCI values on the frame relay service.

When the frame relay router 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 inquiry messages. If the DLCI numbers of the PVC's on your service are determined during startup, the P840 will automatically create a remote site profile for each PVC. The automatically created remote site profiles will be named "LinkxDLCIyyy" where x is the physical link number the PVC is on and yyy is the DLCI of the PVC. These automatically created remote site profiles may be renamed for easier usage by changing the Remote Site Alias within the Edit Remote Site menu.

**Default:** [enabled]

**Considerations:**

If during this learning process the maximum number of remote sites has been reached, the P840 will prompt you that there are no remote sites available. A new remote site cannot be auto-created unless one of the existing remote sites is manually deleted. To remove a particular remote site, the PVC for that site must first be disabled (option 8 of the Main/Configuration/WAN set-up/Remote Site/Edit Remote Site/Connection set-up menu), then removed (option 4 of the Main/Configuration/WAN/Remote Site set-up menu). All remote sites on a link may be cleared by toggling the enable/disable function for the link, toggling the enable/disable function for auto-learning, or doing a soft reset.

**Note:** Auto-leaning with PPP Frame Relay is not compatible with some earlier model routers. In case of problems with auto-learning, try switching to raw 1490 frame relay operation (disable PPP for the remote site connection).

**2 - LMI Type**

The LMI Type option specifies 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 P840 simply creates frame relay packets and sends them on the defined PVCs. The links are not checked for errors. There is no congestion control checking. The link is only monitored for control signals.

**Default:** [none]

**Choices:** ansi, ccitt, lmi, none

**Considerations:**

The "ansi" LMI type operates as defined in the ANSI T1.617 Annex D specification and supports only permanent virtual circuits.

The "ccitt" LMI type operates as defined in the ITU-T Q.933 Annex A specification and supports only permanent virtual circuits.

The "lmi" LMI type operates as defined in the "Frame Relay Specification with Extensions Based on Proposed T1S1 Standards" specification and supports only permanent virtual circuits.

**The following options are only displayed if the auto-learning option is set to "*disabled*" and the LMI type is set to a value other than "*none*":**

**3 - Polling Interval**

The Polling Interval option specifies the time interval at which the P840 will poll the Frame Relay switch for the management status.

**Default:** [10 sec]

**Range:** 5 to 30 seconds

**4 - Enquiry Interval**

The Enquiry Interval option specifies the frequency at which the P840 will request a full status update from the Frame Relay service. The Enquiry Interval is expressed in numbers of Polling Intervals. By default, every 6$^{th}$ poll will be a full status update instead of just a management update.

**Default:** [6]

**Range:** 1 to 255

**5 - Error Threshold**

The Error Threshold option specifies how many unanswered status inquiries to send to the Frame Relay switch before determining that the link has failed.

**Default:** [3]

**Range:** 1 to 10

**6 - Monitored Events**

The Monitored Events option specifies the number of status inquiries that are to be monitored when determining the Error Threshold. By default, if the P840 does not receive responses to 3 of the last 4 status inquiries, the link will be considered failed.

**Default:** [4]

**Range:** 1 to 10

## Terminal Set-Up Menu

```
                          TERMINAL SET-UP MENU

    Option      Value          Description
 1. Terminal   [vt100]      - Define console terminal type
 2. Show                    - Display terminal definitions
 3. Add                     - Create a custom terminal definition
 4. Remove                  - Delete a terminal definition









Enter option number, "=" - main menu, <TAB> - previous menu


>
```

From the **TERMINAL SET-UP MENU,** the terminal used for the router console is defined. A custom definition can be added if the terminal to be used is not presently supported by the router.

**1 - Terminal**

The Terminal option defines the terminal type to be used for the router console. The current terminal type is displayed in the Value column for this option. When this option is selected, the available terminal types are displayed.

**Default:** Terminal type chosen at first power-up

**Choices:** ansi, avt, ibm3101, qvt109, qvt102, qvt119, tvi925, tvi950, vt52, vt100, wyse-50, wyse-vp, teletype

**Considerations:**

If your terminal is not listed:

1) Choose another of the same make to try the features it provides; or,

2) Choose the terminal type **teletype**. This terminal type operates in scroll mode and does not offer the highlighting that may be provided with the pre-defined or custom terminal types. Operating in this mode does not prevent any of the operations of the router.

3) For a complete solution, create your own custom terminal type and add it to the types supported by the router using the Add option.

**2 - Show**

The Show option displays all terminal definitions. This listing may be of use if you need to create a custom terminal definition.

**3 - Add**

The Add option allows you to define a custom terminal type if you will be using a terminal that is not supported as one of the Terminal option choices. You must enclose the definition string for the custom terminal in quotations (“). Use the previous option (Show) to display definition strings for supported terminals.

**4 - Remove**

The Remove option deletes a terminal definition. This will delete a newly created definition. To delete a terminal definition, enter the name of the terminal as shown when the Add or Show option is selected

## Voice Set-Up Menu

```
                              VOICE SET-UP MENU

    Option                    Value          Description
 1. Country set-up            menu         - Set country specific parameters
 2. Directory number 1       [none]        - Phone 1 directory number
 3. Directory number 2       [none]        - Phone 2 directory number
 4. Phone 1 operation        [enabled]     - Enable/disable phone #1
 5. Phone 2 operation        [enabled]     - Enable/disable phone #2
 6. Data call preemption     [enabled]     - Allow data call preemption
 7. Binding                  [disabled]    - Voice call link binding
 8. Multi Voice calls        [disabled]    - Allow Multiple Voice calls


Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **VOICE SET-UP MENU** allows the configuration of the two analog voice ports for the router.

**1 - Country Set Up**

The Country Set Up option allows you to select the country in which this router is installed. The country setting allows this router to properly ring the phone connected to the voice port when there is an incoming voice call.

**Default:** [Europe]

**2 - Directory Number 1**

The Directory Number 1 option defines the phone number of voice port number 1 on the back of this device. The two analog phone directory numbers must be unique.

On an ISDN switch type that requires the use of SPID numbers, this option is read only and the number is the same as the SPID 1 defined.

**Default:** [none]

**3 - Directory Number 2**

The Directory Number 2 option defines the phone number of voice port number 2 on the back of this device. The two analog phone directory numbers must be unique.

On an ISDN switch type that requires the use of SPID numbers, this option is read only and the number is the same as the SPID 2 defined.

**Default:** [none]

**4 - Phone 1 Operation**

The Phone 1 Operation option enables or disables voice port number 1 on the back of this device. When this voice port is disabled, any phone device attached to this port will not operate.

**Default:** [enabled]

**5 - Phone 2 Operation**

The Phone 2 Operation option enables or disables voice port number 2 on the back of this device. When this voice port is disabled, any phone device attached to this port will not operate.

**Default:** [enabled]

**6 - Data Call Preemption**

The Data Call Preemption option allows a second data connection to a multilink connected remote site router to be disconnected when a voice connection is required. When a multilink PPP connection is established to a remote site router, the second B-channel connection is being used for increased bandwidth for the data connection.

If an incoming voice call is received by this P840 when Data Call Preemption is enabled, the data connection on the B-channel associated with that voice call will be disconnected and the incoming voice call will be accepted on that B-channel. The data call preemption also applies if the user at this location wishes to make a voice call and picks up the phone to dial out.

The preemption of the data B-channel connection will occur only when a multilink connection is made to one remote site router.

**Default:** [enabled]

**7 – Binding**

The Binding option enables or disables the binding of the voice ports to their associated B-channels. This option is only valid on an ISDN switch type that requires the use of SPID numbers, and is not available on all other switch types.

Binding is used to force the voice ports to use only the B-channel they correspond to. What this means is that when there is a data connection established on B-channel 1 and the phone on voice port 1 wishes to make a call, with binding enabled, the phone will only have a busy signal. With binding disabled, the P840 will allow the phone on voice port 1 to use B-channel 2 to establish a connection when B-channel 1 is in use.

Binding is usually only required when the destination of the voice calls being placed requires the correct CLID (Calling Line ID) to be displayed. Because the second B-channel may be used when binding is disabled, the CLID may not be displayed properly on the destination end of the call.

**Default:** [disabled]

**8 - Multi Voice Calls**

The Multi Voice Calls option allows the P840 to send or receive two simultaneous voice calls. Remember that when two voice calls are in progress, there are no B-channels available for use as a data connection.

**Default:** [disabled]

## Country Set-up Menu

```
                          COUNTRY SET-UP MENU

   Option                 Value           Description
1. Display countries                      - Display countries supported
2. Select country         "Europe"        - Select country




Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **Country Set-up Menu** screen allows you to select a listing of supported countries or to select the country in which the P840 is to be installed.

**1 - Display Countries**

The Display Countries option will display a list of the countries with a ring format supported by this P840.

```
Australia           61        Singapore         65
Austria             43        South Africa      27
Belgium             32        Spain             34
Canada-USA           1        Sweden            46
Denmark             45        Switzerland       41
Europe             999        United Kingdom    44
Finland            358        USA-Canada         1
France              39
Germany             49
Hong-Kong          852
Ireland            353
Italy               39
Japan               81
Luxembourg         352
Maylasia            60
Netherlands         31
Norway              47
Portugal           351
```

**Default:** [Europe]

**2 - Select Country**

The Select Country option lets you choose the ring format that the P840 will send to the phone connected to the voice port when an incoming voice call is received. A selection may be made by entering either the country code or the name of the country. (Note: as Canada and the USA share the same country code and Canada comes first in the alphabetical listing, the name Canada-USA will be displayed if you select by number 1. To display USA-Canada, enter the name "USA-Canada")

The Europe option may be used as a "best of" setting that should work with the phones in most European countries, although it may not duplicate the ring used in a particular country.

## Connections Set-Up Menu

```
                          CONNECTIONS SET-UP MENU

    Option                Value          Description
 1. Remote site set-up    menu         - Configure remote site access
 2. Security set-up       menu         - Configure security
 3. PPP set-up            menu         - Configure PPP parameters
 4. IP address connect    menu         - Configure IP address connect
 5. Force disconnect                   - Disconnect a link
 6. Link status summary                - Status summary of all links




Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **CONNECTIONS SET-UP MENU** allows

**1 - Remote Site Set-Up**

The Remote Site Set-up option takes you to the Remote Site Set-Up Menu, where configuration parameters required to establish PPP connections to remote devices are maintained.

**2 - Security Set-Up**

The Security Set-up option takes you to the Security Set-Up Menu, where PPP security options are maintained.

**3 - PPP Set-Up**

The PPP Set-up option takes you to the PPP Set-Up Menu, where general PPP options are maintained.

**4 - IP Address Connect**

The IP Address Connect Menu allows you to define PPP remote sites to be called depending upon the destination IP address of IP traffic on the local LAN.

**5 - Force disconnect**

Disconnects the link specified.

**6 – Link status summary**

Displays a summary of the links available on this device, their connections (if any) and the link speed.

```
                              Link StatusSummary

Link       Link      Remote Site                 ISDN                 Link
 ID     Type/State      Alias                   Number               Speed
----  ------------ ------------------------ ---------------------- ------
  1     ISDN/Up          REM1                 1-234-56789            64
  2     ISDN/Down        none                  none                  0
```

**Link ID** – the identification number associated with the link interface module; the same as the physical slot number in which the module is installed.

**Link Type** – the type of interface module for the link
Types: ISDN, Digital Leased, Frame Relay

**Link State** – whether the link is up or down

**Remote Site Alias** – the name assigned to the remote site associated with the link

**ISDN Number** – the ISDN number of the remote site connection (if applicable)

**Link Speed** – the nominal transmission speed of the link in Kilobits per second

## Remote Site Set-Up Menu

```
                          REMOTE SITE SET-UP MENU

    Option                Value          Description
 1. Edit remote site       menu         - Modify/add a remote site entry
 2. Remote site summary                 - Summary of remote sites
 3. Call summary                        - Call summary of remote sites
 4. Remove remote site                  - Delete remote site entry
 5. Manual call                         - Make a manual call to a remote site
 6. Force disconnect                    - Disconnect a call to a remote site


Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **REMOTE SITE SET-UP MENU** allows the display, configuration, and creation of remote site profiles. Remote site profiles are used to establish PPP connections to other PPP routers. The appearance of this menu will vary depending on the interface modules installed and their configuration.

**Important:** When configuring this P840 to be the originator of PPP ISDN calls or leased line connections, always define a remote site for each of the possible remote partner routers that this P840 may connect to. Each of the remote sites created stores all of the configuration information required to properly maintain the PPP connection to that remote PPP router. The remote site alias is used to match against the incoming user name during authentication. If an authenticated user name is the same as one of the configured remote site profiles, that connection will use the configuration defined within the remote site profile.

The configuration parameters for a remote site profile may be set by using another profile as a template. Two remote site table entries have been reserved for ISDN and leased line site profile templates; these are:

| ID number | remote site name |
|---|---|
| 41 | ISDN_TEMPLATE |
| 42 | FR_TEMPLATE |
| 43 | LEASED_TEMPLATE |

Parameters for these profiles may be set under the "Edit Remote Site" menu option If a number of remote sites will have a similar profiles, copying the remote site profile from a template can save considerable time in setting them up.

If this router has an ISDN BRI interface and it is set for Digital Leased Circuit, the ISDN B-channel will be treated as a leased line connection.

When the P840 receives an incoming ISDN call, the Multilink state is taken from the "ISDN_TEMPLATE" remote site profile. After the authentication process is finished, if the remote site is a valid remote site that has already been configured, the remaining call parameters are taken from the configured remote site profile. If the remote site does not match one of the configured remote site profiles, then the remaining call parameters will be taken from the "ISDN_TEMPLATE" remote site profile and a remote site profile for that link will be dynamically created at the next available remote site ID number. The newly created remote site profile will be named "INCOMING n" where "n" is the next unassigned Initial Profile number.

When CallerID security is enabled, an incoming call will not be accepted if the remote site does not match one of the configured remote site profiles.

When displaying status or statistic information on the connections to a remote site PPP router, most of the information is displayed according to a particular remote site. Within the Statistics section, a remote site is chosen and then the information for that connection may be displayed. The name of the remote site that the connection has been attached to may be viewed in the Event log file available within the Network Events menu.

There are 40 configurable remote sites available. Each of these remote sites will have a remote site alias associated with them. When a connection is made to a particular remote site, the call will be attached to that remote site profile after the connection has been established. Statistics for a connection are stored under the remote site profile alias or ID number.

Three remote site profiles, numbered 41, 42 and 43, are reserved as templates that may be used for faster remote site configuration.

| Remote Site ID | Remote Site Alias | Description |
|---|---|---|
| 1 - 40 | (user configurable) | Remote site used for outgoing connections to these specific remote sites. Configuration parameters for the outgoing connection are taken completely from the parameters defined in the remote site profile.<br><br>Remote site profile used for incoming connections that have been authenticated and the incoming user name matches the name of one of the configured remote sites. |
| 41 | ISDN_TEMPLATE | Remote site profile used to set up a template that may be used to configure remote sites with ISDN connections. Multilink state is taken from this profile. If the incoming user name matches the name of one of the configured remote sites, the remaining call parameters will be negotiated from the values defined for that remote site.<br><br>If the incoming user name does not match any of the remote sites defined, the connection is attached to the INCOMING profile for that link (44 or 45). The remaining negotiating parameters, such as BCP, IPCP, and CCP, will be taken from the ISDN_TEMPLATE settings. |
| 42 | FR_TEMPLATE | Remote site profile used to set up a template that may be used to configure remote sites with Frame Relay connections. If autolearning is enabled, this template will be used to auto-create each site learned. Site id numbers are assigned sequentially starting from the first available site number in the remote site table. |
| 43 | LEASED_TEMPLATE | Remote site profile used to set up a template that may be used to configure remote sites with Leased Line connections.<br><br>For incoming connections, a remote site profile is auto-created at the first available location in the remote site table. |

**1 - Edit Remote Site**

The Edit Remote Site option directs you to the Edit Remote Site Menu where the remote site profiles are maintained.

40 remote sites may be defined.

**2 - Remote site summary**

The Display Summary option displays an overview of the remote site profiles configured on this P840. Each of the options is shown as "E" for enabled, "D" for disabled or "NA" for not available.

```
* - Up   @ - Suspended                    Total Remote Site Entries: 7
 E - Enabled   D - Disabled   NA - Not Available

 Id  Alias             FR  AC MP    Pri/Sec    DLCI  BRG IP IPX CCP CMCP BACP
 --- ----------------  --- -- -- ------------ ----  --- -- --- --- ---- ----
   1 LEASED1           NA  D  E  Link02/none    NA   E   E  NA  E   NA   NA
   2 Toronto           NA  D  E    ISDN/none    NA   E   E  NA  E   D    NA
   3 LEASED2           NA  D  E  Link02/ISDN    NA   E   E  NA  E   NA   D
   4 Dallas            NA  D  E    ISDN/ISDN    NA   E   E  NA  E   D    E
  41 ISDN_TEMPLATE     NA  D  E    ISDN/ISDN    NA   E   E  NA  E   D    D
  42 FR_TEMPLATE       PPP D  NA   none/none    16   E   E  NA  D   NA   NA
  43 LEASED_TEMPLATE   NA  D  E    none/none    NA   E   E  NA  E   NA   D
```

Id: Entry number in the Remote Site table. The Index number may be used to reference this entry in the IP Address Connect table or for viewing statistics.

Alias: Text name used to easily reference this entry in the table. The Alias may be used to reference this entry in the IP Address Connect table or for viewing statistics.

FR: Frame Relay – displays whether PPP encapsulation is enabled (PPP) or disabled (RAW) over Frame Relay. This column displays not applicable (NA) in a non-frame relay environment.

AC: The state of the Auto-call option for this remote site profile.

MP: The state of the Multilink option for this remote site profile.

Pri/Sec: The type of primary and secondary links configured for this remote site profile. ISDN/none indicates that the circuit will only use ISDN calls. Link1 or Link2 entries indicates that the circuit has been defined as a digital leased circuit.

DLCI: The Frame Relay DLCI number of this remote site. Not applicable (NA) in a non-frame relay environment.

BRG: The state of the BCP (bridging) option for this remote site profile.

IP: The state of the IPCP (IP routing) option for this remote site profile.

IPX: The state of the IPXCP (IPX routing) option for this remote site profile.

CCP: The state of the CCP (compression) option for this remote site profile.

CMCP: The state of the CMCP (connection management) option for this remote site profile. Not applicable (NA) if the remote site is not an ISDN site.

BACP: The state of the BACP option for this remote site profile..

**3 - Call Summary**

The Display Call Summary option displays the ISDN call parameters for the Remote Site Table

```
* - Up   @ - Suspended                    Total Call Site Entries: 0
                                                          Callback
  Id   Alias              ISDN Numbers     Wildcard        Enabled  Group
  ---  ----------------   --------------   --------------  -------  -----
  1    NEW YORK           1-234-5678       543210          No        1
  2    LOS ANGELES        9-876-543-2100   none            No        2
                          9-876-543-2101
  3    test3              246-8101         none            No        1
```

**Note:** This option will only appear if an ISDN BRI interface module is installed which does not have the digital leased line option enabled.

**3/4 - Remove Remote Site**

The Remove Remote Site option deletes individual entries or all of the entries from the Remote Site table.

```
Enter:
   all, id or alias to delete
>
```

**4/5 - Manual Call**

The Manual Call option is used to establish a manual PPP call to a configured remote site.

```
Enter :
     remote site id or alias to dial (1 to 16 characters)
>
```

Note: This option will only appear if an ISDN BRI interface module is installed which does not have the digital leased line option enabled.

**5/6 - Force Disconnect**

The Force Disconnect option will cause the chosen remote site connection to be disconnected.

```
Enter :
     remote site id or alias to disconnect
>
```

## Edit Remote Site Menu

```
                          EDIT REMOTE SITE MENU

    Option                  Value          Description
 1. Connection set-up      menu         - Configure connections
 2. Protocol set-up        menu         - Configure protocols
 3. Remote site alias    *[         ]   - Alias of remote site entry
 4. Connection           *[         ]   - Select connection configuration
 5. Primary connection   *[         ]   - Select connection type
 6. Remote site type     *[         ]   - Interoperable or spoofing




Enter:
    Remote site id or alias (1 to 16 characters)

>
```

The above display is the first level of the **EDIT REMOTE SITE MENU**. Enter the ID number or alias of the site you wish to edit.

**Note: the options on this menu are not active until the Remote Site ID is entered.**

When creating a new remote site profile, an alias must be entered for the new site. The first available identifier number will be assigned to this alias. The alias may be up to 16 characters long; blank spaces and the character "!" may not be used and the alias must start with a letter of the alphabet. You will then be prompted to enter a Template id number or profile; if this remote site will have a profile similar to an existing site, entering the alias or id number of that site will copy that remote site profile to this one. If you wish to start from the default settings, enter "none" (case sensitive).

After the remote site id or alias is supplied, the next level menu specific to that site appears

```
                          EDIT REMOTE SITE  MENU

   Option                 Value               Description
 1. Connection set-up      menu             - Configure connections
 2. Activation set-up      menu             - Configure remote site activation
 3. Protocol set-up        menu             - Configure protocols
 4. Security parameters    menu             - Configure security parameters
 5. Remote site alias     "LEASED1"         - Alias of remote site entry
 6. Connection            [dual_link]       - Select connection configuration
 7. Primary connection    [Leased]          - Select connection type
 8. Secondary connection  [Leased]          - Select connection type
 9. Remote site type     *[interoperable]   - Interoperable or spoofing




Enter option number, "=" - main menu, <TAB> - previous menu

>
```

**1 - Connection Set-Up**

The Connection Set-up option takes you to the Connection Set-Up Menu for the chosen remote site. Here you define the connection parameters that will be used to establish the connection to the remote site device.

**2 - Activation Set-Up**

The Activation Set-up option takes you to the Activation Set-up menu for the chosen remote site, where activation conditions are defined for the main connection to this remote site. The activation conditions for the primary connection consist of the activation schedule, which determines when the connection may be operational, the usage limits and the load thresholds at which the link will be brought up or down.

The Activation conditions are not applicable when placing a manual call to this remote site.

**Note:** This option does not appear for site profiles with a Frame Relay, PPP disabled connection.

**2/3 - Protocol Set-Up**

The Protocol Set-up option takes you to the Protocol Set-up menu for the chosen remote site, where the BCP, IPCP, CCP, CMCP and BACP protocol parameters are configured.

**3/4 - Security Parameters**

The Security Parameters option allows you to set the password that this remote site will use for incoming security authorization and to set a user name and password for outgoing security authorization.

**Note:** This option will not appear if the remote site is configured for raw 1490 frame relay. Routers configured to have a leased line link operating in conjunction with an ISDN B-Channel (either as backup or bundled link) must have security enabled and with the proper usernames and passwords entered on both partner routers.

**4/5- Remote Site Alias**

The Remote Site Alias option defines the name used to represent this remote site. The remote site alias is used to match against the incoming user name during authentication. If an authenticated user name is the same as one of the configured remote site profiles, that call will use the configuration defined within the corresponding remote site profile.

The remote site alias is case sensitive and may consist of 1 to 16 alphanumeric characters. Use the underscore character instead of a space character.

**5/6 – Connection**

The Connections option defines the type of connection and its usage.

**Options:** single_link, dual_link, threshold, recovery, threshold_with_recovery.

Single link operation: only one link (the primary link) will be used for connection to this remote site.

Dual link operation: Two links will be available for connection to this remote site; both will be brought up any time a connection to this site is established.

Threshold: traffic levels on the primary link will be use to determine whether or not to bring up the secondary link. The conditions controlling the secondary link are set under the Activation menu. This option is not available with raw 1490 Frame Relay (PPP Encapsulation must be enabled).

Recovery: The secondary link will be used as a backup connection in case of failure of the primary link. The conditions controlling the secondary link are set under the Activation menu.

Threshold with recovery: the secondary link will be brought up if traffic on the primary link exceeds a threshold level or if the primary link fails. The conditions controlling the secondary link are set under the Activation menu.

**Considerations:** The "threshold with recovery" option is not compatible with partner routers that are configured to have only "threshold" or only "recovery" available on the link. If a connection of this type is attempted, the link will bob when the connection criteria are met for one router but not for the other. For example, if one is set for "threshold_with_recovery" and the other is set only for "recovery", when the threshold is exceeded the router with "threshold_with_recovery" will attempt to bring up the connection, but because the partner router is not set for threshold activation, the partner router will bring the connection down.

**6/7 – Primary connection**

The Primary connection option defines what type of service will be used on the primary connection. If the currently selected primary link is not configured for the chosen connection type, a warning is displayed: the connection will not be established if the link is not configured for the chosen connection type.

**Options:** Frame_relay, Leased, ISDN_call

**7/8 – Secondary Connection**

The Secondary connection option defines what type of service will be used on the secondary connection. If the currently selected secondary link is not configured correctly for the chosen connection type, a warning is displayed. The primary connection will still be established even if the secondary connection is not correctly configured.

**Options:** Frame_relay, Leased, ISDN_call

**Note:** this option is user configurable only if the connection is not single link. If the connection is single link, the option becomes display only with `*[none]` displayed.

**8/9 - Remote Site Type**

The Remote Site Type option defines whether spoofing is enabled or not with this remote site connection.

**Options:** interoperable, spoofing

**Note:** this option is user configurable only if the primary connection is ISDN_call type, otherwise this option is display only.

**Considerations:** If you are running spoofing with Triggered RIP, both routers must be set to Triggered RIP "link_up_only". The P840 will automatically configure to this setting but the remote partner router should be checked to make certain that it is correctly configured.

## Connection Set-Up Menu

The appearance of the Remote Site Connection Set-Up Menu will vary depending on the WAN modules installed in this router and the options selected.

## A – Link logical type set to ISDN, single or multiple links.

```
                    REMOTE SITE n CONNECTION SET-UP MENU

   Option              Value          Description
 1. ISDN call set-up    menu         - Configure ISDN calls
 2. Auto-call          [disabled]    - Activate auto-call




Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **REMOTE SITE CONNECTION SET-UP MENU** allows the setting of parameters used for connection establishment to the remote site router.

**1 - ISDN Call Set-Up**

The ISDN Call Set-up option takes you to the ISDN Call Set-Up Menu for the chosen remote site. Here you set parameters such as the ISDN numbers of the remote partner ISDN routers and redial timers that pertain to ISDN circuit activation. This option is not available when the ISDN interface on this P840 has been set as a Digital Leased Circuit.

**2 - Auto-Call**

The Auto-Call option is used to define this remote site as one that the P840 will attempt to establish a connection to at all times. Each time the P840 is powered up a connection will be attempted to this remote site.

**Default:** [disabled]

## B - Link logical type set to Digital Leased, single link connection.

```
                    REMOTE SITE n CONNECTION SET-UP MENU

    Option          Value          Description
 1. Primary link    [none]       - Configure primary link number
 2. Auto-call       [disabled]   - Activate auto-call









Enter :
    none, link_number (1 or 2)

>
```

**1 – Primary link**

The Primary link option defines the link number that will be used to connect to this remote site. LAN interfaces is available for the primary link for PPPoE feature. If the primary link is chosen as a LAN interface then the Auto-Call will automatically be enabled.

**Options:** none, Lan, link number (1 or higher)

**Default:** [none]

**2 - Auto-Call**

The Auto-Call option is used to define this remote site as one that the P840 will attempt to establish a connection to at all times. Each time the P840 is powered up a connection will be attempted to this remote site. If the primary link is configured to a LAN interface the Auto-Call option is automatically enabled.

**Default:** [disabled]

## C - Link logical type set to Digital Leased, multiple link connection.

```
                    REMOTE SITE n CONNECTION SET-UP MENU

    Option            Value          Description
 1. Primary link      [4]          - Configure primary link number
 2. Secondary link    [3]          - Configure secondary link number
 3. Auto-call         [disabled]   - Activate auto-call









Enter :
    none, link_number (1 or 2)

>
```

**1 – Primary link**

The Primary link option defines the primary link number that will be used to connect to this remote site.

**Options:** 1, 2, none, Lan.

**Default:** [none]

**2 – Secondary link**

The Secondary link option defines the secondary link number that will be used to connect to this remote site.

**Options:** 1, 2, none

**Default:** [none]

**3 - Auto-Call**

The Auto-Call option is used to define this remote site as one that the P840 will attempt to establish a connection to at all times. Each time the P840 is powered up a connection will be attempted to this remote site.

**Default:** [disabled]

## D – Multiple link connection, primary link set to Leased, secondary link to ISDN.

```
                    REMOTE SITE n CONNECTION SET-UP MENU

   Option              Value          Description
 1. ISDN call set-up    menu         - Configure ISDN calls
 2. Primary link       [none]        - Configure primary link number
 3. Auto-call          [disabled]    - Activate auto-call




Enter option number, "=" - main menu, <TAB> - previous menu

>
```

This version of the **REMOTE SITE CONNECTION SET-UP MENU** allows the configuration of a leased primary link (Digital Leased Line) and an ISDN secondary link.

**1 - ISDN Call Set-Up**

The ISDN Call Set-up option takes you to the ISDN Call Set-Up Menu for the chosen remote site. Here you set parameters such as the ISDN numbers of the remote partner ISDN routers and redial timers that pertain to ISDN circuit activation.

**2 – Primary link**

The Primary link option defines the primary link number that will be used to connect to this remote site.

**Options:** 1, 2, none

**Default:** [none]

**3 - Auto-Call**

The Auto-Call option is used to define this remote site as one that the P840 will attempt to establish a connection to at all times. Each time the P840 is powered up a connection will be attempted to this remote site.

**Default:** [disabled]

## E – Single link connection, primary link set to Frame Relay.

```
                    REMOTE SITE n CONNECTION SET-UP MENU

    Option            Value              Description
 1. Primary link     [7]               - Configure primary link number
 2. DLCI             [16]              - Frame relay address
 3. CIR              [0 Kbps]          - Committed information rate
 4. EIR              [link_speed]      - Excess information rate
 5. Time interval    [10 (1/10th s)]   - Interval for monitoring bandwidth
 6. PPP              [disabled]        - Enable/disable PPP over Frame Relay
 7. State            [disabled]        - Enable/disable PVC



Enter option number, "=" - main menu, <TAB> - previous menu

>
```

This version of the **REMOTE SITE CONNECTION SET-UP MENU** allows the setting of frame relay parameters used to configure the Permanent Virtual Circuit (PVC) that is used to connect to this remote site. Up to 40 remote site PVCs may be defined.

**1 - Primary Link**

The Primary link option defines the primary link number that will be used to connect to this remote site.

**Options:** 1, 2, none

**Default:** [none]

**Considerations:**

The PVC must be toggled (disable – enable option 7. State) before this option may be takes effect.

**2 - DLCI**

The Data Link Connection Identifier (DLCI) option specifies the Frame Relay LAPF address for the PVC. This value **must** be set to be the same as the value provided by the Frame Relay network provider.

When the frame relay router 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 startup, the P840 will automatically create a remote site profile for each PVC. The automatically created remote site profiles will be named "LinkxDLCIyyy" where x is the physical link number the PVC is on and yyy is the DLCI of the PVC.

**Default:** [16]

**Range:** 16 to 991

**Considerations:**

The PVC must be toggled (disable – enable option 7. State) before this option may be takes effect.

**3 - CIR**

The Committed Information Rate (CIR) option specifies the data rate that the Frame Relay service has guaranteed to provide.

This value **must** be set to the same as the value provided by the Frame Relay network provider. If the Frame Relay network provider supplies values for Bc and T only, simply calculate the CIR value by using the following formula: CIR = Bc/T.

**Default:** [0 k]

**Range:** 0 to 2048 Kbps
**NOTE:** only CIR up to 64 Kbps are available over ISDN Digital Leased connections.

**Considerations:**

When changing the CIR option for this PVC, the PVC must be toggled (disable – enable option 7. State) before the new value will take effect.

The value of 0 indicates that there is no commitment on the data rate.

The actual CIR may exceed the configured CIR because only complete frames are transmitted. Frames will not be broken to fit within CIR when the upper limit is met, the final frame will be transmitted in full. The only time this does not happen is when traffic exceeds CIR + EIR, in which case the frame which would cause CIR to be exceeded will not be transmitted.

The only restriction is that CIR + EIR > 0

**4 - EIR**

The Excess Information Rate (EIR) option specifies the data rate that the Frame Relay service indicates may be available for this PVC.

This value **must** be set to the same as the value provided by the Frame Relay network provider.

**Default:** ["link_speed"]

**Range:** 0 to 2048 Kb, "link_speed"
**NOTE:** only EIR up to 64 Kbps are available over ISDN Digital Leased connections.

**Considerations:**

When changing the EIR option for this PVC, the PVC must be toggled (disable – enable option 7. State) before the new value will take effect.

When EIR = 0, no excess burst data is allowed to be transmitted. If EIR is non-zero, bursting is allowed.

The only restriction is that CIR + EIR > 0

**5 - Time Interval**

The Time Interval option specifies the time period (in 10ths of a second) that the P840 uses for monitoring PVC bandwidth.

This value **must** be set to the same as the value provided by the Frame Relay network provider.

**Default:** [10 1/10th sec]

**Range:** 10 to 40 1/10th second

**6 - PPP Encapsulation**

The PPP Encapsulation option enables the P840 to send data to this remote site using the Point to Point Protocol (PPP) over frame relay. When this option is disabled, the P840 will send data to this remote site using standard RFC-1490 frame relay frames.

**Default:** [disabled]

**Considerations:**

When this P840 is configured with PPP Encapsulation disabled and the remote site router has PPP enabled, this P840 will bring the PVC up and there will be no indication that the connection negotiation is not proceeding. This local P840 will indicate that the PVC is up, however there will be no traffic sent over the PVC. If the remote site router is a P840, the remote site router will continue to display the alarm "PPP connection attempt to remote site *n*" until the connection is established.

**7 - State**

The State option toggles between [enabled] and [disabled] to activate the PVC or take the PVC out of service.

**Default:** [enabled]

## F – Multiple link connection, primary link set to Frame Relay, secondary to ISDN.

```
                    REMOTE SITE n CONNECTION SET-UP MENU

   Option              Value              Description
 1. ISDN call set-up    menu            - Configure ISDN calls
 2. Primary link        [7]             - Configure primary link number
 3. DLCI                [16]            - Frame relay address
 4. CIR                 [0 Kbps]        - Committed information rate
 5. EIR                 [link_speed]    - Excess information rate
 6. Time interval       [10 (1/10th s)] - Interval for monitoring bandwidth
 7. PPP                 [disabled]      - Enable/disable PPP over Frame Relay
 8. State               [disabled]      - Enable/disable PVC



Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **REMOTE SITE CIRCUIT SET-UP MENU** allows the setting of frame relay parameters used to configure the Permanent Virtual Circuit (PVC) that is used to connect to this remote site. Up to 40 remote site PVCs may be defined.

**1 - ISDN Call Set-Up**

The ISDN Call Set-up option takes you to the ISDN Call Set-Up Menu for the chosen remote site. Here you set parameters such as the ISDN numbers of the remote partner ISDN routers and redial timers that pertain to ISDN circuit activation.

**2 - Primary Link**

The Primary link option defines the primary link number that will be used to connect to this remote site.

**Options:** 1, 2, none

**Default:** [none]

**Considerations:**

The PVC must be toggled (disable – enable option 8. State) before this option may be takes effect.

**3 - DLCI**

The Data Link Connection Identifier (DLCI) option specifies the Frame Relay LAPF address for the PVC. This value **must** be set to be the same as the value provided by the Frame Relay network provider.

When the frame relay router 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 startup, the P840 will automatically create a remote site profile for each PVC. The automatically created remote site profiles will be named "LinkxDLCIyyy" where x is the physical link number the PVC is on and yyy is the DLCI of the PVC.

**Default:** [16]

**Range:** 16 to 991

**Considerations:**

The PVC must be be toggled (disable – enable option 8. State) before this option takes effect.

**4 - CIR**

The Committed Information Rate (CIR) option specifies the data rate that the Frame Relay service has guaranteed to provide.

This value **must** be set to the same as the value provided by the Frame Relay network provider. If the Frame Relay network provider supplies values for Bc and T only, simply calculate the CIR value by using the following formula: CIR = Bc/T.

**Default:** [0 k]

**Range:** 0 to 2048 Kbps
**NOTE:** only CIR up to 64 Kbps are available over ISDN Digital Leased connections.

**Considerations:**

When changing the CIR option for this PVC, the PVC must be be toggled (disable – enable option 8. State) before the new value will take effect.

The value of 0 indicates that there is no commitment on the data rate.

The actual CIR may exceed the configured CIR because only complete frames are transmitted. Frames will not be broken to fit within CIR when the upper limit is met, the final frame will be transmitted in full. The only time this does not happen is when traffic exceeds CIR + EIR, in which case the frame which would cause CIR to be exceeded will not be transmitted.

The only restriction is that CIR + EIR > 0

**5 - EIR**

The Excess Information Rate (EIR) option specifies the data rate that the Frame Relay service indicates may be available for this PVC.

This value **must** be set to the same as the value provided by the Frame Relay network provider.

**Default:** ["link_speed"]

**Range:** 0 to 2048 Kb, "link_speed"
**NOTE:** only EIR up to 64Kbps are available over ISDN Digital Leased connections.

**Considerations:**

When changing the EIR option for this PVC, the PVC must be be toggled (disable – enable option 8. State) before the new value will take effect.

When EIR = 0, no excess burst data is allowed to be transmitted. If EIR is non-zero, bursting is allowed.

The only restriction is that CIR + EIR > 0

**6 - Time Interval**

The Time Interval option specifies the time period (in 10ths of a second) that the P840 uses for monitoring PVC bandwidth.

This value **must** be set to the same as the value provided by the Frame Relay network provider.

**Default:** [10 1/10$^{th}$ sec]

**Range:** 10 to 40 1/10$^{th}$ second

**7 - PPP Encapsulation**

The PPP Encapsulation option enables the P840 to send data to this remote site using the Point to Point Protocol (PPP) over frame relay. When this option is disabled, the P840 will send data to this remote site using standard RFC-1490 frame relay frames.

**Default:** [disabled]

**Considerations:**

When this P840 is configured with PPP Encapsulation disabled and the remote site router has PPP enabled, this P840 will bring the PVC up and there will be no indication that the connection negotiation is not proceeding. This local P840 will indicate that the PVC is up, however there will be no traffic sent over the PVC. If the remote site router is a P840, the remote site router will continue to display the alarm "PPP connection attempt to remote site *n*" until the connection is established.

**8 - State**

The State option toggles between [enabled] and [disabled] to activate the PVC or take the PVC out of service. You must confirm that this is the action you wish to take by typing "yes" at the prompt.

**Default:** [enabled]

## ISDN Call Set-Up Menu

```
          EDIT REMOTE SITE 1 CONNECTION SET-UP ISDN CALL SET-UP MEN

    Option                  Value          Description
 1. Advanced settings       menu         - Advanced ISDN call settings
 2. ISDN number             [none]       - Set ISDN number
 3. Alternate ISDN number   [none]       - Set alternate ISDN number
 4. Group                   [1]          - Specify dial group
 5. Wildcard                [none]       - Set wildcard ISDN number
 6. Call you                [none]       - Set call you prefix
 7. Call me                 [none]       - Set call me prefix
 8. Callback                [enabled]    - Enable/disable callback



Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **REMOTE SITE ISDN CALL SET-UP MENU** allows the setting of parameters used for ISDN call establishment to the remote site PPP router. This menu is not displayed when the Digital Leased Circuit option is enabled for the ISDN interface.

**1 – Advanced Settings**

This option takes you to the Advanced Settings menu where callback delay and redial parameters may be set.

**2 - ISDN Number**

The ISDN Number option defines the ISDN number to be called to establish a connection to the remote partner PPP router.

**Default:** [none]

**3 - Alternate ISDN Number**

The alternate ISDN number is used for two different situations when Multilink operation is set to enabled for this remote site.

1. ISDN number called when Bandwidth on Demand settings require a second ISDN call to be made after an initial Auto-Call or IP Address Connect call has been placed to the remote site. When the secondary connection is enabled by selecting the ISDN_call option, the first ISDN Number will be used to place the first ISDN call according to the IP Address Connect table, and the Alternate ISDN Number will be used to place the second ISDN call according to the Bandwidth on Demand options defined within the Secondary Activation menu.
2. ISDN number called when both the primary and secondary connections are set to ISDN_call and an Auto-Call or IP Address Connect call is placed. This will cause this alternate ISDN call to be placed to the remote site PPP router once the main ISDN call has been established and Multilink operation has been successfully negotiated.

**Default:** [none]

**4 - Group**

The Group option specifies which group number will be used to make calls to this remote site connection. If hunt group numbers are not used, it is recommended that when using callback between this P840 and a remote site router with only a single BRI, that the links on this P840 be configured into groups of two links. If the links are grouped more than two to a group, a callback request may come in to one ISDN number in the group but be responded to by another link with an ISDN number that is not either the primary or alternate ISDN number that the remote site uses to call to this router. The callback will be rejected by the remote site router in this case. Groups are set up under the Link Set-up Menu.

**Default:** [1]

**Options:** 1 or 2

**5 - Wildcard**

The Wildcard option defines the number used when checking for a match on an incoming callerID identified call. The incoming call is checked for a match against the configured values for the ISDN number, the alternate ISDN number, and then the wildcard number.

This wildcard number may contain don't care values to allow for a broader matching possibility. Don't care values are defined with an "X" in the wildcard number. When the P840 checks the incoming call's callerID against this wildcard value, the P840 starts at the rightmost digit and checks each digit from there. The number of digits compared is determined by the number with the least amount of digits. This means that the checking will only be done to the maximum number of digits of either the incoming callerID or the wildcard value, whichever is less.

For example: The wildcard value is set to 931-1XXX. Refer to the following list for accept and reject examples.

| Incoming callerID | Result |
|---|---|
| 328 | accepted |
| 931-1328 | accepted |
| 2328 | rejected |
| 555-1212 | rejected |

**Default:** [none]

**6 - Call You**

Dialing prefix used to make the ISDN call to the remote site PPP router. The Call You dialing prefix is used to define the area codes, country codes, long distance dialing prefixes, or any other information required to establish an ISDN call to the remote site PPP router.

**Default:** [none]

**7 - Call Me**

Dialing prefix used by the remote partner router to make an ISDN call to this P840. When Connection Management is enabled, this ISDN P840 will pass its directory numbers as well as the Call Me dialing prefix to the remote partner ISDN P840. This allows the remote partner ISDN P840 to correctly dial this P840 when the ISDN circuit needs to be resumed.

The Call Me dialing prefix is used to define the area codes, country codes, long distance dialing prefixes, or any other information required for the remote partner ISDN P840 to establish an ISDN call to this ISDN P840.

**Default:** [none]

**Note:** When CMCP is enabled, the call me prefix to get back to the partner router must be entered so that the link can be re-established after suspension (only the directory number is passed when the call is set up, not the entire connection number). For the same reason, the partner router must also have its call me prefix entered.

**8 - Callback**

The Callback option when set to enabled causes this P840 to refuse an incoming ISDN call for this remote site profile and then initiate an outgoing ISDN call to this remote site. Once a match of an incoming ISDN call is made to an existing remote site profile, the matching remote site profile is checked to determine whether the incoming call is answered or refused and a callback ISDN call initiated.

Callback to this remote site may also be triggerred by a call from another source, such as a voice phone. In this case, the number of the voice phone used to trigger the callback would be entered in the Wildcard option (4).

The Callback option may be used to provide a single point of ISDN billing. By allowing only one of the P840s to establish ISDN calls, the ISDN charges may be centralized in one location.

The CallerID option when enabled will take precedence on determining whether an incoming call is ignored or answered. When calling back this remote site, both the ISDN number and the alternate ISDN number will be tried.

**Default:** [disabled].

**Considerations:**

For this feature to operate, the ISDN service provider must supply the caller's number. Check with your ISDN service provider to see whether this service is available.

## Advanced Settings Menu

```
EDIT REMOTE SITE 1 CONNECTION SET-UP ISDN CALL SET-UP ADVANCED SETTINGS MENU

    Option            Value         Description
 1. Callback delay   [2 s]        - Time to wait until callback
 2. Redial timer     [10 s]       - Time to wait until redial
 3. Redial count     [5]          - Number of redials to try
```

**1 – Callback Delay**

The Callback Delay option specifies the number of seconds that this router will wait before making a call in response to a callback request call from the remote site router. This allows sufficient time for the originating call to complete its disconnect before the response call arrives.

**Default:** [2 sec]

**Range:** 1 to 20 seconds

**2 - Redial Timer**

The Redial Timer option specifies the time the router will wait before attempting to redial an incomplete ISDN call.

**Default:** [10 sec]

**Range:** 4 to 255 seconds

**Considerations:**

When the ISDN switch type is set to KDD or NTT, the default, and minimum redial timer value is 90 seconds.

**3 - Redial Count**

The Redial Count option specifies the number of times the router will attempt to redial an incomplete ISDN call.

**Default:** [5] redials

**Range:** 0 to 255 redials

**Auto-Call Considerations:**

When two ISDN numbers are defined in the ISDN Call Set-Up menu of the remote site entry, the P840 will alternate between the two numbers when re-dialing.

When the P840 attempts to establish an Auto-Call ISDN call and the PPP router at the remote site does not respond, the P840 will try up to the number of times defined in the Redial Count to establish the ISDN call. The interval between the successive attempts is defined by the Redial Timer. If after the defined number of redials the P840 cannot establish a call to the remote partner, the P840 will wait for one minute and then try to establish the ISDN call again using the Redial Count and the Redial Timer values. If the call is not established after these attempts, the P840 will wait for 2 minutes and then try again. The P840 will keep trying to establish the call (according to Redial Count & Redial Time) in blocks with the time intervals: 4 minutes, 8 minutes, 15 minutes, 15 minutes, etc.) until the remote partner answers the call.

When the ISDN switch type is set to KDD or NTT, the minimum time between re-dialing blocks is 3 minutes.

When the Redial Count is set to zero (0), the P840 will redial the remote partner indefinitely at one minute intervals using the defined ISDN numbers for the remote site according to the redial blocks explained earlier. The P840 will alternate between the two defined ISDN numbers for the partner in blocks of #1, #2 with a time between the two ISDN numbers of 4 seconds.

**Address Connect Considerations:**

When the P840 attempts to establish an Address Connect ISDN call and the remote partner does not respond, the P840 will not attempt to redial the remote partner until the next Address Connect connection is required.

If two ISDN numbers are defined in the ISDN Call Set-Up menu of the remote site entry, the P840 will dial the alternate ISDN number after waiting 4 seconds if the first ISDN number does not respond.

## Activation Set-Up Menu

```
                EDIT REMOTE SITE 1 ACTIVATION SET-UP MENU

    Option              Value          Description
 1. Schedule            menu         - Schedule remote site activation
 2. Usage set-up        menu         - Set up line usage parameters
 3. Threshold set-up    menu         - Set up traffic level thresholds
 4. Inactivity timer   [60 sec]      - Set traffic inactivity timer
 5. Recovery timer     [60 s]        - Define recovery steady state time




Enter option number, "=" - main menu, <TAB> - previous menu


>
```

The **ACTIVATION MENU** allows the setting of the activation schedule and usage limits for the primary link used to connect to the remote site router. Traffic activation levels may also be set allowing the secondary link to be used when the throughput of the primary link exceeds the defined levels.

**Note:** the activation schedules of **both** partner routers on the link must be set up identically. If one is set to be active while the other is not, the active router will continuously try to bring up the link to the partner router, which will reject the connection because its activation table is set to have the connection to that remote site inactive. If the routers are in different time zones, you must decide on a standard time to be used by both.

**1 - Schedule**

The Schedule option takes you to the Schedule Menu where the times that the primary link will be activated or deactivated are set.

**2 - Usage Set-Up**

The Usage Set-up option takes you to the Usage Set-up Menu, where the circuit usage limits may be set.

**3 - Threshold Set-Up**

The Traffic Set-up option takes you to the menu where the traffic load conditions and stability timers for activating and deactivating the secondary link may be set.

**4 - Inactivity Timer**

The Inactivity Timer option defines the **Connection Management Idle Timer** that is used to determine when an ISDN call will be suspended or terminated. This timer monitors traffic on the link. If the link traffic is idle, this P840 is set to use Connection Management, and there are LAN sessions using the link, the ISDN call will be suspended.

When the Inactivity Timer is set to off, this P840 will not suspend or terminate the ISDN call. This may be used to allow only one of the P840s to monitor the link traffic to determine when to suspend or terminate the ISDN call.

The Inactivity Timer is also used for **IP Address Connect** configurations. If connection management is not used, the inactivity timer will monitor link traffic. If the traffic on the link is idle for a time longer than the inactivity timer, the link will be terminated and then be made available for the next IP address connect request.

**Default:** [60 sec]

**Range**: off, 20 to 3600 seconds

**5 - Recovery Timer**

The recovery timer sets the delay before the secondary link is activated or deactivated when the primary link goes down or is reestablished. This acts as a stability timer to give the primary link a period to recover before the backup is activated and to ensure that when the primary link is reestablished that it stays up for a significant time before the backup link is dropped.

**Default:** [15 sec] (note: if Frame Relay is enabled, this default changes to 60 sec.)

**Range:** 15 to 300 seconds

**Note:** This option will only be displayed if the Connection option in the Edit Remote Site menu is set to "recovery" or "recovery_with_threshold".

## Schedule Menu

```
              EDIT REMOTE SITE 1 ACTIVATION SET-UP SCHEDULE MENU

    Option                          Description
 1. Activation intervals          - Set activation intervals
 2. Display schedule              - View activation timetable
 3. Display time                  - View current date and time




Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **PRIMARY ACTIVATION MENU** allows the setting of the activation schedule for the primary link to be used to connect to the remote site PPP router. It controls outgoing calls from this router to the remote site router – incoming calls are not controlled by these options.

The Primary Activation conditions are not applicable when placing a manual call to this remote site.

**1 - Activation Intervals**

The Activation Intervals option defines the times that the primary link will be activated or deactivated.

Choose an action:

```
Enter:
 activate, deactivate, remove, clear

> activate
```

The Remove option will let you remove a specified activation time.

The Clear option will clear the entire table of all activation times.

The following example show the set-up for a connection to be active from 7:00 AM to 11:00 PM on weekdays and 10:00 AM to 5:00 PM on Saturdays:

Specify the day(s):

```
Enter:
 Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday,
 Weekends, Weekdays
> Weekdays
```

Specify the time:

```
Enter:
 Time (hour or hour: 00 or hour: 30)
> 07
```

The above Time can be specified in any one of three ways: 7, 07, or 7: 00. Valid hour values are 0 to 23 (24 hour clock). Settings on the half-hour are also permissible, e.g. 7: 30.

Set link disconnect time:

```
> deactivate
> Weekdays
> 23
```

For a deactivation time of midnight on a given day, you must specify hour 0 of the next day. Note that hour 0 starts a given day and hour 23: 30 is the last time specifiable for a given day.

Add Saturday:

```
> activate
> Saturday
> 10
```

```
> deactivate
> Saturday
> 17
```

**2 - Display Schedule**

```
                          Call 1 Activation Schedule

    0  1  2  3  4  5  6  7  8  9  10 11 12 13 14 15 16 17 18 19 20 21 22 23
Sun -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
Mon -- -- -- -- -- -- -- AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA --
Tue -- -- -- -- -- -- -- AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA --
Wed -- -- -- -- -- -- -- AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA --
Thu -- -- -- -- -- -- -- AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA --
Fri -- -- -- -- -- -- -- AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA --
Sat -- -- -- -- -- -- -- -- -- -- AA AA AA AA AA AA AA -- -- -- -- -- -- --

Activation Schedule Entries
 Weekdays -  7: 00 Act      Weekdays - 23: 00 Deact    Saturday - 10: 00 Act
 Saturday - 17: 00 Deact

Type: [s] to redraw, [=] main menu, any other key to end.
```

**note:** the[ s] to redraw is case sensitive; it must be lower case.

The display schedule shows the current schedule of when the primary connection to this remote site will be activated.

- A indicates that the connection will be active at this time
- – indicates that the connection is inactive at this time

**3 - Display Time**

The Display Time option displays the current router time and date in the format::

Day of the week yyyy-mm-dd hh:mm:ss

## Usage Set-Up Menu

```
          EDIT REMOTE SITE 1 ACTIVATION SET-UP USAGE SET-UP MENU

    Option          Value          Description
 1. Usage limit    [unlimited]   - Set line use limit per day
 2. Call limit     [unlimited]   - Set outgoing call limit per day
 3. Restart time   "07:00"       - Set time-of-day to restart limits




Enter option number, "=" - main menu, <TAB> - previous menu


>
```

**1 - Usage Limit**

The Usage Limit option defines the maximum ISDN connection time for this remote site. The time limit is defined in minutes of connection time and is the maximum connection time per day. The Restart Time option determines when the P840 will restart the usage limit timer.

**Default:** [240] minutes

**Range:** 1 to 2880 minutes or unlimited

**2 - Call Limit**

The Call Limit option defines the maximum number of ISDN connections allowed to this remote site per day.

**Default:** [120]

**Range:** 1 to 86400 calls or unlimited

**3 - Restart Time**

The Restart Time option defines the time of day that the call limit and usage limit timers will start recounting. Time is specified as a 24 hour clock and may be set in 30 minute increments. Time can be specified in any one of three ways: 7, 07, or 7: 00. Valid hour values are 0 to 23. Valid minute settings are :00 or :30, e.g. 7: 30.

**Default:** [07:00]

**Range:** 0 to 23:3

**Note:** Changing the Restart Time will reset all statistics counters; all current statistics will be erased.

## Threshold Set-Up Menu

```
          EDIT REMOTE SITE 1 ACTIVATION SET-UP THRESHOLD SET-UP MENU

    Option                  Value         Description
 1. Up threshold           [80 %]       - Set activation traffic level
 2. Up stability timer     [2 min]      - Define up level steady state time
 3. Down threshold         [60 %]       - Set deactivation traffic level
 4. Down stability timer   [2 min]      - Define down level steady state time









Enter option number, "=" - main menu, <TAB> - previous menu
```

The **THRESHOLD SET-UP MENU** allows the traffic load conditions and stability timers for activating and deactivating the secondary link to be set.

**1- Up Threshold**

The Up Threshold value determines the percentage of primary link's capacity that will cause the secondary link to be activated. The primary link must sustain a throughput (either receive or transmit) of greater than the up threshold for a period greater than the up stability timer in order for the secondary link to be activated.

```
Enter:
 Percent of main link capacity (from 50 to 100)
> 80
```

**Default:** 80%

**Note:** In a frame relay environment, the link summary statistics used to determine the up threshold may not be accurate due to the overhead associated with frame relay. The overhead typically adds about 5% at an 80% line load, meaning setting the up threshold at 80% would cause the secondary link to come up when the actual transmission rate reaches about 85% of the maximum line rate. If a more accurate data transmission threshold is required, it may be calculated by using the Frame Relay Protocol Statistics. Go to the Main Menu/Statistics/WAN Statistics/Remote Site Statistics/Protocol Statistics and page down to the FR display. Take the greater of the Rcv or Xmt rate (in KB) and divide it by the stated link speed (in KB) *100 to get the recent percent of the link capacity being used for data. By comparing this to the load shown in the Link Summary Statistics, the amount of overhead may be determined and the threshold adjusted accordingly.

**2 - Up Stability Timer**

To prevent the unnecessary activation of the secondary link if the Up Threshold is only reached for a brief period, the Up Stability Timer is used. It defines how long the primary link's throughput must be at or above the Up Threshold before the secondary call is activated.

For example, using the default values, if a traffic level above the Up Threshold of 80% is maintained on the primary link for a period of 2-min. (length of time the secondary link is "held inactive"), then the secondary link will be activated.

```
Enter:
 time in minutes when link is down (from 1 to 60)
> 2
```

**Default:** 2 minutes

**3 - Down Threshold**

The Down Threshold determines when the secondary link is shut down again. It must be set lower than the Up Threshold.

After the secondary link comes on-line, it will begin to share the load that would have gone across the primary link. For example, if the primary link brings the secondary link on-line at a threshold of 80%, then both links will be carrying the load.

The Down Threshold looks at the total throughput (both links together) to determine if the second link will be brought down. The total throughput is compared to the throughput of a single link. When the total throughput drops below the Down Threshold, the second link will be dropped.

```
Enter:
 Percent of main link capacity (40 to 95)
> 60
```

**Default:** 60%

**4 - Down Stability Timer**

The Down Stability Timer is similar in operation to the Up Stability Timer. When the total link throughput drops below the value set by the Down Threshold for a period of time defined by the Down Stability Timer, the secondary link will be disconnected and placed back in the stand-by mode.

For example, if the total throughput (both links together) drops below 60% of the bandwidth of a single link (64 Kbps) for a period of 10 minutes, the secondary link will be disconnected.

```
Enter:
 time in minutes when link is up (from 1 to 60)
>10
```

**Default:** 2 minutes

## Protocol Set-Up Menu

```
                    EDIT REMOTE SITE 2 PROTOCOL SET-UP MENU

    Option               Value          Description
 1. Bridge parameters    menu         - Configure bridge parameters
 2. IP parameters        menu         - Configure IP parameters
 3. CCP parameters       menu         - Configure CCP parameters
 4. CMCP parameters      menu         - Configure connection management
 5. BACP set-up          menu         - Configure BACP parameters
 6. Multilink protocol   [disabled]   - Allows multilink operation
 7. QOS set-up           menu         - Define Quality of Service for Interface
 8. PPPoE protocol     *[enabled]     - PPP over Ethernet Protocol

Enter option number, "=" - main menu, <TAB> - previous menu

>
```

**1 - Bridge Parameters**

The Bridge Parameters option takes you to the Bridge Parameters menu for the chosen remote site, where the bridge parameters are configured.

**2 - IP Parameters**

The IP Parameters option takes you to the IP Parameters menu for the chosen remote site, where the IP parameters are configured. The type of link is specified as numbered or unnumbered. The type of IP routing is set within this menu: none, RIP1, RIP2 or RIP1_compatible. Both local and peer IP addresses are defined here, NAT and NAPT may be enabled and configured and some connection management parameters are set.

**3 - CCP Parameters**

The CCP Parameters option takes you to the CCP Parameters menu for the chosen remote site, where the CCP (Compression) parameters are configured.

**4 - CMCP Parameters**

The CMCP Parameters option takes you to the CMCP Parameters menu for the chosen remote site, where the CMCP (Connection Management) parameters are configured. The Connection Management parameters determine when the ISDN calls will be suspended and spoofed or when they will be terminated.

Note: this option will only be displayed if this remote site connection is configured as ISDN.

**5 - BACP Set-Up**

The BACP Parameters menu allows you to activate the BACP (Bandwidth Allocation Control Protocol) and set the call conditions used. BACP reduces network charges by adding or dropping the second link based on traffic demands. BACP mediates control of the link between the routers to prevent "link bobbing".

Note: this option will only be displayed if this remote site connection is configured as ISDN or PPP Leased and the dual-link option is enabled.

**6 - Multilink Operation**

This option determines whether the connection to this remote site will operate using single link protocol or PPP multilink protocol. Multilink protocol allows multiple links to be connected between two routers. The physical links may be of different types (e.g. Leased and ISDN)

**Default:** [enabled]

**ISDN Considerations:**

When multilink operation is changed for a group, all active ISDN calls will be disconnected.

When the P840 receives an incoming call, the Multilink state is taken from the "ISDN_TEMPLATE" remote site profile. Note that if Multilink is disabled in the "ISDN_TEMPLATE" and an incoming call requests Multilink, the P840 will negotiate to have Multilink enabled.

When a PPP P840 with Multilink disabled attempts to establish an ISDN connection to an Ascend router with Multilink enabled, the Ascend router will shut down the ISDN call. Simply set the Multilink values on each of the routers to be the same value and then establish the ISDN connection.

**Note:** if the primary connection for this remote site is frame relay, PPP encapsulation must be enabled for this option to be displayed.

**7 - QOS Set-Up**

The QOS Set-up menu allows you to assign a QOS service to this remote site connection

**8 - PPPoE**

This PPPoE field will be displayed when the remote connection primary link is configured for a LAN interface. This option will automatically be enabled. This is a read-only field.

## Bridge Parameters Menu

```
                EDIT REMOTE SITE 1 BRIDGE PARAMETERS MENU

    Option              Value          Description
 1. STP parameters      menu         - Define port specific options
 2. Bridge enabled     [enabled]     - Enable BCP negotiations
 3. Tinygram           [disabled]    - Enable tinygram compression
 4. FCS preservation   [enabled]     - Preserve FCS across WAN




Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **BRIDGE PARAMETERS MENU** allows the setting of the type of Bridge link connection to the remote site PPP router. The parameters defined here are used by the BCP (Bridge Control Protocol) functions of the router for negotiating bridging during call establishment.

**1 - STP Parameters**

The STP Parameters option directs you to the STP Parameters Menu where STP Port parameters for this remote site are set.

**2 - BCP Enabled**

The BCP Enabled option enables or disables the Bridge Control Protocol negotiations for this remote site. When a connection to this remote site does not require bridging, this option may be disabled causing BCP not to be negotiated.

**Default:** [enabled]

**3 - Tinygram**

The Tinygram option enables or disables the compression of bridge frames that are smaller than the minimum frame size of 64 bytes. Tinygram compression simply suppresses the trailing zeroes of a small frame.

**Default:** [disabled]

**4 - FCS Preservation**

The FCS Preservation option enables or disables the transmission of the Frame Check Sequence (FCS) for bridge frames that are passed to the remote site PPP device.

When set to disabled, this P840 will not send the FCS on bridge frames sent to the remote site PPP partner.

This option may need to be disabled when connecting to some Cisco routers.

**Default:** [enabled]

## STP Parameters Menu

```
            EDIT REMOTE SITE 1 BRIDGE PARAMETERS STP PARAMETERS MENU

    Option       Value          Description
 1. State        [enabled]    - Enable/disable port
 2. Path cost    [100]        - Define network cost for port
 3. Priority     [128]        - Set port priority









Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **STP PARAMETERS MENU** allows the setting of the STP port parameters used by the BCP (Bridge Control Protocol) functions of the router for negotiating bridging during call establishment. All of the settings in this menu will be ignored when STP is disabled within the Bridging Set-up menu.

**1 - State**

The State option toggles between enabling and disabling this WAN port when running Spanning Tree Protocol on the WAN connection to this remote site device.

**2 - Path Cost**

The Path Cost option allows the setting of the contributing path cost to the Root for this port.

**Contribution of Path Cost to Root Path Cost:**

The path cost to the Root Bridge is added to path costs of other bridges along the same stream to the Root Bridge. The result is the Root Path Cost.

Once the Root Bridge is selected, a determination of which bridge(s) will become blocked where necessary is made. This determination is made by comparing the sum of the path costs (i.e. the Root Path Cost) to the Root Bridge. Where redundant paths exist, the bridge with the lowest Root Path Cost to the Root Bridge will become the *Designated Bridge* for the LAN. If all contending bridges' ports have the same Root Path Costs, then first their Bridge IDs (Priority/MAC address) and second their Port IDs (Port Priority) will be used as tiebreakers.

**Default:** [100]

**Range:** 1 to 65535

**Considerations:**

Increasing this value increases the total cost of the path to the Root Bridge. This may (depending on the topology) cause a bridge along the path to the Root bridge to be taken out of service and a blocked bridge to come into service.

Decreasing the value may have the opposite effect.

**3 - Priority**

The Priority option allows the setting of the port priority. This value is entered in decimal format and appears in hex format in the Port ID/Designated Port identifier (as applicable) of the Port Status display.

**Default:** [128] (decimal)

**Range:** 0 - 255

**Considerations:**

Increasing this value lowers the probability of this port becoming the Root port to the Root Bridge. Decreasing this value increases the probability.

## IP Parameters Menu

```
            EDIT REMOTE SITE 1 PROTOCOL SET-UP IP PARAMETERS MENU

    Option               Value               Description

 1. IP routing          menu              - Configure IP routing
 2. NAT advanced setup  menu              - Configure NAT address pool
 3. IP enabled         [enabled]          - Enable IP protocol
 4. NAT enabled        [disabled]         - Enable address translation
 5. Link IP type       [numbered]         - Define numbered link
 6. Local IP address   [none]             - Define local IP address
 7. Peer IP address    [none]             - Define peer IP address
 8. Private route      [disabled]         - Do not advertise this route
 9. VJ compression     [disabled]         - Enable VJ header compression


Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **IP PARAMETERS MENU** allows the setting of the type of IP link connection to the remote site PPP router. The parameters defined here are used by the IPCP (Internet Protocol Control Protocol) functions of the router for negotiating IP routing during call establishment. The menu options are shown in the above screen for both the numbered and unnumbered link IP type settings. Some of the above menu options will not be displayed when unnumbered link IP type is enabled

Each side of the connection must have an IP address assigned to the router in order to properly route IP packets between the two routers.

The IP routing parameters defined here are for this connection to the remote site peer IP router only. The IP routing performed on the local LAN is defined within the IP Routing menu under the Configuration menu. This allows the IP routing to be set independently for each interface on this P840 router.

**1 - IP Routing**

The IP Routing option directs you to the IP Routing Parameters Menu where the IP routing parameters for this remote site are set. The parameters include the type of IP routing, the use of triggered RIP, and others.

**2 – NAT Advanced Setup**

The NAT Advanced Setup option takes you to NAT Advanced Setup menu where parameters for the Network Address Translation pool for this remote site may be assigned.

**3 - IP Enabled**

The IP Enabled option enables or disables the Internet Protocol negotiations for this remote site. When a connection to this remote site does not require IP routing, this option may be disabled causing IP not to be negotiated.

**Default:** [enabled]

**4 - NAT Enabled**

Network Address Translation (NAT) is a technique which translates private IP addresses on a private network to valid global IP addresses for access to the Internet. Network Address Port Translation (NAPT) translates both the IP address and the port. The advantage of port translation is that more than one private IP address can be translated to the same single global IP address. NAPT allows data exchanges initiated from hosts with private IP addresses to be sent to the Internet via the P840 using a single global IP address. Port translation can also be used from one private network to another private network if the two networks have conflicting IP addresses.

A global IP address must be assigned to the WAN link upon which NAT is enabled for NAT to work. The global IP address may be configured locally or negotiated if numbered links are enabled. If unnumbered links are enabled, the router must accept an IP address for the WAN link from the remote site.

When NAT is enabled this router will not send RIP messages out. The router will be able to receive RIP requests. IP pattern filters and Firewall use the non-translated IP address (i.e. the private IP address that is used on the private network).

Remember: if NAT is enabled with IP addressing and Firewall is enabled, then the IP address for this remote site must be in the firewall table.

**Default:** [disabled]

**Note:** In a raw 1490 frame relay environment, if NAT is changed from enabled to disabled, any static IP addresses at the remote site will become invalid. In this case, clear the static routes entries with a "Remove Static routes – all" command from the NAT Advanced Menu.

**5 - Link IP Type**

The Link IP Type option defines the type of link connection that will be established with the remote site PPP router. The link may be numbered, in which both sides of the WAN connection have IP addresses assigned; or unnumbered, in which the peer (remote partner PPP router) and the calling router use their device IP address.

When operating in unnumbered mode, each of the two IP routers operates as half of a complete router. The WAN connection is considered a common internal data path with the IP routing actually taking place between the two remote LANs.

When the link IP type is set to unnumbered, the Local IP Address option is not available. For an unnumbered link, the local IP address is taken from the IP address assigned to this router in the Internet Set-Up menu.

**Default:** [unnumbered]

**Choices:** numbered, unnumbered

**6 - Local IP Address**

The Local IP Address option allows the definition of an Internet Protocol (IP) address and corresponding subnet size for the link of this router.

**When the link IP type is set to unnumbered, the Local IP Address option is not available.** For an unnumbered link, the local IP address is taken from the IP address assigned to this router in the Internet Set-Up menu.

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. 92.3.1.10). Each decimal number must be less than or equal to 255, that is the maximum value of each 8-bit field.

The Subnet Mask Size variable partitions the host field of an IP address into two parts: a *subnet number* and a *host number*. The subnet mask is defined as a series of contiguous bit locations from the start of the IP address.

**Default:** [none]

```
Enter :
    IP address (up to 15 characters)
>

Enter :
    subnet mask size(from 8 to 32)
>
```

**Caution:** when using numbered links, both the local IP address AND the subnet mask size MUST be entered. If only the IP address is entered and no subnet mask size, the router has no way of determining the subnet location – the link will not operate.

**6/7 - Peer IP Address**

The Peer IP Address option allows the definition of an Internet Protocol (IP) address and corresponding subnet size for the link side of the PPP IP router at the remote site. If the link IP type is set to numbered, the peer IP address must be on the same network as the local IP address.

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. 92.3.1.10). Each decimal number must be less than or equal to 255, that is the maximum value of each 8-bit field.

The subnet mask size is not specified when the link IP type is set to numbered. The subnet mask is defined as a series of contiguous bit locations from the start of the IP address.

**Default:** [none]

```
Enter :
    IP address (up to 15 characters)
>

Enter :
    subnet mask size(from 8 to 32)
>
```

**7 - Negotiate Address**

The Negotiate Address option is only available when the **Link IP Type is set to unnumbered**. Address negotiation causes this P840 to negotiate with the peer IP router to determine the IP addresses of each device. This allows this P840 to supply an IP address to the peer IP router if the Peer IP Address option is defined.

When address negotiation is enabled, this P840 will accept an IPCP PPP connection from a peer IP router even if the global IP address of this P840 is not configured. This P840 will use the negotiated address that the peer has provided.

When address negotiation is disabled, this P840 will not initiate address negotiations but will respond to address negotiations if requested by the peer IP router.

**Default:** [enabled]

**8 - Private Route**

The Private Route option is only available when the **Link IP Type is set to numbered**. Setting this numbered link connection to be a private link causes the IP connection to the peer IP router to not be advertised in the RIP information.

**Default:** [disabled]

**8/9 - VJ Compression**

The VJ Compression option enables or disables Van Jacobson header compression on packets send to this remote site.

**Default:** [disabled]

## IP Routing Menu

```
        EDIT REMOTE SITE 1 PROTOCOL SET-UP IP PARAMETERS IP ROUTING MENU

    Option                Value                Description
 1. Routing protocol      [rip1_compatible]   - Define link routing protocol
 2. RIP mode              [both]              - Define RIP send/receive mode
 3. Triggered RIP         [disabled]          - Define triggered RIP
 4. Auto Default Route    [disabled]          - Add default route on connect
 5. Link cost             [0]                 - Define cost added to routes




Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **IP PARAMETERS - IP ROUTING MENU** allows the setting of the IP routing parameters to use for this IPCP connection to the peer IP router. The parameters defined here are used by the IPCP (Internet Protocol Control Protocol) functions of the router for negotiating IP routing during call establishment.

**1 - Routing Protocol**

The Routing Protocol option defines the type of IP routing protocol to be used on this link interface. The P840 may be set up to use different types of IP routing protocols on each of it's interfaces: LAN and links.

When the routing protocol is defined as none, the P840 will operate as an IP router but will NOT participate in the exchange of RIP messages between the other IP routers in the network. All IP routing is accomplished by using the static routes table. All routes within the network must be manually entered in the static routing table.

When the routing protocol is defined as rip1, the P840 will operate as a RIP1 IP router. All routing information will be sent and received via broadcast RIP packets.

When the routing protocol is defined as rip1_compatible, the P840 will operate as a RIP2 IP router in broadcast mode. All routing information will be sent via broadcast RIP2 packets. Routing information may be received as broadcast RIP1, broadcast RIP2, or multicast RIP2.

When the routing protocol is defined as rip2, the P840 will operate as a RIP2 IP router. All routing information will be sent via multicast RIP2 packets. Routing information may be received as broadcast RIP2 or multicast RIP2.

Partner routers connected on the WAN do not need to have their IP routing protocols set to the same values. An IP router at a central site may have it's routing protocol set to RIP so that it may continue to listen to RIP messages and adapt to the changes of the local network, while the remote locations, with their default routes back to the main router, cannot propagate any incorrect routing information that might be present on the remote segments. Each of the routers at the remote sites would have their routing protocol set to none.

**Default:** [rip1_compatible]

**Choices:** none, rip1, rip1_compatible, rip2

**2 - RIP Mode**

The RIP Mode option defines how this P840 will participate in RIP IP routing messages over the link to this remote site.

When the RIP mode is set to both, the P840 will send and receive RIP routing messages over the link to this remote site.

When the RIP mode is set to send_only, the P840 will only send RIP routing messages over the link to this remote site.

When the RIP mode is set to receive_only, the P840 will only receive RIP routing messages over the link to this remote site.

**Default:** [both]

**Choices:** both, send_only, receive_only

**3 - Triggered RIP**

The Triggered RIP option disables or defines the type of triggered RIP to use on the link to this remote site.

Disabling this option will cause the RIP routing tables to be transmitted every 60 seconds.

Entering "standard" enables triggered RIP; the P840 will only send RIP messages over the link to this remote site when the routing information has actually changed.

Entering "link_up_only" enables triggered RIP; the P840 will only send RIP messages over the link to this remote site when the routing information has actually changed **and** the link is currently up. If the link is down due to suspension, the routing information will be queued and then sent the next time the link is brought up for user data.

When triggered RIP is enabled, if the remote site router refuses to negotiate triggered RIP on the initial connection, this router will attempt to negotiate triggered RIP for 5 minutes. During the 5 minutes, this router will use normal RIP. If triggered RIP has not been negotiated after the 5 minutes, this router will fall back to using normal RIP.

**Default:** [disabled]

**Choices:** disabled, standard, link_up_only

**Considerations:** If you are running spoofing with Triggered RIP, both routers must be set to Triggered RIP "link_up_only". The P840 will automatically configure to this setting but the remote partner router should be checked to make certain that it is correctly configured.

**4 - Auto Default Route**

The Auto Default Route option allows a default IP route to be added to the routing tables when a connection is established to this remote site. When the link to this remote site goes down, the auto default route will be removed from the routing table.

**Default:** [disabled]

**5 - Link Cost**

The Link Cost option defines the amount of extra routing cost to add to routes that are learned from this link connection. This added link cost may be useful in forcing learned routes to have a higher cost when they are across a slower link connection.

**Default:** [0]

## NAT Advanced Set-Up Menu

```
    EDIT REMOTE SITE 1 PROTOCOL SET-UP IP PARAMETERS NAT ADVANCED SETUP MENU

    Option                Value                Description
 1. Translation type      [port]             - Define translation method
 2. Show address pool                        - Display IP mappings
 3. Dynamic IP pool       [none]             - Dynamically assigned mappings
 4. Add static entry                         - Specify IP-IP mappings
 5. Remove static entry                      - Remove static IP mapping
 6. TCP mss               [enabled]          - Modify TCP mss
 7. TCP mss value         [1452]             - Maximum TCP mss value



Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The NAT Advanced Set-Up Menu allows you to set parameters for the NAT address pool for this remote site router.

**1 - Translation Type**

This option sets the address translation method to be used for NAT. The address may be translated as either a port or an internal IP address. With IP address translation, each internal IP address is mapped to one global IP address; with port translation, several internal IP addresses may be mapped to a single global IP address.

**Default:** [port]

**2 - Show Address Pool**

This option displays the IP address pool for this remote site.

```
                              NAT ADDRESS POOL

Pool Address          Type    Actual Address                 Status
------------          -----   --------------                 ---------
12.34.5.6             Static  196.23.45.6                    In use
12.34.5.12            Static  196.23.45.24                   Reserved
23.45.6.10            Dynamic 123.45.67.8                    In use
23.45.6.11            Dynamic None assigned                  Available
23.45.6.12            Dynamic None assigned                  Available
23.45.6.13            Dynamic None assigned                  Available
```

The Pool Address is the internal address to be used on this network, the Actual Address is the global IP address to which the internal address is assigned.

When the last dynamically assigned address in the address pool is reached, the router will automatically use port translation with that address in order to allow as many connections as possible. If there are zero or one address specified for the pool, then NAPT will be used for all connections. If zero, the address assigned by the remote router IPCP or the address specified in the "Peer IP address" option will be used. If one address is specified, that address will be used.

**3 - Dynamic IP Pool**

The Dynamic IP Address Pool option defines the block of global IP addresses that may be used to map to internal addresses. The router will assign a global IP address from this pool to the internal address of a device on the network.

The first address in the range must be specified followed by the number of addresses in the pool.

**4 - Add Static Entry**

The Add Static Address option assigns a specific internal IP address of a device to a specific global IP address. When this option is selected, first enter the internal IP address to be assigned, then the global IP address.

**5 - Remove Static Address**

The Remove static address option removes the static address assignment from the address pool. Addresses may be removed individually by entering the global IP address to be taken off, or the entire list of static address assignments may be cleared by entering "all".

**6- TCP mss enabled**

When enabled the TCP Maximum Segment Size (MSS) value will be evaluated for determining the maximum amount of TCP data in a single IP datagram. When disabled this value is ignored.

**Options:** enabled, disabled
**Default:** disabled

**7 - TCP mss value**

The TCP Maximum Segment Size (mss) value can be configured to specify the maximum amount of TCP data in a single IP datagram. The default value is set to 1460 which is typical for an Ethernet interface.

**Range:** 536 to 1460
**Default:** 1460

## Compression Parameters Menu

```
                    EDIT REMOTE SITE 1 CCP PARAMETERS MENU

    Option                Value          Description
 1. Compression          [enabled]    - Allows compression operation
 2. Extended sequence    [disabled]   - Two byte sequence field









Enter option number, "=" - main menu, <TAB> - previous menu


>
```

The **COMPRESSION (CCP) PARAMETERS MENU** allows the setting of data compression on the link connection to the remote site PPP router. The parameters defined here are used by the CCP functions of the router for negotiating data compression during call establishment.

**1 - Compression**

The Compression option enables or disables the negotiation of compression for data packets sent from the remote site PPP router and received by this router. The P840 performs data compression at the bundle level and not at the link level. Link based compression will be rejected. The P840 supports CCP option 17 - PPP Stac LZS Compression Protocol.

When the Compression option is enabled, data compression will be negotiated with the remote site router for data that is sent from this router to the remote site router.

When compression is disabled, this router will not allow data compression to be negotiated for the connection.

**Default:** [enabled]

**2 - Extended Sequence**

The Extended Sequence option enables or disables the use of a two-byte sequence number for inter-router communications. When disabled, the sequence number is one byte.

This option should be enabled when connecting to a PPP router that uses a two-byte sequence number instead of a one-byte sequence number. Some Cisco routers with software versions IOS 11.0 and IOS 11.1 use a two-byte sequence number.

**Default:** [disabled]

**Considerations:**

If compression has been negotiated for the connection but many data errors are received and very little data, the Extended Sequence number may need to be enabled.

## CMCP (Connection Management) Parameters Menu

```
            EDIT REMOTE SITE 1 PROTOCOL SET-UP CMCP PARAMETERS MENU

    Option                Value          Description
 1. IP spoofing           menu         - Configure IP spoofing
 2. CMCP enabled         [disabled]    - Enable CMCP negotiations
 3. Bridge traffic       [enabled]     - Spoof bridge traffic
 4. Disc after last      [off]         - Disconnect after last session
 5. Suspension timeout   [off]         - Set maximum suspension interval




Enter option number, "=" - main menu, <TAB> - previous menu


>
```

The **CONNECTION MANAGEMENT (CMCP) PARAMETERS MENU** allows the configuration of the Connection Management options for this remote site.

Note: this menu will only appear if this router has an ISDN BRI module installed.

**1 - IP Spoofing**

The IP Spoofing option directs you to the IP Spoofing Parameters Menu where the IP spoofing parameters for this remote site are set. The parameters define how to interact and keep track of the TCP sessions while connection management is enabled on the link to this remote site.

**2 - CMCP Enabled**

The CMCP Enabled option enables or disables the Connection Management Control Protocol negotiations for this remote site. When a connection to this remote site does not require connection management, this option may be disabled causing CMCP not to be negotiated.

Connection Management is used to minimize the amount of connection time used when connected to partner P840s.

When Connection Management is enabled, the active ISDN calls are monitored for "Interesting Traffic", suspended, and resumed when required to transfer user data between P840s.

**Default:** [disabled]

**Considerations:** if this remote site is set as spoofing, CMCP will be set to enabled.

**Note:** When CMCP is enabled, the call me prefix to get back to the partner router must be entered so that the link can be re-established after suspension (only the directory number is passed when the call is set up, not the entire connection number). For the same reason, the partner router must also have its call me prefix entered.

**3 - Bridge Traffic**

The Bridge Traffic option enables or disables spoofing of bridge frame traffic while Connection Management is enabled.

When the P840 is spoofing bridge traffic (this option enabled), the bridge traffic received from the LAN will not be used to resume a suspended ISDN call or to keep an existing ISDN call up. While the ISDN call is up for other reasons, the bridge traffic received from the local LAN will be passed.

When this option is disabled, the P840 will pass all bridge traffic received from the local LAN. This will cause ISDN calls to be resumed if suspended.

**Default:** [enabled]

**4 - Disconnect After Last**

The Disconnect After Last option sets the time delay for disconnecting the link connection to this remote site after all of the connection management monitored sessions have been terminated. If set to off, the link connection will be disconnected when the Inactivity Timer expires.

**Default:** [off]

```
Enter :
    off, immediately, delay in seconds (from 5 to 300)
>
```

**5 - Suspension Timeout**

The Suspension Timeout option allows the definition of a maximum time that the link connection may be in the suspended state. If the link connection has been suspended for the time period defined by the suspension timeout, the link connection will be silently dropped and the sessions logged on that connection will be removed from the table. Silently dropping the link connection means that the peer remote site router will not be notified that the connection has been dropped.

**Default:** [off]

```
Enter :
    Time in minutes (from 1 to 10080), off
>
```

## IP Spoofing Menu

```
      EDIT REMOTE SITE 1 PROTOCOL SET-UP CMCP PARAMETERS IP SPOOFING MENU

    Option          Value          Description
 1. TCP idle       [3600 sec]    - Set interval till first TCP keepalive
 2. TCP interval   [60 sec]      - Set interval between TCP keepalives
 3. TCP retries    [5]           - Set maximum TCP keepalive retries
 4. TCP aging      [7200 sec]    - Set TCP connection aging interval



Enter option number, "=" - main menu, <TAB> - previous menu


>
```

The **IP SPOOFING PARAMETERS MENU** allows the setting of connection management parameters that control the IP spoofing portion of the link connection. The timers and values defined within this menu will be used for each of the TCP sessions monitored by this P840.

**1 - TCP Idle**

The TCP Idle option defines the idle time in seconds that the P840 will wait before sending the first fake (spoofed) keepalive to the TCP session endpoint. Idle time is the time when the P840 does not receive TCP keepalive messages for that TCP session.

When the TCP Idle option is set to off, the P840 will never send out fake keepalive messages.

The TCP keepalive messages are used to determine if the station at the end of the TCP session is still alive.

**Default:** [3600 sec]

```
Enter :
    time in seconds (from 60 to 7200), off
>
```

**2 - TCP Interval**

The TCP Interval option defines the internal interval time in seconds that the P840 will wait before sending the next TCP keepalive. These additional keepalive messages will be sent when there has not been a response to the initial keepalive messages sent from the P840.

The TCP keepalive messages are used to determine if the station at the end of the TCP session is still alive.

**Default:** [60 sec]

```
Enter :
    time in seconds (from 5 to 120)
>
```

**3 - TCP Retries**

The TCP Retries option defines the number of unacknowledged fake TCP keepalive messages that this P840 will send before the TCP session is considered dead.

The TCP keepalive messages are used to determine if the station at the end of the TCP session is still alive.

**Default:** [5]

```
Enter :
    Number of retries (from 1 to 20)
>
```

**4 - TCP Aging**

The TCP Aging option defines the amount of idle time in seconds that the P840 will wait before the TCP session is aged out and considered dead. The aging timer starts counting when there is no session traffic.

The TCP aging timer can be used in conjunction with the IP address connect feature. When the TCP session traffic is idle for a time longer than the inactivity timer, the link will be suspended. If the TCP session continues to be idle, the aging timer will age out the session. Once all of the sessions are aged out, the link will be quietly taken from suspended to down. This process allows the link to be available for use with another IP address connect request.

When a TCP session has been aged out and the P840 then receives a TCP keepalive for that session, the link will be re-established to send the keepalive. The link is re-established because the TCP keepalive messages are not easily discernable from normal TCP session traffic. The TCP aging timer should be set to a value larger than the frequency of TCP keepalive messages on the network. TCP keepalive messages can have intervals as long as 60 minutes.

The TCP keepalive messages are used to determine if the station at the end of the TCP session is still alive.

**Default:** [7200 sec]

```
Enter :
    time in seconds (from 60 to 604800), off
>
```

## BACP Set-Up Menu

```
            EDIT REMOTE SITE PROTOCOL SET-UP BACP SET-UP MENU

   Option           Value  Description
1. BACP            [disable]   - Enable/disable BACP operation
2. Call mode       [local]     - Device to initiate second call
3. Request number  [disabled]  - Partner provides second call number




Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **BACP PARAMETERS MENU** allows you to activate the BACP (Bandwidth Allocation Control Protocol) and set the call conditions used.

**Note:** in Net3 ISDN environments with BACP enabled, directory numbers must be configured for BACP to function.

**1 - BACP**

The BACP option enables or disables the BACP for the secondary link. The parameters to add or drop the secondary link are set at the Main/Configuration/WAN Set-up/Remote Site Set-up/Edit Remote Site/Secondary Link Activation Menu.

**Default:** [disabled]

**2 - Call Mode**

The Call Mode option toggles between local and partner modes. Call mode allows you to set where the call to bring up the secondary link will originate from, so that all connections may be made from one router for centralized billing.

In local mode, this P840 will initiate an outgoing call back to the remote site to re-establish the link.

In partner mode, this P840 will send a request to the other router (via the primary link) to bring up the link from that end.

**Default:** [local]

***3 - Request Number***

The Request Number option is functional when BACP is in local mode. If enabled, the partner remote site ISDN number is requested. When disabled, the acknowledge message from this P840 tells the partner remote site router that its ISDN number does not need to be sent (it is in the lookup table already).

**Default:** [disabled]

**Note:** this option is only displayed if Call Mode is [local].

## QOS Menu

```
                        REMOTE SITE QOS MENU

   Option                Value                 Description
1. Queuing Strategy    [priority][1]        - Define type of queuing strategy




Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The QOS MENU allows the setting of the queuing strategy applicable to the remote site connection. The QOS parameters defined here are used by the outbound traffic to the connection to the remote router.

**1. Queuing Strategy**

The first parameter of the Queuing Strategy assigns the type of QOS mechanism applied to the remote connection.
**Default** : [none]

**Choices**: none, priority

The second parameter for the Queuing Strategy assigns the QOS priority list applicable to the remote site connection. The QOS priority list are defined by numbers and only one QOS priority list (each list can contain several QOS items) can be defined for each remote connection.

**Default**: [No default value]
**Range**: 1 to 16

Note:
This parameter only appears if the first parameter has been set to priority.

## Security Parameters Menu

```
            EDIT REMOTE SITE SECURITY PARAMETERS MENU

    Option                  Value            Description
 1. Incoming PAP password  [none]          - Set incoming PAP password
 2. Incoming CHAP secret   [none]          - Set incoming CHAP secret
 3. Outgoing user name     "DEV050607"     - Set outgoing user name
 4. Outgoing PAP password  [none]          - Set outgoing PAP password
 5. Outgoing CHAP secret   [none]          - Set outgoing CHAP secret


Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **EDIT REMOTE SITE SECURITY PARAMETERS MENU** allows you to set outgoing and incoming password data and an outgoing user name for PPP security on the connection to this remote site router.

Note: routers configured to have a leased line link operating in conjunction with an ISDN B-Channel (either as backup or bundled link) must have security enabled and with the proper usernames and passwords entered on both partner routers.

**1 - Incoming PAP password**

The Incoming PAP Password option defines the PAP password that this P840 PPP router expects to receive from the remote site PPP router in response to authentication requests from this router.

**Default:** [none]

**2 - Incoming CHAP secret**

The Incoming CHAP Secret option defines the CHAP secret that this P840 PPP router expects to receive from the remote site PPP router in response to authentication requests from this router.

**Default:** [none]

**3 - Outgoing user name**

The Outgoing User Name option defines the user name that this P840 PPP router will be sending to the remote site PPP router when responding to authentication requests from the remote site PPP router. The outgoing user name defaults to the device name. If the device name is changed, all remote sites are searched and any remote site whose outgoing user name matches the old device name will be updated to use the new device name.

The outgoing user name must be defined the same as the user name defined in the PPP security settings for the remote site router.

The outgoing user name is case sensitive and may consist of 1 to 32 alphanumeric characters. Use the underscore character instead of a space character.

**Default:** [*] Default device name

**4 - Outgoing PAP password**

The Outgoing PAP Password option defines the PAP password that this P840 will use when responding to authentication requests from the remote site PPP router.

**Default:** [none]

**5 - Outgoing CHAP secret**

The Outgoing CHAP Secret option defines the CHAP secret that this P840 will use when responding to authentication requests from the remote site PPP router.

**Default:** [none]

## Security Set-Up Menu

```
                          SECURITY SET-UP MENU

    Option                  Value            Description
 1. Default parameters      menu           - Set default outgoing security
 2. Security level         [none]          - Set security protocol
 3. Request security       [incoming-only] - Set security operation
 4. CHAP challenges        [once]          - CHAP Authentication
 5. CallerID security      [disabled]      - Enable/disable CallerID security


Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **SECURITY SET-UP MENU** allows the configuration of the PPP security options used between this router and the remote site for which a profile is currently being configured.

Note: routers configured to have a leased line link operating in conjunction with an ISDN B-Channel (either as backup or bundled link) must have security enabled (security level set to either [PAP] or [CHAP]) and with the proper usernames and passwords entered on both partner routers.

**1 - Default parameters**

The Default Parameters option takes you to the Default Parameters menu where the outgoing PPP security options to be used by this router when calling the remote site are configured.

**2 - Security Level**

The Security Level option defines the type of PPP security to use for incoming connections. When a security level is set, the P840 will always require authentication on incoming connections. The P840 will ask for authentication on outgoing calls when a security request is set to always (see below).

**Default:** [none]

**Choices:** none, PAP, CHAP

**3 - Request security**

This specifies when the remote site router should be requested to authenticate:

- always (when this router makes an outgoing call OR receives an incoming call)
- incoming_only (ONLY when this router receives an incoming call)

**Default:** If an ISDN module is installed: [incoming only]
If only leased line module(s) installed: [always]

**Choices:** always, incoming only

**4 - CHAP Challenges**

The CHAP Challenges option defines the frequency of CHAP challenges that this P840 PPP router will require when authenticating a remote site PPP router.

**Default:** [once]

**Choices:** once, continuous

**5 - CallerID Security**

The CallerID Security option enables or disables the use of incoming callerID information to do a security check for valid devices. This option may be used to refuse incoming ISDN calls from routers located at an unknown site. Incoming callerID information received is matched against the ISDN number, alternate ISDN number, and wildcard values of each remote site profile. If a match is not found after checking each of the three numbers in each of the remote site profiles, the incoming ISDN call will be ignored.

The CallerID Security option must only be enabled on a P840 that is connected to an ISDN service that provides callerID functions. Check with your ISDN service provider about the availability of this service. This option is only applicable to incoming data calls.

When this option is set to enabled, this P840 will ignore any incoming ISDN call that does not provide callerID information or the callerID information does not match one of the configured values.

This option is only available when an ISDN BRI module is installed with the digital leased line option is disabled.

**Default:** [disabled]

## Default Parameters Menu

```
                          DEFAULT PARAMETERS MENU

   Option                  Value              Description
1. Outgoing user name      "DEV050607"       - Set outgoing user name
2. Outgoing PAP password   "*"               - Set outgoing PAP password
3. Outgoing CHAP secret    [none]            - Set outgoing CHAP secret
```

The **DEFAULT PARAMETERS MENU** allows you to set default outgoing PPP security options for this router. The values set in this menu will be used for any calls originating from this router rather than from a remote site (calls originating from a remote site will use the security parameters set for that site).

**1 - Outgoing user name**

The Outgoing User Name option defines the user name that this P840 PPP router will send to the called remote site PPP router when responding to authentication requests from the remote site PPP router. The outgoing user name defaults to the device name. If the device name is changed, all remote sites are searched and any remote site whose outgoing user name matches the old device name will be updated to use the new device name.

The outgoing user name must be defined the same as the user name defined in the PPP security settings for the remote site router.

The outgoing user name is case sensitive and may consist of 1 to 32 alphanumeric characters. Use the underscore character instead of a space character.

**Default:** [*] Default device name

**2 - Outgoing PAP password**

The Outgoing PAP Password option defines the PAP password that this P840 PPP will use when responding to authentication requests from the remote site PPP router.

**Default:** [none]

**3 - Outgoing CHAP secret**

The Outgoing CHAP Secret option defines the CHAP secret that this P840 PPP will use when responding to authentication requests from the remote site PPP router.

**Default:** [none]

## PPP Set-Up Menu

```
                              PPP SET-UP MENU

   Option                  Value          Description
 1. Advanced PPP set-up     menu         - Configure advanced PPP parameters
 2. Restart timer          [3000 msec]   - Set restart timer
 3. Configure count        [10]          - Set configure count
 4. Failure count          [5]           - Set failure count
 5. Terminate count        [2]           - Set terminate count









Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **PPP SET-UP MENU** configures PPP circuit parameters used during LCP (Link Control Protocol) negotiations with a remote site PPP router.

This P840 PPP router will request the configuration parameters defined here when initiating a PPP connection to a remote site PPP router.

When negotiating the LCP parameters for incoming PPP connections initiated by the remote site PPP router, this P840 will use these values as defaults but will accept a request for different values from the remote site PPP router.

If any of these LCP configuration parameters are required to be of a known value for a particular PPP connection, the parameters should be set to the same values on the routers on each end of the PPP link.

### 1 - Advanced PPP Set-Up

The Advanced PPP Set-up option takes you to the Advanced PPP Set-Up Menu. Here you set the advanced LCP parameters such as field compression, Quality protocol, and the type of multilink sequencing.

### 2 - Restart Timer

The Restart Timer option specifies the time between retransmissions of Configure Request or Terminate Request packets. When attempting to establish a PPP link connection, if the Restart Timer expires before a response is received for a Configure Request, another Configure Request will be sent.

**Default:** [3000 msec]

**Range:** 50 to 20000 msec

**3 - Configure Count**

The Configure Count option specifies the number of Configure Request packets that will be sent without receiving a valid Configure Ack, Configure Nak, or Configure Reject packet. If a valid response packet is not received within the count specified, it is assumed that the peer PPP router is unable to respond.

**Default:** [10]

**Range:** 1 to 100

**4 - Failure Count**

The Failure Count option specifies the number of Configure Nak packets that will be sent without sending a Configure Ack before assuming that the configurations requested are not converging. A Configure Nak packet is sent when one of the PPP routers wishes to negotiate the particular LCP parameter to be a different value than the one proposed by the initiating PPP router.

**Default:** [5]

**Range:** 1 to 100

**5 - Terminate Count**

The Terminate Count option specifies the number of Terminate Request packets that will be sent without receiving a Terminate Ack before assuming that the peer PPP router is unable to respond.

**Default:** [2]

**Range:** 1 to 10

## Advanced PPP Set-Up Menu

```
                          ADVANCED PPP SET-UP MENU

    Option              Value            Description
 1. ACFC                [enabled]       - Address/control field compression
 2. PFC                 [disabled]      - Protocol field compression
 3. Echo monitoring     [enabled]       - Allow echo monitoring of link
 4. Quality protocol    [disabled]      - Set quality protocol
 5. Quality interval    [10 sec]        - Set quality interval
 6. MP encapsulation    [enabled]       - Use MP headers for NCP negotiation
 7. MP sequencing       [normal]        - Set multilink sequence numbers
 8. MP discriminator    [MAC_address]   - Set multilink endpoint discriminator
 9. MP minimum          [50]            - Set minimum fragmentation size



Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **ADVANCED PPP SET-UP MENU** provides for more advanced PPP circuit parameter set-up. The parameters configurable from this menu are used during LCP (Link Control Protocol) negotiations with a remote site PPP router. This P840 PPP router will request the configuration parameters defined here when initiating a PPP connection to a remote site PPP router.

When negotiating the LCP parameters for incoming PPP connections initiated by the remote site PPP router, this P840 will use these values as defaults but will accept a request for different values from the remote site PPP router.

If any of these LCP configuration parameters are required to be of a known value for a particular PPP connection, the parameters should be set to the same values on the routers on each end of the PPP link.

**1 - ACFC**

The ACFC (Address/Control Field Compression) option determines if this P840 PPP router will request Address and Control Field Compression on the PPP link.

**Default:** [enabled]

**2 - PFC**

The PFC (Protocol Field Compression) option determines if this P840 PPP router will request Protocol Field Compression on the PPP link.

**Default:** [disabled]

**3 - Echo Monitoring**

The Echo Monitoring option determines if this P840 PPP router will generate Echo-Request messages on the PPP link.. Echo monitoring is used to help debug a link and verify data transmission. A change to the Echo Monitoring state will take effect the next time the link starts.

**Default:** [enabled]

**4 - Quality Protocol**

The Quality Protocol option determines if this P840 PPP router will request Link Quality Protocol monitoring on the PPP link.

**Default:** [disabled]

**5 - Quality Interval**

The Quality Interval option specifies the time interval between Link Quality Report packets that are generated and sent to the peer PPP router.

**Default:** [10 sec]

**Range:** 1 to 60 seconds

**6 - MP Encapsulation**

The MP Encapsulation option when set to enabled, specifies that the NCP negotiation messages are encapsulated within a Multilink header.

**Default:** [enabled]

**7 - MP Sequencing**

The MP Sequencing option specifies the size of the Multilink sequencing number used in the Multilink header during frame transmission. A setting of normal will use a 4 byte sequencing number and a setting of short will use a 2 byte sequencing number.

**Default:** [normal]

**Choices:** normal, short

**Considerations:**

When connecting to a Combinet PPP device, the MP Sequencing should always be set to short.

**8 - MP Discriminator**

The MP Discriminator option specifies the type of identification used to identify this P840 PPP router during a Multilink connection. The MP Discriminator allows the remote site PPP router to uniquely identify this Multilink link when it requests establishment.

**Default:** [MAC_address]

**Choices:** MAC_address, IP_address, directory_number

**9 - MP Minimum**

The MP Minimum option specifies the minimum size of PPP frame that will not be fragmented when sent to the remote site PPP router. PPP frames equal to or larger than this value will be fragmented across the links in a Multilink connection. A value of zero causes all inter-router frames to be fragmented.

**Default:** [50]

**Range:** 0 to 1600

## IP Address Connect Menu

```
                          IP ADDRESS CONNECT MENU

    Option                    Value         Description
 1. Edit IP address entry                 - Modify/add IP address entry
 2. IP address connect        [disabled]  - Activate IP address connect
 3. Show IP address entries               - Display IP address entries
 4. Remove IP address entry               - Delete IP address entry
 5. Remote site summary                   - Summary of remote sites




Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **IP ADDRESS CONNECT MENU** allows the display and configuration of the IP Address Connect table entries. IP Address Connect is used to establish ISDN calls to specific remote sites based on specific destination IP addresses.

### 1 - Edit IP Address Entry

The Edit IP Address Entry option allows the definition of an entry in the IP Address Connect table. The IP Address connect table allows this P840 to establish a PPP ISDN call to a specific remote site PPP router when IP traffic destined for a specific IP network is received from the local LAN. The IP addresses in the table are searched sequentially according to entry id number.

An entry of the IP address 0.0.0.0 causes any IP traffic to initiate a call to the specified remote site. Adding one of these default entries to the end of the table, e.g. id number 128, causes all IP traffic for destinations not listed in the address connect table to be sent to this default entry. Having this default entry at the end of the table causes all other entries to be checked first and then the remaining IP traffic will cause a connection to this default remote site.

To change any of the values of an entry that already exists, simply re-enter the values and substitute the new values where appropriate.

```
Enter :
    Set the IP address connect entry id (from 1 to 128)

>

Enter :
    Set the IP Address (up to 15 characters)

>

Enter :
    Size of subnet mask (from 1 to 32)

>

Enter :
    Remote site alias or id (up to 16 characters), none
```

**2 - IP Address Connect**

The IP Address Connect option enables or disables the IP Address connect operation of the router. When IP Address Connect is enabled, all IP traffic on the local LAN is checked against the IP routing table. If the IP address is not present in the IP routing table, the address is checked in the IP Address Connect table.

**Default:** [disabled]

**3 - Show IP Address Entries**

The Show IP Address Entries option displays all of the IP addresses and their corresponding remote site profile alias currently in the IP Address connect table. There may be up to 128 IP network addresses defined in the table.

```
  ID   IP Address        Subnet Mask Size   Subnet Mask       Remote Site
  --   ---------------   ----------------   ---------------   ----------------
   1   12.12.12.12              1          128.0.0.0         Vancouver

Type: [s] to redraw, [=] main menu, any other key to end.
```

**note:** the[ s] to redraw is case sensitive; it must be lower case.

| | |
|---|---|
| ID: | Entry number in the IP Address Connect table. |
| IP Address: | Network IP address of the remote network or device. |
| Subnet Mask Size: | IP address mask size defined |
| Subnet Mask: | IP address mask created from the mask size defined. The mask is used to allow all IP addresses of a destination IP network to apply to the Address connect function. |
| Remote Site: | Remote site profile entry to be used to call a remote partner P840 when IP traffic destined for the IP address is seen on the local LAN. |

**4 - Remove IP Address Entry**

The Remove IP Address Entry option allows you to remove a selected IP Address Connect entry from the database. The entries may be removed individually by using the index number or all at once.

```
Enter :
    all, id

>
```

**5 - Remote site summary**

The Display Summary option displays an overview of the remote site profiles configured on this P840. Each of the options is shown as "E" for enabled, "D" for disabled or "NA" for not available.

```
* - Up   @ - Suspended                    Total Remote Site Entries: 7
 E - Enabled   D - Disabled   NA - Not Available

 Id  Alias             FR  AC MP    Pri/Sec    DLCI  BRG IP IPX CCP CMCP BACP
 --- ----------------  --- -- -- ------------- ----  --- -- --- --- ---- ----
   1 Xanadu1           NA  D  E  Link01/none    NA   E   E  NA  E   NA   D
   2 Toronto           NA  D  E    ISDN/none    NA   E   E  NA  E   D    D
   3 FR_REL4           RAW D  E  Link04/ISDN    16   E   E  NA  E   NA   NA
   4 Dallas            NA  D  E    ISDN/ISDN    NA   E   E  NA  E   D    D
  41 ISDN_TEMPLATE     NA  D  E    ISDN/ISDN    NA   E   E  NA  E   D    D
  42 FR_TEMPLATE       PPP D  E    none/none    16   E   E  NA  D   NA   NA
```

Id: Entry number in the Remote Site table. The Index number may be used to reference this entry in the IP Address Connect table or for viewing statistics.

Alias: Text name used to easily reference this entry in the table. The Alias may be used to reference this entry in the IP Address Connect table or for viewing statistics.

FR: Frame Relay – displays whether PPP encapsulation is enabled (PPP) or disabled (RAW) over Frame Relay. This column displays not applicable (NA) in a non-frame relay environment.

AC: The state of the Auto-call option for this remote site profile.

MP: The state of the Multilink option for this remote site profile.

Pri/Sec: The type of primary and secondary links configured for this remote site profile. ISDN/none indicates that the circuit will only use ISDN calls. Link1 or Link2 entries indicates that the circuit has been defined as a digital leased circuit.

DLCI: The Frame Relay DLCI number of this remote site. Not applicable (NA) in a non-frame relay environment.

BRG: The state of the BCP (bridging) option for this remote site profile.

IP: The state of the IPCP (IP routing) option for this remote site profile.

IPX: The state of the IPXCP (IPX routing) option for this remote site profile.

CCP: The state of the CCP (compression) option for this remote site profile.

CMCP: The state of the CMCP (connection management) option for this remote site profile. Not applicable (NA) if the remote site is not an ISDN site.

BACP: The state of the BACP option for this remote site profile. Not applicable (NA) if the remote site is a frame relay site.

## Packet Services Set-Up Menu

```
                        PACKET SERVICES SET-UP MENU

    Option                 Value          Description
 1. Bridging set-up        menu         - Define bridging environment
 2. IP routing set-up      menu         - Define IP routing environment
 3. IP security set-up     menu         - Define IPsec services
 4. Filter set-up          menu         - Filter operations
 5. QOS set-up             menu         - Define QOS set-up




Enter option number, "=" - main menu, <TAB> - previous menu
>
```

The **PACKET SERVICES SET-UP MENU** provides

**1 - Bridging Set-Up**

The Bridging Set-up option takes you to the Bridging Set-Up Menu, where the parameters for bridging are configured.

**2 - IP Routing Set-Up**

The IP Routing Set-up option takes you to the IP Routing Set-Up Menu, where the parameters for IP routing are configured. IP routing may be enabled or disabled in this menu.

**3 - IP Security Set-Up**

The IP Security Set-up option takes you to the IP Security Set-up Menu, where parameters for IPSec may be configured.

**4 - Filter Set-Up**

The Filter Set-up option takes you to the Filter Set-Up Menu, where you can create filters based on protocol types and custom specifications.

**5 - QOS Set-Up**

The QOS Set-up option takes you to the QOS menu where you are able to define QOS Priority Lists and its associated items.

## Bridging Set-Up Menu

```
                          BRIDGING SET-UP MENU

    Option                  Value         Description
 1. Spanning tree           menu        - Configure STP communications
 2. Bridge forwarding      [enabled]    - Enable/disable bridge forwarding
 3. Bridge aging timer     [300 sec]    - Set MAC address aging interval
 4. Show bridging table                 - View MAC address table
 5. Show permanent table                - View permanent addresses only
 6. Clear bridging table                - Delete all non-permanent entries


Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **BRIDGING SET-UP MENU** provides access to management of the bridge/router frame-routing functions. These include Spanning Tree settings, management of the address tables, and adjustment of the aging timer.

**1 - Spanning Tree**

The Spanning Tree option directs you to the Spanning Tree Menu, where parameters of the Spanning Tree Protocol for this bridge are set and viewed.

**2 - Bridge Forwarding**

The Bridge Forwarding option enables or disables the frame forwarding operation of the bridge.

**Default:** [enabled]

**3 - Bridge Aging Timer**

The Bridge Aging Timer option sets the interval after which unused, non-permanent entries are removed from the address table.

**Default:** [300 sec]

**Range:** off (disabled), 10 to 1,000,000 seconds.

**Considerations:**

Increasing the value of the bridge aging timer will remove unused entries less frequently. This will offer an increase in bridge performance, as the table will not be rebuilt as often when stations come on and off the LAN.

Decreasing the bridge aging timer will remove unused entries more frequently. This will cause the table to be rebuilt more often, which may, depending on the size of the network, consequently decrease bridge performance.

Balancing the bridge aging timer according to the size of the local LAN and the frequency of station usage and moves can assist in optimizing bridge performance. If a closely managed topology remains stable with high usage and few station additions or moves, it could be advantageous to initially let the bridge learn all station addresses and then increase or disable the aging timer. When a station deletion or move occurs, the timer value can be temporarily reduced to clear the entry from the table more quickly. In any case, learning never stops, and the new/moved station will be learned and added to the address table when encountered.

**4 - Show Bridging Table**

The Show Bridging Table option displays all addresses in the Bridge Filter Table, identifies the active/inactive and permanent/non-permanent addresses, identifies addresses to be filtered if they are a source and/or destination, describes their location, and gives the total number of address table entries.

```
                          ALL Known MAC Addresses
Total entries : 20
                              Filter If  WAN
Address            Active Perm Src  Dest Access Location
Start of table
01-80-c2-00-00-01                                Internal
01-80-c2-00-00-02                                Internal
01-80-c2-00-00-03                                Internal
01-80-c2-00-00-04                                Internal
01-80-c2-00-00-05                                Internal
01-80-c2-00-00-06                                Internal
01-80-c2-00-00-07                                Internal
01-80-c2-00-00-08                                Internal
01-80-c2-00-00-09                                Internal
01-80-c2-00-00-0a                                Internal
01-80-c2-00-00-0b                                Internal
01-80-c2-00-00-0c                                Internal
01-80-c2-00-00-0d                                Internal
01-80-c2-00-00-0e                                Internal
01-80-c2-00-00-0f                                Internal
02-44-00-c8-9a-ff     *      *                 *   LAN050607
02-44-00-c8-9a-ee     *                        *   LAN050607
12-34-56-78-99-99     *      *   *      *          LAN050607(fixed)
11-11-11-11-11-11                       *         unknown
ff-ff-ff-ff-ff-ff                                Internal
end of table
```

**Address**

The sixteen addresses **01-80-c2-00-00-01** to **01-80-c2-00-00-0f** are reserved for future use in the 802.1d standard.

The address (**ff-ff-ff-ff-ff-ff**) is a permanent address that, in its default state (unknown), will not filter any frames. Only one choice—Filter if Destination is available for this broadcast address. If applied, this will prevent broadcast frames from being put onto the LAN the bridge is connected to.

The address (**12-34-56-78-99-99**) is an active, permanent address that resides on LAN050607 (in this example, this is the LAN the bridge is attached to). Frames to and from this address will not cross the bridge, since they are identified as both filter-if-destination and filter-if-source. The "(fixed)" descriptor is added when the location of the address has been identified by management action.

The address (**11-11-11-11-11-11**) is an inactive, permanent address with a currently unknown location. Frames to this address will not cross the bridge, since they are identified as filter-if-destination. Note that this address should be made permanent, because if it is not encountered within the aging-timer interval it will be removed from the table.

The address (**02-44-00-c8-9a-ff**) is an active, permanent address that resides on LAN050607 and is allowed to transmit data on the WAN connection. This address is marked permanent because the operator enabled the permanent option within the Edit MAC Address menu of the MAC Address Filters menu.

The address (**02-44-00-c8-9a-ee**) is an active address that resides on LAN050607 and is allowed to transmit data on the WAN connection. Since this address is marked as having WAN access but not marked as permanent, this indicates that this address has been learned from the local LAN and assigned to have WAN access because it was one of the first 10 addresses encountered.

**Active**

A * in the Active column indicates the address is active. An address is considered active if it has been encountered within the aging-timer interval. Permanent addresses are not subject to the aging timer, but will be reported as active if they are encountered.

**Perm**

A * in the Perm column indicates the address is permanent. An address is considered permanent if it has been identified as such by the bridge manager. Permanent addresses are not subject to the aging timer, but will be reported as active if they are encountered.

**Filter if Src**

This indicates that a bridge/router manager has specified that frames having this source address will be filtered.

**Filter if Dest**

This indicates that a bridge/router manager has specified that frames having this destination address will be filtered.

**Filter if Src / Dest**

This indicates that a bridge/router manager has specified that frames having this source or destination address will be filtered. (This station can neither send data across the bridge/router, nor receive data from across the bridge/router.)

**WAN Access**

This indicates that the LAN device with this MAC address is allowed to pass data over the WAN connection to the remote site.

**Location**

**Internal**

These are the STP Multicast and LAN port MAC addresses that are internal to the bridge/router itself. Note that the bridge/router's MAC address is used for the default bridge/router and LAN names. Partner bridge/router's MAC addresses will also be listed as internal. Internal addresses are not subject to the aging timer, but will be reported as active if they are encountered.

**LANxxxxxx (unknown)**

These addresses are identified as to their location on a specific LAN, or as an (unknown) location. Their LAN location is identified either by manual entry or through the Learning Process when encountered.

**5 - Show Permanent Table**

The Show Permanent Table option displays all of the permanent filter-table addresses entered by the bridge/router manager for which the locations were identified (Internal addresses are not displayed.) The "(fixed)" Location descriptor indicates that a manager made the entry and specified the LAN location.

```
                          Operator Defined MAC Addresses
                                    Filter if  WAN
Address            Active Perm Src  Dest Access Location
Start of table
02-44-00-c8-9a-ff     *     *              *    LAN050607
12-34-56-78-99-99     *     *   *     *         LAN050607(fixed)
End of table
```

**6 - Clear Bridging Table**

The Clear Bridging Table option removes all non-permanent filter table addresses.

**Considerations:**

To prevent accidental removal of all non-permanent addresses, this option must be confirmed by entering "yes" at the prompt. (Refuse by entering "no" or use the TAB key to back out).

## Spanning Tree Menu

```
                              SPANNING TREE MENU

    Option                Value          Description
 1. STP state             [enabled]    - Enable/disable Spanning Tree Protocol
 2. Bridge priority       [32768]      - Define root bridge selection priority
 3. Forwarding delay      [15 sec]     - Set delay before forwarding begins
 4. Message age timer     [20 sec]     - Receive hello message interval
 5. Hello time            [2 sec]      - Set hello message transmission interval
 6. Show bridge                        - View bridge STP status
 7. Show ports                         - View STP port status



Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **SPANNING TREE MENU** allows the management and display of the 802.1D Spanning Tree Protocol (STP) parameters.

**Note:** For remote bridge/routers in a WAN, the following values set on one bridge/router will be automatically set the same on all other remote bridge/routers in the WAN. (This is because all remote bridge/routers function together as one unified bridge).

| | |
|---|---|
| STP state | Option 2 |
| Bridge Priority | Option 3 |
| Forwarding delay | Option 4 |
| Message age timer | Option 5 |
| Hello time | Option 6 |

**If these values are set differently upon start-up, the values set on the bridge/router with the lowest MAC address will prevail.**

### 1 - STP State

The STP State option toggles between the [enabled] / [disabled] states of the Spanning Tree Protocol for the bridge.

**Considerations:**

STP needs to be [enabled] only if a known or potential loop is probable in the network.

If the Spanning Tree Protocol is to be [disabled], Options 1, 3, and 5 - 8 have no relevance. Note that Option 4 (Forwarding Delay) is used as the Learning timer in a non-STP configuration.

The default state for STP is **disabled**.

**2 - Bridge Priority**

The Bridge Priority option specifies the bridge's priority for becoming the *Root Bridge*. The bridge with the lowest bridge priority is elected to be the Root Bridge.

**Default:** [32768] * (IEEE 802.1D recommendation)

**Range:** 0 to 65535

**Considerations:**

*** This value is the first part of the Bridge ID For example: 32768-0000d0111111**

If you want the bridges to decide among themselves which is to be the Root bridge, then set all bridges' bridge priorities to the IEEE 802.1D default 32768. In this instance, with all bridge priorities being the same, the bridge with the lowest MAC address will be chosen as the Root Bridge.

**Lower Value**

If you want this bridge to become the Root Bridge, then set this number to be lower than the other bridges in the network.

**Higher Value**

If you want this bridge to become blocked (become the standby bridge where a redundant path exists), then set this number higher than the other bridge(s) competing to be the *designated bridge* for a LAN.

**3 - Forwarding Delay**

During a change in topology, the Forwarding Delay value specifies the time the bridge will wait in each of the *Listening* and *Learning States* before forwarding of frames begins.

In the *Listening State,* the bridge "listens" for the other bridges' topology and configuration information. (Non-permanent addresses are aged-out and cleared from the address table before the *Learning State* is entered.)

In the *Learning State,* the bridge learns the addresses of as many stations as possible, so when entering the *Forwarding State* it avoids flooding the network with packets destined for unknown addresses.

During the Listening and Learning State intervals, forwarding is blocked although during the Learning State, learned station information is included in the address table.

**Default:** [15 sec] (IEEE 802.1D recommendation)

**Range:** 4 to 30 seconds

**Considerations:**

The Forwarding Delay time of the bridge is applicable only if the bridge is, or becomes, the Root bridge, since the Root values override a non-root's Forwarding delay time value. The Root value is known as the Network Forward(ing) Delay.

**Lower Value**

If this bridge is the Root, or becomes the Root, setting the Forwarding Delay to a lower value might cause the network to flood with packets destined for addresses not yet learned. During the *Listening State*, the Root Bridge might also miss another bridge's information about a *Topology Change* if the Forwarding Delay is set too low.

**Higher Value**
Setting the value higher will increase the time spent in each of the *Listening and Learning States* when a reconfiguration is under way. A higher value will increase the time the network is unavailable for use during reconfiguration.

**Recommendations:**
The default value of 15 seconds is recommended by the IEEE 802.1D standard as a reasonable balance of performance. If a change is deemed necessary, increasing the value in consideration with Message (Max) Age is the recommended course of action.

The following relationship to Message (Max) Age must be maintained:
**2 x (fwd_delay - 1.0) > max_age**

### 4 - Message Age Timer

The Message Age Timer option specifies the length of time stored protocol information is considered valid. If a non-root bridge hasn't received protocol confirmation from the Root within this interval, it will broadcast to the other bridges that the topology has changed, and a reconfiguration calculation will be performed.

**Default:** [20 sec] (IEEE 802.1D recommendation)

**Range:** 6 to 40 seconds

**Considerations:**

The Maximum Age of the bridged network is set by the Root Bridge. If a reconfiguration of the bridged network occurs and this bridge becomes the Root, the value set at this bridge becomes the Network's value.

**Lower Value**

A much lowered Maximum Age value may cause more frequent reconfigurations of the bridged network (even if not necessary) if configuration information is delayed. A slightly lower value may trigger a reconfiguration more quickly should a bridge fail or a management action requests a change.

**Higher Value**

A higher Maximum Age value will allow more time for confirmation of the network configuration. This could be beneficial if delays are introduced and the network is frequently "going down" for unnecessary reconfigurations.

**Recommendations:**

The default value of 20 seconds is recommended by the IEEE 802.1D standard as a reasonable balance of performance. If a change is deemed necessary, increasing the value in consideration with Forwarding Delay and Hello Time is the recommended course of action.

The following relationship to Forwarding Delay must be maintained:
**2 x (fwd_delay - 1.0) > max_age**

The following relationship to Hello Time must be maintained:
**Max Age > 2x (Hello Time + 1.0)**

**5 - Hello Time**

The Hello Time option specifies the interval between the transmission of protocol configuration information by a bridge that is, or is attempting to become, the Root. In the Spanning Tree Protocol, only one bridge can be the Root Bridge. The Root Bridge generates a Configuration message after an interval set by this timer. (The Root is saying, "Hello, I'm still here".) All other bridges in the network wait for this Configuration message within the Network Hello Time to confirm that the topology is stable. If any bridge does not receive the Configuration message within the expected time, it will send out Topology Change messages to the other bridges in order to calculate a new configuration.

**Default:** [2 sec] (IEEE 802.1D recommendation)

**Range:** 1 to 10 seconds

**Considerations:**

This value is not directly used in configuration calculations but the bridged network uses the value set at the Root Bridge. (I.e. Network Hello Time).

**Lower Value**

Reducing this value increases the frequency of Configuration messages on the network, potentially creating excessive network traffic.

**Higher Value**

A higher value results in a slower response to a change in the topology of the network (e.g. addition/deletion/failure of bridges or communications paths).

**Recommendations:**

The default value of 2 seconds is recommended by the IEEE 802.1D standard as a reasonable balance of performance. If a change is deemed necessary, increasing the value in small steps is the recommended action.

The following relationship to Max Age must be maintained:
**Max Age > 2 x (Hello Time + 1.0)**

**6 - Show Bridge**

The Show Bridge option displays the Spanning Tree Protocol status of the bridge. The display of a Root bridge is shown below:

```
Bridge Status

Spanning Tree Protocol : Enabled
Bridge ID              : 32768-0000d0010101
Topology change        : 0
Designated Root        : 32768-0000d0010101
Root path cost         : 0
Root port              : None
Network Forward delay  : 15 seconds
Network Max age        : 20 seconds
Network Hello time     : 2 seconds
Bridge Forward delay   : 15 seconds
Bridge Max age         : 20 seconds
Bridge Hello time      : 2 seconds
```

**Spanning Tree Protocol** : Enabled

Indicates whether the Spanning Tree Protocol is Enabled or Disabled.

**Bridge ID** : 32768-0000d0010101
**Designated Root** : 32768-0000d0010101

The first part of each string indicates the (default) decimal Bridge Priority (32768). Refer to Option 4.

The remaining part of the string is the MAC address of the bridge and of the Root Bridge respectively.

If the Bridge ID string is identical to the Designated Root (bridge) string, then this bridge is the Root Bridge.

The Designated Root is the bridge sending/receiving frames to/from the attached LAN towards the Root Bridge.

**Topology change** : 0

If the topology is stable, this value is 0.
If the topology is changing, this value is 1.

**Root path cost** : 0
**Root port** : None

If this bridge is the Root Bridge, the Root path cost is 0 and the Root port value is None, as shown in the above display.

If this bridge is a non-root bridge, the cost is determined by the sum of this bridge's path costs leading to the Root Bridge.

The Root port of a non-root bridge is the port closest to the Root Bridge. It sends and receives protocol messages to/from the bridge and the Root Bridge. If this bridge is not the Root Bridge, the Root Port value will be in the format 0x8001. The "0x" is an indicator that the values to follow are in hex. Following the "0x" is the hex value of the decimal Port Priority. (The default Port priority of decimal 128 yields a hex value of 80.) Following the hex value is the port number (01). Default port priority values therefore yield a Root port value of 0x8001.

**Network Forward delay : 15 seconds ***
**Network Max age : 20 seconds ***
**Network Hello time : 2 seconds ***

**Bridge Forward delay : 15 seconds ****
**Bridge Max age : 20 seconds ****
**Bridge Hello time : 2 seconds ****

* These parameters are defined by the Root bridge.

** These parameters are defined at each bridge with Options 4, 5, and 6.

If this bridge is the Root bridge, corresponding parameters will be the same. If it is not the Root Bridge, these values may differ. (It is very possible that these values can be the same if this is not the Root Bridge, since these are the values recommended by the IEEE 802.1D standard. Check and compare the Bridge ID to the Root ID for confirmation of the Root.)

**7 - Show Ports**

The Show Ports option displays the status of this bridge's STP ports.

```
Port Status Summary


                                          Designated       Designated
                                            Bridge           Port
Name             State     Id Pri  Cost    Address    Pri   Id Pri  Cost
---------------- -------- --- --- ----- ------------ ----- --- --- -----
LAN              Forward    1 128 100           Self          Self
SITE2            Forward   44 128 100   020304050607 32768  44 128     0
```

**Name**

The **Name** column shows either the name of the STP port. LAN for the local LAN, or the remote site profile alias name for a properly connected remote site device.

**State**

The **State** column indicates the current port states that may be Disabled (by management action); or either Listen(ing), Learn(ing), Forward(ing) or Block(ing) (by STP action).

**ID**

In the above display, there are two indicators of the LAN port identifying numbers. They are found under the **ID** columns. They may not fall in order, as the listing is based on the MAC address of each bridge.

**Cost**

The **Cost** columns indicate the contributing cost of each port's path to the Root Path Cost.

**Designated Bridge**

If "self" is listed, then the bridge is the designated bridge for the LAN it is attached to.

**Address**

This is the MAC address for the designated bridge attached to the specified LAN.

**Priority**

This is the port priority given to the designated bridge.

**Designated Port**

**ID**

This is the Port ID number.

**Priority**

This is the priority of the Designated Port.

**Cost**

If this is the Root Port, the priority is 0.

## IP Routing Set-Up Menu

```
                          IP ROUTING SET-UP MENU

    Option               Value          Description
 1. IP routes            menu         - Modify/view routes
 2. ARP set-up           menu         - Configure ARP operation
 3. IP routing          [enabled]     - Enable/disable IP router
 4. IP forwarding       [enabled]     - Enable/disable IP routing
 5. ARP proxy           [disabled]    - Support proxy-ARP




Enter option number, "=" - main menu, <TAB> - previous menu


>
```

The **IP ROUTING SET-UP MENU** allows the display and configuration of the IP Routing parameters for the router.

**1 - IP Routes**

The IP Routes option directs you to the IP Routes Menu, where the routing tables are displayed and changed.

**2 - ARP Set-Up**

The ARP Set-up option directs you to the ARP Set-Up Menu, where the ARP timers may be set and the ARP table may be viewed.

**3 - IP Routing**

The IP Routing option enables or disables the IP routing functions of the router.

**Default:** [enabled]

**Considerations:**

When IP Routing is disabled, all learned RIP routes will be cleared from the routing table.

**4 - IP Forwarding**

The IP Forwarding option enables or disables the forwarding of IP traffic when IP routing is enabled. When the IP forwarding option is disabled, IP traffic across the WAN links will be blocked

**Default:** [enabled]

**5 - ARP Proxy**

When this option is enabled, the P840 will respond to local network ARP requests destined for other networks. The P840 will reply to any matching route in the routing table. The P840 will also reply for a station that is supposed to be on the local LAN but is connected through a remote route in the routing table.

**Default:** [disabled]

## IP Routes Menu

```
                              IP ROUTES MENU

    Option                  Value          Description
 1. Edit route               menu        - Modify a route in the table
 2. Default gateway         [none]       - Define default gateway
 3. Show all routes                      - Display the route table
 4. Show static routes                   - Display only static routes
 5. Clear static routes                  - Remove all permanent entries









Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **IP ROUTES MENU** allows the display and configuration of the routing tables.

**1 - Edit Route**

The Edit Route option directs you to the Edit Route Menu where the routing tables are modified.

**2 - Default Gateway**

The Default Gateway option allows the identification of a default gateway (i.e. *router*). Messages destined for hosts not on this (sub-)network are forwarded to the default gateway. The default gateway may be located on the local LAN or may be one of the remote site peer IP routers.

**Note:** If using raw 1490 Frame Relay, either enable "Auto Default Route" or configure the Default Gateway remote site peer address to access the Default Gateway.

If PPP is used and the IP address of the remote site peer IP router is not known, the default gateway may be defined as the remote site ID. This will cause the default gateway to become whatever device is currently connected at that remote site.

When an SNMP message is to be sent to an NMS, first the routing table is checked for a known route. If a route to the NMS is unknown, the SNMP message will then be sent to the default gateway. If the default gateway cannot provide the best route, it will send the message to the gateway that can provide the best route. After the default gateway sends the message to the other gateway for delivery, the default gateway will send an ICMP Redirect message back to the router that points to the best route gateway. In this manner, the router is informed of the best route for future SNMP message delivery.

A configured Default Gateway will override a default route learned from RIP. If there is more than one default gateway defined within the routing table, the default gateway with the lowest cost will be used and displayed in this option.

**Default:** [none]

```
Enter :
    none, gateway IP address, remote site ID or alias (up to 18 characters)
>
```

**3 - Show All Routes**

The Show All Routes option displays all of the routes currently in use by the router. The table is sorted by destination IP address. The default gateway, either learned or defined, will be displayed as "default route."

There is a maximum of 512 route entries allowed in the table.

```
                              All IP Routes
Total entries : 0 R: al 0, fr 512, tot 512  N: al 0, fr 1024, tot 1024

 Destination      Mask    Next Hop        Interface                    Route
 IP Address       Size   IP Address     Up / Identifier  Cost  Age    Type
---------------  ---- ---------------  ---------------  ----  ----   ------
 --Start of table--
 5.5.5.0           24  5.5.5.1          * LAN.1            1     0    DIRECT
 5.5.5.1           32  5.5.5.1          * LAN.1            1     0    DIRECT
 192.168.12.0      24  192.168.12.1     * LAN              1     0    DIRECT
 192.168.12.1      32  192.168.12.1     * INTERNAL         1     0    DIRECT
 192.168.15.1      32  192.168.15.1     * RS2              2     0    CONNECT
 192.168.84.0      24  192.168.84.1       RS4              2     0    CONNECT
 192.168.84.1      32  192.168.84.1       RS4              2     0    CONNECT
 198.169.1.150     32  198.169.1.150      RS5              2     0    CONNECT
--End of table--
```

| | |
|---|---|
| Destination IP Address: | Network IP address of the remote network. Routes listed with a "+" indicate that these are secondary routes to the same destination network. If the main route goes away, the secondary route will be used. |
| Mask Size: | Subnet mask size defined for the route. |
| Next Hop IP Address: | IP address of the next hop router to use to reach the Destination IP Address. |
| Interface Up | An asterisk will be displayed if this route is up. |
| Interface Identifier | RS followed by a number indicates the Remote site profile ID number that this route is currently using. LAN indicates that this route is on the local LAN. A decimal point and number following the LAN indicates that this is a secondary network. INTERNAL indicates that this is the IP address of a port on this device |
| Cost: | Number of hops to reach the Destination IP Address. |
| Age: | Actual cost to reach the Destination IP Address. Triggered RIP routes will be indicated as RIP routes with a constant age of 0. |
| Route Type: | Type of route used: RIP, LOCAL, CONNECT, DIRECT, or OTHER.<br>LOCAL is used for static routes.<br>CONNECT indicates the route is on a connected peer IP router on an unnumbered link.<br><br>DIRECT indicates that the route is directly connected to one of the interfaces. This could also indicate the peer IP router of a numbered link. |

**4 - Show Static Routes**

The Show Static Routes option displays all of the static routes currently in use by the router.

```
                        Static IP Routes
 Destination      Mask    Next Hop        Interface                    Route
 IP Address       Size   IP Address     Up / Identifier  Cost  Age     Type
---------------  ---- ---------------  ---------------  ----  ----   ------
 --Start of table--
 5.5.5.0           24  5.5.5.1          * LAN.1            1     0    DIRECT
 5.5.5.1           32  5.5.5.1          * LAN.1            1     0    DIRECT
 192.168.12.0      24  192.168.12.1     * LAN              1     0    DIRECT
 192.168.12.1      32  192.168.12.1     * INTERNAL         1     0    DIRECT
 192.168.15.1      32  192.168.15.1     * RS2              2     0    CONNECT
 192.168.84.0      24  192.168.84.1     * RS4              2     0    CONNECT
 192.168.84.1      32  192.168.84.1     * RS4              2     0    CONNECT
 198.169.1.150     32  198.169.1.150    * RS5              2     0    CONNECT
--End of table--
```

**5 - Clear Static Routes**

The Clear Static Routes option clears all of the static routes from the routing table.

**Note:** any Default Gateway static routes that were automatically created will be deleted by this operation. A warning will be displayed if there was a default gateway defined in the static routing table.

## Edit Route Menu

```
                              EDIT ROUTE MENU

    Option           Value           Description
 1. Destination    "none" [0]     - Destination IP address
 2. Next hop       "none"         - Next hop address
 3. Network mask  *"none"         - The network mask for the route
 4. Status        *[undefined]    - Is the address in the table




Enter:
    destination IP address (up to 15 characters)


> 192.3.44.0
```

The above display is the first level of the **EDIT ROUTE MENU**. The destination network IP address must be entered as well as the subnet mask size associated with the destination IP address. Once the destination network IP address and mask size have been entered, the next hop IP address or remote site ID/alias must be entered.

The menu title will change to indicate the destination IP network address and the subnet size that are being edited.

```
                              EDIT ROUTE MENU

     Option          Value                    Description
 1. Destination    "199.45.67.00" [26]    - Destination IP address
 2. Next hop       "198.65.43.21"         - Next hop address
 3. Type          *"LOCAL"                - Type of route
 4. Cost           [1]                    - Cost to reach destination in hops
 5. Private        [disabled]             - Do not advertise route
 6. Add/Remove                            - Add/Remove information in table
 7. Network mask  *"255.255.255.192"      - The network mask for the route
 8. Status        *[absent]               - Is the address in the table



Enter option number, "=" - main menu, <TAB> - previous menu



>
```

**NOTE**: A Static Route will **NOT** be replaced with a RIP route, even if the cost is lower.

**1 - Destination**

The destination IP address to be entered into the static routes table. The IP address is entered as four decimal numbers between 1 and 255, separated by decimal points. After the IP address is entered, the mask size will be requested; enter a number between 1 and 32 to indicate the number of bits to be used for the subnet mask. A mask size of 32 will specify the exact destination address entered.

**2 - Next Hop**

The Next Hop option defines the IP address or remote site profile ID or alias of the next-hop router to be used to reach the destination IP address.

**3 - Type**

The Type option displays the type of route. The route type may be either RIP or LOCAL. RIP is a learned route from the RIP updates on the network. LOCAL is a static route entered by the operator of the router.

**4 - Cost**

The Cost option defines the number of hops required to reach the destination IP address.

**Default:** [1]

**Range:** 1 - 15

**5 - Private**

The Private option when set to enabled causes the P840 to not advertise this route in the RIP messages.

**Default:** [disabled]

**6 – Add/Remove**

This option toggles between Add and Remove depending on whether the entry is present in the route table or not.
The Add option adds the IP address to the routing table.
The Remove option removes the IP address from the routing table. If the route is a RIP route, the route may be re-learned by the next RIP route update from partner routers.

**7 - Network Mask**

The subnet mask for the destination IP network is calculated from the entered destination IP network address and the subnet size value. The resulting subnet mask is displayed here. This is a display only value.

**8 - Status**

The Status option tells whether the address is "Present" or "Not Present" in the Routing Table. When the address is first entered, "Added" is the Status value. The * beside the value indicates that this value is changed automatically as an address is added or deleted and cannot be manually redefined.

**Default:** * [Not Present]

## ARP Set-Up Menu

```
                              ARP SET-UP MENU

    Option              Value          Description
 1. ARP aging timer    [2 min]       - Interval to remove entries
 2. ARP retry timer    [2 sec]       - Interval to retry ARP
 3. Add ARP entry                    - Add static ARP entry
 4. Remove ARP entry                 - Delete static ARP entry
 5. Show ARP table                   - View ARP table









Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **ARP SET-UP MENU** contains options used to view and maintain the ARP table for this device.

**1 - ARP Aging Timer**

The ARP Aging Timer option sets the ARP (Address Resolution Protocol) aging timer. Upon the expiration of the ARP aging timer, unused entries are removed from the ARP cache.

**Default:** [2 min]

**Range:** 1 to 1440 minutes (1 day)

**2 - ARP Retry Timer**

The ARP Retry Timer option sets the time-out value after which an ARP message will be resent.

**Default:** [2 sec]

**Range:** 1 - 20 seconds

**3 – Add ARP Entry**

The Add ARP Entry option allows the manual entry of static addresses into the ARP table. When this option is selected, you are requested to enter the IP address, then to enter the MAC address of the node to be added.

**4 – Remove ARP Entry**

The Remove ARP Entry option allows removal of node addresses from the ARP table. Entries may be removed individually by entering the IP address of the node to be removed. Groups of addresses may also be removed: all static addresses may be taken out by entering "static", all dynamically assigned addresses by entering "dynamic" or the entire table may be cleared by entering "all".

**5 - Show ARP Table**

The Show ARP Table option displays all of the devices that have responded to ARP requests from this router and the devices that this router has responded to with an ARP reply. IP address information learned (possibly via RIP) will also be added to the table to eliminate the need for generating an ARP request when data needs to be sent to that address in the future.

```
                          Arp Table

 Interface      IP Address            MAC Address        Type
 ------------------------------------------------------------
 LAN            164.44.25.142         00-00-d0-00-23-24  dynamic
 LAN            164.44.25.98          00-00-d0-00-24-24  dynamic
 LAN            164.44.25.37          00-00-d0-00-25-24  dynamic
 LAN            164.44.25.13          00-00-d0-00-26-24  dynamic
 LAN            164.44.25.33          00-00-d0-00-27-24  dynamic
 Link 1         164.44.26.53          00-00-d0-00-28-24  dynamic
 Link 2         164.44.27.76          00-00-d0-00-23-25  dynamic

Type: [s]tart, [n]ext, [=] main menu, any other key to end.
```

| | |
|---|---|
| Interface: | Interface on which the ARP mapping applies. |
| IP Address: | IP address of the device in the ARP table. |
| MAC Address: | MAC address of the device in the ARP table. |
| Type: | Type of entry in the table, either dynamic (learned via ARP requests) or static (configured via SNMP or console). |

## IP Security Set-Up Menu

```
                          IP SECURITY SET-UP MENU

    Option              Value          Description
 1. IP security       [enabled]     - Enable/disable IP security
 2. Generate RSA keys menu          - Generate local RSA key pair
 3. IKE peer set-up   menu          - Define IKE peers
 4. Protection set-up menu          - Define protection suites
 5. Policy set-up     menu          - Define IPsec policy
 6. Interfaces        menu          - Define IPsec interfaces
 7. Statistics        menu          - IPsec statistics
 8. Diagnostics       menu          - IPsec diagnostic tools

Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **IP SECURITY SET-UP MENU** allows IPSec to be enabled or disabled and provides menus for setting IPSec policies, for defining where the IPSec interface is to be, for IPSec statistics and to set up and send IPSec diagnostic packets.

**1 – IP Security**

The IP Security option toggles the IPSec protocol suite of IP extensions that provide network security through a suite of cryptography methods.

**Default:** [enabled]

**2 – Generate RSA keys**

The Generate RSA Keys menu allows you to generate local RSA key pairs.

**3 – IKE peer Set-up**

The IKE peer Set-up menu allows you to define IKE peers

**4 – Protection Set-up**

The protection Set-up menu allows you to define protection suites.

**5 – Policy Set-up**

The Policy set-up option takes you to the IP Policy Set-up Menu where IPSec policy items may be reviewed and edited.

**6 – Interfaces**

The Interfaces option takes you to the Interfaces Menu where the interface at which IPSec is to operate is set.

**7 – Statistics**

The Statistics option takes you to the IPSec Statistics Menu where IPSec policy and item stats be reviewed.

**8 – Diagnostics**

The Diagnostics option takes you to the IPSec Diagnostics Menu where an IPSec test packet may be set up and tested against the policy table to see which item (if any) matches the test packet.

## Generate RSA Keys menu

```
                          GENERATE RSA KEYS MENU

    Option                  Value         Description
 1. Generate RSA Keys       [512]     - Generate local RSA key pair
 2. Show RSA public key               - Display local RSA public pair

Enter option number, "=" - main menu, <TAB> - previous menu

>
```

**1 - Generate RSA keys**

The Generate RSA keys option allows you to generate local RSA keys. You need to generate RSA keys (private key and public key) first if you intend to use RSA encrypted nonces as authentication method. You also need to select a key size.
A key size must be provided to generate RSA keys. The key size supported is a 512 bit key. The longer the key the more secure however the CPU time to generate these keys significantly increase with key size.

**Range :** 360 to 512

**2 - Show RSA public key**

The Show RSA public key option display the router's own RSA public key and the key size.

```
Local RSA public key:

305c300d 06092a86 4886f70d 01010105 00034b00 30480241 00c6b443 dc3a83f8
3ea046a5 60f314e2 d95e699f 9ad22c2c 047d9fd6 f045027e 9f9014d7 5a203b05
68d5e9a1 e858aec2 8b65ae93 a5baab91 501d87e2 625ae4ef 79020301 0001


Enter option number, "=" - main menu, <TAB> - previous menu

>
```

## IKE Peer Setup Menu

```
                          IKE PEER SET-UP MENU

    Option                  Value         Description
 1. Edit IKE peer           menu        - Modify/create peer entry
 2. Show IKE peer summary               - Show summary of IKE peers
 3. Show auth summary                   - Show summary of authentications
 4. Remove IKE SA                       - Delete IKE SA
 5. Remove peer                         - Delete IKE peer


Enter option number, "=" - main menu, <TAB> - previous menu

>
```

**1 - Edit IKE Peer**

The Edit IKE Peer menu allows you to define IKE peers.

**2 - Show IKE Peer Summary**

The Show IKE Peer Summary option lists all the IKE peers defined.

**3 - Show Auth Summary**

The Show Auth Summary option shows the authentication method and keys for each peer.

**4 - Remove IKE SA**

The Remove IKE SA option allows you to deletes IKE SA.

**Options:** all, id or alias to delete

**5 - Remove Peer**

The Remove IKE SA option allows you to deletes IKE peers.

**Options:** all, id or alias to delete

## Edit IKE peer menu

```
                          EDIT IKE PEER MENU

    Option                  Value        Description
 1. Peer alias             [      ]    - Peer alias
 2. Peer IP address        [      ]    - Define peer IP address
 3. Peer pre shared key     menu        - Define peer pre-shared key
 4. Peer public key         menu        - Define peer RSA public key
 5. IKE phase1 negotiation menu         - Define IKE phase1 proposals



Enter option number, "=" - main menu, <TAB> - previous menu

>
```

**1 - Peer alias**

The Peer alias option shows the current alias for this IKE peer and allows you to change it if desired.The alias may be up to 16 alpha-numeric characters long, no spaces, use underscore.

**2 - Peer IP address**

The Peer IP address option defines the address of remote end of this IKE SA connection. This address will be checked on each incoming IKE packets.

**Default:** [none]
**Options:** none, IP address

**3 - Peer pre shared key:**

The Peer pre shared key option defines a pre-shared authentication key.
You must configure this key if you specify pre-shared key as the authentication method for this IKE peer.
This key may be any combination of 6 to 128 alpha-numeric characters. It is used to authenticate remote peer and must be identical at both sites.

**Default:** [none]
**Option:** none, define pre-shared key (6 to 128 characters)

**4 - Peer public key:**

The Peer public key option specifies the RSA public key generated from remote peer.It should be a string of hex charectors. You must configure this key if you choose RSA encrypted nonces as the authentication method for this IKE peer. You need to divide the RSA public key into multiple lines with up to 64 charectors each line and enter the key manually.

**Default:** [none]
**Option:** none, define RSA public key

## IKE phase1 negotiation menu

```
                EDIT PEER 1 IKE PHASE1 NEGOTIATION MENU

    Option                  Value        Description
 1. Authentication method  [      ]    - Define authentication method
 2. Integrity algorithm    [      ]    - Define integrity algorithm
 3. Encryption algorithm   [      ]    - Define encryption algoritm
 4. DH group               [      ]    - Define DH group
 5. Lifetime (seconds)     [      ]    - Define lifetime
 6. Proposal               [      ]    - Define proposal state

Enter:
     Proposal id (from 1 to 3)
>
```

**1 - Authentication method:**

The Authentication method option defines the method used to authenticate the remote peer in IKE phase 1 negotiation. There are two method currently supported, Pre-shared key and RSA encrypted nonces.You have to configure the key for the method which you have selected.

**Default:** [Pre-shared]
**Option:** Pre-shared, RSA-encr

**2 - Integrity algorithm:**

The Integrity algorithm option defines the authentication algorithm used to protect IKE negotiation. It has two options: HMAC-MD5 and HMAC-SHA1. HMAC-MD5 has a smaller digest and is considered to be slightly faster then HMAC-SHA1.

**Default:** [HMAC-MD5]
**Option:** HMAC-MD5, HMAC-SHA1

**3 - Encryption algorithm:**

The Encryption algorithm option defines the algorithm used to encrypte and decrypte IKE data. It has two options: DES and 3DES. 3DES is securer, but require mach more CPU time to execute.

**Default:** [DES]
**Option:** DES, 3DES

**4 - DH group:**

The DH group option specifies Diffie-Hellman groups used for key exchange in IKE phase 1. It has two options group1(768-bit MODP) and group2(1024-bit MODP). Group2 is harder to crack, but require mach more CPU time to execute.

**Default:** [group1]
**Option:** group1, group2

**5 - Lifetime (seconds):**

The Lifetime (seconds) option specifies the lifetime for IKE security association.

**Default:** [none]
**Option:** none, time in seconds
**Range:** 86400 or lower

**6 - Proposal:**

The Proposal Option shows the state for the current proposal and allows you to change it if desired. Only active proposals will be used.

**Default:** [Inactive]
**Option:** Inactive, Active

## Protection Suite Setup menu

```
                PROTECTION SET-UP MENU

   Option                  Value        Description
 1. Edit protection suite   menu       - Modify/create protection entry
 2. Show summary                       - Display all protection suites
 3. Remove protection suite            - Remove protection suite

Enter option number, "=" - main menu, ,TAB> - previous menu:
>
```

**1 - Edit Protection Suite**

The Edit Protection Suite menu allows you to define protection suites, used to configure IPsec security associations.

**2 - Show Summary**

The Show Summary option lists all the protection suites defined.

**3 - Remove Protection Suite**

The Remove Protection Suite option allows you to deletes protection suites.

**Options:** all, id or alias to delete

## Edit protection suite menu

```
                        EDIT PROTECTION SUITE MENU

    Option           Value         Description
 1. Suite alias     [       ]    - Define proetction suite name
 2. SA mode         [       ]    - Define IPSEC SA mode
 3. Lifetime        [       ]    - Lifetime for SA (seconds)
 4. Lifetime data   [       ]    - Lifetime for SA (Kbytes)
 5. Transform-1     [       ]    - Encryption/Authentication
 6. Transform-2     [       ]    - Encryption/Authentication
 7. Transform-3     [       ]    - Encryption/Authentication

Enter:
     Protection id or alias (1 to 16 characters)
>
```

**1 - Suite alias:**

The Suite alias option shows the current alias for this protection suite and allows you to change it if desired. The alias may be up to 16 alpha-numeric characters long, no spaces, use underscore.

**2 - SA mode:**

The SA mode option defines whether the IPsec Security Association is to operate in tunnel or transport mode. For details see manual IPsec.

**Default:** [tunnel]
**Option:** tunnel, transport

**3 - Lifetime:**

The Lifetime option specifies the lifetime in seconds for IPsec security association.

**Default:** [none]
**Option:** none, time in seconds
**Range:** 3600s - 86400s

**4 - Lifetime data:**

The Lifetime data option specifies the lifetime in kilobytes for IPsec security association.

**Default:** [none]
**Option:** none, Data lifetime in kilobytes
**Range:** 4608000 - 110592000

**5 - Transform-x:**

The Transform-1 option defines the transform with highst priority for current protection suite. Each protection suite can have up to 3 transforms. Each tranform defines the encryption and authentication algorithms used for IPsec SA. The transforms are disabled at default. You can enabled it by choosing an encryption algorithm.

**Default:** [disabled]
**Option:** disabled, DES, 3DES, null

## Policy Set-Up Menu

```
                          POLICY SET-UP MENU

    Option                Value              Description
 1. Edit item             menu             - Modify/create policy item
 2. Show item                              - Display policy item
 3. Show summary                           - Display policy item summary
 4. Show active items                      - Display active item summary
 5. Show SA summary                        - Display SA summary
 6. Remove item                            - Remove policy item
 7. Local IP address     [none]            - Define local IP address
 8. Default action       [bypass-IPsec]    - Define default frame processing




Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **POLICY SET-UP MENU** displays IPSec policy items, lets you set up policy items, defines a local IP address and sets the action to be taken with packets that fail to match an IPSec policy item.

An IPSec Policy consists of the table of items that define IPSec processing for any packet that passes through the IPSec interface(s).

A policy item consists of the set of rules that packets will be tested against, the Security Association that defines the connection parameters between the two end points of the link, and the processing actions that are performed on the packets.

A Security Association defines a dedicated secure virtual connection between two nodes. The nodes are typically IPSec enabled routers (also known as security gateways) with a LAN as one connection and an unsecure network (such as the Internet) on another. The SA is identified by of the IP Address of the destination, identification codes for the SA, and the protocol to be used (always Encapsulating Security Payload protocol for this software release). Included within th SA are the algorithms used for authentication and encryption of the packets, and the keys for encodeing and decoding packets with those algorithms.

An SA is defined from an originating node to a destination node; it is, therefor a one way connection. To allow secure two way traffic across the unsecured network, two corresponding SAs will be defined on the peer routers that will be mirror images of each other, that is, all outbound parameters on one node will be set as inbound parameters on the peer and vice versa.

An essential part of the security provided by IPSec is the encapsulating of the original packet for transmission across the unsecured portion of the network. Both the data and header information, including original source and destination address, protocol, and packet size, are encrypted and wrapped in a packet with only the addresses of the end points on the unsecured network and the SA idendifier code visible during transmission across the SA. What this provides in effect is a secure tunnel between the two nodes through the unsecured network.

With this software release, only one IPSec policy may be set; Policy and Security Association (SA) parameters such as encryption and authentication keys must be set manually. An IPSec policy is made up of one or more (up to a maximum of 32) items.

### 1 – Edit Item

The Edit Item option takes you to the Edit Item Menu where IPSec Policy Items may be configured.

**2 – Show Item**

```
                        Policy Item 1 - [ IPSec_1 ]

Policy Item Parameters
Status:                    Active            Priority:              10
Action:               Apply-IPsec          SA Creation:          Manual

Manual SA Parameters
Local IP Addr:      198.169.1.109         Peer IP Addr:     192.168.2.1
SA Mode:                  Tunnel            Protocol:             ESP
Authentication:         HMAC-MD5          Encryption:             DES
Outbound SPI:         0xffffffff          Inbound SPI:      0x11111111

Selection Rules
Source IP:          198.169.1.109 / 255.255.255.0
Destination IP:       192.168.2.1 - 192.168.2.3
Protocol:                    ANY
Source Port:                 ANY
Destination Port:            ANY
```

The Show Item option displays a detailed listing of the settings for the requested item:

**Policy Item Parameters**

**Status:** policy item is active, inactive or modified

**Action:** processing that will be applied to packets that match this policy item: apply-IPsec, bypass-IPsec, discard

**Priority:** indicates the priority of this item in the policy list. Items are checked from lowest to highest priority

**SA Creation:** IKE, Manual

**Manual SA Parameters**

**Local IP Addr:** IP address for the local end of IPSec Security Association (SA(s))

**SA Mode:** tunnel or transport

**Authentication:** MD5 or none

**Outbound SPI:** 32 bit (8 hex character) Security Parameter Index transmitted with the outbound packet as part of the identification of the outbound IPSec SA

**Peer IP Addr:** IP address for the remote end of IPSec SA(s)

**Protocol:** always ESP

**Encryption:** DES, 3-DES (if option enabled) or null

**Inbound SPI:** 32 bit (8 hex character) Security Parameter Index that is used to identify the IPSec SA for an inbound packet.

**Selection Rules**

**Source IP:** the source address against which packets will be tested for this item. The address may appear as:.

A single address listing indicates that the source must be this specific IP address

Two addresses seperated by a dash indicates that the source may be within a range of IP addresses; any address that falls on or between the addresses shown will match the rule.

An address followed by a slash and a number indicates that the destination may be on a subnet as specified by the address and the mask size shown. Any address on the subnet will match the rule.

**Destination IP:** the destination address against which packets will be tested for this item. The address may appear as:

A single address listing indicates that the destination must be this specific IP address

Two addresses seperated by a dash indicates that the destination may be within a range of IP addresses; any address that falls on or between the addresses shown will match the rule.

An address followed by a slash and a number indicates that the destination may be on a subnet as specified by the address and the mask size shown. Any address on the subnet will match the rule.

**Protocol:** Protocol number to compare against the protocol of a packet (any or a protocol number between 1 and 255)

**Source Port:** any port or a specific port number (between 1 and 65535)

**Destination Port:** any port or a specific port number (between 1 and 65535)

**3 – Show Summary**

```
                                                Total Entries: 1

[*] - Entry has been modified
Id Alias            Pri Action  Active  Mode  Peer            Prot Encr Auth
-- ---------------- --- ------- ------ ------ --------------- ---- ---- ----
 1 IPSec_1           10 IPsec   Yes    Tunnel 192.168.2.1      ESP DES  MD5









Type: [s] to redraw, [=] main menu, any other key to end.
```

The Show Summary option lists all the items in the policy table in order if their ID numbers, with the following parameters for each item:

**Id:** the identification number assigned to this item

**Alias:** the user defined name assigned to this item

**Pri:** the priority level of this item, packet matching is done from lowest to highest priority

**Action:** processing that will be applied to packets that match this policy item: apply-IPsec, bypass-IPsec, discard

**Active:** yes if this policy item is active, no if the item has been modified but not activated

**Mode:** tunnel or transport

**Peer:** IP address of the remote end of the IPSec SA(s)

**Prot:** Protocol used with this item – always ESP

**Encr:** type of encryption – DES, 3-DES (if option enabled), or null

**Auth:** authentication mode – MD5 or none

**4 – Show Active Items**

```
 Device: DEV050607                                Total Entries: 0

[*] - Entry has been modified
Pri Id Alias            Action  Active  Mode  Peer            Prot Encr Auth
--- -- ---------------- ------- ------ ------ --------------- ---- ---- ----
 10  1 IPSec_1          IPsec   Yes    Tunnel 192.168.2.1      ESP DES  MD5




Type: [s] to redraw, [=] main menu, any other key to end.
```

Active Items are shown in order of priority, lowest to highest, with the following parameters for each item:

**Pri:** the priority level of this item, packet matching is done from lowest to highest priority

**Id:** the identification number assigned to this item

**Alias:** the user defined name assigned to this item

**Action:** processing that will be applied to packets that match this policy item: apply-IPsec, bypass-IPsec, discard

**Active:** will always be yes as this is the active policy items display

**Mode:** tunnel or transport

**Peer:** IP address of the remote end of the IPSec SA(s)

**Prot:** Protocol used with this item – always ESP

**Encr:** type of encryption – DES, 3-DES (if option enabled), or null

**Auth:** authentication mode – MD5 or none

**5 – Show SA Summary**

```
SA Id Dir Source Address  Dest Address    SPI(hex) Mode   Prot Encr Auth
----- --- --------------- --------------- -------- ------ ---- ---- -----
    7 OUT 198.169.1.109   192.168.2.1     ffffffff Tunnel ESP  DES  HMAC_MD5
    8 IN  192.168.2.1     198.169.1.109   11111111 Tunnel ESP  DES  HMAC_MD5

    9 OUT 201.19.53.121   188.54.2.18     fafafafa Tunnel ESP  DES  HMAC_MD5
   10 IN  188.54.2.18     201.19.53.121   12345678 Tunnel ESP  DES  HMAC_MD5




Type: [s] to redraw, [=] main menu, any other key to end.
```

The Show SA Summary option displays a listing of current Security Associations, each related SA pair is shown grouped together.

**SA Id:** an arbitrary identification number assigned to this security association

**Dir:** the direction of the SA – inbound or outbound

**Source Address:** the IP address of the originating SA connection

**Dest Address:** the IP address of the receiving SA connection

**SPI:** Security parameter index – the 32 bit (8 hex characters) number assigned when this SA was created; used by each router to identify this SA.

**Mode:** tunnel or transport

**Prot:** Protocol used with this item – always ESP

**Encr:** type of encryption – DES, 3-DES (if option enabled) or null

**Auth:** authentication mode – MD5 or none

**6 – Remove Item**

The Remove Item option deletes and item from the policy table.

**7 – Local IP Address**

The Local IP Address to be used for Security Association negotiations. This must be a public address of this device known to the local network. This address should not be dynamically assigned.

**Default:** [none]

**Options:** none, LAN, IP address

**8 – Default Action**

The Default Action option defines the processing that will be applied to packets, which fail to match any of the items in the policy table.

Note: bypass-IPSec is intended for set-up purposes only as it allows packets from any source to any destination across the interface. This is useful for remote configuration of the router but is insecure and should be changed to discard for normal operation.

**Default:** [bypass-IPsec]

**Options:** apply-IPSec, bypass-IPSec, discard

## Edit Item Menu

```
                          EDIT POLICY 1 ITEM 1 MENU

    Option              Value             Description
 1. Name               "IPSec_1"        - Define item name
 2. Status            *[inactive]       - Item status
 3. Activate                            - Activate this item
 4. Priority           [10]             - Define item priority
 5. Action             [apply-IPsec]    - Define IPsec frame processing
 6. SA creation        [IKE]            - Define SA creation method
 7. IKE ESP SA          menu            - Define IKE ESP SA
 8. Manual ESP SA       menu            - Define manual ESP SA
 9. Selection rules     menu            - Define selection rules




Enter option number, "=" - main menu, <TAB> - previous menu


>
```

The **EDIT ITEM MENU** will appear as above until the ID number or alias for the policy item is entered. If the policy item is being created, enter an alias name for the item (up to 16 alphanumeric characters, no spaces); the next sequential ID number will be automatically assigned. Once the identity of the item has been established, the will change to reflect the characteristics of that item, as shown on the following page.

## Edit Policy 1 Item x Menu

```
                          EDIT POLICY 1 ITEM 1 MENU

    Option              Value             Description
 1. Name               "IPSec_1"        - Define item name
 2. Status            *[inactive]       - Item status
 3. Activate                            - Activate this item
 4. Priority           [10]             - Define item priority
 5. Action             [apply-IPsec]    - Define IPsec frame processing
 6. SA creation        [IKE]            - Define SA creation method
 7. IKE ESP SA          menu            - Define IKE ESP SA
 8. Manual ESP SA       menu            - Define manual ESP SA
 9. Selection rules     menu            - Define selection rules




Enter option number, "=" - main menu, <TAB> - previous menu


>
```

The **EDIT POLICY 1 ITEM x MENU** defines the parameters of a policy item. A policy may have up to 32 items.

A policy item consists of the set of rules that packets will be tested against, the Security Association that defines the connection parameters between the two end points of the link, and the processing actions that are performed on the packets. Packet matching tests are performed in the order of priority of the items in the policy table, lowest to highest.

When a policy item is configured, the reference direction will be OUTBOUND from this interface; parameters for both outbound and inbound Security Associations are to be set according to this reference. Remember that for two-way communication, the peer router (security gateway) must be set up with a coresponding policy item that mirrors the parameters of this item.

**1 – Name**

The Name option shows the current alias for this policy item and allows you to change it if desired. The alias may be up to 16 alpha-numeric characters long, no spaces, use underscore.

**2 – Status**

The Status option shows whether this item is active or inactive. Only active policy items are used in IPSec processing. An item is initially inactive when it is created. When an item has been modified, the status field will change to reflect this, but the item will remain active with the original settings until the modification is updated with option 4 below.

**3 – Activate/Dectivate**

The Activate option enables an inactive policy item; Deactivate disables an active item.

**4 – Update**

Update enables a modified policy item. When an item is modified, the changes made by editing have no effect until the item is updated.

Note: this option appears only when the item has been modified and not yet updated.

**4/5 – Priority**

The Prority option sets where this item test will occur compared to other items in the policy table. Packets are processed and applied against Active Policy Items in order of item priority from lowest to highest priority.

When an item is created, it is automatically assigned a priority of 10 more than the current largest priority. This number may be changed to put the item in the desired order of processing. Leaving a gap between item priority numbers allows room for insertion of future items into a desired spot in list.

**Default:** [10 + current highest priority ]

**Range:** 1 - 999

**5/6 – Action**

The Action option defines the processing that will be applied to packets matching this policy item.

**Default:** [apply-IPSec]

**Options:** apply-IPSec, bypass-IPSec, discard

**6/7 – SA Creation**

The SA creation option specifies how this security association will be created. It has two options: manaul and IKE.

**Default:** manual
**Options:** manual, IKE

**7/8 – IKE ESP SA**

The IKE ESP SA menu defines the parameters used for establishing IPsec security association through IKE negotiation.

**8/9 – Manual ESP SA**

The Manual ESP SA option takes you to the Manual ESP SA menu where Encapsulating Security Payload Security Association parameters may be set.

**9/10 – Selection Rules**

The Selection Rules option takes you to the Selection Rules menu where the source and destination packet selection rules for this policy item may be set.

## IKE ESP SA Menu

```
                    EDIT POLICY 1 ITEM 1 IKE ESP SA MENU

    Option              Value              Description
 1. Peer IP address    "172.16.43.200"   - Define item name
 2. IKE phase2 PFS      [none]           - Define PFS for IKE phase2
 3. Ipsec SA proposals   menu            - Define Ipsec protection suites



Enter:
     None, group1, group2

>
```

**1 - Peer IP address**

The Peer IP address option defines the address of remote end of this IPsec SA connection. It should match the IP address in the IKE peer menu.

**Default:** [none]
**Options:** none, IP address

**2 - IKE phase2 PFS**

The IKE phase2 PFS option defines a optional IKE feature to provide perfect forwared secrecy(PFS). PFS adds another level of security because every time a new security association is negotiated, a new Diffie-Hellman exchange occurs (This exchange requires additional processing time). It has two options: group1(768-bit MODP) and group2(1024-bit MODP). Group2 is harder to crack, but require mach more CPU time to execute.

**Default:** [none]
**Option:** none, group1, group2

**3 - IPsec SA proposals**

The protection suite option shows the name of the protection suite used to establish IPsec security association. Before you enter the name for the protection suite, you must first define it in protection suite menu

**Default:** [none]
**Option:** none, name of the protection suite

## Edit Policy 1 Item x Manual ESP SA Menu

```
                EDIT POLICY 1 ITEM 1 MANUAL ESP SA MENU

   Option              Value          Description
 1. Peer IP address    [none]       - Define peer IP address
 2. SA mode            [tunnel]     - Define IPsec SA mode
 3. Authentication     [none]       - Define ESP athentication
 4. Encryption         [DES]        - Define ESP encryption
 5. Outbound SPI       [0]          - Define outbound SPI
 6. Inbound SPI        [0]          - Define inbound SPI
 7. Keys                menu        - Define manual ESP keys



Enter option number, "=" - main menu, <TAB> - previous menu


>
```

The **EDIT POLICY 1 ITEM x MANUAL ESP MENU** allows you to manually set the Encapsulating Security Payload Security Association parameters for this policy item. The SA of a policy item is identified by

**1 – Peer IP Address**

The Peer IP Address option defines the address of remote end of this SA connection. This address will be checked on incoming packets, along with the Inbound SPI and the portocol of the packet.

**Default:** [none]

**Options:** none, IP address

**2 – SA Mode**

The SA mode option defines whether the IPSec Security Association is to operate in tunnel or transport mode. In tunnel mode, the originating and destination IP addresses are encapsulated in the packet transmitted over the network, only the addresses of the gateways at either end of the connection are not encrypted. This option should be set to tunnel mode for regular IPSec communication over the network. In transport mode, the data packet is encrypted, but the origin and destination addresses will be those of the security gateway routers. Transport mode is intended to bu used for router management communication, such as setting IPSec parameters.

**Default:** [tunnel]

**Options:** tunnel, transport

**3 – Authentication**

The Authentication option defines whether or not this policy item is to use HMAC MD5 authentication. The "none" option is available only if encryption (option 4) has been set to a value other than "null"; ie. you can't turn off both authentication and encryption at the same time.

**Default:** [MD5]

**Options:** none, MD5

**4 – Encryption**

The Encryption option defines the type of encryption, if any, to be used for this policy item. 3-DES encryption is available as an upgrade option, please see page 27 for upgrade information. The "null" option is available only if authentication (option 3) has been set to a value other than "none"; ie. you can't turn off both authentication and encryption at the same time.

**Default:** [DES]

**Options:** DES, 3-DES (if option enabled), null

**5 – Outbound SPI**

The Outbound SPI option defines the 8 hexadecimal character (32 bit) Security Parameter Index to be sent with outbound packets to identify this IPSec Security Association. This SA will be identified by the receiving gateway by matching this SPI, plus the destination address (Peer IP address in option 1), plus the protocol (ESP).

**Default:** [0]

**Options:** up to 8 hex characters

**6 – Inbound SPI**

The Inbound SPI option defines the 8 hexadecimal character (32 bit) Security Parameter Index to be checked for on inbound packets to identify if they were sent using this Security Association. Packets will be tested against this SPI, plus the destination address (Local IP address of this router) and the protocol (ESP). Packets that match will use this SA for decryption.

**Default:** [0]

**Options:** up to 8 hex characters

Note: when setting up an SA connection between two routers, the SPI entries in this menu on each router will be mirror images; for example, the Outbound SPI on one router will be the Inbound SPI on the peer router at the other end of the connection.

**7 – Keys**

The Keys option takes you to the Keys menu where the Encryption and Authentication keys may be set.

## Edit Policy 1 Item x Manual ESP SA Keys Menu

```
                EDIT POLICY 1 ITEM 1 MANUAL ESP SA KEYS MENU

   Option                  Value
 1. Outbound encrypt key   [none]
 2. Inbound encrypt key    [use_outbound]
 3. Outbound auth key      [none]
 4. Inbound auth key       [use_outbound]




Enter option number, "=" - main menu, <TAB> - previous menu


>
```

The **EDIT POLICY 1 ITEM x MANUAL ESP SA KEYS MENU** allows you to manually set the values for the Encapsulating Security Payload Security Association keys to be used with this policy item.

Note: when setting up an SA connection between two routers, the key entries in this menu on each router will be mirror images; for example, the Outbound encryption key on one router will be the Inbound encryption key on the peer router at the other end of the connection.

**1 – Outbound Encrypt Key**

The Outbound Encrypt Key option defines the 16 or 48 hex character key to be used for encrypting the Encapsulating Security Payload (ESP) portion of outbound data packets.

**Note**: the DES keys must be exactly 16 hex characters, 3-DES keys must be exactly 48 hex characters.

**Default:** [none]

**Options:** none, 16 hex characters (DES), 48 hex characterd (3-DES)

**2 – Inbound Encrypt Key**

The Inbound Encrypt Key option defines the 16 or 48 hex character key to be used for decrypting the Encapsulating Security Payload (ESP) portion of inbound data packets.

**Note**: DES keys must be exactly 16 hex characters, 3-DES keys must be exactly 48 hex characters.

**Default:** [none]

**Options:** none, use_outbound, 16 hex characters (DES), 48 hex characterd (3-DES)
use_outbound copies the outbound encryption key entered for option 1 into the inbound encryption key

**3 – Outbound Auth Key**

The Outbound Auth Key option defines the 32 hex character key to be used for the authentication algoritm (MD5) applied to outbound data packets.

**Note**: the entry must be exactly 32 hex characters.

**Default:** [none]

**Options:** none, 32 hex characters

**4 – Inbound Auth Key**

The Inbound Auth Key option defines the 32 hex character key to be used for the authentication algoritm (MD5) applied to inbound data packets.

**Note**: the entry must be exactly 32 hex characters.

**Default:** [none]

**Options:** none, use_outbound, 32 hex characters
use_outbound copies the outbound authentication key entered for option 1 into the inbound authentication key

## Edit Policy 1 Item x Selection Rules Menu

```
                EDIT POLICY 1 ITEM 1 SELECTION RULES MENU

   Option       Value          Description
 1. Src IP      [any]        - Define Source IP address
 2. Dest IP     [any]        - Define Destination IP address
 3. Protocol    [any]        - Define protocol
 4. Src port    [any]        - Define source port
 5. Dest port   [any]        - Define dest port









Enter option number, "=" - main menu, <TAB> - previous menu


>
```

The **EDIT POLICY 1 ITEM x SELECTION RULES MENU** defines the policy item rules against which a packet will be tested.

When a policy item is configured, parameters for both outbound and inbound cases must be set. For this menu the reference direction will be OUTBOUND; the source and destination parameters will automatically be swapped to configure the inbound case.

Note that the policy item rules for inbound IPSec packets will not be tested until the packet has passed SA identification, authorization and decryption

**1 – Src IP**

The Src IP option defines the source IP address (specific or range) to match against packets.

**Default:** [any]

**Options:** any address, or a specific IP address, (press enter when prompted for a second address) or a range of addresses specified by first and last addresses, or a range of addresses specified by starting address and a mask size

**2 – Dest IP**

The Dest IP option defines destination the IP address (specific or range) to match against packets.

**Default:** [any]

**Options:** any address, or a specific IP address (press enter when prompted for a second address), or a range of addresses specified by first and last addresses, or a range of addresses specified by starting address and a mask size

**3 – Protocol**

The Protocol option defines the protocol number (between 1 and 255 inclusive) to match against packets for this policy item. The most common protocol numbers are: 6 (TCP), 17 (UDP) and 1 (ICMP – e.g. Ping).

**Default:** [any]

**Options:** any, protocol number (from 1 to 255)

**4 – Src Port**

The Src Port option defines the port number to match against packets for this policy item.

**Default:** [any]

**Options:** any, port number (from 1 to 65535)

**5 – Dest Port**

The Dest Port option defines the to match against packets for this policy item.

**Default:** [any]

**Options:** any, port number (from 1 to 65535)

## Interfaces Menu

```
                          INTERFACES MENU

    Option              Value          Description
 1. IPsec Interface    [LAN]         - Define IPsec Interface









Enter option number, "=" - main menu, <TAB> - previous menu


>
```

**1 – IPSec Interface**

The IPSec Interface option defines the interface at which IPSec protocols are to be applied. Selecting the "none" option will effectively turn IPSec off.

**Default:** [LAN]
**Options:** none, LAN, WAN

## Statistics Menu

```
                          STATISTICS MENU

    Option              Description
 1. Show policy statistics       - Show policy statistics
 2. Show item statistics         - Show item statistics
 3. Clear Policy statistics      - Clear policy statistics
 4. Clear item statistics        - Clear item statistics









Enter option number, "=" - main menu, <TAB> - previous menu


>
```

The **STATISTICS MENU**displays the statistics for an IPSec policy or a policy item and allows the statistics to be reset.

**1 – Show Policy Statistics**

```
                        IPsec Policy Statistics

Outbound             Packets/Bytes      Inbound             Packets/Bytes
------------------------------------ ------------------------------------
      Inspected:       7081/1153911          Inspected:       6381/1145276
        Discard:          0/0                  Discard:        641/38460
         Bypass:       3692/866075              Bypass:       5659/1092496
   Encapsulated:       3389/464104        Decapsulated:         81/9996
       Tunneled:       3389/464104            Tunneled:         81/9996
      Transport:          0/0                Transport:          0/0
      Encrypted:       3389/328616           Decrypted:         81/9996
  Authenticated:       3383/395844            Verified:         81/11728
Default discard:          0/0           Default discard:          0/0
 Default bypass:       3648/862475       Default bypass:       5615/1088896

Errors
  Error discard:             0             Error discard:             8
Internal errors:             0           Internal errors:           0
                                          Decrypt errors:            0
                                            Auth failure:            0
                                          Policy failure:            8


Type: [s] to redraw, [=] main menu, any other key to end.
```

The Show Policy Statistics displays IPSec traffic statistics for all items of this policy

**Inspected:** count of total packets / bytes tested against this policy

**Discard:** count of total packets / bytes discarded after matching an item under this policy or by the default action for this policy

**Bypass:** count of total packets / bytes bypassed around IPSec processing after matching an item under this policy

**Encapsulated:** count of total transmitted or default action packets / bytes encapsulated by IPSec processing after testing against this policy

**Decapsulated:** count of total received packets / bytes decapsulated by IPSec processing

**Tunneled:** count of total packets / bytes transmitted or received through IPSec tunneling after testing against this policy

**Transport:** count of total packets / bytes transmitted or received through IPSec transport after testing against this policy

**Encrypted:** count of total Outbound packets / bytes encrypted by IPSec processing after testing against this policy

**Decrypted:** count of total Inbound packets / bytes decrypted by IPSec processing after testing against this policy

**Authenticated:** count of total Outbound packets / bytes authenticated by IPSec processing after testing against this policy

**Verified:** count of total Inbound packets / bytes with authentication verified by IPSec processing after testing against this policy

**Default discard:** count of total packets / bytes discarded after failing to match an item under this policy

**Default bypass:** count of total packets / bytes bypassed around IPSec processing after failing to match an item under this policy

**Error Discards:** summation count of packets discarded due to one of the errors listed below

**Internal Errors:** count of packets discarded due to being received with an unknown authorization or encryption algorithm

**Decrypt Errors:** count of packets discarded due to detection of a corrupted packet by the decryption algorithm.

**Auth Failure:** count of packets discarded due to authentication failure

**Policy Failures:** count of packets which passed authentication but were discarded due to failure to match any item in the policy table after decapsulation, decryption and authentication (post processing for incoming tunnel packets)

**2 – Show Item Statistics**

```
                          IPsec Policy Item 1 Statistics          V 51V4.6.2.3
MH

Outbound             Packets/Bytes      Inbound              Packets/Bytes
------------------------------------- -------------------------------------
      Inspected:       3373/282732          Inspected:          64/5840
        Discard:          0/0               Discard:          12/720
         Bypass:         44/3600             Bypass:          44/3600
   Encapsulated:       3329/452168       Decapsulated:       20/1200
       Tunneled:       3329/452168           Tunneled:       20/1200
      Transport:          0/0              Transport:          0/0
      Encrypted:       3329/319080          Decrypted:       20/1200
  Authenticated:       3323/385108           Verified:       20/1600

Errors
  Error discard:           0              Error discard:           0
Internal errors:           0            Internal errors:           0
                                         Decrypt errors:           0
                                           Auth failure:           0



Type: [s] to redraw, [=] main menu, any other key to end.
```

The Show Policy Statistics displays IPSec traffic statistics for a selected item of this policy. After selecting this option, you will be requested to enter the ID number or alias of the policy item you wish to view statistics for.

The display descriptions are the same as for the previous statistics display.

**3 – Clear Policy Statistics**

The Clear Policy option resets the statistics counters in the Show Policy display to zero.

**Options:** totals – resets only the totals summed from the policy list but leaves the stats for individual items
all – resets both overall totals and individual item ststs

**4 – Clear Item Statistics**

The Clear Item option resets the statistics counters for the item ID number or alias entered to zero.

## Diagnostics Menu

```
                              DIAGNOSTICS MENU

    Option          Value          Description
 1. Test IPsec      menu         - Send test packet through system




Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **DIAGNOSTICS MENU** contains one option, which takes you to the Test IPSec menu on the following page.

## Test IPSec Menu

```
                              TEST IPSEC MENU

   Option          Value         Description
 1. Src IP         ""           - Define source IP address
 2. Dest IP        ""           - Define destination IP address
 3. Protocol       [50]         - Define protocol
 4. Src port       [100]        - Define source port
 5. Dest port      [100]        - Define dest port
 6. Direction      [inbound]    - Incoming or outgoing
 7. Perform test                - Test packet



Enter option number, "=" - main menu, <TAB> - previous menu


>
```

The **TEST IPSec MENU** allows formatting of an IPSec test packet and internal testing of that pacet against the IPSec table of policy items.

**1 – Src IP**

The Src IP option defines the source IP address to set for the test packet.

**2 – Dest IP**

The Dest IP option defines destination the IP address to set for the test packet.

**3 – Protocol**

The Protocol option defines the protocol number (between 1 and 255 inclusive) to set for the test packet packets. The most common protocol numbers are: 6 (TCP), 17 (UDP) and 1 (ICMP – e.g. Ping).

**Default:** [any]

**Options:** any, protocol number (from 1 to 255)

**4 – Src Port**

The Src Port option defines the source port number to set for the test packet.

**Default:** [any]

**Options:** any, port number (from 1 to 65535)

**5 – Dest Port**

The Dest Port option defines the destination port number to set for the test packet

**Default:** [any]

**Options:** any, port number (from 1 to 65535)

**6 – Direction**

The Direction option defines the direction to set for the test packet to cross the IPSec interface

**Default:** [Inbound]

**Options:** Inbound, Outbound

**7 – Perform Test**

The Perform Test option matches the test packet configured above against the items in the policy table until a match is found or the end of the table is reached and displays the results of the test. As shown below:

```
                          POLICY TEST

* - Match   ! - No Match   NA - Not Applicable   <-- - Selected Policy

Id  Pri   SrcIP  DstIP  Prot  SrcPort  DstPort    Action     Match?
--  ---   -----  -----  ----  -------  -------  -----------  ------
 1   10     !      !      *       *        !      Apply IPsec   NO
 4   40     *      *      *       *        *      Apply IPsec   YES  <--

-- End of Active Policy list  --

-- Press <Tab> or <Esc> to return to menu  --
```

## Filter Set-Up Menu

```
                          FILTER SET-UP MENU

    Option                      Value         Description
 1. MAC address filters         menu        - Define MAC address filters
 2. Bridge pattern filters      menu        - Define bridge pattern filters
 3. IP router pattern filters   menu        - Define IP pattern filters









Enter option number, "=" - main menu, <TAB> - previous menu


>
```

The **FILTER SET-UP MENU** provides paths to Menus for complete filter configuration.

**1 - MAC Address Filters**

The MAC Address Filters option takes you to the MAC Address Filters Menu, where you can define parameters for Source MAC Filters.

**2 - Bridge Pattern Filter**

The Bridge Pattern Filter option takes you to the Bridge Pattern Filter Menu, where you can create bridge filters based on custom specifications.

**3 - IP Router Pattern Filter**

The IP Router Pattern Filter option takes you to the IP Router Pattern Filter Menu, where you can create IP filters based on custom specifications.

## MAC Address Filters Menu

```
                          MAC ADDRESS FILTERS MENU

    Option                      Value        Description
 1. Edit MAC address filter     menu       - Configure MAC address filter
 2. Filter operation           [positive]  - Set operation of filters
 3. Broadcast address          [forward]   - Filter MAC broadcast frames
 4. Show bridging table                    - View MAC address table
 5. Show permanent table                   - View permanent addresses only
 6. Clear bridging table                   - Delete all non-permanent entries









Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **MAC ADDRESS FILTERS MENU** allows the display and configuration of the MAC Address Filters for the router.

**1 - Edit MAC Address Filter**

The Edit MAC Address Filter option takes you to the Edit MAC Address Filter Menu, where the MAC Address Filters are modified.

**2 - Filter Operation**

The Filter Operation option changes the operation of the MAC address filters defined in the bridging table from positive to negative.

When Filter Operation is positive, all frames with MAC addresses as defined in the bridging table will be filtered.

When Filter Operation is negative, all frames with MAC addresses as defined in the bridging table will be forwarded.

Internal addresses will not be affected by the current state of the Filter Operation. All internal addresses will automatically be corrected for proper operation regardless of the current setting of Filter Operation.

**Default:** [Positive]

**3 - Broadcast Address**

The Broadcast Address option allows the choice of filtering or forwarding of MAC broadcast frames for bridged data.

When set to forward, all MAC broadcast frames will be forwarded.

When set to filter, all MAC broadcast frames will be filtered.

**Default:** [forward]

**4 - Show Bridging Table**

The Show Bridging Table option displays all addresses in the Bridge Filter Table, identifies the active/inactive and permanent/non-permanent addresses, identifies addresses to be filtered if they are a source and/or destination, describes their location, and gives the total number of address table entries.

```
                          ALL Known MAC Addresses
Total entries : 20
                               Filter If
Address            Active Perm Src  Dest         Location
Start of table
01-80-c2-00-00-01                                Internal
01-80-c2-00-00-02                                Internal
01-80-c2-00-00-03                                Internal
01-80-c2-00-00-04                                Internal
01-80-c2-00-00-05                                Internal
01-80-c2-00-00-06                                Internal
01-80-c2-00-00-07                                Internal
01-80-c2-00-00-08                                Internal
01-80-c2-00-00-09                                Internal
01-80-c2-00-00-0a                                Internal
01-80-c2-00-00-0b                                Internal
01-80-c2-00-00-0c                                Internal
01-80-c2-00-00-0d                                Internal
01-80-c2-00-00-0e                                Internal
01-80-c2-00-00-0f                                Internal
02-44-00-c8-9a-ff     *      *                 *   LAN050607
02-44-00-c8-9a-ee     *                        *   LAN050607
12-34-56-78-99-99     *      *    *      *         LAN050607(fixed)
11-11-11-11-11-11                       *         unknown
ff-ff-ff-ff-ff-ff                                 Internal
end of table
```

Refer to the Show Bridging Table option of the Bridging Set-up menu for more details.

**5 - Show Permanent Table**

The Show Permanent Table option displays all of the permanent filter table addresses entered by the router manager for which the locations were identified (Internal addresses are not displayed.) The "(fixed)" Location descriptor indicates that a manager made the entry and specified the LAN location.

```
                          Operator Defined MAC Addresses
                                    Filter if  WAN
Address             Active Perm Src  Dest Access Location
Start of table
02-44-00-c8-9a-ff     *     *              *    LAN050607
12-34-56-78-99-99     *     *   *     *         LAN050607(fixed)
End of table
```

**6 - Clear Bridging Table**

The Clear Bridging Table option removes all non-permanent filter table addresses.

**Considerations:**

To prevent accidental removal of all non-permanent addresses, this option must be confirmed by entering "yes" at the prompt. (Refuse by entering "no" or use the TAB key to back out).

## Edit MAC Address Filter Menu

```
                        EDIT MAC ADDRESS FILTER MENU

    Option              Value          Description
 1. Status             *[        ]   - Is the address in the table?
 2. Location           *[        ]   - Location of MAC address
 3. Filter if source    [        ]   - Filter all frames from this address
 4. Filter if dest      [        ]   - Filter all frames to this address
 5. Permanent           [        ]   - Address is not subject to aging
 6. Remove                           - Delete address









Enter:
    MAC address in hexadecimal (up to 17 characters)

> d0456789
```

The above display is the first level of the **Edit MAC Address Filter Menu**. Once the MAC address is entered (leading 0s are padded), the address specified is added to the menu title bar, the values are shown for the address, and the options become available, as shown below:

```
                EDIT MAC ADDRESS 00-00-d0-45-67-89 FILTER MENU

    Option              Value            Description
 1. Status             *"Not Present"   - Is the address in the table?
 2. Location           *"unknown"       - Location of MAC address
 3. Filter if source    [disabled]      - Filter all frames from this address
 4. Filter if dest      [disabled]      - Filter all frames to this address
 5. Permanent           [disabled]      - Address is not subject to aging
 6. Remove                              - Delete address


>
```

**1 - Status**

The Status option tells whether the address is "Present" or "Not Present" in the Address Table. When the address is first entered, "Not Present" is the Status value, and a Location value of [unknown] is shown. The * beside the value indicates that this value is changed automatically as an address is added or deleted and cannot be manually redefined.

**Default:** * [Not Present]

**2 - Location**

The Location option identifies the location of the MAC address. The locations will either be "unknown" or the LAN name of one of the partner connected P840 routers. The * beside the value indicates that this value is changed automatically as the location is learned and cannot be manually redefined.

**Default:** ***** [unknown]

**3 - Filter *(Forward)* If Source**

The Filter If Source option toggles between Enabling and Disabling of the Source Filtering (Forwarding) feature for the specified address.

**Default:** [disabled]

**Considerations:**

When the Filter Operation is set to positive, enabling this option will prevent frames from this address from crossing the bridge/router to the associated LAN. Once Filter if Source is chosen, the Permanent value is set to [enabled]. This may be toggled back to [disabled] if a non-permanent entry is desired.

When the Filter Operation is set to negative, enabling this option will allow frames from this address to cross the bridge/router to the associated LAN. Once Forward if Source is chosen, the Permanent value is set to [enabled]. This may be toggled back to [disabled] if a non-permanent entry is desired.

**4 - Filter *(Forward)* If Destination**

The Filter If Destination option toggles between Enabling and Disabling of the Destination Filtering feature for the specified address.

**Default:** [disabled]

**Considerations:**

When the Filter Operation is set to positive, enabling this option will prevent access to this address from another LAN station located across the bridge/router. Once Filter if Destination is chosen, the Permanent value is set to [enabled]. This may be toggled back to [disabled] if a non-permanent entry is desired.

When the Filter Operation is set to negative, enabling this option will allow access to this address from another LAN station located across the bridge/router. Once Forward if Destination is chosen, the Permanent value is set to [enabled]. This may be toggled back to [disabled] if a non-permanent entry is desired.

**5 - Permanent**

The Permanent option toggles between Enabling and Disabling of the Permanent Address Value.

**Default:** [disabled]

**Considerations:**

This Value must be [enabled] if you want to make the Address Permanent. If [enabled] the Address will not be subject to removal by the expiration of the Aging Timer or the Clear Filter Table option (found in the Bridging Set-Up Menu or the MAC Address Filters Menu).

If a station is not expected to move, making the address Permanent will offer a slight increase in bridge/router performance.

**6 - Remove**

Select the Remove option to remove the specified address (permanent or non-permanent). Internal and system-supplied addresses cannot be removed.

## Bridge Pattern Filter Menu

```
                          BRIDGE PATTERN FILTERS MENU

    Option                  Description
 1. Show alias            - View pattern filter aliases
 2. Add alias             - Create an alias for a pattern filter
 3. Remove alias          - Delete a pattern filter alias
 4. Show pattern          - View current pattern filters
 5. Add pattern           - Create a pattern filter
 6. Remove pattern        - Delete a pattern filter
 7. Help                  - Read pattern filter and alias description









Enter option number, "=" - main menu, <TAB> - previous menu



>
```

The **BRIDGE PATTERN FILTER MENU** allows for the inclusion of custom-programmable filters in the filter table to provide increased security and maximum local LAN usage.

The bridge/router supports up to 64 patterns and 32 aliases (including the defaults). Each pattern may be up to 80 characters in length. The total number of characters in all defined patterns must not exceed 500.

| | |
|---|---|
| **EXAMPLES:** | Refer to the Programmable Filtering section of the Reference Manual file, for detailed filter construction information with examples. |

**1 - Show Alias**

The Show Alias option displays existing default Aliases and those created with the Add Alias option.

```
                          Bridge Pattern Filter Aliases

 1. IP          - 12-0800
 2. TCP         - IP & 23-06
 3. UDP         - IP & 23-11
 4. ARP         - 12-0806
 5. NETWARE     - 12-8137 | 12-8138
 6. APPLE       - 12-809B
 7. DECNET      - 12-6003
 8. LAT         - 12-6004
 9. XNS         - 12-0807


Type: [s] to redraw, [=] main menu, any other key to end.
```

**note:** the[ s] to redraw is case sensitive; it must be lower case.

**2 - Add Alias**

The Add Alias option allows the creation of an easily identifiable string of characters to identify a complex Filter Mask:

```
Enter:
 alias name (up to 8 characters)

> bmCast


Enter:
 filter pattern for alias (up to 80 characters)
> 0-fffffffffff


Enter:
 alias ID number (from 1 to 32)

> 3
```

Once an alias is created, you must use Add Pattern to add the alias to the filter table and make it operational:

```
Enter:
 filter pattern (up to 80 characters)
> bmCast


Enter:
 pattern ID number (from 1 to 64)
>5
```

Check the alias filter assignment with the Show Pattern option:

```
                          Bridge Filter Patterns

ID    Pattern
--    ---------------------------
1     12-600x
2     0-010203040506&12-809B
...
5     bmCast
```

**3 - Remove Alias**

The Remove Alias option deletes an Alias from the Alias Table. (Confirm with Show Alias.)

```
Enter:
 alias ID number, alias name

> bmCast
```

| | |
|---|---|
| **"bmCast" is used on LAN 1** | **(Prevents blanket removal when an alias is in use:** carefully **check usage** of the alias with **Show Pattern** and then, **if removal of the alias is still desired**, use the **Remove Pattern** option first to remove all occurrences of the alias in the Filter Pattern table, **then use** the **Remove Alias** option). |

**4 - Show Pattern**

The Show Pattern option displays the filter masks that have been defined with the Add Pattern option:

```
Enter:
 all, global, lan, Remote site id or alias
>
```

**global**

```
                          Global Bridge Filter Patterns
Id    Pattern
--    ----------------------------
1     12-600x
3     LAT
```

**MARKETING** - (Remote Site Alias)

```
                       Bridge Filter Patterns to MARKETING
Id    Pattern
--    ----------------------------
2     0-010203040506&12-809B
```

**all**

```
                      Summary of all Bridge filter patterns
Type      Id    Pattern
--------  --    ----------------------------
Global     1     12-600x
           3     LAT
MARKETING  2     0-010203040506&12-809B
```

**5 - Add Pattern**

The Add Pattern option allows the definition of a filter mask and adds it to the filter table. *Filter masks are checked against the frame in the order of their index numbers, so those that are most likely to be encountered should have the lowest index numbers.*

```
Enter:
 global, lan, Remote site id or alias
>

Enter:
 filter pattern (up to 80 characters)
> 12-600x

Enter:
 pattern ID number (from 1 to 64)
> 1
```

A **global** filter pattern will be applied to all bridge data.

A **LAN** filter pattern will be applied to all bridge data being sent to the local LAN.

A **Remote Site Id or Alias** filter pattern will be applied to all bridge data being sent to the specified remote site only. The Remote Site Alias specified must be defined on this device.

**6 - Remove Pattern**

The Remove Pattern option deletes a previously created filter mask (in this case, a filter mask with the pattern ID of "2"). (Confirm the removal with Show Pattern).

```
Enter:
 all, pattern ID number
>2
```

**7 - Help**

The Help option provides Help screens describing the creation of Filter Masks.

To move between the Help screens, type: [s]tart, [n]ext, or [p]rev. (You must use lower-case letters)

## IP Router Pattern Filter Menu

```
                        IP ROUTER PATTERN FILTER MENU

    Option                Description
 1. Show alias          - View pattern filter aliases
 2. Add alias           - Create an alias for a pattern filter
 3. Remove alias        - Delete a pattern filter alias
 4. Show pattern        - View current pattern filters
 5. Add pattern         - Create a pattern filter
 6. Remove pattern      - Delete a pattern filter
 7. Help                - Read pattern filter and alias description









Enter option number, "=" - main menu, <TAB> - previous menu


>
```

The **IP ROUTER PATTERN FILTER MENU** allows for the inclusion of custom programmable filters in the filter table to provide increased security and maximum local LAN usage.

The router supports up to 64 patterns and 32 aliases (including the defaults). Each pattern may be up to 80 characters in length. The total number of characters in all defined patterns must not exceed 500.

| | |
|---|---|
| **EXAMPLES:** | Refer to the Programmable Filtering section of the Reference Manual file, for detailed filter construction information with examples. |

**1 - Show Alias**

The Show Alias option displays existing default Aliases and those created with the Add Alias option.

```
                        IP Router Pattern Filter Aliases

 1. TCP        - 09-06
 2. UDP        - 09-11
 3. MSBROWSE   - 20-0089003


Type: [s] to redraw, [=] main menu, any other key to end.
```

**note:** the[ s] to redraw is case sensitive; it must be lower case.

**2 - Add Alias**

The Add Alias option allows the creation of an easily identifiable string of characters to identify a complex Filter Mask:

```
Enter:
 alias name (up to 8 characters)

> bmCast

Enter:
 filter pattern for alias (up to 80 characters)
> 0-fffffffffff

Enter:
 alias ID number (from 1 to 32)

> 3
```

**3 - Remove Alias**

The Remove Alias option deletes an Alias from the Alias Table. (Confirm with Show Alias.)

```
Enter:
 alias ID number, alias name

> bmCast
```

| | |
|---|---|
| **"bmCast" is used on LAN 1** | **(Prevents blanket removal when an alias is in use:** carefully **check usage** of the alias with **Show Pattern** and then, **if removal of the alias is still desired**, use the **Remove Pattern** option first to remove all occurrences of the alias in the Filter Pattern table, **then use** the **Remove Alias** option). |

**4 - Show Pattern**

The Show Pattern option displays the filter masks that have been defined with the Add Pattern option:

```
Enter:
 all, global, lan, remote site id or alias
>
```

**global**

```
                          Global IP Pattern Filters
Id    Pattern
--    ----------------------------
1     12-600x
3     LAT
```

**Vancouver** (Remote Site alias)

```
                        IP Pattern Filters to Vancouver
Id    Pattern
--    ---------------------------
2     0-010203040506&12-809B
```

**all**

```
                        Summary of all IP Pattern Filters
Type      Id    Pattern
--------  --    ----------------------------
Global     1     12-600x
           3     LAT
Vancouver  2     0-010203040506&12-809B
```

**5 - Add Pattern**

The Add Pattern option allows the definition of a filter mask and adds it to the filter table. *Filter masks are checked against the frame in the order of their index numbers, so those that are most likely to be encountered should have the lowest index numbers.*

```
Enter:
 global, lan, Remote site id or alias
> Vancouver

Enter:
 filter pattern (up to 80 characters)
> 12-600x

Enter:
 pattern ID number (from 1 to 64)
> 2
```

A **global** filter pattern will be applied to all IP routed data.

A **LAN** filter pattern will be applied to all IP routed data being sent to the local LAN.

A **Remote Site Id or Alias** filter pattern will be applied to all IP routed data being sent to the specified remote site only. The Remote Site Alias specified must be defined on this device.

**6 - Remove Pattern**

The Remove Pattern option deletes a previously created filter mask (in this case, a filter mask with the pattern ID of "2"). (Confirm the removal with Show Pattern.)

```
Enter:
 all, pattern ID number
> 2
```

**7 - Help**

The Help option provides Help screens describing the creation of Filter Masks.

To move between the Help screens, type: [s]tart, [n]ext, or [p]rev. (You must use lower-case letters)

## QOS Set-up Menu

```
                              QOS SET-UP MENU

    Option                    Value          Description
 1. Priority Queuing         menu          - Define priority queuing values




Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **QOS SET-UP MENU** allows the router to support QOS features.

**1 - Priority Queuing**
The Priority Queuing options allows you to define an assignment of priority to outbound packets onto outbound priority queues consisting of high, medium, normal or low.

```
                       PRIORITY QUEUING MENU

    Option                    Description
 1. Edit list                 - modify or create priority list
 2. Show Priority List        - Display priority list summary
 3. Remove Priority List      - Remove priority list
 4. Show Statistics           - Show statistics for priority queuing
 5  Clear Statistics          - Clear statistics for priority queuing


Enter option number, "=" - main menu, <TAB> - previous menu

>
```

**1 - Edit List**
The Edit List menu takes you to the Edit Priority List menu where items can be defined and associated to a specific priority list

**2 - Show Priority List**
The Show Priority List options displays all of the Priority Lists configured for this router.

```
                        PRIORITY QUEUING MENU

List Id    Item Count    Default Queue    Queue Limits (high/medium/normal/low)
-------    ----------    -------------   --------------------------------------
1          1             normal           20/40/60/80


Type [s] to redraw, [=] main menu, any other key to end. -

>
```

| | |
|---|---|
| List ID: | Identifier for a priority list |
| Item Count: | Number of items within the priority list |
| Default Queue: | Default queue assigned to the priority list |
| Queue Limits: | Size of each priority queue (high, medium, normal, low) |

**3 - Remove Priority List**
The Remove Priority List option deletes priority list from the router configuration

```
Enter :
       All, priority list ID number

>
```

Enter:
All, priority list ID number

**4 - Show Statistics**

The Show Statistics option displays priority list assigned to interfaces and the statistics of the queues for those interfaces.

```
                QOS PRIORITY QUEUING INTERFACE STATISTICS
              (current-size/queue-limit/dropped //total packets)

Interface     List ID        High         Medium          Normal         Low
-----------   -------      --------     ----------      ----------     --------
LAN             2          0/ 20/ 0     0/ 40/ 0        1/ 60/ 0       0/ 80/ 0
                                  0            0             367              0

LEASED1         1          0/ 20/ 0     0/ 40/ 0        0/ 60/ 0       0/ 80/ 0
                                  0            0               0              0


Type [s] to redraw, [=] main menu, any other key to end. -

>
```

Interface: Displays the interface that have priority lists assigned
List ID: Displays the priority list id assigned to the specific interface
High Current status of the high priority queue associated with the specific interface
Medium: Current status of the medium priority queue associated with the specific interface
Normal: Current status of the normal priority queue associated with the specific interface
Low: Current status of the low priority queue associated with the specific interface

**5 - Clear Statistics**

The Clear Statistic option resets all the statistical parameters for a specific interface, all interfaces or a specific remote site
Enter:

All, lan, Remote site id or alias

## Edit Priority List Menu

```
                        EDIT PRIORITY LIST MENU

    Option               Value       Description
 1. Edit item            menu      - Modify/Create priority list item
 2. Show items                     - Display priority list item summary
 3. Remove item                    - Remove priority list item
 4. Default priority   [       ]   - Define the default priority queue
 5  Queue limit setup   menu      - Define the limits of priority queues


Enter :
     Priority list ID number (from 1 to 16)

>
```

The **EDIT PRIORITY LIST MENU** defines the specific items associated with a Priority List. A Priority List consists of a table of items that define which priority queue it is assigned for any packet that matches all item criteria within the Priority List. A maximum of 16 priority lists can be defined. Within each Priority List up to 32 Items can be defined that matches any or all item criteria within the Priority List..

In order to perform priority queuing using a Priority List, a Priority List must be assigned to a specific interface. Once a Priority List is assigned to an interface, all outbound packets are matched up with the items defined within the Priority List. Each packet is compared to the items defined in the priority list based upon the order of entry within the priority list. For example, the item #1 defined in the priority list will be matched first and if assigned to a specific priority queue the remaining items defined are not compared and the next outbound packet is then examined based upon the order of the item numbers within the Priority List..

Before any Priority List menu options can be entered, you must provide the Priority List number which requires modification or defining.

Enter:

Priority list ID number (from 1 to 16)

**1 - Edit Items**

The Edit Items options takes you to the Edit Item Menu where items associated with the requested Priority List can be defined or modified.

**2 - Show Items**
The Show Items option displays the items that are currently implement with the specified Priority List

```
                QOS PRIORITY LIST ITEM SUMMARY
Item Id    Priority        Selector            Parameter
-------    --------        ---------------     -----------------------------
1          high            incoming_interface  LAN




Type [s] to redraw, [=] main menu, any other key to end. -

>
```

Item ID: Identifier for the item
Priority: Displays the priority queue for the packet if all item criteria matches
Selector: Displays the top level criteria for the priority item such as incoming interface or protocol like ip, ipx or bridging
Parameter: Display the protocol parameter criteria

**3 - Remove Item**
The Remove Item option can remove a specific item from the specified Priority List

Enter:
All, priority list item ID number

**4 - Default Priority**
The Default Priority option assigns a priority queue for those packets that do not match any item criteria in the Priority List. The default queue can be assigned to the high, medium, normal or low queues

Default: [normal]
Choices: [high, medium, normal, low]

**5 - Queue Limit Setup**
The Queue Limit Setup option directs you to a menu allowing each priority queue associated with the Priority List to be specified a maximum number of packets within the queue.

## Queue Limit Setup Menu

```
                EDIT PRIORITY LIST 4 QUEUE LIMIT SETUP MENU

    Option          Value       Description
 1. High            [20]      - Define the High queue limit.
 2. Medium          [40]      - Define the Medium queue limit
 3. Normal          [60]      - Define the Normal queue limit
 4. Low [normal]    [80]      - Define the Low queue limit


Enter option number, "=" - main menu, <TAB> - previous menu


> _
```

The QUEUE LIMIT SETUP MENU specifies the maximum number of packets allowed in each of the priority queues. The High, Medium, Normal and Low outbound queues can be assigned a value between (between 1 to 65535).

**1-High**
High option defines the high queue maximum capacity
Default: [20]
Range: [1 to 65535]

**2- Medium**
Medium option defines the medium queue maximum capacity

Default: [40]
Range: [1 to 65535]

**3- Normal**
Normal option defines the normal queue maximum capacity

Default: [60]
Range: [1 to 65535]

**4- Low**
Low option defines the low queue maximum capacity

Default: [80]
Range: [1 to 65535]

# PRIORITY LIST X EDIT ITEM Y MENU

```
                EDIT PRIORITY LIST 1 ITEM 1 MENU

   Option              Value       Description
 1. Priority           [normal]    - Define the priority level
 2. Selection          [ip]        - Define the packet selection type
 3. Protocol parameter [none]      - Define protocol parameters


Enter option number, "=" - main menu, <TAB> - previous menu


> _
```

The **EDIT ITEM MENU** defines each item criteria associated with a priority list.

**1 - Priority**
The Priority option specifies what level of priority queue an outbound packet is assigned to when the packet matches all item criteria.

Default: [normal]
Choices:[high, medium, normal, low]

**2 - Selection**
The Selection option specifies what type of protocol or specific incoming interface you wish to use to filter an outbound packet.

Default: [ip]
Choices [incoming_interface, bridging, ip, ipx]

**3 - Interface number**

When the Selection option is configured for incoming_interface, the interface number must be configured. Depending upon the configuration of the router, interface number options will vary. For example, the LAN option will be an available option but Link1 and Link2 option will be displayed depending upon the router hardware configuration.
These options will only become available when the Selection option is configured for incoming_interface.

Default: [lan]
Choices:[lan, link number (1 or 2)]

**4- Protocol Parameters**
When the Selection option is configured for a protocol such as bridging, ip or ipx, this option allows you to configure specific protocol options such as filter, byte_count, fragment or none.

Default: [none]
Choices:[none, byte_count, filter, fragment (IP only)]

*None* option configured the protocol list item to have no specific protocol criteria and all protocol (selection) packets will apply to this configured item

*Byte_count* displays allows you to specify packets greater than (gt) or less than (lt) a specified byte count value of (65535 or less).

*Filter* option will direct you to the protocol filter menus (IP Filter Menu, Bridge Filter Menu or IPX Filter Menu). Depending upon the protocol configured in the Selection field, the filter menu will allow you to configure specific protocol filters in which outgoing packets are assigned to a specific priority queue.

*Fragment* option is only available if the Selection protocol is configured for IP. Fragment IP packets do not have header information in which to prioritize the packet. Enabling the fragment option allows for fragmented packets with an offset of non-zero to be prioritized onto an appropriate queue.

**5 - Byte Count**
The byte count defines the packet size in which the IP, IPX or Bridging packets are assigned to a priority queue. The byte_count option can specified less than (lt) or greater than (gt) a set value of 65535 or less.

The Byte Count option will only be displayed when the Protocol Parameter is defined to byte_count.

**6 - Bridging Filter Menu**
The Bridging Filter Menu directs you to a menu that allows you to define the bridging filter including source and destination MAC address. The Bridging Filter Menu will only be displayed when the selection field is configured for the *bridging* protocol and the Protocol Parameter field is configured for *filter*.

**7 - IPX Filter Menu**
The IPX Filter Menu directs you to a menu that allows you to define the IPX filter including source and destination network, node, subnet mask and socket parameters that define the IPX filter. The IPX Filter Menu will only be displayed when the Selection field is configured for *IPX* and the Protocol Parameter is configured to *filter*.

**8 - IP Filter Menu**
The IP Filter Menu directs you to a menu defining the IP filter including source and destination IP address, subnet mask, port and protocol type. The IP Filter Menu will only be displayed when the Selection field is configured for the *IP* and the Protocol Parameter is configured to *filter*.

# PRIORITY LIST X EDIT ITEM Y IPX FILTER MENU

```
                EDIT PRIORITY LIST 1 ITEM 1 IPX FILTER MENU

   Option                  Value       Description
 1. Destination network    [all]      - Destination network number
 2. Destination node       [all]      - Destination node number
 3. Destination node mask  [none]     - Destination node mask
 4. Destination socket     [all]      - Destination socket number
 5. Source network         [all]      - Source network number
 6. Source node            [all]      - Source node number
 7. Source mask            [none]     - Source node mask
 8. Source socket          [all]      - Source socket number
 9. Protocol type          [all]      - Allow specific protocols




Enter option number, "=" - main menu, <TAB> - previous menu

> _
```

The **ITEM IPX FILTER MENU** defines the protocol parameter of the IPX filter for the Priority List item. By specifying the IPX Filter parameters any IPX packets with matching source or destination network and node address will be assigned to the items configured priority queue.

**1 - Destination network**
The Destination network option defines the number of the network to which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. The default is set to all so all IPX packets with a destination address will be filtered unless otherwise defined.

Default: [all]

**2 - Destination node**
The Destination node defines the node on destination-network to which the packet is being sent. The node and node mask are respresented by 6 sets of 2 digit hexidecimal numbers each separated by a dot.(xx.xx.xx.xx.xx.xx). The default is set to all so all IPX packets with a destination node will be filtered unless otherwise defined.

Default: [all]

**3 - Destination node mask**
The Destination node mask defines Mask to be applied to the *destination-node* argument The node and node mask are respresented by 6 sets of 2 digit hexidecimal numbers each separated by a dot.(xx.xx.xx.xx.xx.xx). Place ones in the bit positions you want to mask. The default is set to none so no mask is defined unless otherwise defined.

Default: [none]

**4 - Destination socket**
The Destination socket option defines the number (hexadecimal) to which the packet is being sent.

Default: [all]
Range: [1 to ffff]

**5 - Source network**
The Source network defines number of the network from which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. The default is set to all so all IPX packets with a source network number will be filtered unless otherwise defined.
Default: [all]

**6 - Source node**
The Source node option defines node on the source-network from which the packet is being sent The node and node mask are respresented by 6 sets of 2 digit hexidecimal numbers each separated by a dot.(xx.xx.xx.xx.xx.xx). The default is set to all so all IPX packets with a source node number will be filtered unless otherwise defined.
Default: [all]

**7- Source node mask**
The Source node mask option defines the mask to be applied to the *source-node* argument The node and node mask are respresented by 6 sets of 2 digit hexidecimal numbers each separated by a dot.(xx.xx.xx.xx.xx.xx). Place ones in the bit positions you want to mask. The default is set to none so no mask is defined unless otherwise defined.

Default: [none]

**8 - Source socket**
The Source socket option defines the number (hexadecimal) from which the packet is being sent.
Default:[all]
Range: [1 to ffff]

**9 - Protocol type**
The Protocol type option defines the IPX packet type. Packet types that can be specified include rip(1), sap(4), spx(5), ncp(17), netbios(20).
Default: [all]
Choices: [all, RIP, SAP, SPX, NCP, packet number (255 or lower)]

# PRIORITY LIST X EDIT ITEM Y IP FILTER MENU

```
                EDIT PRIORITY LIST 4 ITEM 1 IP FILTER MENU

   Option                  Value        Description
 1. Destination addr       [all]       - Destination IP address of frame
 2. Destination mask       [none]      - Network mask for dest address
 3. Source address         [all]       - Source IP address of frame
 4. Source mask            [none]      - Network mask for source address
 5. Protocol type          [all]       - Allow specific protocol types
 6. Destination port       [0] [65535] - Destination port range to allow
 7. Source port            [0] [65535] - Source port range to allow




Enter option number, "=" - main menu, <TAB> - previous menu

> _
```

The **ITEM IP FILTER MENU** defines the protocol parameter of the IP filter for the Priority List item. By specifying the IP Filter parameters any IP packets with matching source or destination ip addresses or ports will be assigned to the items configured priority queue.

**1 - Destination Addr**
The Destination Addr option defines the IP Address to which the packet is being sent.

Default: [all]
Option: Any IP Address. The IP address must consist of 4 eight-bit fields, each field is specified by a decimal number and the fields are separated by a decimal point (e.g. 92.3.1.10). Each decimal number must be less than or equal to 255 (the maximum decimal value of an 8-bit binary number).

**2 - Destination Mask**
The Destination Mask option defines the mask to be applied to the Destination IP Address.
Default: [none]
Options: The address mask consists of 4 octets and is represented by 4 fields separated by periods ("**.**"), where each field is specified by a decimal number (e.g. 255.255.255.0). Each decimal number must be less than or equal to 255, that is the maximum value of each 8-bit field.

**3 - Source Addr**
The Source Addr option defines the IP Address from which the packet is being sent.
Default: [none]
Option: Any IP Address. The IP address must consist of 4 eight-bit fields, each field is specified by a decimal number and the fields are separated by a decimal point (e.g. 92.3.1.10). Each decimal number must be less than or equal to 255 (the maximum decimal value of an 8-bit binary number).

**4 - Source Mask**
The Source Mask option defines the mask to be applied to the Source IP Address
Default: [none]
Options: The address mask consists of 4 octets and is represented by 4 fields separated by periods (“.”), where each field is specified by a decimal number (e.g. 255.255.255.0). Each decimal number must be less than or equal to 255, that is the maximum value of each 8-bit field.

**5 - Protocol Type**
The Protocol Type option specifies the protocol type in which the packet would be filtered upon.

Default: [all]
Options: TCP, UDP or any protocol type in HEX

**6 - Destination Port**
The Destination Port option defines the starting and ending port numbers from the Destination IP address(es) defined above to which outbound frames filtered to a specific priority queue. The default setting of this option allows the router to send outbound frames to all ports to a specific priority queue. Setting specific destination port or range of ports allows for greater restrictions in priority.

Default: [0][65535]
Range: 0 to 65535

**7 - Source Port**
The Source Port option defines the starting and ending port numbers from the Source IP address(es) defined above from which outbound frames are to be filtered to a specific priority queue. The default setting of this option allows all ports from a defined source to send outbound frames to be assigned a specific priority. Setting a specific source port or range of ports allows for greater specification for priority.

Default: [0][65535]
Range: 0 to 65535

# PRIORITY LIST X EDIT ITEM Y BRIDGE FILTER MENU

```
                EDIT PRIORITY LIST 4 ITEM 1 BRIDGE FILTER MENU

    Option                  Value        Description
 1. Destination addr        [all]      - Define destination MAC address
 2. Destination mask        [none]     - Destination MAC address mask
 3. Source address          [all]      - Define source MAC address
 4. Source mask             [none]     - Source MAC address mask


Enter option number, "=" - main menu, <TAB> - previous menu

> _
```

The **ITEM BRIDGE FILTER MENU** defines the protocol parameters of the Bridge filter for the Priority List item. By specifying the Bridge filter parameters any traffice with matching source or destination addresses or ports will be assigned to the configured priority queue within this item list.

**1 - Destination Addr**
The Destination Addr option defines the Destination MAC Address which bridging packets will be matched against.
Default: [all]
Option: Any MAC Address

**2 - Destination Mask**
The Destination Mask option defines the mask that will be applied to the Destination MAC Address of the packet. The address and mask values are respresented by 6 sets of 2 digit hexidecimal numbers each separated by a dot.(xx.xx.xx.xx.xx.xx) Place ones in the bit positions you want to mask. The default is set to none so no mask is defined unless otherwise defined
Default: [none]

**3 - Source Addr**
The Source Addr option defines the Source MAC Address which bridging packets will be matched against.
Default: [all]
Option: any MAC Address

**4 - Source Mask**
The Source Mask option defines the mask that will be applied to the Source MAC address of the packet.. The address and mask values are respresented by 6 sets of 2 digit hexidecimal numbers each separated by a dot.(xx.xx.xx.xx.xx.xx). Place ones in the bit positions you want to mask. The default is set to none so no mask is defined unless otherwise defined
Default: [none]

## Applications Set-Up Menu

```
                          APPLICATIONS SET-UP MENU

   Option              Value           Description

 1. SNMP set-up         menu         - Define SNMP communications
 2. DHCP set-up         menu         - Define DHCP configuration
 3. Firewall set-up     menu         - Define firewall parameters
 4. NAT exports         menu         - Define exported services for NAT
 5. Syslog set-up       menu         - Define Syslog configuration
 6. Time to live       [32]          - Router hops allowed
 7. Traceroute                       - Trace a route
 8. Ping                             - ICMP echo requests
 9. SNTP set-up         menu         - Define SNTP configuration




Enter option number, "=" - main menu, <TAB> - previous menu
>
```

The **APPLICATIONS SET-UP MENU** provides paths to menus for Internet communication management applications.

**1 - SNMP Set-Up**

The SNMP Set-up option takes you to the SNMP Set-Up Menu, where you to define the parameters necessary to allow the router's SNMP agent and corresponding MIB information to be accessed by an SNMP Network Management Station. Traps (Alarms) will also be sent by the router to the NMS to inform it of a significant event (cold start, warm start, link up, link down, and authentication failure).

**2 - DHCP Set-Up**

The DHCP Set-up option directs you to the DHCP Set-Up Menu, where the DHCP (Dynamic Host Configuration Protocol) parameters may be set and the IP address pool may be viewed.

**3 - Firewall Set-Up**

The Firewall Set-up option directs you to the Firewall Set-Up Menu, where the IP Firewall parameters may be set.

**4 - NAT Exports**

The NAT Exports option directs you to the NAT Exports Menu, where Internet services available for export on this network may be set up, checked, or removed.

**5. Syslog Set-Up**

The Syslog Set-up option directs you to the Syslog Set-up Menu, where a system message logging service to forward event messages to servers using the Syslog utility may be set up.

**6 - Time To Live**

The Time To Live option sets the maximum number of router hops that an IP packet generated by the router is allowed before being discarded.

IP packets that are being routed through the P840 router will have their time-to-live value decremented by two.

**Default:** [32]

**Range:** 1 - 255

**7 – Traceroute**

Sends a UDP packet to the destination you specify and lists the IP addresses of the devices that the packet passes through along the route to that destination.

**8 - Ping**

The Ping option generates ICMP Ping messages to the specified destination IP address. The size and number of packets transmitted is entered within the command options. If you enter a broadcast address, you will be additionally prompted for LAN or Remote Site ID information. The ping broadcast will then be sent out the LAN port or to the remote site router.

```
Enter :
    Destination (up to 15 characters)
> 25.25.25.25


Enter :
    Length of data in bytes (1472 or lower)
> 15


Enter :
    Number of packets to send (from 1 to 32767)
> 1
```

The results of the Ping messages received will be displayed on the screen. The example below shows the results of an unsuccessful Ping command.

```
Ping to 25.25.25.25, 15 bytes, count 1

Enter <Tab> or <Esc> to stop

No Reply from 25.25.25.25 sequence 0 for 2.0 seconds
Ping results for 25.25.25.25, packets transmitted 1, received 0


Press any key to return to menu.
```

## SNMP Set-Up Menu

```
                              SNMP SET-UP MENU

    Option              Value           Description
 1. Edit community      menu          - Modify SNMP community
 2. Message size       [1472 bytes]   - Define maximum message size
 3. Show communities                  - View SNMP communities
 4. Remove community                  - Delete SNMP community









Enter option number, "=" - main menu, <TAB> - previous menu


>
```

The **SNMP SET-UP MENU** allows the display and configuration of the Simple Network Management Protocol (SNMP) parameters for the router. For information on the P840s compliance with the SNMP Management Information Bases (MIBs) and details of the proprietary MIB, please refer to the MIB files on the CD-ROM included with the unit.

The SNMP Set Up Menu contains two default communities:
- "public" which is a read-only community accessible by all Network Management Station (NMS) addresses
- "GUI_Config" which is a read-write community accessible by all NMS addresses

**1 - Edit Community**

The Edit Community option takes you to the Define Community Menu, where the router's agent and NMS are brought under a management community.

**2 - Message Size**

The Message Size option allows the setting of the maximum message size sent by the router's SNMP agent.

**Default:** [1472 bytes]

**Range:** 484 to 1472 bytes

**Considerations:**

The message size sent by the router is determined by what the NMS can accept. The default size of 1472 bytes, combined with the "overhead," totals the maximum Ethernet frame size.

**3 - Show Communities**

The Show Communities option displays the defined SNMP communities.

```
SNMP Communities

Number of defined communities  :  3

Community Name   Write Access      Addresses          Trap Format
GUI_Config       enabled           all                    -

Public           disabled          all                    -

NMS_1            enabled           92.0.0.1           SNMPv1
                                   111.1.1.1          SNMPv2









Type: [s] to redraw, [=] main menu, any other key to end.
```

**note:** the[ s] to redraw is case sensitive; it must be lower case.

**4 - Remove Community**

The Remove Community option deletes the specified SNMP community from the list of available communities. Enter either the community name for a single deletion or "all" if the entire SNMP community list is to be deleted. Note that removing all communities will prevent access from any NMS until replacements are added.

## Edit Community Menu

```
                          EDIT COMMUNITY MENU

    Option                 Value          Description
 1. Write access          [        ]    - Allow write access
 2. Show addresses                      - View address lists
 3. Add address                         - Add address and trap format
 4. Remove address                      - Delete address from list




Enter:
    community name string (up to 32 characters)

>
```

**Note:** only alphanumeric characters and the underscore ("_") character may be used in the community name. In addition, the characters are **case-sensitive**. Once the community name is defined, it is added to the Menu title (as shown below), and the options become available.

```
                      EDIT COMMUNITY Marketing MENU

    Option                 Value          Description
 1. Write access          [disabled]    - Allow write access
 2. Show addresses                      - View address lists
 3. Add address                         - Add address and trap format
 4. Remove address                      - Delete address from list




Enter:

>
```

**1 - Write Access**

The Write Access option defaults to [disabled] when a SNMP Community name string is entered. This allows an NMS to have read-only access to this SNMP Community. Write access [enabled] allows a NMS to have read/write access to the SNMP community.

**Considerations:**

If several NMSs are available at one site, a community might be named "Public" with read-only access. This allows all NMS managers to view SNMP information for the router, although only the community(ies) with read/write access [enabled] will be able to modify parameters. (Note that the community name "all" should not be used, since, if it were ever removed, other defined communities would be removed along with it).

**2 - Show Addresses**

The Show Addresses option provides a display of existing NMS and trap addresses for this Community name (e.g. Marketing).

```
Address Lists for Community Marketing
Total NMS addresses      :  3

Addresses                Trap Format
192.24.56.1              SNMPv1
111.1.1.1                SNMPv2
all                      -
```

**3 - Add Address**

Up to 10 addresses may be added to the address list. If the address list is empty, the router's SNMP agent will not accept requests from a NMS, even if it correctly provides this community name. If the list contains the single entry "all," the router's SNMP agent will accept requests from any NMS providing this community name. Addresses must be entered in standard IP format (four fields separated by a periods, with each field specifying a decimal number).

When a trap is generated by the router's SNMP agent, it will be sent (along with the Community name) to each of the destination addresses specified.

**Considerations:**

If "all" is initially chosen for the address list, and (one or more) specific addresses are desired as a replacement, remove "all" with *Option 4, Remove address,* to allow the addition of the new address(es).

**4 - Remove Address**

The Remove Address option deletes the specified address associated with the SNMP Community. Other addresses remain unaffected. (If "all" is specified, all addresses are deleted.)

## DHCP Set-Up Menu

```
                              DHCP SET-UP MENU

    Option                    Value          Description
 1. Server IP address pool    menu         - Range of allowable addresses
 2. DNS set-up                menu         - Define DNS address(es)
 3. NetBIOS setup             menu         - NetBIOS parameters
 4. DHCP services            [none]        - Set DHCP operational mode
 5. Relay destination        [none]        - BOOTP/DHCP server IP address
 6. ICMP echo verification   [enabled]     - Ping allocated IP address
 7. Lease period             [60 min]      - Length of lease
 8. Default gateway          [automatic]   - Gateway for client



Enter option number, "=" - main menu, <TAB> - previous menu


>
```

The **DHCP SET-UP MENU** contains options used to dynamically configure and maintain the DHCP parameters for remote devices on a network via a central DHCP server. Dynamic Host Configuration Protocol (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 P840's LAN(s) or on remote site networks connected over the WAN links. It will supply minimal configuration needed to allow hosts to operate in an IP network.

**1 - Server IP Address Pool**

The Server IP address pool option directs you to the Server IP address pool Menu, where the range of allowable IP addresses may be set.

**2 - DNS Set-Up**

The DNS Set-up option directs you to the DNS Set-Up Menu, where the Primary and Secondary DNS (Domain Name Server) addresses may be set.

**3 - NetBIOS Set-Up**

The NetBIOS set-up option directs you to the NetBIOS set-up Menu, where the NetBIOS parameters may be set.

**4 - DHCP Services**

The DHCP services option sets the DHCP operational mode as none, server or relay. Selecting "none" disables the option. Selecting "server" enables this P840 to act as a simple DHCP server for its LAN. Selecting "relay" enables the P840 to relay DHCP service data to a remote DHCP server.

**Default:** none

**Choices:** none, server, relay

**5 - Relay Destination**

The Relay destination option allows you to enter the IP address of the remote DHCP server to which DHCP client data will be routed. **Note:** BootP Relay should only be used with leased line connections, it is not recommended when using any form of connection management (spoofing, IP address connect) on a dial-up line.

**Default:** none

**6 - ICMP Echo Verification**

The ICMP echo verification option enables or disables the ping allocated IP address. If enabled, ICMP Ping messages may be sent to the specified IP address when a Ping command is issued.

**Default:** enabled

**7 - Lease Period**

The Lease period option sets the length of time (in minutes) that an assigned IP address will be allocated to a DHCP client.

**Default:** 60

**Range:** 10 to 65535 minutes

**8 - Default gateway**

The Default Gateway option allows the identification of a default gateway (i.e. *router*). Messages destined for hosts not on this (sub-)network are forwarded to the default gateway. The default gateway may be located on the local LAN or may be one of the remote site peer IP routers.

**Note:** If using raw 1490 Frame Relay, either enable "Auto Default Route" or configure the Default Gateway remote site peer address to access the Default Gateway.

If PPP is used and the IP address of the remote site peer IP router is not known, the default gateway may be defined as the remote site ID. This will cause the default gateway to become whatever device is currently connected at that remote site.

When an SNMP message is to be sent to an NMS, first the routing table is checked for a known route. If a route to the NMS is unknown, the SNMP message will then be sent to the default gateway. If the default gateway cannot provide the best route, it will send the message to the gateway that can provide the best route. After the default gateway sends the message to the other gateway for delivery, the default gateway will send an ICMP Redirect message back to the router that points to the best route gateway. In this manner, the router is informed of the best route for future SNMP message delivery.

A configured Default Gateway will override a default route learned from RIP. If more than one default gateways are defined within the routing table, the default gateway with the lowest cost will be used and displayed in this option.

**Default:** [automatic]

```
Enter :
       automatic, none, ip_address (up to 15 characters)
>
```

## Server IP Address Pool Menu

```
                          SERVER IP ADDRESS POOL MENU

    Option                Value          Description
 1. IP address pool      [none]        - Specify IP address pool
 2. Show address pool                  - Display allocated addresses
 3. Add static Address                 - Specify clients IP/MAC address
 4. Remove static address              - Remove static IP address









Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **SERVER IP ADDRESS POOL MENU** contains options used to view and maintain the Server IP address pool for the DHCP server of this device.

**1 - IP Address Pool**

The IP address pool option sets the IP address pool. A block of IP addresses may be configured from which the server will hand out IP addresses. The first address in the range must be specified followed by the number of addresses desired.

**Default:** none

**Range:** 1 to 253 addresses

**Considerations:**

IP address assigned to the pool must be on the same IP network or the LAN of which this P840 is a part.

The IP address pool is not allowed to contain a network broadcast address (all binary 1s in the host portion of the address) for the network or subnetwork in which the pool resides or for a standard Class A, B or C network.

If a pool assignment will contain a disallowed address, the following message will appear:

```
Size will create addresses outside network's valid range,
```

Use a smaller pool size or a different starting address.

**2 - Show Address Pool**

```
                          DHCP Server IP Address Pool
Pool Address         Type     Hardware Address      Lease Remaining
---------------      ----     -----------------     ---------------
129.0.0.25           Dynamic  00-00-D0-00-12-34           45
129.0.0.26           Dynamic  00-00-D0-00-12-35        Reserved
129.0.0.27           Static   00-00-D0-00-12-36           55
129.0.0.28           Static   00-00-D0-00-12-3         Reserved
129.0.0.29           Dynamic     Available

Type: [s] to redraw, [=] main menu, any other key to end.
```

**note:** the[ s] to redraw is case sensitive; it must be lower case.

**3 - Add Static Address**

The Add static address option assigns a specific IP address to a specific device, such as a network server, from the central DHCP server. When this option is selected, first enter the IP address to be assigned to the device, then the MAC of the device.

**4 - Remove Static Address**

The Remove static address option removes the static address assignment from a device. Devices may be removed individually by entering the MAC address of the device to be taken off, or the entire list of static address assignments may be cleared by entering “all”.

## DNS Set-up Menu

```
                              DNS SET-UP MENU

    Option            Value          Description
 1. Primary DNS      [none]        - Address of Primary DNS
 2. Secondary DNS    [none]        - Address of Secondary DNS
 3. Domain name      [none]        - Network name









Enter option number, "=" - main menu, <TAB> - previous menu
>
```

The **DNS SET-UP MENU** contains options used to configure and maintain the DNS parameters for this device. The DHCP server will supply the IP address of the primary and secondary Domain Name Servers when this router is configured as a DHCP server. The DHCP server will not return an IP address if the DNS entries in this menu are set to none.

**1 - Primary DNS**

The Primary DNS option defines the IP address of the primary network Domain Name Server (DNS).

**Default:** [none]

**2 - Secondary DNS**

The Secondary DNS option defines the IP address of the secondary network Domain Name Server (DNS)

**Default:** [none]

**3 - Domain Name**

The Domain Name option allows the specification of a domain name of up to 254 characters.

**Default:** [none]

**Considerations:**

When setting up a router using IP addressing that will have a DNS server on the local network as well as a connection to an external DNS server (such as in Internet Service Provider), the local DNS server should be set as the Primary DNS and the external DNS server as the Secondary DNS.

## NetBIOS Set-Up Menu

```
                          NETBIOS SETUP MENU

   Option                   Value              Description
 1. Send NetBIOS node type  [enabled]          - Send node type to client
 2. Send NetBIOS scope      [enabled]          - Send scope identifier
 3. Send NetBIOS name srv   [enabled]          - Send name server address
 4. NetBIOS node type       [B]                - Type of name resolution
 5. NetBIOS scope Id        "DEV050607_scope"  - Scope identifier
 6. NetBIOS name server     [none]             - IP address of name server




Enter option number, "=" - main menu, <TAB> - previous menu


>
```

The **NETBIOS SET-UP MENU** contains options used to configure and maintain the NetBIOS parameters for this device. NetBIOS is used by Windows NT or Windows 95 clients to advertise themselves and to locate resources. When a netBIOS client initializes, it must advertise its machine name; the Windows NT server then finds the IP address associated with that name.

### 1 - Send NetBIOS Node Type

The Send NetBIOS node type option sends the node type to the client when enabled. If disabled, broadcasts will be used to advertise and locate resources.

**Default:** disabled

### 2 - Send NetBIOS Scope

The Send NetBIOS scope option sends the scope identifier to the client when enabled. The scope identifier is a name for the group of computers to which the NetBIOS name of this router is known

**Default:** disabled

### 3 - Send NetBIOS Name Srv

The Send NetBIOS name srv option sends the name server address to the client when enabled.

**Default:** disabled

**4 - NetBIOS Node Type**

The NetBIOS node type option allows you to set the type name resolution. The Send NetBIOS node type option must be enabled before this option will be displayed.

**Default:** disabled

**Choices:** B - broadcasts node names and queries
P - point-to-point communication with the NetBIOS name server to resolve and register NetBIOS names.
M - mixed; a combination of B and P communication. Traffic is first broadcast on the local segment and attached segments configured to propogate NetBIOS broadcasts. Once a NetBIOS name server is located, point-to-point communication across routers is allowed.
H -hybrid; a mixture of B and P communications. P is used if a NetBIOS name server is available, otherwise B is used.

**5 - NetBIOS Scope Id**

The NetBIOS scope Id option allows you to set the scope identifier. The default scope identifier will be the device name followed be "_scope" (i.e. DEVXXX_scope). The Send NetBIOS scope option must be enabled before this option will be displayed.

**Default:** DEVXXX_scope

**6 - NetBIOS Name Server**

The NetBIOS name server option allows you to set the IP address of the NetBIOS name server. The Send NetBIOS name srv option must be enabled before this option will be displayed.

**Default:** none

## Firewall Set-Up Menu

```
                          FIREWALL SET-UP MENU

   Option                  Value        Description
 1. LAN firewall setup      menu        - LAN specific firewall setup
 2. WAN firewall setup      menu        - Remote site firewall setup
 3. Block src IP spoofing  [enabled]    - Discard ext pkts with local src IP









Enter option number, "=" - main menu, <TAB> - previous menu
>
```

The **FIREWALL SET-UP MENU** contains options used to view and maintain the IP firewall settings for this device. The P840 firewalls are set on a per interface basis, so the set up of the LAN and WAN firewalls is identical. The direction of traffic is specified from the perspective of the P840, so incoming traffic is from the specified interface to the P840, outgoing traffic is from the P840 to the specified interface.

**1 – LAN Firewall Set-up**

The LAN Firewall Set-up option directs you to the LAN Firewall Set-Up Menu, where the IP Firewall parameters for IP traffic to and/or from Local Area Network(s) may be set.

**2 - WAN Firewall Set-up**

The WAN Firewall Set-up option directs you to the WAN Firewall Set-Up Menu, where the IP Firewall parameters for IP traffic to and/or from individual remotes site on Wide Area Networks may be set.

**3 - Block Source IP Spoofing**

When the Block Source IP Spoofing option is enabled, all of the traffic external to this LAN that uses a source IP address the same as the local network IP address will be filtered. This prevents devices located on an external network from attempting to gain access to the local network by using a local IP address as their source address. The P840 will discard any IP traffic that is received with a source IP address the same as an IP address located on the LAN.

**Default:** [disabled]

## LAN Firewall Set-Up Menu

```
                          FIREWALL - LAN MENU

   Option                  Value        Description
 1. Designated servers      menu       - Edit entry for a specific server
 2. Edit firewall entry     menu       - Edit/Add firewall entries
 3. Firewall               [both]      - Block inbound/outbound/both
 4. Firewall statistics                - View firewall statistics
 5. Clear statistics                   - Clear firewall statistics
 6. Show firewall entries              - Display firewall entries
 7. Remove entry                       - Remove a firewall entry




Enter option number, "=" - main menu, <TAB> - previous menu
>
```

The **LAN FIREWALL SET-UP MENU** contains menu options to control the IP firewall settings for LAN connections to this device. The **LAN FIREWALL SET-UP MENU** and **WAN FIREWALL SET-UP MENU** contains identical menu options. They control the IP firewall settings for LAN and WAN connections to this device.

**Remember** that when the firewall function is set to *both*, **all incoming and outgoing IP traffic to and/or from the LAN** interface (including secondary LANs) will be **filtered**. All IP traffic (TCP, UDP (ping), TFTP and PPP) received from or sent to the LAN(s) will be filtered out and not allowed through the firewall.

To allow specific IP traffic to be passed between another network connection and this LAN, either a firewall entry must be specified or a designated server must be specified or a combination of the two. The direction in which the firewall is to filter traffic (inbound, outbound or both) is specified under the *Firewall* option (3) or may be set on an individual firewall table entry basis via the *Edit firewall entry* option (2).

**1 - Designated Servers**

The Designated Servers option directs you to the Designated Servers Menu, where the IP addresses may be defined for the designated servers on the LAN. A designated server is a device that is legally accessible from another network connection. An example, designated servers may be the HTTP server and the FTP server on the LAN that may be accessed by devices located at remote sites.

**2 - Edit Firewall Entry**

This option directs you to the Edit Firewall Entry Menu, where a table of entries that are to be allowed to pass IP traffic through the firewall is defined. The Firewall table may have up to 15 entries.

**3 - Firewall**

The Firewall option controls the direction in which Firewall filtering is to be applied by this P840 to all traffic through the LAN interface.

By default, the direction in which filtering will be applied for all entries in the firewall table is initially set to the direction specified by this option. This direction may be changed for individual entries using the *Edit firewall entry* option (2). Once the direction of filtering for some entries has been altered, changing the overall direction applied to the firewall table will not affect those entries that have been changed; if a change to these entries is required, each entry that needs to be changed must be edited individually.

If *Block incoming* is selected, a**ll incoming IP traffic** from the LAN(s) to the P840 will be **filtered out, EXCEPT what is specified in the Designated Server or Firewall Entry table**. This means that only the specified traffic will be allowed through the firewall for forwarding through the P840 to another network. All outbound traffic from the P840 to the LAN will be forwarded.

If *Block outgoing* is selected, a**ll outgoing IP traffic** through the P840 to the LAN(s) will be **filtered out, EXCEPT what is specified in the Designated Server or Firewall Entry table**. This means that only the specified traffic will be allowed through the P840 out onto the LAN(s). All inbound traffic from the LAN to the P840 will be forwarded.

If *Block both* is selected a**ll outgoing AND incoming IP traffic** through the P840 will be **filtered out, EXCEPT what is specified in the Designated Server or Firewall Entry table**. This means that only the specified traffic will be allowed through the P840 in either direction.

If *disabled* is selected, all traffic is allowed to pass without being filtered.

**Default:** [disabled]

**Choices:** Block inbound/outbound/both/disabled

**4 - Firewall Statistics**

The Firewall Statistics option displays a summary of the number of frames discarded by the firewall function.

```
                          LAN 1 FIREWALL STATISTICS

Frames discarded                      Totals
-------------------------------------------------------------------------
Source IP spoofed                    0

Source IP address                    0
Destination IP address               0
Protocol number                      0
Port number                          0

Total frames discarded               0
```

| | |
|---|---|
| Source IP Spoofed: | Frames outbound to the LAN discarded due to source IP address being the same as an IP address already on the local network. |
| Source IP Address: | Frames outbound to the LAN discarded because the source IP address is not allowed to access this local network. |
| Destination IP Address: | Frames outbound to the LAN discarded because the destination IP address on the local network is not allowed to be accessed from another network. |
| Protocol Number: | Outgoing frames to the LAN discarded because the protocol type is not allowed. |
| Port Number: | Outgoing frames to the LAN discarded because the port number is not allowed.. |
| Total Number: | Total number of Outgoing frames to the LAN discarded due to firewall filtering. |

**5 - Clear Statistics**

The Clear Statistics option clears all of the firewall statistics.

Note: The firewall statistics may also be cleared with the Clear All Statistics option in the Statistics Set-up menu.

**6 - Show Firewall Entries**

The Show Firewall Entries option displays all of the entries in the Firewall table. Entries marked with a "**" indicate an entry from the Designated Servers menu.

```
                              Firewall Entries
       Source /          Source /              Source / Dest
 #   Dest address    Destination mask  Type  Port 1  Port n  Alias
--  ---------------  ----------------  ----  ------  ------  --------------
**  All addresses         None         TCP   20      21      FTP server
    199.167.3.145         None
**  All addresses         None         TCP   80      80      WWW server
    199.167.3.139         None
 1  199.167.4.0      255.255.255.0     TCP   1       65535   Manual entry
    199.167.3.0      255.255.255.0
```

| | |
|---|---|
| #: | Entry number in the Firewall table. |
| Source/Destination Address: | IP addresses to be checked for in IP traffic. |
| Source/Destination Mask: | IP address masks to be used for checking the source and destination addresses. |
| Type: | Type of IP packet. TCP, UDP, or another user defined value. |
| Port 1: | Starting port of the range of ports to allow through the firewall. |
| Port n: | Ending port of the range of ports to allow through the firewall. |
| Alias: | Name used to indicate the type of entry in the port, either a manual entry or a name from the Designated Servers menu. |

**7 - Remove Entry**

The Remove Entry option deletes individual entries or all of the entries from the Firewall table.

```
Enter :
    all, index number (from 1 to 15)

>
```

## WAN Firewall Set-Up Menu

```
                          FIREWALL – REMOTE SITE MENU

    Option                    Value        Description
 1. Designated servers        menu        – Edit entry for a specific server
 2. Edit firewall entry       menu        – Edit/Add firewall entries
 3. Firewall                 [both]       – Block inbound/outbound/both
 4. Firewall statistics                   – View firewall statistics
 5. Clear statistics                      – Clear firewall statistics
 6. Show firewall entries                 – Display firewall entries
 7. Remove entry                          – Remove a firewall entry




Enter option number, "=" – main menu, <TAB> – previous menu
>
```

A remote site name or ID number designating a remote site that has been configured under the WAN Set-up Menu must be entered before the options on this menu are made operational.

The **WAN FIREWALL SET-UP MENU** and **LAN FIREWALL SET-UP MENU** contains identical menu options. They control the IP firewall settings for LAN and WAN connections to this device.

**Remember** that when the firewall function is set to *both*, **all incoming and outgoing IP traffic to and/or from the specified WAN remote site** will be **filtered**. All. IP traffic (TCP, UDP (ping), PPP and TFTP) received from or sent to the specified remote site will be filtered out and not allowed through the firewall. To allow specific IP traffic to be passed between another network connection and this remote site, either a firewall entry must be specified or a designated server must be specified or a combination of the two. The direction in which the firewall is to filter traffic (inbound, outbound or both) is specified under the *Firewall* option (3) or may be set on and individual firewall table entry basis via the *Edit firewall entry* option (2).

### 1 - Designated Servers

The Designated Servers option directs you to the Designated Servers Menu, where the IP addresses may be defined for the designated servers on this remote site network. A designated server is a device that is legally accessible from other networks.

### 2 - Edit Firewall Entry

This option directs you to the Edit Firewall Entry Menu, where a table of entries that are to be allowed through the firewall is defined. A firewall entry allows passage of IP traffic to and/or from this remote site and another IP network. The Firewall table may have up to 15 entries per remote site.

### 3 - Firewall support

The Firewall option controls the direction in which Firewall filtering is to be applied by this P840 to all traffic to and/or from this remote site.

By default, the direction in which filtering will be applied for all entries in the firewall table is initially set to the direction specified by this option. This direction may be changed for individual entries using the *Edit firewall entry* option (2). Once the direction of filtering for some entries has been altered, changing the overall direction applied to the firewall table will

not affect those entries that have been changed; if a change is required, each entry that needs to be changed must be edited individually.

If *Block incoming* is selected, a**ll incoming IP traffic** from the remote site network to the P840 will be **filtered out, EXCEPT what is specified in the Designated Server or Firewall Entry table**. This means that only the specified traffic will be allowed through the firewall for forwarding through the P840 to another network. All outbound traffic from the P840 to the remote site will be forwarded.

If *Block outgoing* is selected, a**ll outgoing IP traffic** through the P840 to the remote site network will be **filtered out, EXCEPT what is specified in the Designated Server or Firewall Entry table**. This means that only the specified traffic will be allowed through the P840 out onto the remote site. All inbound traffic from the remote site to the P840 will be forwarded.

If *Block both* is selected a**ll outgoing AND incoming IP traffic** through the P840 for this remote site network will be **filtered out, EXCEPT what is specified in the Designated Server or Firewall Entry table**. This means that only the specified traffic will be allowed through the P840 in either direction.

If *disabled* is selected, all traffic is allowed to pass to and from the remote site without being filtered.

**Default:** [disabled]

**Choices:** Block inbound/outbound/both/disabled

**4 - Firewall Statistics**

The Firewall Statistics option displays a summary of the number of frames destined to the specified WAN remote site discarded by the firewall function.

The firewall statistics may be cleared with the Clear All Statistics option in the Statistics Set-up menu.

```
                          Firewall Statistics

Frames discarded                    Totals
------------------------------------------------------------------------
Source IP spoofed                   0

Source IP address                   0
Destination IP address              0
Protocol number                     0
Port number                         0

Total frames discarded              0
```

| | |
|---|---|
| Source IP Spoofed: | Frames outbound to this WAN remote site discarded due to source IP address being the same as an IP address already on the remote site network. |
| Source IP Address: | Frames outbound to this WAN remote site discarded because the source IP address is not allowed to access this remote site network. |
| Destination IP Address: | Frames outbound to this WAN remote site discarded because the destination IP address on the remote site network is not allowed to be accessed from another network. |
| Protocol Number: | Outgoing frames to this WAN remote site discarded because the protocol type is not allowed. |
| Port Number: | Outgoing frames to this WAN remote site discarded because the port number is not allowed. |

| | |
|---|---|
| Total Number: | Total number of Outgoing frames to this WAN remote site discarded due to firewall filtering. |

Additional information on events in Firewall operation is available under the **Syslog** menu.

**5 - Clear Statistics**

The Clear Statistics option clears all of the firewall statistics.

**6 - Show Firewall Entries**

The Show Firewall Entries option displays all of the entries in the Firewall table. Entries marked with a "**" indicate an entry from the Designated Servers menu.

```
                              Firewall Entries
       Source / Dest    Source /              Source / Dest
  # Dir Network Address Destination mask Type Port 1 Port n Alias
--- --- --------------- ---------------- ---- ------ ------ --------------
**   in All addresses        None         TCP   20      21      FTP server
     in 199.167.3.145        None
**   in All addresses        None         TCP   80      80      WWW server
     in 199.167.3.139        None
 1  out 199.167.4.0     255.255.255.0     TCP   1       65535   Manual entry
    out 199.167.3.0     255.255.255.0
```

| | |
|---|---|
| #: | Entry number in the Firewall table. |
| Source/Destination Address: | IP addresses to be checked for in the IP traffic. |
| Source/Destination Mask: | IP address masks to be used for checking the source and destination addresses. |
| Type: | Type of IP packet. TCP, UDP, or another user defined value. |
| Port 1: | Starting port of the range of ports to allow through the firewall. |
| Port n: | Ending port of the range of ports to allow through the firewall. |
| Alias: | Name used to indicate the type of entry in the port, either a manual entry or a name from the Designated Servers menu. |

**7 - Remove Entry**

The Remove Entry option deletes individual entries or all of the entries from the Firewall table.

```
Enter :
    all, index number (from 1 to 15)

>
```

## Designated Servers Menu

```
                        DESIGNATED SERVERS MENU

   Option                    Value          Description
 1. E-mail (SMTP) server     [none]       - Specify E-Mail server IP address
 2. POP 2/3 server           [none]       - Specify E-Mail POP server address
 3. FTP server               [none]       - Specify FTP server IP address
 4. WWW (HTTP) server        [none]       - Specify WWW server IP address
 5. Telnet server            [none]       - Specify Telnet IP address
 6. Local DNS                [none]       - Specify local DNS IP address
 7. Remote DNS               [none]       - Specify remote DNS IP address
 8. Secondary local DNS      [none]       - Specify local DNS IP address
 9. Secondary remote DNS     [none]       - Specify remote DNS IP address

 Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **DESIGNATED SERVERS MENU** contains options used to define the IP address of specific services on this local or remote site network that may be accessed by devices on other networks. Defining a Designated Server allows for simpler set up when configuring what traffic is to be allowed through the firewall.

**1 - E-mail (SMTP) Server**

The E-mail Server option defines the IP address of the E-mail (SMTP) Server on this network that may be accessed by devices on other networks.

**Default:** [none]

**2 - POP 2/3 Server**

The POP Server option defines the IP address of the POP 2/3 Server on this network that may be accessed by devices on other networks.

**Default:** [none]

**3 - FTP Server**

The FTP Server option defines the IP address of the FTP Server on this network that may be accessed by devices on other networks.

**Note**: depending on the FTP software used, a client may not be able to reach an FTP server through a router using NAPT with firewall security enabled unless a port is opened for user authentication communications. This port may be set up in the Edit Firewall Entry Menu.

**Default:** [none]

**4 - WWW (HTTP) Server**

The WWW Server option defines the IP address of the WWW (HTTP) Server on this network that may be accessed by devices on other networks.

**Default:** [none]

**5 - Telnet Server**

The Telnet Server option defines the IP address of the Telnet Server on this network that may be accessed by devices on other networks.

**Default:** [none]

**6 - Local DNS**

The Local DNS option defines the IP address of the Domain Name Server (DNS) on this network that may be accessed by devices on other networks. This entry allows access to the designated IP address only on port 53.

**Default:** [none]

**7 - Remote DNS**

The Remote DNS option defines the IP address of the Domain Name Server (DNS) on another network that may be accessed by devices on this network. This setting would be used when connecting to an ISP for example and the DNS is located external to your network within the ISP. This entry allows access to the designated IP address on port 53 as well as on ports 1024 to 65535.

**Default:** [none]

**8 - Secondary local DNS**

The Secondary local DNS option defines the IP address of the secondary DNS Server on this network that may be accessed by devices on other network connections. This entry allows access to the designated IP address only on port 53.

**Default:** [none]

**9 – Secondary remote DNS**

The Secondary remote DNS option defines the IP address of the secondary Domain Name Server (DNS) on another network that may be accessed by devices on this network. This entry allows access to the designated IP address on port 53 as well as on ports 1024 to 65535.

**Default:** [none]

## Edit Firewall Entry Menu

```
                          FIREWALL ENTRY MENU

    Option               Value          Description
 1. Destination addr   [         ]   - Destination IP address of frame
 2. Destination mask   [         ]   - Network mask for dest address
 3. Source address     [         ]   - Source IP address of frame
 4. Source mask        [         ]   - Network mask for source address
 5. Protocol type      [         ]   - Allow specific protocol types
 6. Source port        [         ]   - Source port range to allow
 7. Destination port   [         ]   - Destination port range to allow.
 8. Description        [         ]   - Describe the entry
 9. Entry direction    [         ]   - Direction this entry applies to




Enter :
    Firewall filter id (from 1 to 15)

> 1
```

The above display is the first level of the **EDIT FIREWALL ENTRY MENU**. Once the firewall entry index number is entered, the number specified is added to the menu title bar and the Options are as shown below:

```
                        FIREWALL ENTRY 1 MENU

    Option               Value          Description
 1. Destination addr   [none]           - Destination IP address of frame
 2. Destination mask   [none]           - Network mask for dest address
 3. Source address     [all]            - Source IP address of frame
 4. Source mask        [none]           - Network mask for source address
 5. Protocol type      [all]            - Allow specific protocol types
 6. Source port        [0] [65535]      - Source port range to allow
 7. Destination port   [0] [65535]      - Destination port range to allow.
 8. Description        "Manual entry"   - Describe the entry
 9. Entry direction    [outbound]       - Direction this entry applies t




Enter option number, "=" - main menu, <TAB> - previous menu

>
```

A Firewall entry allows the creation of a specific IP connection type of communication path to be allowed through the firewall. The Source IP address of a known network may be defined to be allowed to access either a specific device or network.

**1 - Destination Addr**

The Destination IP Address option defines a hole in the firewall for the IP address (or range of addresses) for frames outbound from this P840 to a destination on the network in question.

The IP address consists of 4 eight-bit fields, each field is specified by a decimal number and the fields are separated by a decimal point (e.g. 92.3.1.10). Each decimal number must be less than or equal to 255 (the maximum decimal value of an 8-bit binary number).

**Default:** [none]

**2 - Destination Mask**

The Destination Mask option defines the address mask to be used on the Destination IP Address defined in option 1 for this entry. To have the firewall entry apply to an individual IP address a mask of none should be used.

The address mask consists of 4 eight-bit fields, each field is specified by a decimal number and the fields are separated by a decimal point (e.g. 92.3.1.10). Each decimal number must be less than or equal to 255 (the maximum decimal value of an 8-bit binary number).

**Default:** [none]

**3 - Source Address**

The Source IP Address option defines a hole in the firewall for the IP address (or range of addresses) for frames inbound to this P840 from the network in question. The default setting of this option allows all IP addresses on this network to send frames out through the P840. Setting specific source IP addresses allows for greater restrictions on who can access external networks.

The IP address consists of 4 eight-bit fields, each field is specified by a decimal number and the fields are separated by a decimal point (e.g. 92.3.1.10). Each decimal number must be less than or equal to 255 (the maximum decimal value of an 8-bit binary number).

**Default:** [all]

**4 - Source Mask**

The Source Mask option defines the address mask to be used on the Source IP Address defined in option 3 for this entry. To have the firewall entry apply to an individual IP address a mask of none should be used.

The address mask consists of 4 octets and is represented by 4 fields separated by periods ("**.**"), where each field is specified by a decimal number (e.g. 255.255.255.0). Each decimal number must be less than or equal to 255, that is the maximum value of each 8-bit field.

**Default:** [none]

**5 - Protocol Type**

The Protocol Type option defines the protocol type to allow through the firewall for this entry. The protocol type may be defined as TCP, UDP, or any other protocol type. Other protocols are defined as a valid IP protocol type in hex.

**Default:** [TCP]

**Choices:** TCP, UDP, (any protocol type number in hex)

**6 - Source Port**

The Source Port option defines the starting and ending port numbers from the Source IP address(es) defined above from which inbound frames are to be allowed through the firewall. The default setting of this option allows all ports from a defined source to send inbound frames through the P840 to other networks. Setting a specific source port or range of ports allows for greater restrictions on who can access external networks.

**Default:** [0] to [65535]

**Range:** 0 to 65535

**7 - Destination Port**

The Destination Port option defines the starting and ending port numbers from the Destination IP address(es) defined above to which outbound frames are to be allowed through the firewall. The default setting of this option allows the P840 to send outbound frames to all ports on a defined IP Destination. Setting specific destination port or range of ports allows for greater restrictions on who can access this network from outside.

**Default:** [0] to [65535]

**Range:** 1 to 65535

**8 - Description**

This option allows a text description of up to 19 characters of this entry in the firewall table. If blank spaces are used in the description, it must be enclosed in double quotation marks.

**9 - Entry direction**

The Entry Direction option determines which direction the filtering operation for this entry will take place. Filtering direction is determined from the point of view of the P840; that is outbound is traffic from the P840 to the network, inbound is from the network to the P840.

*None* will allow the direction selected in the LAN or WAN Firewall setup menu to operate without restriction by this option.

.

*Outbound* will perform filtering of traffic from the P840 to the selected network, i.e. traffic from other networks.

*Inbound* will perform filtering on traffic from the network to the P840; i.e. traffic destined for other networks.

*Both* will filter all traffic.

Note: The direction specified in this option will operate in conjunction with the general direction specified in the LAN or WAN Firewall Set-up menu. For example: a general firewall direction of *Both* would filter all traffic to and from the network to the P840. Setting a specific address entry to have a direction of *Inbound* would then allow the device with that address to communicate through the firewall. Please see the *Installation and Applications Manual* for some specific examples of firewall operation.

By default, the direction in which filtering will be applied for all entries in the firewall table is initially set to the direction specified by the *Firewall support* option (3). This direction may be changed for individual entries using the *Edit firewall entry* option (2). Once an the direction of filtering for some entries has been altered, changing the overall direction applied to the firewall table will not affect those entries that have been changed; if a change is required, each entry that needs to be changed must be edited individually.

## NAT Exports Menu

```
                              NAT EXPORTS MENU

    Option                  Value          Description
 1. Edit Services           menu         - Add/remove exported services
 2. Router port             menu         - Change router server ports for export
 3. Show services                        - Display exported services
 4. Clear services                       - Clear all exported services









Enter option number, "=" - main menu, <TAB> - previous menu


>
```

The **NAT Exports Menu** has options for setting, clearing and reviewing exported Internet services available on this network. Using Network Address Translation (NAT). NAT maps arbitrary internal network IP addresses to valid global IP addresses used on the Internet. Network Address Port Translation (NAPT) allows a number of internal hosts to map to the same global IP address via port assignment to that address. NAT exported services are only available through port translation.

**NOTE:** Exported services from a remote site are only available if NAPT is enabled for that site (under the Configuration/WAN Set-up/Remote Site Set-up/Edit Remote Site/Protocol Set-up/IP Parameters menu).

**1 - EDIT Services**

The Edit Services option takes you to the Edit Services Menu, where the host devices for the various Internet services that will be offered on this network may be added to or removed from the export services table.

**2 - Router Port**

The Router Port option takes you to the Router Port Menu where the port number for services provided by this router may be assigned.

**3 - Show Services**

Displays a list if the Internet services available for export on this network.

**4 - Clear Services**

Clears the NAPT table of IP addresses of services available for export on this network.

## Edit Services Menu

```
                              EDIT SERVICES MENU

    Option                  Value          Description
 1. Other Services          menu         - Add/remove other exported services
 2. E-mail                 [none]        - E-mail server's IP address
 3. POP2/POP3              [none]        - POP2/POP3 server's IP address
 4. FTP                    [none]        - FTP server's IP address
 5. WWW (HTTP)             [none]        - WWW (HTTP) server's IP address
 6. Telnet                 [none]        - Telnet server's IP address
 7. DNS                    [none]        - DNS server's IP address



Enter option number, "=" - main menu, <TAB> - previous menu


>
```

The **EDIT SERVICES MENU** allows you to set the internal IP address of the device where each Internet service that will be available for export on this network can be accessed. The NAT port used for Network Address Port Translation for the services in options 2 through 8 will be the well-known port number for that service.

When a service is added using this menu, it will also be automatically added to the firewall designated servers list, even if firewall is not enabled.

**1 - Other Services**

The Other Services option takes you to a menu where the internal IP address of an Internet service not offered in the list below may be set up.

**2 - E-mail**

The IP address of the E-mail server on this network may be set. (port 25)

**3 - POP2/POP3**

The IP address of the POP2/POP3 server on this network may be set. (POP2 - port 109, POP3 – port 110)

**4 - FTP**

The IP address of the FTP server on this network may be set. (port 21, FTP data – port 20)

**Note**: depending on the FTP software used, a client may not be able to reach an FTP server through a router using NAPT with firewall security enabled unless a port is opened for user authentication communications. See Main/Configuration/Applications/Firewall/ Edit Firewall Entry Menu.

**5 - WWW (HTTP)**

The IP address of the WWW (HTTP) server on this network may be set. (port 80)

**6 - Telnet**

The IP address of the Telnet server on this network may be set. (port 23)

**7 - DNS**

The IP address of the DNS server on this network may be set. (port 53)

## Other Services Menu

```
                              OTHER SERVICES MENU

    Option                 Value          Description
 1. NAT port             *[      ]      - Port number exported by NAT
 2. Status               *[      ]      - Is service in export's table?
 3. Host IP address       [      ]      - Enter location of service
 4. Host port             [      ]      - Enter port number of service on host
 5. Description           [      ]      - Describe the service
 6. Remove                              - Remove the service


Enter option number, "=" - main menu, <TAB> - previous menu


>
```

The **OTHER SERVICES MENU** allows the set up of an Internet service not listed in the Edit Services menu.

**1 - NAT Port**

This option displays the port number that NAT will use to export this service

**Range:** 1 to 65535

**2 - Status**

This option displays whether or not this port has an IP address present in the export table and is being used by another service. If the port is already present in the table, the host address and port will be displayed and may be changed; the NAT Port and Status for this entry may not be changed if already present – you must return to the previous menu, re-enter this one and use another port number.

**Default:** [not present]

**3 - Host IP Address**

Enter the internal IP address of the host for this service.

**Default:** [0.0.0.0]

**4 - Host Port**

Enter the internal port number of the host for this service.

**Default:** [port number entered for NAT Port]

**Range:** 1 to 65535

**5 - Description**

Enter a description of the service. If blank spaces are used in the description, it must be enclosed in double quotation marks.

**Range:** up to 20 characters

**6 - Remove**

Remove this service from the export table. The service must be present in the export table before this option will be displayed.

## Router Port Menu

```
                              ROUTER PORT MENU

    Option            Value          Description
 1. Telnet           [default]      - Change telnet server ports for export
 2. TFTP             [default]      - Change TFTP server ports for export
 3. SNMP             [default]      - Change SNMP server ports for export




Enter option number, "=" - main menu, <TAB> - previous menu


>
```

The **EDIT ROUTER SERVICES MENU** contains options to set alternate port numbers to export the Telnet, TFTP and SNMP services of this router. If one of these services is offered on another server through NAT, then that server will use the well-known port number for that service; this router must use a different port number for its service.

**1 - Telnet**

The Telnet option defines a port number to use for Telnet services on this router.

**2 - TFTP**

The TFTP option defines a port number to use for TFTP services on this router.

**3 - SNMP**

The SNMP option defines a port number to use for SNMP services on this router.

## SYSLOG Set-Up Menu

```
                              SYSLOG SET-UP MENU

    Option                 Value          Description
 1. Syslog                 [enabled]    - Enable/disable syslog logging
 2. Syslog IP address      [none]       - Define host IP address
 3. Events facility        [none]       - Define network events facility
 4. Security facility      [none]       - Define security facility
 5. Activation facility    [local2]     - Define activation facility
 6. Firewall facility      [none]       - Define firewall facility



Enter option number, "=" - main menu, <TAB> - previous menu


>
```

The **SYSLOG Set-Up Menu** configures this P840 to send messages to a standard Syslog service running on a specified host. Syslog is a utility, typically on a UNIX type system but also available for other systems, that forwards system messages to a user selected destination, known as a facility. A facility may be a file, another device, such as a printer, or another utility, such as an e-mail service. A listing of available facilities is given at the end of this section. It is recommended that you choose the "local*n*" facilities for logging messages from this router unless you are certain that a specified facility is not used by any other part of the system.

For a listing of system messages and their descriptions, please see Appendix A of the P840 Reference Manual file on the accompanying disk. For information on Syslog, please see your UNIX (or equivalent) operating system reference manual.

This router will generate one of four classes of message: events, security, activation or firewall. Each type may be sent to a separate facility. All messages are sent at severity level 6 (information level).

**Note:** if Syslog is set up to send messages to a host across a WAN link and spoofing or traffic initiated connection is enabled, the link will be brought up every time a system event occurs, i.e. very frequently. Depending on how link service charges are accrued, this may not be desirable. It is recommended that the Syslog host be on the same LAN as this router.

**Note:** Time of day should be synchronized between this P840 and the Syslog daemon host; if this is not done, interpreting a sequence of logged events becomes more difficult.

**1 – Syslog**

The Syslog option toggles the Syslog operation between enabled and disabled.

**Default:** [disabled]

**2 – Syslog IP address**

Enter the IP address of the Syslog host to which the system messages are to be forwarded for logging.

**3 – Events Facility**

A network event message generated by this router will be forwarded to the selected facility for logging on the Syslog host.

**Default:** [none]

**Choices:** (see below for details)
none, local0, local1, local2, local3, local4, local5, local6, local7,
auth, cron, daemon, kern, lpr, mail, news, syslog, user, uucp

**4 – Security Facility**

A security message generated by this router will be forwarded to the selected facility for logging on the Syslog host.

**Default:** [none]

**Choices:** (see below for details)
none, local0, local1, local2, local3, local4, local5, local6, local7,
auth, cron, daemon, kern, lpr, mail, news, syslog, user, uucp

**5 – Activation Facility**

An activation message generated by this router will be forwarded to the selected facility for logging on the Syslog host.

**Default:** [none]

**Choices:**
none, local0, local1, local2, local3, local4, local5, local6, local7,
auth, cron, daemon, kern, lpr, mail, news, syslog, user, uucp

**6 – Firewall Facility**

A firewall message generated by this router will be forwarded to the selected facility for logging on the Syslog host.

**Default:** [none]

**Choices:**
none, local0, local1, local2, local3, local4, local5, local6, local7,
auth, cron, daemon, kern, lpr, mail, news, syslog, user, uucp

**Facilities available on Syslog:**

| | |
|---|---|
| none | Message will not be sent |
| local0-7 | Reserved for user defined service – recommended choice. |
| user | Messages generated by user processes. |
| kern | Messages generated by the kernel. |
| mail | The mail system. |
| daemon | System daemons, such as ftpd(1M), routed(1M), etc. |
| auth | The authorization system: login(1), su(1M), getty(1M), etc. |
| syslog | Syslog daemon |
| lpr | The line printer spooling system: lpr(1), lpc(1M), lpd(1M), etc. |
| news | Reserved for the USENET network news system. |
| uucp | Reserved for the UUCP system. |
| cron | The cron/at facility; crontab(1), at(1), cron(1M), etc. |

## SNTP Set-up Menu

```
                              SNTP SETUP MENU

    Option                Value              Description
 1. SNTP Mode             [none]             - Set SNTP operational mode
 2. Primary IP Address    [171.45.24.1]      - Primary server IP Address
 3. Secondary IP Address  ]171.45.24.2]      - Secondary server IP Address
 4. Version               [3]                - SNTP version
 5. Status                                - Display SNTP status


Enter option number, "=" - main menu, <TAB> - previous menu

>
```

The **SNTP SETUP MENU** contains SNTP options to set the SNTP protocol version and operational mode in which to obtain the network clock from a SNTP or NTP server.

**1 – SNTP Mode**

The SNTP Mode option enabled SNTP within the router. Setting the SNTP mode to *none* will disable the SNTP feature on the router. *Unicast* option will display the primary and secondary server IP Address options to specify the server in which to send request time packets. In *Multicast* mode, the router will wait to receive a broadcast from any NTP server to and adjust the router's internal clock. In *anycast* mode, the router will send a IP broadcast on the LAN and the first NTP server to response the router to continue then to communicate with that particular NTP server to obtain the network time.

**Default:** [none]
**Range:** none, unicast, multicast, anycast

**2 – Primary IP Address**

The Primary IP Address option defines the IP Address of the primary NTP server you wish to obtain the time from. This option is only displayed in *unicast* mode. 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. 92.3.1.10). Each decimal number must be less than or equal to 255, that is the maximum value of each 8-bit field.

**Default:** [none]

**3 – Secondary IP Address**

The Seconday IP Address option defines the IP Address of the secondary NTP server you wish to obtain the time from. This option is only displayed in *unicast* mode. 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. 92.3.1.10). Each decimal number must be less than or equal to 255, that is the maximum value of each 8-bit field.

**Default:** [none]

**4 – Version**

The Version option specifies the type of SNTP version you wish to communicate with and is put in the request packet when communicating with the NTP server.

**Default:** 3
**Range:** 1 to 4

**5 – Status**

The Status option displays SNTP information regarding the packets received from the SNTP server and updated status regarding the changes that have taken place with the router's internal clock.

```
        SNTP STATUS
        ===========

        Server IP Address:      172.16.33.200
        Last Update:            2003-06-12  14:41:53 UTC (yyyy-mm-dd hh:mm:ss)
        Leap Indicator:         0
        Version:                3
        Mode:                   4
        Stratum:                5
        Reference Identifier:   7f7f0100
        Correction:             -0 seconds


Type : [s] to redraw, [=] main menu any other key to end.
>
```

Each SNTP status item is described below:

**Server IP Address**
The IP Address of the SNTP or NTP server that last sent the router an NTP message reply with an updated time reference

**Last Update**
The time that the last SNTP or NTP server updated the internal clock on the router

**Leap Indicator, Version, Mode, Stratum and Reference Identifier**
Theses field values are obtained from the last SNTP server message received. The fields are fully described with RFC 2030, Simple Network Time Protocol Version 4.

**Correction**
The correction filed is the number of seconds that the router internal clock was changed when the last SNTP message was received.

## Statistics Menu

```
                              STATISTICS MENU

    Option                          Value         Description
 1. Statistics set-up               menu        - Define statistics operation
 2. Remote site information         menu        - Remote site stats/status
 3. LAN statistics                  menu        - Access LAN statistics
 4. Link stats                                  - Detailed link statistics
 5. Link summary                                - Summary stats of all links
 6. Interface stats                             - Statistics of all interfaces
 7. Interface status                            - Status of all interfaces
 8. Clear statistics                            - Reset link & interface stats




Enter option number, "=" - main menu, <TAB> - previous menu


>
```

The **STATISTICS MENU** provides access to complete router statistics and status displays.

**1 - Statistics Set-Up**

The Statistics Set-up option takes you to the Statistics Set-Up Menu, where the interval and the range of reported statistics may be set. All statistics counts may also be reset from this menu.

**2 – Remote Site Information**

The Remote Site Information option takes you to the Remote Site Information Menu, where remote site statistics, status and usage information can be examined.

**3 - LAN Statistics**

The LAN Statistics option takes you to the LAN Statistics Menu, where statistics can be examined to evaluate LAN performance.

**4 - Link Stats Display**

```
Enter:
   Link to display (1 or 2)
```

The link to display must first be entered, the stats for that link will then be displayed:

```
                                  Link  1 Status
State: Enabled, Up, Network, Opened
Remote Site: Atlanta

Interface State         Frame Counts  (Rcv/Xmt)       Frame Errors
Speed   : 64000 bps     Bytes :      47648/47639       Cgt disc   : 0
Type    : BRI           Frames:       3536/3536        CRC        : 0
Circuit : Outgoing                                     Rcv abort  : 0
State   : IDLE                                       Overrun    : 0
                                                       Rcv miss   : 0
Partner Number:                                        Too large  : 0
5551212                                                Misaligned : 0
                                                       Underrun   : 0
                              Throughput
Rcv   0%       0.0 KB |
Xmt   0%       0.0 KB |
                      |----|----|----|----|----|----|----|----|----|----|
                     0   10   20   30   40   50   60   70   80   90  100%
```

**State :**

This identifies the current state of the ISDN call. The state may be one of "Idle, Proceeding, Disconnecting, or Connected".

**Remote Site :**

This displays the name of the current remote site to which this link is connected.

**Speed :**

This displays the speed at which the link is operating. The speed will be as set by the connection. If the link is disconnected, no speed (0) will be shown.

**Type :**

The interface type is identified in this display.

**Frame Counts**

**Bytes :**

This indicates the total number of bytes received/transmitted across the link.

**Frames :**

This indicates the total number of frames received/transmitted across the link.

**Frame Errors**

These frames are considered invalid because they do not conform to valid frame checking parameters. These frames usually result from a hardware error on either the LAN or the router.

**Cgt Disc** Congestion Discards — This is generated when a frame is discarded due to congestion.

**CRC** Cyclic Redundancy Check — This often indicates a problem with the transmitting hardware and/or communications line (a modem, noisy line, router link problem) that has been detected by the receiver.

**Rcv abort** Receiver Abort — This reports that an incoming frame has been aborted. This results when the transmitter doesn't receive all of a frame to be sent, and it sets an abort flag at the point this is discovered in the transmission. The receiver notes this as a statistic and discards the frame.

**Overrun** The link controller could not empty the link FIFO into common memory before the next frame from the link is written to the FIFO. This indicates a problem with the memory inside the router.

**Rcv miss** Receiver Miss — This reports that an incoming frame has been aborted. This results when the frame is missed because of a lack of receive buffers. The remote router will retransmit the frame.

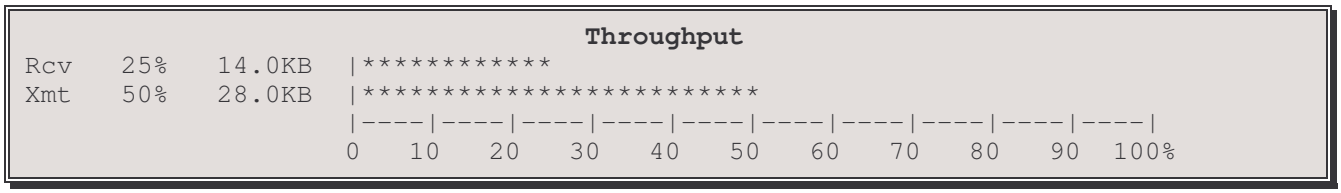
**Too large** This reports that an incoming frame has been discarded because the frame exceeded the maximum length. This may be caused by a frame being overrun by another frame on the link, so that the router thinks both frames are one frame.

**Misaligned** This reports that frames detected on this link have a number of bits not exactly divisible by eight.

**Underrun** The link controller could not read the rest of the frame from common memory before the link FIFO emptied. This indicates a problem with the memory inside the router.

**Throughput**

Both receive and transmit call utilization are displayed by the two bar graphs. Utilization describes the total bits received or sent (including protocol overhead) divided by the total bits possible based on the call speed. For each statistic, the numerical percentage is printed along with its equivalent baud rate and the bar graph.




**Circuit :**

This identifies the type of ISDN call. The call may be "Incoming, Outgoing, or Cleared".

**State :**

This identifies the current state of the ISDN call. The state may be one of "Idle, Proceeding, Disconnecting, or Connected".

**Partner Number :**

This identifies the ISDN number of the remotely connected PPP ISDN router.

**5 – Link Summary**

```
                                Link Summary

Link       Link       Remote Site        Throughput          %        Frame
 ID     Type/State      Alias          Kbps (Rcv/Xmt)    (Rcv/Xmt)   Errors
----  ------------ ---------------- ------------------------------ ----------
  1     ISDN/Up       DEV012345           0.0/0.0          0/0            0
  2     ISDN/Down        none             0.0/0.0          0/0            0
```

**Link ID :**

The link numbers (1 to 2).

**Link Type/State :**

The link module types and states of each link.

**Remte Site Alias :**

The names assigned to the remote sites currently associated with each link.

**Throughput :**

The received and transmitted throughput rates for each link in kilobits per second.

**% :**

The received and transmitted throughput as a percentage of the available link speed.

**Frame Errors :**

The number of invalid frames received on each link since the last "Clear link statistics" command.

**6 – Interface Statistics**

```
                          Interface Statistics

Interface#            Total Frames (Rcv/Tx)          Total Bytes (Rcv/Tx)
----------            ---------------------          --------------------
  0                          2/106                        128/0
  1                          0/0                            0/0
```

**Interface # :**

The interface module number. Interface 0 is the primary LAN interface. A BRI interface pair will display only as interface 1, as in the example above. All other interface types will show as interface 1 and interface 2.

**Total Frames :**

The count of frames received and transmitted through this interface since the stats were last cleared.

**Total Bytes :**

The count of bytes received and transmitted through this interface since the stats were last cleared.

**7 – Interface Status**

```
                              Interface Status

 Interface    Interface           Link#    Logical              Interface
 number        Type                        Type                 Speed(Kbps)
---------   -------------------   -----   ------------------   -----------
   0          10BaseT              NA     LAN                   10000
   1          BRI ST               1,2    ISDN                     64
```

**Interface number :**

The interface number.

**Interface Type :**

The physical type of interface module installed on this interface.

**Link # :**

The link number associated with this interface.

**Logical Type :**

The logical type assigned to this interface.

**Interface speed :**

The nominal data transfer rate for this interface in kilobytes per second.

**8 - Clear Statistics**

The Clear Statistics option clears all fields in the Link statistics to zero.
.

## Statistics Set-Up Menu

```
                          STATISTICS SET-UP MENU

    Option                  Value         Description
 1. Extended statistics    [disabled]   - Enable/disable extended statistics
 2. Interval               [60 sec]     - Set display interval
 3. Clear all statistics                - Reset all statistics




Enter option number, "=" - main menu, <TAB> - previous menu

>
```

**1 - Extended Statistics**

Choosing the Extended Statistics option enables extended statistics causing additional statistics to be calculated and reported.

When extended stats are [disabled], limited information is available from:
- **Link Status**, WAN Statistics Menu (throughput section is not available).
- **Bridged Traffic**, LAN Statistics Menu (only the total column is available).
- **IP Traffic**, LAN Statistics Menu (only the total column is available).
- **Total LAN Traffic**, LAN Statistics Menu (only the total column is available).

**Default:** [disabled]

**Considerations:**

Enabling this option will decrease router performance, as additional processing is required. You must confirm a change by entering "yes" at the prompt.

**2 - Interval**

The Interval option sets the timer that updates the statistics.

**Default:** [60 sec]

**Range:** 10 to 3,600 seconds.

**Considerations:**

Lowering the time interval will require more router processing power while increasing the time interval will require less.

**3 - Clear All Statistics**

The Clear All Statistics option clears ALL of the statistics and resets all fields to zero.

## Remote Site Information Menu

```
                        REMOTE SITE INFORMATION MENU

    Option                          Description
 1. Common protocols stats       - Counts of IP/IPX/Brg Frames
 2. PPP statistics               - Total counts of PPP protocols
 3. Status                       - Status of a particular RMS
 4. Usage information            - Display usage information
 5. Clear remote site stats      - Reset remote site statistics




Enter :
    Remote site id or alias (up to 16 characters)

>
```

The above display is the first level of the **REMOTE SITE INFORMATION MENU**. Once the remote site identification number or alias is entered, the alias of the specified remote site is added to the menu title bar and the Options are as shown below:

```
                     REMOTE SITE INFORMATION test1 MENU

    Option                          Description
 1. Common protocols stats       - Counts of IP/IPX/Brg Frames
 2. PPP statistics               - Total counts of PPP protocols
 3. Frame Relay statistics       - Total counts of FR protocol
 4. Status                       - Status of a particular RMS
 5. Usage information            - Display usage information
 6. Clear remote site stats      - Reset remote site statistics









Enter option number, "=" - main menu, <TAB> - previous menu

>
```

**1 – Common Protocol Stats**

```
                          Common Protocols Stats

                      Remote Site Name: test1 (Id: 1)
Frame Type        Total Counts    Average Rate    Recent Rate    Highest Rate
----------        ------------    ------------    -----------    ------------
All Rcvd                     0
All Tx                       0

IP Rcvd                      0
IP Tx                        0
IP Rcv Discards              0
IP Tx Discards               0


Brg Rcvd                     0
Brg Tx                       0
Brg Rcv Discards             0
Brg Tx Discards              0
```

The Common Protocol Stats display lists frame counts with number of frames received, transmitted and discarded for each of the various transmission protocols.

**Frame Type** The frame transmission protocol

**Total Counts** The total number of occurrences since the statistics were last reset.

**Average Rate** The average rate of occurrences per second since the statistics were last reset.

**Recent Rate** The averaged rate of occurrences per second of the last statistics interval.

**Highest Rate** The highest recent rate encountered since the statistics were last reset or a re-powering of the bridge/router occurred.

**2 - PPP Stats**

```
                                PPP Stats

                        Remote Site Name: test1 (Id: 1)
Frame Types          Total (Rcvd/Tx)      Frame Types          Total(Rcvd/Tx)
-------------      --------------------  -------------      ------------------
IPXCP                      0/0           CMCP                       0/0

IPCP                       0/0           BCP                        0/0
VJ Compression             0/0           BPDU                       0/0
VJ Uncompression           0/0           BPDU Discards              0/0

LCP                        0/0           BACP                       0/0
LCP Discard                0/0           BAP                        0/0
LQR                        0/0           BAP Discard                0/0
PAP                        0/0
CHAP                       0/0
```

Screen 1 of PPP Stats display

```
                                PPP Stats

                        Remote Site Name: test1 (Id: 1)
Frame Types          Total (Rcvd/Tx)      Frame Types          Total(Rcvd/Tx)
-------------      --------------------  -------------      ------------------
MP Frames                  0/0           CCP                        0/0
MP Fragments               0/0           Reset Req                  0/0
Frame Header Err           0/-           Reset Ack                  0/0
Frag Header Err            0/-           Restarts                   0/-
Frame Discards             0/-           Resynchs                   0/-
Frag Discards              0/-           Cmprs Discards             0/0
                                         Zero Pad                   0/-
                                         Decompress Err             9/-
                                         Recent Comp Ratio        -:-/-:-
                                         Avrg Comp Ratio          -:-/-:-
```

Screen 2 of PPP Stats display

The PPP Stats display shows frame counts received and transmitted for each of the frame types listed.

Note that the PPP Stats display does not do on screen updates; to update the screen display, switch screens with the “n” (next) or “p” (previous) key or tab out and key “2” to re-enter this display. Note: the “n” or “p” must be lower case.

```
                          Frame Relay Stats
                  Remote Site Name: test2_Leased (Id: 4)


Frame Types          Frame Counts
------------         ----------------
Frames Rcvd                   0
Frames Tx                     0
Frames Discards Rcv           0
Frames Discards Tx            0
FECN Frames Rcv               0
BECN Frames Rcv               0
```

This display shows counts of:

**Frames Rcvd:** Frames received since the statistics were last cleared.

**Frames Tx:** Frames transmitted since the statistics were last cleared.

**Frames Discards Rcvd:** Received Frames discarded since the statistics were last cleared.

**Frames Discards Tx:** Transmitted Frames discarded since the statistics were last cleared.

**FECN:** Forward Explicit Congestion Notification Frames received since the statistics were last cleared (high count indicates possible link congestion for received traffic).

**BECN:** Backward Explicit Congestion Notification received since the statistics were last cleared (high count indicates possible link congestion for transmitted traffic).

**3/4 - Status**

Status of a remote site connection is displayed on a series of screens. To navigate from one display to another, enter "n" to go to the next screen, "p" to go to the previous screen, "s" to go to the starting screen or any other key to return to the Remote Site Stats Menu. Note: the "n", "p" and "s" are case sensitive; they must be lower case. The display will vary depending on the type of connection to the selected remote site; the status of more than one protocol option may be displayed on a screen.

**Status – ISDN Link**

```
                          Protocols Configurations
                      Remote Site Name: test_ISDN (Id: 1)

    * - Up   E - Enabled   D - Disabled   NA - Not Available
FR   AC  MP      Pri/Sec    DLCI  BCP  IPCP  CCP  BACP CMCP
---  --  --  -------------  ----  ---  ----  ---- ---  ----
D    D   E   Link04/none    NA    E    E     E     E    E
```

**Protocol Status – Frame Relay**

```
                          Protocols Configurations
                      Remote Site Name: test_FRELAY (Id: 3)

    * - Up   E - Enabled   D - Disabled   NA - Not Available
FR   AC  MP      Pri/Sec    DLCI  BCP  IPCP  CCP  BACP CMCP
---  --  --  -------------  ----  ---  ----  ---- ---  ----
PPP  D   E     none/none    16    E    E     E    NA    NA
```

**FR :** Frame Relay PPP, Raw 1490 or disabled for this remote site.

**AC :** Auto-call enabled / disabled for this remote site.

**MP :** Multipoint enabled / disabled for this remote site.

**Pri/Sec :** The Primary and Secondary (if applicable) links for this remote site.

**BCP :** Bridge Control Protocol enabled / disabled status.

**IPCP :** IP Control Protocol enabled / disabled status.

**CCP :** Compression Control Protocol enabled / disabled status.

**BACP :** Bandwidth Allocation Control Protocol enabled / disabled status (if this is an ISDN connection, otherwise Not Applicable).

**CMCP :** Connection Management Control Protocol enabled / disabled status (if this is an ISDN connection, otherwise Not Applicable).

**Protocol Configurations – Frame Relay**

```
                                        FR
PVC State     : Disabled, Idle
Link/DLCI     : 0/16
CIR/EIR       : 0/0 Kbps
```

**PVC State:**

The state of the permanent Virtual Circuit on this link: whether the link is Enabled or Disabled, and if enabled, whether it is Idle, Up, Opening or PPP Opening.

**Link/DLCI:**

The Link and Data Link Circuit Identifier numbers associated with this remote site

**CIR/EIR:**

The Committed Information Rate and Excessive (burst) Information Rate for this link.

**Protocol Configurations – BCP**

```
 Status                   Local                    Remote
                                  BCP
802.3/Ethernet        :  disabled                 disabled
Tinygram Compression  :  disabled                 disabled
MAC Address           :  00-00-00-00-00-00        00-00-00-00-00-00
```

**802.3/Ethernet:**

This displays the resulting bridging state for this protocol after the advisory notices are sent by the local and remote bridges. The advisory notices indicate what frame types are supported by the device.

This may display disabled if the partner bridge sends a configure reject for the advisory notice for this frame type. When this happens, the device that originally sent the advisory notice will continue to send bridge frames in the frame formats originally reported in the advisory notice.

**Tinygram Compression:**

This displays the negotiated state of Tinygram Compression for the local and remote devices.

**MAC Address:**

This displays the MAC addresses of the local and remote devices which are used for bridging data between the devices.

**Protocol Status – BACP**

```
 Status                   Local                    Remote
                                  BACP
Magic Number          :  1850971031               1851377123
Call Mode             :  Partner
Request number Option:   disabled
```

**Magic Number:**

This displays the control code numbers passed between the two routers. The router with the lower magic number will have control of setting up and tearing down the connection.

**Call Mode:**

This displays the selected origination of the secondary call to this remote site.

**Request number Option:**

The status of the Request number option for obtaining the ISDN number of the partner router.

**Protocol Status – CCP**

```
Status                  Local                    Remote
                                 CCP
Protocol              : Stac LZS (17)            Stac LZS (17)
Histories             :  1                        1
Check mode            :  Sequence Number         Sequence Number
```

**Protocol :**

This displays the current compression protocol for this end of the CCP link connection as well as the compression protocol for the remote end.

**Histories :**

This displays the current number of histories which have been negotiated for both the local end and the remote end of the connection.

**Check Mode :**

This displays the compression check modes, which have been negotiated for both the local end and the remote end of the connection.

**Protocol Status – IPCP**

```
 Status                  Local                    Remote
                                 IPCP
IP Address            :  0.0.0.0                 0.0.0.0
Subnet Mask Size      :  0                       0
Link IP type          :  unNumbered
VJ Compression        :  none                    none
Max slot id           :  0                       0
Slot id Comp          :  disabled                disabled
```

**IP Address :**

This displays the current IP addresses for this end of the IPCP link connection as well as the IP address for the remote end.

**Subnet Mask Size :**

This displays the current subnet mask size for this end of the IPCP link connection as well as the subnet mask size for the remote end.

**Link IP Type :**

This displays the type of IP link connection between this P840 and the remote site router, either numbered or unnumbered.

**VJ Compression :**

This displays the negotiated type of compression protocol for this end of the IPCP link connection as well as the compression protocol for the remote end: none, VJ TCP.

**Max Slot Id :**

This displays the negotiated value for the Van Jacobson max slot identifier for this end of the IPCP link connection as well as the value for the Van Jacobson max slot identifier for the remote end.

**Slot Id Comp :**

This displays the negotiated state of the Van Jacobson slot identifier compression for this end of the IPCP link connection as well as the state of the Van Jacobson slot identifier compression for the remote end.

**Protocol Status – Multilink**

```
 Status                    Local                      Remote
                                  Multilink
MRRU                   :  1800                       1800
SSNHF                  :  normal                     normal

Local  EPD             :  class MAC 00-00-d0-00-d1-1a
Remote EPD             :  class MAC 00-00-d0-00-af-1f
```

**MRRU :**

This displays the negotiated MRRU (Maximum Receive Reconstructed Unit) value for this end of the link connection as well as the MRRU value for the remote end.

**SSNHF :**

This displays the negotiated SSNHF (Short Sequence Number Header Format ) value for this end of the link connection as well as the SSNHF value for the remote end: normal / short.

**EPD :**

This displays the negotiated EPD (End Point Discriminator) value for this end of the link connection and the EPD value for the remote end.

**Protocol Status – CMCP**

```
 Status                    Local                      Remote
                                  CMCP
Callback number  1     :  6681048                    2447072
Callback number  2     :  9954321                    3435566
```

**Callback number n:**

This displays the callback ISDN numbers used by each interface and by the remote site connected to that interface.

**4/5 – Usage information**

```
                          Usage Summary
                    Remote Site Name: test1 (Id: 1)

  Day of Week     Usage          Outgoing Calls
  Sunday      : 0      min       0       calls
  Monday      : 0      min       0       calls
  Tuesday     : 0      min       0       calls
  Wednesday   : 0      min       0       calls
  Thursday    : 0      min       0       calls
  Friday      : 0      min       0       calls
  Saturday    : 0      min       0       calls

  Current     : 0      min       0       calls
```

Note: The day-of-weeks are the 24-hour time intervals starting from 7:00 the same day.

**Usage :**

This displays the total number of minutes of line usage.

**Outgoing Calls :**

This displays the total number of outgoing calls to this remote site for the indicated day of the week.

**5/6 Clear Remote Site Stats**

The Clear Remote Site Statistics option clears all fields in all of the remote site statistics displays to zero.

## LAN Statistics Menu

```
                          LAN STATISTICS MENU

   Option                      Description
 1. Bridged traffic         - Summary of Bridge traffic
 2. IP traffic              - Summary of IP Router traffic
 3. Total LAN traffic       - Summary of LAN traffic
 4. LAN error               - View LAN errors history
 5. Clear LAN statistics    - Reset LAN statistics
 6. Clear LAN errors        - Reset LAN errors




Enter option number, "=" - main menu, <TAB> - previous menu

>
```

**1 - Bridged Traffic**

The Bridged Traffic option displays a summary of Bridged LAN traffic since the statistics were last reset.

**2 - IP Traffic**

The IP Traffic option displays a summary of IP Router LAN traffic since the statistics were last reset.

**Note**: only statistics on the primary LAN are kept, none are available for secondary LANs.

**3 - Total LAN Traffic**

The Total LAN Traffic option displays a summary of Total LAN traffic since the statistics were last reset.

**4 - LAN Error**

The LAN Error option displays a summary of LAN and router errors since the statistics were last reset.

**5 - Clear LAN Statistics**

The Clear LAN Statistics option clears all statistic fields in the LAN statistics to zero.

**6 - Clear LAN Errors**

The Clear LAN Errors option clears all error fields in the LAN statistics to zero.

**Bridged Traffic Summary Display (Option 1)**

This screen displays Bridged LAN traffic statistics gathered since the statistics were last reset and reports statistics generated within the current statistics interval.

```
                        Bridged Traffic Summary for LAN
                                                 Average     Recent     Highest
Statistic                              Total      Rate       Rate       Rate
-------------------------------------------------------------------------------
Frames from LAN                            0
Bytes from LAN                             0
Frames filtered from LAN                   0
Frames to LAN                              0
Bytes to LAN                               0




Type: [s] to redraw, [=] main menu, any other key to end.
```

**note:** the[ s] to redraw is case sensitive; it must be lower case.

If a second LAN module is present, statistics for both LANs will be displayed.

**Column Analysis**

**Total** Indicates the total number of occurrences since the statistics were last reset. (Available with extended statistics disabled.)

**Average Rate** Indicates the average rate of occurrences per second since the statistics were last reset.

**Recent Rate** Indicates the averaged rate of occurrences per second of the last statistics interval.

**Highest Rate** Indicates the highest recent rate encountered since the statistics were last reset or a re-powering of the router occurred.

## Bridged Traffic Summary Statistics Definitions

| | |
|---|---|
| **Frames from LAN** | All bridge data frames successfully received from the LAN. |
| **Bytes from LAN** | All bridge data bytes successfully received from the LAN. |
| **Frames filtered from LAN** | All bridge data frames received from the LAN and filtered by the router. This includes frames filtered because the frame meets pattern filtering criteria or the frame was unsuccessfully received because of an error. |
| **Frames to LAN** | All bridge data frames successfully placed upon the LAN. |
| **Bytes to LAN** | All bridge data bytes successfully placed upon the LAN. |

**IP Traffic Summary Display (Option 2)**

This screen displays IP Routed LAN traffic statistics gathered since the statistics were last reset and reports statistics generated within the current statistics interval.

```
                          IP Traffic Summary for LAN
                                              Average      Recent     Highest
Statistic                            Total        Rate        Rate        Rate
-------------------------------------------------------------------------------
Frames from LAN                          0
Bytes from LAN                           0
Frames filtered from LAN                 0
Frames to LAN                          780
Bytes to LAN                         59060
ARP Discards From LAN                    0
Redirect Sent From LAN                   0
Unreachable Sent From LAN                0


Type: [s] to redraw, [=] main menu, any other key to end.
```

**note:** the[ s] to redraw is case sensitive; it must be lower case.

If a second LAN module is present, statistics for both LANs will be displayed.

**Column Analysis**

**Total** Indicates the total number of occurrences since the statistics were last reset. (Available with extended statistics disabled.)

**Average Rate** Indicates the average rate of occurrences per second since the statistics were last reset.

**Recent Rate** Indicates the averaged rate of occurrences per second of the last statistics interval.

**Highest Rate** Indicates the highest recent rate encountered since the statistics were last reset or a re-powering of the router occurred.

| IP Traffic Summary Statistics Definitions | |
|---|---|
| **Frames from LAN** | All IP frames successfully received from the LAN. |
| **Bytes from LAN** | All IP bytes successfully received from the LAN. |
| **Frames filtered from LAN** | All IP frames received from the LAN and filtered by the router. This includes IP frames filtered because the frame meets pattern filtering criteria or the frame was unsuccessfully received because of an error. |
| **Frames to LAN** | All IP frames successfully received from partner routers and placed upon the LAN. |
| **Bytes to LAN** | All IP bytes successfully received from partner routers and placed upon the LAN. |
| **ARP Discards from LAN** | Data frames discarded because local LAN stations not responding to an ARP request. This occurs when an IP frame destined for this LAN is received from a partner router, but there is no entry in the ARP table for that IP address, and the station does not respond to an ARP request. |
| **Redirect Sent from LAN** | The number of ICMP Redirect messages generated. |
| **Unreachable Sent from LAN** | The number of ICMP Destination Unreachable messages generated. |

NOTE: The IP frames and bytes in the above table refer to frames properly routed to this router. A properly routed frame will be MAC addressed to the router and IP addressed for a station on another network or sub-network.

**Total LAN Traffic Summary Display (Option 3)**

This screen displays statistics gathered since the statistics were last reset and reports statistics generated within the current statistics interval.

```
                          Total LAN Traffic Summary


                                        Average      Recent     Highest
Statistic                      Total      Rate        Rate        Rate
-------------------------------------------------------------------------
Frames from LAN              4348699       228         416         840
Bytes from LAN             278317248     14616       26667       53785
Frames filtered from LAN       132982         6           0         840
Adapter discards                    0         0           0           0
Congestion discards from LAN        0         0           0           0

Frames forwarded             4215689       221         416         441
Bytes forwarded            269806208     14171       26667       28236
Frames to LAN                4169752       219         416         441
Bytes to LAN               268464916     14024       26667       28250
Congestion discards to LAN         0         0           0           0




Type: [s] to redraw, [=] main menu, any other key to end.
```

**note:** the[ s] to redraw is case sensitive; it must be lower case.

If a second LAN module is present, you will be asked to select which LAN statistics to display.

**Column Analysis**

| | |
|---|---|
| **Total** | Indicates the total number of occurrences since the statistics were last reset. (Available with extended statistics disabled.) |
| **Average Rate** | Indicates the average rate of occurrences per second since the statistics were last reset. |
| **Recent Rate** | Indicates the averaged rate of occurrences per second of the last statistics interval. |
| **Highest Rate** | Indicates the highest recent rate encountered since the statistics were last reset or a re-powering of the router occurred. |

| Total LAN Traffic Summary Statistics Definitions | |
|---|---|
| **Frames from LAN** | All frames successfully received from the local LAN. |
| **Bytes from LAN** | All bytes successfully received from the local LAN. |
| **Frames filtered from LAN** | All frames received from the local LAN and filtered by the router. This includes frames filtered because the router is in Learn mode, the destination address resides on the same LAN, the source address is specified for filtering, or the frame meets pattern filtering criteria. |
| **Adapter Discards** | All incoming frames lost because of an overflow error, receive buffer congest, missed frame detection, CRC errors, or framing errors. This is a case where LAN traffic exceeds the processing capability of the router, primarily because the router is engaged in other functions such as filtering. |
| **Congestion Discards from LAN** | This occurs when the router has to discard frames from the LAN because too many frames are waiting for processing inside the router and buffer space is unavailable. |
| **Frames Forwarded** | All frames successfully forwarded to partner routers. |
| **Bytes Forwarded** | All bytes successfully forwarded to partner routers. |
| **Frames To LAN** | All frames successfully placed upon the local LAN. |
| **Bytes To LAN** | All bytes successfully placed upon the local LAN. |
| **Congestion Discards to LAN** | This occurs when the router has to discard frames destined for the local LAN because too many frames are waiting for processing inside the router and buffer space is unavailable. |

**LAN Error Display (Option 4)**

```
                        LAN Calgary Error Summary

Device Errors                              LAN Errors
-------------------------------------------------------------------------------
Loss of Carrier           : 0              CRC Errors                 : 0
Transmit Babble Errors    : 0              Framing Errors             : 0
Underflow Errors          : 0              Single Collision           : 0
Overflow Errors           : 0              Multiple Collisions        : 0
Receive Buffer Congest    : 0              Transmit Retry Failures    : 0
Receiver Misses           : 0              Late Collisions            : 0
Transmit Buffer Errors    : 0              Heartbeat Failure          : 0
Memory Errors             : 0              Oversized frames received  : 0


Type: [s] to redraw, [=] main menu, any other key to end.
```

**note:** the[ s] to redraw is case sensitive; it must be lower case.

If a second LAN module is present, you will be asked to select which LAN statistics to display.

## Device Errors

| | |
|---|---|
| **Loss of Carrier** | This usually indicates a problem with the LAN hardware either on the Router or in the transceiver. |
| **Underflow Errors** | This is a hardware error. The LAN hardware could not read the contents of a frame to be transmitted from memory. |
| **Transmit Babble Errors** | Currently unused |
| **Overflow Errors** | The software could not supply a receive buffer in time to receive frames because of congestion. |
| **Receive Buffer Congest** | The router missed a frame; because of congestion, the software did not supply sufficient receive buffers to the LAN hardware fast enough to receive all segments of a frame. |
| **Receiver Misses** | The router missed the frame because there were no receive buffers available for storing the frame. Note that this statistic counts only this specific case—whereas the Traffic Summary Receiver Misses statistic counts two additional receive buffer errors and combines them into one statistic. |
| **Transmit Buffer Errors** | This is a hardware or software error. The transmit buffers are corrupted or the memory could not be read by the LANCE chip. |
| **Memory Errors** | This reports errors occurring with the router's memory. |

| LAN Errors | |
|---|---|
| **CRC Errors** | A frame was received with a bad CRC and was discarded. |
| **Framing Errors** | A frame was received that did not contain an integral number of bytes (some bits were missing). |
| **Single Collision** | The number of times exactly one retry was needed to transmit a packet. |
| **Multiple Collisions** | The number of times more than one retry was needed to transmit a packet. |
| **Transmit Retry Failures** | The LAN transceiver has made 16 attempts to transmit a packet and has been blocked each time because of collisions. The transmission is aborted. |
| **Late Collisions** | A collision should only be seen when the transceiver transmits the first 64 bytes of a packet. The likely cause is a faulty transceiver that has started transmitting after this point. |
| **Heartbeat Failure** | This is also called an "SQE" error. As a check for LAN presence, the transceiver is supposed to test the collision presence circuit whenever a transmission is made. The LANCE is complaining that this did not happen. Ethernet Version 1 does not support Heartbeat, so Heartbeat should be disabled when the router is connected to Version 1. |
| **Oversized frames received** | A count of oversized (>1518 bytes) frames received |

# Diagnostics Menu

```
                              DIAGNOSTICS MENU

    Option              Value          Description

    Option            Value          Description
 1. Soft reset                     - Reset device (retain configuration)
 2. Full reset                     - Reset device (use factory defaults)
 3. Heartbeat       [enabled]      - Report transceiver heartbeat failures
 4. WAN trace        menu          - Trace link frames
 5. WAN loopback     menu          - Access WAN loopback diagnostics



Enter option number, "=" - main menu, <TAB> - previous menu

>
```

**1 - Soft Reset**

Selecting the Soft Reset option resets the router software and restarts the router. The current configuration is retained.

Note: a reset may also be performed by toggling the switch behind the hole on the lower right side of the faceplate.

**2 - Full Reset**

Selecting the Full Reset option resets the router configuration to factory default settings and restarts the router. The factory default settings include the terminal type and password.

**CAUTION:** Use this option with caution. All configuration settings will be lost.

**3 - Heartbeat**

The Heartbeat option enables or disables reporting of transceiver heartbeat failures. This failure is not a router fault but a transceiver fault. As a check for LAN presence, the transceiver should ensure that the collision-presence circuit is working whenever a transmission is made. When Heartbeat is enabled, the router will report these failures. Ethernet Version 1 does not support Heartbeat, so all transceivers should have Heartbeat Disabled on these Version 1 Ethernet networks.

**Considerations:**

Enabling this option can help in determining transmission line performance, although it will decrease router performance, since additional processing must be done by the router to report these errors. (Disable for Version 1 Ethernet.)

**4 - WAN trace**

The WAN diagnostics option takes you to the WAN Trace Menu, where trace operations can be [enabled] or [disabled] for each link in order to evaluate link operation.

**5 – WAN Loopback**

The WAN Loopback option takes you to the WAN Loopback Menu, where loopback tests can be performed on a specified link in order to evaluate link operation.

## WAN Trace Menu

```
                                WAN TRACE MENU

    Option          Value                  Description
 1. Trace link      [1]                  - Enter the link to be traced
 2. Real time       [disabled]           - Display frames in real-time
 3. Capture         [enabled]            - Capture frames in buffer
 4. End             [disabled]           - End capture at link down
 5. Data display    [hex] [single_line]  - Set frame display format
 6. Time            [disabled]           - Add time to display
 7. Show                                 - View capture buffer




Enter option number, "=" - main menu, <TAB> - previous menu


>
```

The **WAN TRACE MENU** can be used to monitor the link with features such as statistics capture, frame and packet level tracing, and link-utilization and efficiency histograms. Note that these features will hamper the performance of the bridge/router; therefore, the tracing functions should only be [enabled] when needed.

**1 - Trace Link**

Enable the trace for the specified link after the other options below are set. These options also determine which link is displayed with the Show option.

**2 - Real Time**

Enable this option when the display of frames in real-time is desired. When [enabled], the trace starts immediately and scrolls off the bottom of the screen. Return to the menu by entering "2" to disable real-time (You will have to wait 7-8 seconds or more for this to take effect).

**3 - Capture**

Enabling this option allows for frame capture and display after the buffer is allocated. Use Option 7, Show, to display the capture.

**4 - End**

With this option [enabled], if the link goes down while a trace is underway, the Capture function will end and the data from the trace can be examined up until the point of failure. If this option is [disabled], the Capture function will end when the allocated capture buffer is full.

If the link goes down and then comes back up, the recovery can be examined with End [disabled].

**5 - Data display**

Three possibilities are offered for the display of data. Data may be displayed in **hex** or **ASCII,** or, since in most cases the data being sent doesn't itself need to be examined, **off** may be chosen, which will display only the protocol frame information. Note that command completion may be used (i.e. only the first letter (or letters) need to be entered for recognition). After a data from a trace is captured, you may move from off to ASCII or hex, as this information resides in the background.

```
Enter:
 ascii, hex, off
>

Enter:
 all_lines, single_line
>
```

**6 - Time**

[Enable] this option to add time to the trace display in thousands of a second (h.mm.ss.xxx). Time is always available and does not need to be enabled to capture data during a trace (i.e. may be enabled after the data from the trace is captured). Time is relative to the time of power-up.

**7 - Show**

This option appears once the buffers are allocated

This option displays the frames captured by the Trace and stored in the capture buffer. (BOB = Beginning of Buffer; EOB = End of Buffer.) The trace shown below is with the data display in the "off" mode.

| BOB | **This Bridge/Router** | **Partner Bridge/Router** |
|---|---|---|
| rRR 0 | | expects 0 |
| xI 4,0 122 | expects 4, sends 0 | gets 0 |
| rRR 1 | | expects 1 |
| rI 1,4 68 | gets 4 | still expecting 1, sends 4 |
| xRR 5 | expects 5 | |
| rI 1,5 68 | gets 5 | still expecting 1, sends 5 |
| xI 5,1 122 | still expecting 5, sends 1 | gets 1 |
| xRR 6 | expects 6 | |
| rRR 2 | | expects 2 |
| xI 6,2 236 | still expecting 6, sends 2 | gets 2 |
| rRR 3 | | expects 3 |
| rI 3,6 68 | gets 6 | still expecting 3, sends 6 |
| xRR 7 | expects 7 | |
| rI 3,7 68 | gets 7 | still expecting 3, sends 7 |
| xI 7,3 144 | still expecting 7, sends 3 | gets 3 |
| xRR 0 | expects 0 | |
| rRR 4 | | expects 4 |
| xI 0,4 122 | still expecting 0, sends 4 | gets 4 |
| rRR 5 | | expects 5 |
| rI 5,0 68 | gets 0 | still expecting 5, sends 0 |
| xRR 1 | expects 1 | |
| rI 5,1 68 | gets 1 | still expecting 5, sends 1 |
| xI 1,5 122 | still expecting 1, sends 5 | gets 5 |
| xRR 2 | expects 2 | |
| rRR 6 | | expects 6 |
| xI 2,6 258 | still expecting 2, sends 6 | gets 6 |
| rRR 7 | | expects 7 |
| rI 7,2 68 | gets 2 | still expecting 7, sends 2 |
| xRR 3 | expects 3 | |
| rI 7,3 68 | gets 3 | still expecting 7, sends 3 |
| xI 3,7 68 | still expecting 3, sends 7 | gets 7 |
| xRR 4 | expects 4 | |
| rRR 0 | | expects 0 |
| EOB | | |

**Format:**

Receive frames (r) are indented.
Transmit frames (x) are not.

Valid frames are as follows:

| | | |
|---|---|---|
| I | - | Information |
| RR | - | Receiver Ready |
| RNR | - | Receiver Not Ready |
| REJ | - | Reject |
| SABM | - | Set Asynchronous Balance Mode |
| DM | - | Disconnect Mode |
| DISC | - | Disconnect |
| UA | - | Unnumbered Acknowledgment |
| FRMR | - | Frame Reject |

**Information (I) Frame** traces will be displayed with the following:

Link (L1/L2) (x/r)I N(r), N(s) Data Field Length Data Field (hex)

As much of the Data Field as will fit on one line will be displayed if hex or ASCII format is specified. If **off** is specified, only the Data Field Length is given.

**Supervisory (S) frame** traces will be displayed with the following:

Link (L1/L2) (x/r)(RR / RNR / REJ) N(r)

**Unnumbered (U) frame** traces will be displayed with the following:

Link (0/1) (x/r) (SABM / DM / DISC / UA / FRMR)

Any illegal or unknown frame will be completely dumped in hex. Note that any frame with a CRC error will not be displayed and a Level 2 error will be output.

**LAPB *control field*** formats:

Three types of Link Access Procedures (Balanced) **LAPB** control field formats are used to perform:

1) numbered information transfer (**I** format),
2) numbered supervisory functions (**S** format) and
3) unnumbered control functions (**U** format).

The numbered **I** format is used to perform information transfer.

The numbered **S** format is used to perform data link supervisory control functions such as:
- acknowledge **I** frames,
- request transmission of **I** frames, and
- to request a temporary suspension of **I** frames.

The unnumbered **U** format is used to provide additional data link control functions.

## INFORMATION FRAMES:

**I** **I**nformation

The (**I**) statistic indicates a transfer of a sequentially numbered frame containing an (**I**) information field.

To allow the sending of an **I**nformation frame a Receive Ready (**RR**) supervisory frame is sent by the remote bridge/router requesting the connection.

## SUPERVISORY FRAMES:

**RR** **R**eceiver **R**eady

A Receive Ready (**RR**) supervisory frame is sent by the bridge/router in order to:

1) indicate that it is ready to receive an **I** frame;
2) acknowledge previously received **I** frames numbered up to and including N(R) - 1.

An **RR** frame may be used to indicate the clearance of a busy condition reported by the earlier transmission of an **RNR** frame by that same bridge/router.

**RNR** **R**eceiver **N**ot **R**eady

The **RNR** statistic is generated by either remote bridge/router to indicate a busy condition. A busy condition essentially indicates a temporary inability to accept incoming **I** frames. **I** frames numbered up to and including N(R) - 1 are acknowledged.

**I** frame N(R) and any subsequent **I** frames received, are not acknowledged; the acceptance state of these unacknowledged frames will be indicated in subsequent exchanges.

**REJ** **REJ**ect

The **REJ** supervisory frame is generated when a remote bridge/router requests transmission of **I** frames starting with the frame numbered N(R). **I** frames numbered N(R) - 1 and below are acknowledged. Additional **I** frames (pending initial transmission) may be transmitted following the retransmitted **I** frame(s).

Only one **REJ** exception condition for a given transfer direction may be established at any time. This **REJ** exception condition is reset (cleared) upon the receipt of an **I** frame with an N(S) equal to the N(R) of the **REJ** frame. A **REJ** frame may be used to indicate the clearance of a busy condition that was reported by the earlier transmission of an **RNR** frame by that same bridge/router.

## UNNUMBERED FRAMES:

**SABM** **S**et **A**synchronous **B**alanced **M**ode

The **SABM** unnumbered command is generated to place the addressed bridge/router into an asynchronous balanced mode information-transfer phase, where all command/response control fields will be one octet in length.

The receiving bridge/router confirms acceptance of the **SABM** by the transmission, at the first opportunity, of a **UA** response.

Previously transmitted **I** frames that are unacknowledged when a **SABM** command is generated remain unacknowledged. It is the responsibility of a higher level (e.g. TCP, XNS, LAT) to recover from the loss of the contents (packets) of such **I** frames.

**DISC** **DISC**onnect

The **DISC** statistic is generated when the bridge/router sending the **DISC** informs the other bridge/router that it (the sending bridge/router) is suspending its own operation.

Before the **DISC** is acted upon, the bridge/router receiving the **DISC** confirms its acceptance of the **DISC** command by the transmission of a **UA** response. The bridge/router sending the **DISC** enters the disconnected phase when it receives the acknowledged **UA** response.

Previously transmitted **I** frames that are unacknowledged when **DISC** is generated remain unacknowledged. It is the responsibility of a higher-level protocol (e.g. TCP, XNS, LAT) to recover from the possible loss of the contents (packets) of such **I** frames.

**UA** **U**nnumbered **A**cknowledgment

A **UA** response and statistic is generated to acknowledge the receipt and acceptance of the mode-setting commands. Received mode-setting commands are not acted upon until the **UA** response is transmitted.

**DM** **D**isconnected **M**ode

The **DM** unnumbered response and statistic is generated to report a status where the bridge/router is logically disconnected from the link, and is in the disconnected phase.

1) The **DM** may be sent to indicate that the bridge/router has entered the disconnected phase without having received a **DISC** command.
2) If sent in response to the reception of a mode-setting command, the **DM** is sent to inform the other bridge/router(s) that this bridge/router is still in the disconnected phase and cannot execute the Set Mode command.

A bridge/router in the **DM** phase will monitor received commands and will react to a **SABM** command. It will send a **DM** response with the F bit set to 1 in response to another command received with the P bit set to 1.

**FRMR** **FR**a**M**e **R**eject

The **FRMR** statistic is generated by the bridge/router to report an error condition not recoverable by the re-transmission of an identical frame. This may result from at least one of the following conditions:

1) the receipt of a command or response control field that is undefined or not implemented;
2) the receipt of an I frame with an information field that exceeds the maximum established length;
3) the receipt of an invalid N(R); or
4) the receipt of a frame with an information field that is not permitted or the receipt of a supervisory or unnumbered frame with incorrect length.

An undefined or not implemented control field is any control field encoding not identified in Table 5, LAPB commands and responses.

A valid N(R) must be within the range from the lowest send sequence number N(S) of the still unacknowledged frame(s) to the current logical DCE send state variable, inclusive.

An information field that immediately follows the control field, and consists of 3 to 5 octets, is returned with the FRMR and provides the reason for the FRMR response.

## Network Events Menu

```
                          NETWORK EVENTS MENU

    Option                    Description
 1. Acknowledge alarm       - Clear alarm status display
 2. Show events             - View event history
 3. Clear events            - Clear event history
 4. Show security log       - View security failure log
 5. Clear security log      - Clear security failure log
 6. Show activation log     - View resume event log
 7. Clear activation log    - Clear resume event log




Enter option number, "=" - main menu, <TAB> - previous menu


>
```

The **NETWORK EVENTS MENU** allows the display and management of alarm histograms.

Event, link Activation and Security Logs are listed and explained in the Reference Manual file on the accompanying disk.

**1 - Acknowledge Alarm**

The Acknowledge Alarm option clears the screen ALARM display for the current alarm.

**2 - Show Events**

The Show Events option displays the 199 most recent events and alarms since the router was last powered up or Cleared with option 3. A listing of events and alarms is available in Appendix A of the P840 Reference Manual. Alarms are indicated by an asterisk (*).

```
#1 1999-01-26 13:39:05   SNMP is running
#2 1999-01-26 13:39:06 * IP Routing is enabled
#3 1999-01-26 13:39:07   Configuration restored
#4 1999-01-26 13:39:08   Running in OPERATIONAL mode
#5 1999-01-26 13:39:09 * LAN connection established
#6 1999-01-26 13:39:35 * LAN started forwarding
time is 1999-01-26 14:24:32, 8 items since last clear.



Type: [s]tart, [n]ext, [p]rev, [=] main menu, any other key to end.
```

The format of the time stamp for each event is: year-month-day  hour:minute:second

These will be according to the date and time set in the Device Set-Up menu.

**3 - Clear Events**

The Clear Events option removes all events from the table.

**4 - Show Security Log**

The Show Security Log option displays the 99 most recent security logs since the router was last powered up or Cleared with option 5.

```
#1 1999-01-26 16:26:53   Link 1 PAP failed for one (5551313)
#2 1999-01-26 16:28:19   Link 1 CHAP failed for one (5551313)
time is 1999-01-26 16:28:19, 2 items since last clear.

Type: [s]-to redraw, [=] main menu, any other key to end.
```

**note:** the[ s] to redraw is case sensitive; it must be lower case.

The format of the time stamp for each security log entry is: year-month-day  hour: minute: second

These will be according to the date and time set in the Device Set-Up menu.

**5 - Clear Security Log**

The Clear Security Log option removes all security logs from the table.

**6 - Show Activation Log**

The Show Activation Log option displays the 100 most recent connection management link activation logs since the router was last powered up or Cleared with option 7. The entries in the log indicate the device that was called, the protocol that caused the activation, the source and destination addresses within the frame that caused the activation, and a hex dump of the frame that caused the activation. The hex dump of the frame may be used for debugging purposes when the link is being resumed incorrectly.

```
#1 1999-01-26 14:53:27   Resume event to DEV000d05
#2 1999-01-26 14:53:27   Dst 0000411b:000000000001:0451 Src
                       + 00001515:00001b02446b:4003
#3 1999-01-26 14:53:27   Length = 46 - ff ff 00 29 01 11 00 00 41 1b 00 00 00
                       + 00 00 01 04 51 00 00 15 15 00 00 1b 02 44 6b 40 03 22
                       + 22 17 03 01 00 16 00 02 15 01 01 00 01 bf bf
#4 1999-01-26 15:06:10   Resume event to DEV000d05 (IP)
#5 1999-01-26 15:06:10   Dst 192.168.95.196 Src 198.169.1.149
#6 1999-01-26 15:06:10   Length = 335 - 45 00 01 4f 00 00 00 00 1f 29 b1 db c6
                       + a9 01 95 c0 a8 5f c4 02 54 48 45 20 51 55 49 43 4b 20
                       + 42 52 4f 57 4e 20 46 4f 58 20 4a 55 4d 50 53 20 4f 56
                       + 45 52 20 54 48 45 20 4c 41 5a 59 20 44 4f 47 20 31 32
time is 1999-01-26 15:06:16, 9 items since last clear.

Type: [s]-to redraw, [=] main menu, any other key to end.
```

**note:** the[ s] to redraw is case sensitive; it must be lower case.

The format of the time stamp for each alarm is as follows:  year-month-day  hour: minute: second

These will be according to the date and time set in the Device Set-Up menu.

**7 - Clear Activation Log**

The Clear Activation Log option removes all connection management link activation logs from the table.