IO LINK- SOHO
IO LINK- SH- SR
Ethernet Bridge/ Router

Frame Relay Menus

Reference Manual

Issue 1

Software Version F5P.03.04.X

 10/98

Part # 168-34806

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 displayed on the console connected to the router when it is powered up and runs its self-diagnostics:

```
Testing hardware
Testing EEPROM .... Successful
Testing Flash .... Successful
Testing RAM .... Successful
Completed hardware tests
```

The above tests will take approximately a minute to complete. When they are done, the router will initialize and display the following:

```
Initializing hardware

Initializing software
```

After initialization the operational software will be started up and control passed to the console:

```
Running in OPERATIONAL mode. Press enter to access console
```

If this is the first time the router is powered up, you will be requested to choose a terminal type:

```
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, the initial screens 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.

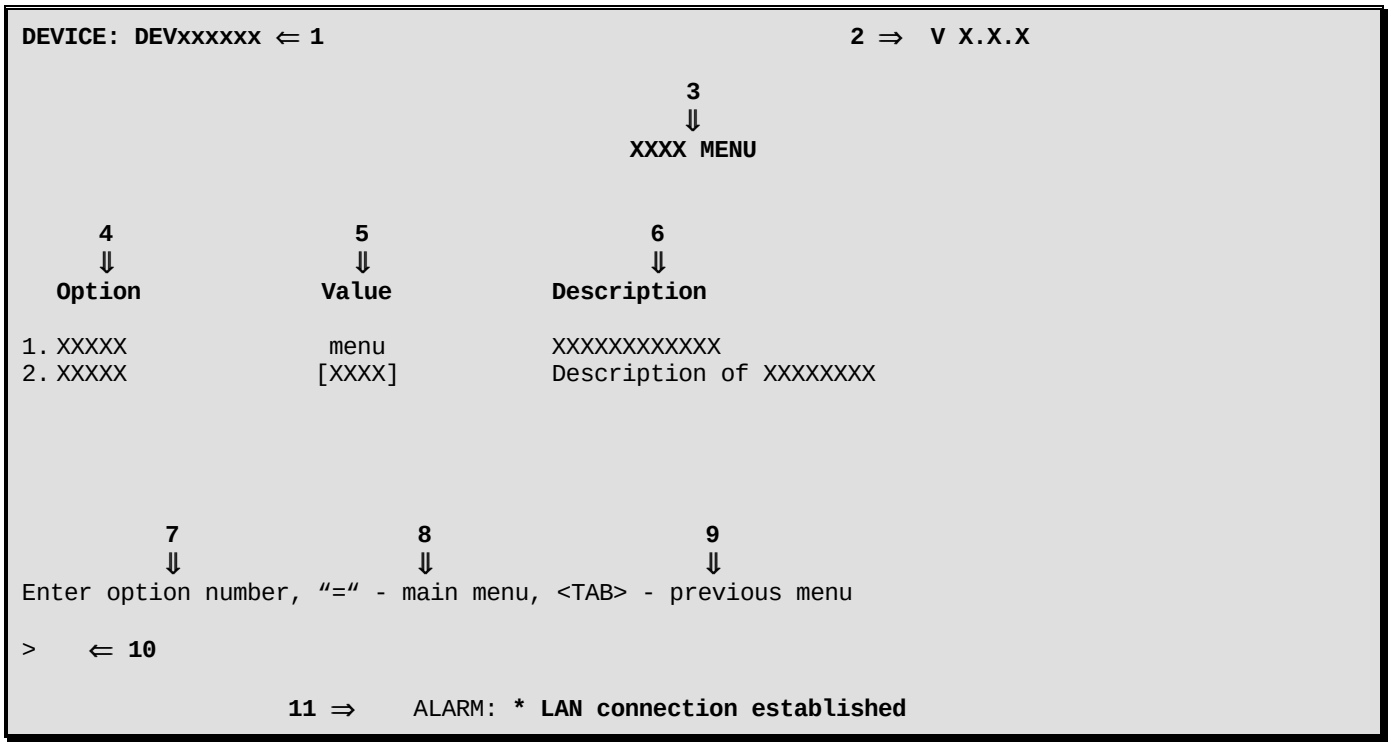
The IOLINK-SH-SR Ethernet router uses a “hotkey “ Menu. A menu option is chosen by selection of the desired option number.

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.

Important

The IOLINK-SH-SR uses FLASH memory to store the configuration information. Configuration settings are stored to FLASH memory after there has been 30 seconds of idle time. Idle time is when there is no selection or modification of the value in the built-in menu system.

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 major paths, simply enter " = ").

9. **Returning to the Previous Menu**
   To go back one menu step, 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 42 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         - Quick start configuration 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 1-5 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 initial connection set up may done be without having to configure a large number of parameters.

On initial start up, the IOLINK-SH-SR 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 IOLINK-SH-SR 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.

Once the PVC's have been automatically configured, the IOLINK-SH-SR should be connected to the frame relay routers located on the other ends of the PVC connections. Since the IOLINK-SH-SR is configured by default to route IPX and bridge, the only remaining parameter required for a "Quick Start" will be the IP address and possibly security settings.

2 - Configuration

The Configuration option takes you to the Configuration Menu, where all the various router parameters can be 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 200 latest Alarms can be examined.

6 - Save Configuration

The Save Configuration option performs an immediate save of the configuration to flash memory.

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. Device name        "DEV050607"   - Name this device
 2. Security level     [none]        - Set security protocol
 3. IP address         [none]        - Define IP address and mask
 4. Default gateway    [none]        - Define default gateway
 5. Force disconnect                 - Disconnect a call
 6. Link status                      - View status of link
 7. Soft reset                       - Reset device (retain configuration)



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

>
```

The **QUICK START MENU** provides configuration options to make a PVC connection.

1 - 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).

2 - Security level

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

Default: [none]

```
Enter :
    none, PAP, CHAP

>
```

3 - IP Address

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

The IP address consists of 4 eight-bit numbers and is represented by 4 fields separated by periods ("**.**"), where each field is specified by a decimal number (e.g. 192.38.1.10). Each decimal number must be less than or equal to 255 (the maximum decimal value represented by an 8-bit binary number).

A single IP network address may be divided into multiple logical networks by the process of *subnetting.* The host field of an IP address is partitioned into two parts: a *subnet number* and a *host number*; the subnet numbers are then used to address the resulting subnetworks. The subnet mask is defined as a series of contiguous bit locations from the start of the IP address that includes the network number and the subnet number; the subnet mask size is the number of bits in the subnet mask. For example, the subnet mask 255.255.255.192 would have a subnet mask size of 26.

Default: [none]

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

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

4 - 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.

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 are more than one default gateways 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)
>
```

5 - Force Disconnect

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

```
Enter :
     Link to disconnect (1)
>
```

6 - Link Status

The Link Status option displays the status of the link.

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

7 - Soft Reset

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

Note that a hardware (and software) reset may be performed by toggling the switch behind the small access hole at the bottom of the faceplate on the right side.

Configuration Menu

```
                          CONFIGURATION MENU

    Option                Value         Description
 1. Access set-up         menu        - Establish access parameters
 2. Internet set-up       menu        - Define IP environment
 3. Applications set-up   menu        - Configure Internet applications
 4. WAN set-up            menu        - Configure WAN operation
 5. Bridging set-up       menu        - Define bridging environment
 6. IP routing set-up     menu        - Define IP routing environment
 7. IPX routing set-up    menu        - Define IPX environment
 8. Filter set-up         menu        - Filter operations



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


>
```

The **CONFIGURATION MENU** provides paths to menus for total device configuration.

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 - Internet Set-Up

The Internet Set-up option takes you to the Internet Set-Up Menu, where the parameters for the Internet configuration are selected.

3 - Applications Set-Up

The Applications Set-up option takes you to the Applications Set-up Menu, where a number of internet connection management applications may be accessed.

4 - WAN Set-Up

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

5 - Bridging Set-Up

The Bridging Set-up option takes you to the Bridging Set-Up Menu, where the parameters for bridging are selected.

6 - 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 selected. IP routing may be enabled or disabled in this menu.

7 - IPX Routing Set-Up

The IPX Routing Set-up option takes you to the IPX Routing Set-Up Menu, where the parameters for IPX routing are selected. IPX routing may be enabled or disabled in this menu.

8 - 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.

Access Set-Up Menu

```
                          ACCESS SET-UP MENU

   Option              Value          Description
 1. Terminal set-up    menu         - Define operator's console
 2. Device set-up      menu         - Set security/time/names
 3. Telnet set-up      menu         - Establish remote communications
 4. Load FLASH set-up  menu         - Prepare for software update
 5. Hardware status                 - Display hardware information
 6. TFTP access       [disabled]    - Allow TFTP configuration saves/loads
 7. Dump                            - Back-up configuration from console
 8. Restore                         - Load configuration from console




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 - 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.

2 - 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.

3 - 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.

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.

5 - Hardware Status

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

```
                      Hardware Status

Boot Code version     : xxxxxx
Boot Code revision    : xxxxxx
System Code revision  : 1330
MAC address           : 02-03-04-05-06-07
MAC check code        : 23d4a6
Service reference     : 0/0
LAN interface type    : 10BaseT
Link 1 interface type : v.35
Ram size              : 4 MB
ROM size              : 2MB
CPU type              : 68EN360
CPU speed             : 25 Mhz
Compression           : enabled
```

Boot Code version	The software boot code version currently installed in this IOLINK-SH-SR. This is the number that is displayed in the upper right of the menu screens
Boot Code revision	The software boot code revision number currently installed in this IOLINK-SH-SR. A control number for tracking minor software revisions.
System Code revision	The system code software revision number currently installed in this IOLINK-SH-SR.
MAC Address	The MAC Address of the LAN port for this router.
MAC Check Code	Check code used for feature upgrades.
Service Reference	Internal factory reference number.
LAN Interface Type	The type of LAN interface currently in use on this router.
Link 1 Interface Type	The type of link interface of this router.
RAM size	The amount of RAM in this router.
ROM Size	Indicates the size of the FLASH EEPROM installed.
CPU type	The CPU type installed in this IOLINK-SH-SR.
CPU speed	The CPU speed (in megahertz) of the processor installed in this IOLINK-SH-SR.
Compression	Indicates whether data compression is enabled or disabled.

6 - 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.

When you need to change the battery, you can dump the configuration to a PC disk. Then, when the new battery is installed, you can reload the configuration.

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.

4) Once you are satisfied that the configuration dump was successful, the battery may be safely changed (if this was the reason for the dump).

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.

7 - Dump

The Dump option lists the configuration so it may be captured and stored to a disk on a PC running a terminal-emulation package.

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

The command "Configuration Access_Set-Up erase_config", is used at the time the dumped configuration is loaded back into the router. At that time, this command prepares the database by first clearing any information back to the default settings, and then allows the restoration of the saved configuration. The last command, "Configuration Access_Set-Up end_load", completes the loading of the saved 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.

8 - Restore

The Restore option restores a configuration to the router that was previously saved to a disk file with the Dump command.

Considerations:

The terminal-emulation package selected should have the capability to pace the loading of commands into the 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 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 disk.
4) When the transfer is complete, the configuration will have been restored to the router.

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.

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.

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









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)
> EURRNO\1

Enter:
  verification of new password (1 to 8 characters)
> EURRNO\1
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)
> Bridge5
```

3 - Show Time

The Show Time option allows you to view the current day of the week, date and time. The format is:

```
Monday 1998-06-21 08:12:28
```

4 - Set Time

Use the Set Time option to set the date and 24-hour Time Clock. Note that if your network uses the Bandwidth-On-Demand features of the IOLINK-SH-SR Ethernet router across time zones, you must standardize on one time zone on the routers.

```
Enter:
  Date in format yyyy-mm-dd, no_change
1998/07/27

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

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
 3. Show names                  - Display known remote device names
 4. Add name                    - Name remote devices
 5. 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 devices to make Telnet connections to this router for management. Once the connection is established, the LAN 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.

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.

Noting the Device name at the top left of each Menu may identify 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 AM
Amsterdam              92.0.0.5          on link 1 PM

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

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 10 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
>
```

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.01.02.03).

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).

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 Operational Code diskette.

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, open the case, remove the strap from the center set of pins at J2, power up the bridge/router. The bridge/router should now restart and be in ZMODEM receive mode. Re-install the strap and replace the cover. 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 interface and the WAN interface will be disabled. The router will only accept information from the console management port.

The BOOT code of the IOLINK-SH-SR may be upgraded by performing a load of the "###.all" file from the BOOT Code directory on the upgrade diskette.

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 Operational Code diskette.
(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, open the case, remove the strap from the center set of pins at J2, power up the bridge/router. The bridge/router should now restart and be in ZMODEM receive mode. Re-install the strap and replace the cover. 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.

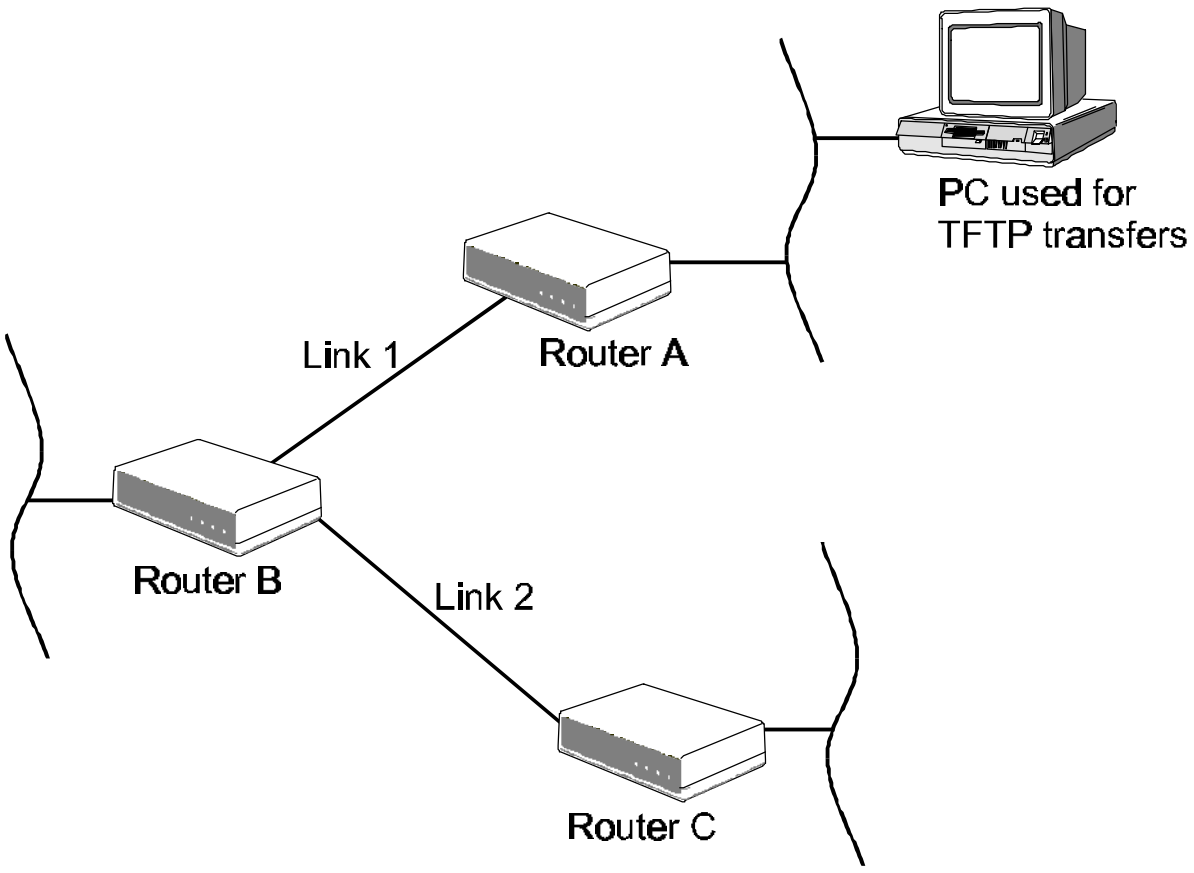
In the following diagram of a cluster of routers, when upgrading the three IOLINK-SH-SR routers in the diagram, the upgrade order should be Router C, then Router B, and finally Router A.

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

- Using TFTP, get config.txt from each router and save.
- Telnet to Router C. Enter the ID or alias of Router B in the Network (TFTP) option to put Router C in Network Load mode. When Router C restarts in Network Load mode, the connection to "Router B" will be re-established only if autocall is enabled on router B.
- The TFTP transfer of the upgrade code may now be performed from the PC to Router C. Once Router C has completed programming the flash and has restarted in operational mode, the connection to Router B will be re-established only if autocall is enabled on router B.

Router B upgrades would be performed 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.

Once all the routers are operating with the new software, the PC may be used to reload the config.txt file back to Router C, then Router B, then Router A.



Internet Set-Up Menu

```
                          INTERNET SET-UP MENU

    Option                 Value          Description
 1. ARP set-up             menu         - Configure ARP operation
 2. DNS set-up             menu         - Define DNS address(es)
 3. Secondary IP set-up    menu         - Configure Secondary IP
 4. Nonstandard subnets   [enabled]     - Allow subnet zero
 5. IP address            [none]        - Define IP address
 6. Default gateway       [none]        - Define default gateway
 7. Time to live          [32]          - Router hops allowed
 8. Ping                                - ICMP echo requests


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

>
```

The **INTERNET SET-UP MENU** contains options used to enable the router to be recognized as a device on the network. This is important to be able to route IP data and connect to other routers across the LAN, and for SNMP Network Management Stations to be able to access the router's SNMP agent.

1 - 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.

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 - Secondary IP set-up

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

4 - Nonstandard Subnets

The Nonstandard Subnets option allows the use of subnet addresses containing all zeroes or all ones.

Allows the definition of a subnet size starting at 1 instead of 2. When this option is enabled, the subnet size may be defined as values from 1 to 24. The use of a subnet size of 1 allows a single IP network address to be split into two equal sized sub-networks each containing half of the number of allowable hosts of the original IP network address. A subnet size of 1 is accomplished by using all zeroes or all ones in the subnet portion of the address, this is not allowable with standard subnet masks.

Default: [enabled]

5 - 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 IOLINK-SH-SR Ethernet 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 eight-bit fields, each field is specified by a decimal number and the fields are separated by a decimal point (e.g. 192.36.1.10). Each decimal number must be less than or equal to 255(the maximum decimal value of an 8-bit binary number).

A single IP network address may be divided into multiple logical networks by the process of *subnetting.* The host field of an IP address is partitioned into two parts: a *subnet number* and a *host number*; the subnet numbers are then used to address the resulting subnetworks. The subnet mask is defined as a series of contiguous bit locations from the start of the IP address that includes the network number and the subnet number; the subnet mask size is the number of bits in the subnet mask. For example, the subnet mask 255.255.255.192 would have a subnet mask size of 26. The minimum subnet mask size is equal to the number of bits in the network address for that IP address class.

Default: [none]

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

Enter :
    size of subnet mask (from 8 to 30)
>
```

6 - 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 the device 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 are more than one default gateways 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)
>
```

7 - 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 IOLINK-SH-SR Ethernet router will have their time-to-live value decremented by two.

Default: [32]

Range: 1 - 255

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 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.
```

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).

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 256 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.

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 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 this router on 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 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 IOLINK-SH-SR 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 IOLINK-SH-SR 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 IOLINK-SH-SR 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 IOLINK-SH-SR 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 IOLINK-SH-SR will participate in RIP IP routing message exchange for this subnet.

When the RIP mode is set to both, the IOLINK-SH-SR will send and receive RIP routing messages.

When the RIP mode is set to send_only, the IOLINK-SH-SR will only send RIP routing messages and not receive.

When the RIP mode is set to receive_only, the IOLINK-SH-SR will only receive RIP routing messages and not send.

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]

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




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. This menu is only available when Firewall Support is enabled for this device.

4 - NAT Exports

The NAT Exports option directs you to the NAT Exports Menu, where Network Address Translation for the exported services from this LAN may be configured.

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 SNMP parameters for the router. For information on the IOLINK-SH-SRs compliance with the SNMP MIBs and details of the proprietary MIB, please refer to the MIB diskette included with the unit.

The SNMP Set Up Menu contains two default communities:
- "public" which is a read-only community accessible by all 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  :  2

Community Name     Write Access     NMS Addresses    Trap Addresses
GIU_Config         enabled          all

public             disabled         all

NMS_1              enabled          92.0.0.1          92.0.0.2
                                    111.1.1.1         111.1.1.2









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

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 NMS address                     - Insert NMS address into list
 4. Add trap address                    - Insert trap address into list
 5. Remove NMS address                  - Delete NMS address from list
 6. Remove trap address                 - Delete trap address from list
 7. Help                                - Read address list description




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 NMS address                     - Insert NMS address into list
 4. Add trap address                    - Insert trap address into list
 5. Remove NMS address                  - Delete NMS address from list
 6. Remove trap address                 - Delete trap address from list
 7. Help                                - Read address list description




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      :  2
Total Trap Addresses     :  3

NMS Addresses            Trap Addresses
92.0.0.1                 92.0.0.2
111.1.1.1                94.0.1.1
                         111.1.1.2
```

3 - Add NMS Address

Up to five NMS addresses may be added to the NMS 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).

Considerations:

If "*all*" is initially chosen for the NMS address list, and (one or more) specific NMS addresses are desired as a replacement, remove "*all*" with Option 5 - Remove NMS address, to allow the addition of the new address(es).

4 - Add Trap Address

The Add Trap Address option allows the addition of up to five trap addresses to the trap address list. 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. Addresses must be entered in standard IP format (four fields separated by a periods, with each field specifying a decimal number). If the list is empty, traps will not be sent.

5 - Remove NMS Address

The Remove NMS Address option deletes the specified NMS address associated with the SNMP Community. Other NMS addresses and the Trap addresses remain unaffected. (If "all" is specified, all NMS addresses are deleted.)

6 - Remove Trap Address

The Remove Trap Address option deletes the specified trap address associated with the SNMP Community. Other trap addresses and the NMS addresses remain unaffected. (If "all" is specified, all trap addresses are deleted.)

7 - Help

The Help option offers a brief description of the address list's purpose and format.

DHCP Set-Up Menu

```
                              DHCP SET-UP MENU

    Option                    Value          Description
 1. Server IP address pool    menu         - Range of allowable addresses
 2. NetBIOS setup             menu         - NetBIOS parameters
 3. DHCP services            [none]        - Set DHCP operational mode
 4. Relay destination        [none]        - BOOTP/DHCP server IP address
 5. ICMP echo verification   [enabled]     - Ping allocated IP address
 6. Lease period             [60]          - Length of lease (minutes)




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 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 IOLINK-SH-SR's LAN and 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 - NetBIOS Set-Up

The NetBIOS set-up option directs you to the NetBIOS set-up Menu, where the NetBIOS parameters may be set.

3 - 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 IOLINK-SH-SR to act as a simple DHCP server for its LAN. Selecting "relay" enables the IOLINK-SH-SR to relay DHCP service data to a remote DHCP server.

Default: none

Choices: none, server, relay

4 - 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

5 - 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

6 - 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

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 IOLINK-SH-SR is a part.

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.
```

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 of the device to be taken off, or the entire list of static address assignments may be cleared by entering “all”.

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 propagate 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. Designated servers      menu       - Edit entry for a specific server
 2. Edit firewall entry     menu       - Edit/Add firewall entries
 3. Firewall support       [disabled]  - Enable/disable firewall support
 4. Block src IP spoofing  [disabled]  - Discard WAN pkts with local src IP
 5. Firewall statistics                - View firewall statistics
 6. Show firewall entries              - Display firewall entries
 7. Remove entry                       - Remove a firewall entry
 8. Clear statistics                   - Clear firewall statistics




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.

Remember that when the firewall function is enabled, **all incoming IP traffic EXCEPT normal TCP traffic** from the Wide Area Network (WAN) will be **filtered**. This means that only regular TCP connection traffic will be allowed through the firewall. Other IP traffic like UDP, (ping), and TCP connection initiation data received from remote sites will be filtered and not allowed through the firewall.

To allow specific IP traffic to be passed from the connected remote site to this local LAN, either a firewall entry must be specified or a designated server must be specified or a combination of the two.

TCP connections initiated from the local LAN will be allowed to remote site resources. Once the TCP connections have been established, normal TCP connection traffic will be allowed between the local and remote device.

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 local LAN. A designated server is a device that is legally accessible from the remote site locations. Such designated servers may be the HTTP server and the FTP server on the local LAN that may be accessed by devices located on remote site LANs.

2 - Edit Firewall Entry

The Edit Firewall Entry option directs you to the Edit Firewall Entry Menu, where firewall table entries are defined. A firewall entry may be allowing all IP traffic from a specific remote site IP network to access the local LAN.

3 - Firewall support

The Firewall Support option enables or disables the IP Firewall functions of this IOLINK-SH-SR. **All incoming IP traffic EXCEPT normal TCP traffic** from the Wide Area Network (WAN) will be **filtered**. This means that only regular TCP connection traffic will be allowed through the firewall. Other IP traffic like UDP, ICMP (ping), and TCP connection initiation data received from remote sites will be filtered and not allowed through the firewall.

Incoming TCP connections that are allowed must be defined within the Firewall Set-up menu. To allow specific IP traffic to be passed from the connected remote site to this local LAN, either a firewall entry must be specified or a designated server must be specified or a combination of the two.

TCP connections initiated from the local LAN will be allowed to external remote site resources. Once the TCP connections have been established, normal TCP connection traffic will be allowed between the local and remote device.

Once the Firewall function is enabled, the IP traffic that is allowed to be received from the remote sites must be defined within the Firewall Set-Up Menu.

Default: [disabled]

4 - Block Source IP Spoofing

When the Block Source IP Spoofing option is enabled, all of the WAN traffic that uses a source IP address the same as the local network IP address will be filtered. This prevents devices located on a remote site network from attempting to gain access to the local network by using a local IP address as their source address. The IOLINK-SH-SR will discard any IP traffic that is received from the WAN with a source IP address the same as an IP address located on the locally connected LAN.

Default: [disabled]

5 - Firewall Statistics

The Firewall Statistics option displays a summary of the number of frames 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:	Incoming WAN frames discarded due to source IP address being the same as an IP address already on the local network.
Source IP Address:	Incoming WAN frames discarded because the source IP address on the remote site network is not allowed to access this local network.
Destination IP Address:	Incoming WAN frames discarded because the destination IP address on the local network is not allowed to be accessed from any remote site network.
Protocol Number:	Incoming WAN frames discarded because the protocol type is not allowed.
Port Number:	Incoming WAN frames discarded because the port number is not allowed.
Total Number:	Total number of incoming WAN frames discarded due to firewall filtering.

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 /
 #   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 the incoming IP traffic from the WAN.
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)

>
```

8 - Clear Statistics

The Clear Statistics option clears all of the firewall statistics.

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. Gopher server           [none]       - Specify Gopher server IP address

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

>
```

The **DESIGNATED SERVERS MENU** contains options used to define the IP address of specific local network services that may be accessed by remote site network devices. 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 local network E-mail (SMTP) Server that may be accessed by remote site network devices.

Default: [none]

2 - POP 2/3 Server

The POP Server option defines the IP address of the local network POP 2/3 Server that may be accessed by remote site network devices.

Default: [none]

3 - FTP Server

The FTP Server option defines the IP address of the local network FTP Server that may be accessed by remote site network devices.

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 local network WWW (HTTP) Server that may be accessed by remote site network devices.

Default: [none]

5 - Telnet Server

The Telnet Server option defines the IP address of the local network Telnet Server that may be accessed by remote site network devices.

Default: [none]

6 - Local DNS

The Local DNS option defines the IP address of the local network Domain Name Server (DNS) that may be accessed by remote site network devices. 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 remote network Domain Name Server (DNS) that may be accessed by local network devices. 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 - Gopher Server

The Gopher Server option defines the IP address of the local network Gopher Server that may be accessed by remote site network devices.

Default: [none]

Edit Firewall Entry Menu

```
                        EDIT FIREWALL ENTRY MENU

    Option               Value          Description
 1. Dest IP address     [        ]   - Incoming IP destination address
 2. Destination mask    [        ]   - Destination subnet mask
 3. Source IP address   [        ]   - Incoming IP source address
 4. Source mask         [        ]   - Source subnet mask
 5. Protocol type       [        ]   - Allow specific protocol types
 6. Initial port        [        ]   - First port to allow traffic in
 7. Last port           [        ]   - Last port in range
 8. Description         [        ]   - describe the entry




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:

```
                      EDIT FIREWALL ENTRY 1 MENU

    Option               Value          Description
 1. Dest IP address     [none]        - Incoming IP destination address
 2. Destination mask    [none]        - Destination subnet mask
 3. Source IP address   [all]         - Incoming IP source address
 4. Source mask         [none]        - Source subnet mask
 5. Protocol type       [TCP]         - Allow specific protocol types
 6. Initial port        [1]           - First port to allow traffic in
 7. Last port           [65535]       - Last port in range
 8. Description         [        ]    - describe the entry




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 remote site network may be defined to be allowed to access either a specific local device or the entire local network.

1 - Destination IP Address

The Destination IP Address option defines the IP address of a local device that may be accessed through the firewall for this entry. On all incoming frames from the WAN, this address will be the destination IP address.

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 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]

3 - Source IP Address

The Source IP Address option defines the IP address of a remote site device or network that may be allowed access through the firewall for this entry. On all incoming frames from the WAN, this address will be the source IP address. By default, this option allows all remote site source IP addresses to access the local device specified. Specifying a specific remote site IP address for an individual device or a network allows for greater restrictions on incoming frames.

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 - Initial Port

The Initial Port option defines the starting port number to be allowed through the firewall for this entry.

Default: [1]

Range: 1 to 65535

7 - Last Port

The Last Port option defines the last port number to be allowed through the firewall for this entry. Specifying a port number greater than the Initial Port number allows all of the port numbers within the range to be allowed.

Default: [1]

Range: 1 to 65535

8 - Description

This option allows a text description of up to 19 characters of this entry in the firewall table

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
 8. Gopher                [none]        - Gopher 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)

8 - Gopher

The IP address of the Gopher server on this network may be set. (port 70)

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.

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. SMNP             [default]      - Change SMNP 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.

WAN Set-Up Menu

```
                              WAN SET-UP MENU

    Option                Value          Description
 1  Frame Relay set-up    menu         - Configure Frame Relay
 2. Link set-up           menu         - Configure link parameters
 3. Remote site set-up    menu         - Configure remote site access
 4. Security set-up       menu         - Configure security
 5. PPP set-up            menu         - Configure PPP parameters



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


>
```

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

1 - Frame Relay Set-Up

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

2 - Link Set-Up

The Link Set-up option takes you to the Link Set-Up Menu, where the link interfaces are configured.

3 - 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 connections to remote devices are maintained.

4 - Security Set-Up

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

5 - PPP Set-Up

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

Frame Relay Set-Up Menu

```
                          FRAME RELAY SET-UP MENU

    Option              Value         Description
 1. Down Link1                       - Bring down frame relay on link1
 2. Up Link1                         - Bring up frame relay on link1
 3. Link 1 LMI set-up   menu         - Set up LMI parameters
 4. Link 1             [enabled]     - Enable/disable frame relay on link 1




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

>
```

The **FRAME RELAY SET-UP MENU** allows the configuration of the frame relay parameters for link 1 of this IOLINK-SH-SR.

1 - Down Link1

Bring down the frame relay PVC on link1

2 - Up Link1

Bring up the frame relay PVC on link1

3 - Link 1 LMI Set-Up

This option takes you to the LMI Set-up menu for link 1, where the Link Management Interface parameters may be set.

4 - Link 1

The Link 1 option toggles the frame relay function for this link between enabled and disabled. If frame relay is disabled, this device will operate as a PPP leased line router.

Default: [enabled]

LMI Set-Up Menu

```
                              LMI 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 **LMI SET-UP MENU** allows the configuration of the LMI parameters of this IOLINK-SH-SR. Only the first two options will be displayed for this menu until the LMI type is known.

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 IOLINK-SH-SR 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 IOLINK-SH-SR 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 5 of the Main/Configuration/WAN set-up/Remote Site/Edit Remote Site/Circuit set-up menu), then removed (option 5 of the Main/Configuration/WAN/Remote Site set-up menu). All remote sites on a link may be cleared by toggling the enable/disable frame relay option.

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 IOLINK-SH-SR 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: [ansi]

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 after the LMI type is learned or set manually to some value other than "none":

3 - Polling Interval

The Polling Interval option specifies the time interval at which the IOLINK-SH-SR 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 IOLINK-SH-SR will request a full status update from the Frame Relay service. The Enquiry Interval is expresses in numbers of Polling Intervals. By default, every 6th 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 IOLINK-SH-SR does not receive responses to 3 of the last 4 status inquiries, the link will be considered failed.

Default: [4]

Range: 1 to 10

Link Set-Up Menu

```
                          LINK SET-UP MENU

   Option                Value          Description
 1. Link 1 operation     [enabled]    - Allow link 1 to communicate
 2. Link 1 speed         [64 kbps]    - Set speed for link 1
 3. Link 1 CD wait time  [60 sec]     - Set CD wait time for link 1




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

>
```

The **LINK SET-UP MENU** allows the configuration the link connection on this IOLINK-SH-SR.

1 - Link 1 Operation

The Link 1 Operation option toggles between [enabled] and [disabled] to allow link 1 to be used for connections.

Default: [enabled]

2 - Link 1 Speed

The Link 1 Speed option allows the definition of the clock speed generated internally by the bridge/router for link 1.

The link will clock both transmit and receive data from the clock it receives from the DCE device.

This internally generated clock may be used to clock this bridge/router and a partner bridge/router by using a custom back-to-back cable to connect the two bridge/routers together. This back-to-back connection is usually required only for testing purposes.

Choices: 9.6, 14.4, 19.2, 48, 50, 56, 64, 72, 76, 100, 128, 256, 384, 512, 768, 1024, 1544 and 2048 Kbps.

Default: [64 kbps]

3 - Link 1 CD Wait Time

The Link 1 CD Wait Time option specifies the time the bridge/router will wait for Carrier Detect on link 1. This is used primarily when interface modules must cycle through various speeds to find the one used for the link.

Default: [60 sec]

Range: 0 to 255 seconds

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. Display summary                    - Display summary of remote sites
 3. Display leaned summary             - Display summary learned
 4. Remove remote site                 - Delete remote site entry




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 frame relay PVC connections to other frame relay routers.

There are 20 configurable remote sites available, with identification numbers from 1 to 20. Each of these remote sites will have a remote site alias associated with it. Each PVC on the frame relay service must be configured within an individual remote site profile. When the frame relay router first starts up it will query the frame relay service to try to determine the PVC configurations. If the DLCI numbers of the PVC's on your service are determined during startup, the IOLINK-SH-SR 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. The alias may be up to 16 characters long; blank spaces and the character "!" are not allowed and the alias must start with a letter of the alphabet.

Considerations:

If during this learning process the maximum number of remote sites has been reached, the IOLINK-SH-SR 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 5 of the Main/Configuration/WAN set-up/Remote Site/Edit Remote Site/Circuit 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.

When configuring the IOLINK-SH-SR to use PAP or CHAP security authentication after the IOLINK-SH-SR has automatically created remote site profiles for each of the PVC's, the remote site profile alias must be changed to match the Outgoing User Name configured on the remote site router. If the local remote site alias and the remote site routers outgoing user name do not match, the PVC will always fail with a security violation.

For viewing the statistics for a particular PVC, you must view the statistics for the remote site profile configured to use that PVC.

1 - Edit Remote Site

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

Up to 20 remote sites may be defined.

2 - Display Summary

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

```
              * - Up  E - Enabled  D - Disabled   NA - Not Available

Id  Alias             FR  AC MP   Primary     DLCI  BRG IP IPX CCP CMCP BACP
 --  ---------------- --- -- -----------     ---- ---- -- --- --- ---  ----
  1  New York          RAW D  D     Link1      46   E    E  E   D   E   NA
  2  Atlanta           RAW D  D     Link1      25   E    E  E   D   E   E
  3  Vancouver         PPP D  D     Link1      18   E    E  E   D   E   D
  4  Singapore         PPP D  D     Link1      44   E    E  E   D   E   D
 41  INITIAL_PROFILE   D   D  D     none       NA   E    E  E   D   D   E
 42  LEASED1           D   D  D     none       NA   E    E  E   D   D   E
```

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: The state of the Frame Relay option for this remote site profile. *PPP* indicates that PPP encapsulation is enabled for this site. RAW indicates that PPP is disabled for this site.

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.

Primary: The link number on which the PVC has been defined. *none* indicates that the remote site has not been assigned to the link.

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

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.

3 - Display Learned Summary

The Display Learned Summary option displays the current results of the latest full status update. This display will show the DLCI's reported from the frame relay service and their corresponding state. This status display will be updated after each enquiry interval.

```
Link 1 LMI State: Up
                                        * - Up   E - Enabled   D - Disabled
 Link  DLCI  State     Link  DLCI  State     Link  DLCI  State
 ----  ----  -----     ----  ----  -----     ----  ----  -----
 1     902   *E        1     903    D        1     904    D
 1     909    D        1     910    D        1     911    D
 1     916    D        1     17     D        1     19     D
 1     21     E
```

Link: The link interface used for this PVC in this remote site profile.

DLCI: The Data Link Connection Identifier (DLCI) value used for this PVC in this remote site profile.

State: The state of the PVC in this remote site profile. An asterisk (*) beside the state indicates that the PVC is currently up.

Edit Remote Site Menu

```
                          EDIT REMOTE SITE MENU

    Option                  Value          Description
 1. Circuit set-up          menu         - Configure circuits
 2. Primary activation      menu         - Configure primary activation
 3. Protocol set-up         menu         - Configure protocols
 4. Security parameters     menu         - Configure security parameters
 5. Remote site alias      [       ]     - Alias of remote site entry
 6. Multilink operation    [       ]     - Allows multilink operation




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. When creating a new remote site profile, an alias must be entered for the new site. The first empty identifier number will be assigned to this alias and the remote site profile will be created.

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

If PPP encapsulation is disabled options 3 and 5 will not be shown.

1 - Circuit Set-Up

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

2 – Primary Activation Menu

The Primary Activation option takes you to the Primary Activation 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.

Note: this option will only appear if frame relay is disabled on this router (i.e. the device is operating as a PPP leased line router).

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, IPXCP and CCP 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 only appear if PPP encapsulation is enabled.

3/4/5 - 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 connection 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. The first character must be a letter of the alphabet.

5/6 - Multilink Operation

The Multilink Operation option defines the type of link operation that will be established to the router defined for this remote site.

When the IOLINK-SH-SR receives an incoming connection request, the Multilink state is taken from the "INITIAL_PROFILE" remote site profile. Note that if Multilink is disabled in the "INITIAL_PROFILE" and an incoming connection requests Multilink, the IOLINK-SH-SR will negotiate to have Multilink enabled.

Default: [disabled]

Note: this option will only appear if PPP encapsulation is enabled. It determines if the PPP frames sent on this PVC will be sent with Multilink headers or not.

Circuit Set-Up Menu (frame relay enabled)

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

   Option              Value              Description
 1. Frame Relay set-up menu             - Advanced Frame Relay settings
 2. Leased link       [1]               - Choose port for PVC
 3. DLCI              [16]              - FR address
 4. PPP               [disabled]        - Enable/disable PPP over Frame Relay
 5. 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 20 remote site PVCs may be defined. This version of the Circuit set up menu will be displayed if frame relay is enabled on this router.

1 - Frame Relay Set-UP Menu

The Frame Relay Set-up option takes you to the advanced set-up menu where the CIR, EIR and Time Interval parameters may be set.

2 - Leased Link

The Leased Link option defines the physical link on which this PVC will be present.

Default: [1]

Options: 1, none

Considerations:

The PVC must be disabled before this option may be changed.

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 IOLINK-SH-SR 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 disabled before this option may be changed (option 5 - State).

4 - PPP Encapsulation

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

Default: [disabled]

Considerations:

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

5 - 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]

Frame Relay Set-Up Menu

```
          EDIT REMOTE SITE n CIRCUIT SET-UP FRAME RELAY SET-UP MENU

                  Option          Value              Description

 1. CIR             [10 Kbps]           - Committed information rate
 2. EIR             [0 Kbps]            - Excess information rate
 3. Time interval   [10 (1/10th sec)]   - Interval for monitoring bandwidth




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


>
```

1 - 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

Considerations:

When changing the CIR option for this PVC, the PVC must be disabled and then enabled 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

2 - 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"

Considerations:

When changing the EIR option for this PVC, the PVC must be disabled and then enabled 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

3 - Time Interval

The Time Interval option specifies the time period (in 10ths of a second) that the IOLINK-SH-SR 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

Circuit Set-Up Menu (frame relay disabled)

```
                EDIT REMOTE SITE n CIRCUIT SET-UP MENU

   Option              Value          Description
 1. Usage set-up       menu         - Set up line useage parameters
 2. Primary link      [none]        - Configure primary link number
 3. Inactivity timer  [60 sec]      - Set traffic inactivity timer
 4. Auto-call         [disabled]    - Activate auto-call




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

>
```

The **REMOTE SITE CIRCUIT SET-UP MENU** allows the setting of parameters used for connection establishment to the remote site PPP router. This version of the menu will be displayed if the frame relay option is disabled so that this device is operating as a PPP leased line router.

1 - Usage Set-Up

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

2 - Primary Link

The Primary Link option is used to define which link interface will be used as the primary leased link to the remote site PPP router on leased line only IOLINK-SH-SRs.

When a link is removed from another remote site profile to be assigned to this remote site profile, the link will be force disconnected and then re-assigned.

Default: [none]

3 - Inactivity Timer

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

When the Inactivity Timer is set to off, this IOLINK-SH-SR will not suspend or terminate the connection. This may be used to allow only one of the IOLINK-SH-SRs to monitor the link traffic to determine when to suspend or terminate the connection.

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

4 - Auto-Call

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

Default: [disabled]

Usage Set-Up Menu

```
          EDIT REMOTE SITE 1 CIRCUIT 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 IOLINK-SH-SR will restart the usage limit timer.

Default: [unlimited]

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: [unlimited]

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 23:30

Primary Activation Menu

```
                EDIT REMOTE SITE 1 PRIMARY ACTIVATION MENU

   Option                  Value          Description
 1. Activation schedule                 - Set activation intervals
 2. Display schedule                    - View activation timetable
 3. Display time                        - View current date and time
 4. Conditional operation  [disabled]   - Allow conditional operation









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.

This menu is only displayed when frame relay is disabled on this router so that it is operating as a PPP leased line device.

1 - Activation Schedule

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

Set link establish time:

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

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

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.

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

The Remove option will remove one of the activation times.

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.
```

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.

4 - Conditional Operation

The Conditional Operation option determines if the Activation Schedule will take effect for the primary link to the remote site PPP router. When enabled, the primary link may only be established and active during the times defined within the activation schedule.

Default: [disabled]

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. IPX parameters     menu         - Configure IPX parameters
 4. CCP parameters     menu         - Configure CCP parameters




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: either RIP1 or RIP2. Both local and peer IP addresses are defined here as well.

3 - IPX Parameters

The IPX Parameters option takes you to the IPX Parameters menu for the chosen remote site, where the IPX parameters are configured. The type of link is specified as numbered or unnumbered. Both local and peer IPX addresses are defined here as well.

If PPP encapsulation is enabled with frame relay, the following option will be displayed:

4 - 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.

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 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 device.

When set to disabled, this IOLINK-SH-SR will not send the FCS on bridge frames sent to the remote site 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        [unnumbered]      - Define numbered link
 6. Peer IP address     "0.0.0.0" [none]  - Define peer IP address
 7. Negotiate address   [enabled]         - IPCP address negotiation
 8. 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 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 with the defaults for both the numbered and unnumbered link IP type settings.

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 IOLINK-SH-SR 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 that 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 IOLINK-SH-SR 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 NAPT is enabled for NAPT to work. The global IP address may be configured locally (if RAW 1490 frame relay is used) or negotiated (if PPP encapsulation is enabled) 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. (ie. the private IP address that is used on the private network).

Note: if NAT is enabled with IP addressing (under the NAT Advanced menu) and Firewall is enabled, then the IP address for this remote site must be in the firewall table.

Default: [disabled]

5 - Link IP Type

The Link IP Type option defines the type of link connection that will be established with the remote site 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 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: [numbered]

Choices: numbered, unnumbered

6 - Peer IP Address

The Peer IP Address option allows the definition of an Internet Protocol (IP) address and corresponding subnet size of the IP router at the remote site.

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 - 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 - VJ Compression

The VJ Compression option enables or disables Van Jacobson header compression on packets send to this remote site.

Default: [disabled]

IP Parameters - 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 IOLINK-SH-SR 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 IOLINK-SH-SR 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 IOLINK-SH-SR 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 IOLINK-SH-SR 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 IOLINK-SH-SR 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 IOLINK-SH-SR will participate in RIP IP routing messages over the link to this remote site.

When the RIP mode is set to both, the IOLINK-SH-SR will send and receive RIP routing messages over the link to this remote site.

When the RIP mode is set to send_only, the IOLINK-SH-SR will only send and not receive RIP routing messages over the link to this remote site.

When the RIP mode is set to receive_only, the IOLINK-SH-SR will only receive and not send 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 IOLINK-SH-SR 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 IOLINK-SH-SR 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 and SAP. If triggered RIP has not been negotiated after the 5 minutes, this router will fall back to using normal RIP and SAP.

Default: [disabled]

Choices: disabled, standard, link_up_only

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]

IP Parameters – 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




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”.

IPX Parameters Menu

```
                EDIT REMOTE SITE 1 IPX PARAMETERS MENU

   Option              Value                Description
 1. IPX   enabled      [enabled]          - Enable IPX protocol
 2. Link IPX type      [unumbered]        - Define numbered link
 3. Static routes only [disabled]         - Only use static IPX routes
 4. IPX DMR enabled    [disabled]         - Enable Demand RIP
 5. Force RIP update   [disabled]         - Enable forced regular RIP updates


 1. IPX   enabled      [enabled]          - Enable IPX protocol
 2. Link IPX type      [numbered]         - Define numbered link
 3. IPX net            "0"                - Define IPX network number
 4. Local IPX node     "00-00-00-00-00-00" - Define local IPX node number
 5. Peer IPX node      "00-00-00-00-00-00" - Define peer IPX node number
 6. Static routes only [disabled]         - Only use static IPX routes
 7. IPX DMR enabled    [disabled]         - Enable Demand RIP
 8. Force RIP update   [disabled]         - Enable forced regular RIP updates

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

>
```

The **IPX PARAMETERS MENU** allows the setting of the type of IPX link connection to the remote site router. The parameters defined here are used by the IPX (Internet Packet Exchange) functions of the router for negotiating IPX routing during call establishment. The menu options are shown in the above screen with the defaults for both the numbered and unnumbered link IPX type settings.

1 - IPX Enabled

The IPX Enabled option enables or disables the Internet Packet Exchange negotiations for this remote site. When a connection to this remote site does not require IPX routing, this option may be disabled.

Default: [enabled]

2 - Link IPX Type

The Link IPX Type option defines the type of link connection that will be established with the remote site router. The link may be:

1. Numbered - This is where both sides of the WAN connection have IPX node addresses assigned and the WAN connection has it's own IPX network number.
2. Unnumbered - This is where the local and peer (remote partner router) routers use their internal LAN side IPX node numbers.

When operating in unnumbered mode, each of the two IPX routers operates as half of a complete router. The WAN connection is considered a common internal data path with the IPX routing actually taking place between the two remote LANs.

When the link IPX type is set to unnumbered, the IPX Net, Local IPX Node, and Peer IPX Node options are not available.

When the link IPX type is set to numbered, the IPX network and local and peer IPX node numbers should be defined to ensure proper IPXCP negotiations between the local and peer IPX routers.

Default: [unnumbered]

Choices: numbered, unnumbered

Note: if NAT is used with RAW Frame Relay (PPP encapsulation disabled), and if numbered links are used, then both the local and peer IPX node addresses must be entered (options 4 and 5) – IPX addresses are not negotiated with PPP encapsulation disabled. If the remote router uses unnumbered links, only the peer address is required.

3 - IPX Net

The IPX Net option allows the definition of the IPX network number to use for the WAN connection when operating in numbered mode for this IPXCP link to the remote site router.

Default: [0]

```
Enter :
    Network number (up to 8 characters)
>
```

4 - Local IPX Node

The Local IPX Node option allows the definition of an Internet Packet Exchange (IPX) node address for the link of this router.

When the link IPX type is set to unnumbered, the Local IPX Node option is not available.

The IPX Node address consists of 12 hexadecimal bytes. The address may be entered with or without the hyphens. An example of an IPX node address may be 00-00-d0-00-12-13, and would be entered as such or simply as 0000d0001213.

Default: [00-00-00-00-00-00]

```
Enter :
    IPX node number (up to 17 characters)
>
```

5 - Peer IPX Node

The Peer IPX Node option allows the definition of an Internet Packet Exchange (IPX) node address for the link side of the IPX router at the remote site.

When the link IPX type is set to unnumbered, the Peer IPX Node option is not available.

Default: [00-00-00-00-00-00]

```
Enter :
    IPX node number (up to 17 characters)
>
```

3 / *6* - Static Routes Only

The Static Routes only option determines the type of IPX routing to perform on the connection with the peer IPX router. By enabling this option, only the static IPX routes and services defined in the IPX Routing Set-up menu will be used to perform IPX routing with the peer IPX router.

Default: [disabled]

4 / *7* - IPX DMR Enabled

The IPX DMR Enabled option defines or disables demand RIP for IPX routing with the peer IPX router. Demand RIP allows the IPX routing tables to be updated only when there has been a change in the routing table.

Disabling this option will cause the IPX RIP routing tables to be transmitted every 60 seconds.

Entering "standard" enables demand RIP; the IOLINK-SH-SR will only send RIP messages over the link to this remote site when the routing information has actually changed.

Entering "link_up_only" enables demand RIP; the IOLINK-SH-SR 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 demand RIP is enabled, if the remote site router refuses to negotiate demand RIP on the initial connection, this router will attempt to negotiate demand RIP for 5 minutes. During the 5 minutes, this router will use normal RIP and SAP. If demand RIP has not been negotiated after the 5 minutes, this router will fall back to using normal RIP and SAP.

Default: [disabled]

Choices: disabled, standard, link_up_only

5 / *8* - Force RIP Update

The Force RIP Update option determines if the IOLINK-SH-SR will send a RIP update request to the WAN peer IPX router when a local LAN RIP update is sent. Operating under normal RIP update times forces the WAN partners to provide their RIP tables when requested to maintain proper routing information.

Default: [disabled]

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 data compression for data packets sent from the remote site PPP router and received by this router. The IOLINK-SH-SR performs data compression at the bundle level and not at the link level. Link based compression will be rejected. The IOLINK-SH-SR supports CCP option 17 - PPP Stac LZS Compression Protocol.

When the Compression option is enabled, this router will allow data compression to be negotiated from the remote site PPP 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 to allow for the two byte sequence numbering.

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 security on the connection to this remote site router.

1 - Incoming PAP password

The Incoming PAP Password option defines the PAP password that this Orbiter router expects to receive from the remote site 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 Orbiter router expects to receive from the remote site 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 IOLINK-SH-SR router will be sending to the remote site router when responding to authentication requests from the remote site 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 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 Orbiter will use when responding to authentication requests from the remote site router.

Default: [none]

5 - Outgoing CHAP secret

The Outgoing CHAP Secret option defines the CHAP secret that this Orbiter will use when responding to authentication requests from the remote site router.

Default: [none]

Security Set-Up Menu

```
                          SECURITY SET-UP MENU

    Option                  Value            Description
 1. Security level         [none]          - Set security protocol
 2. Request security       [always]        - Set security operation
 3. CHAP challenges        [once]          - CHAP Authentication



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

>
```

The **SECURITY SET-UP MENU** allows the display and configuration of the security database as well as the outgoing security options for this router.

1 - Security Level

The Security Level option defines the type of security to use for incoming calls. When a security level is set, the IOLINK-SH-SR will always require authentication on incoming calls. The IOLINK-SH-SR will ask for authentication on outgoing calls when a security request is set to always (see below).

Default: [none]

Choices: none, PAP, CHAP

2 - Request security

This specifies when the remote site router should be requested to authenticate:

- always (when this router makes an outgoing call OR receive an incoming call)
- incoming_only (ONLY when this router receives an incoming call)

Default: [always]

Choices: always, incoming only

3 - CHAP Challenges

The CHAP Challenges option defines the frequency of CHAP challenges that this IOLINK-SH-SR router will require when authenticating a remote site router.

Default: [once]

Choices: once, continuous

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** provides for general 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 IOLINK-SH-SR 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 IOLINK-SH-SR 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 IOLINK-SH-SR 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 IOLINK-SH-SR 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 IOLINK-SH-SR PPP router will request Address and Control Field Compression on the link that is established to the peer PPP router.

Default: [enabled]

2 - PFC

The PFC (Protocol Field Compression) option determines if this IOLINK-SH-SR PPP router will request Protocol Field Compression on the link that is established to the peer PPP router.

Default: [disabled]

3 - Echo Monitoring

The Echo Monitoring option determines if this IOLINK-SH-SR PPP router will generate Echo-Request messages on the link that is established to the peer PPP router. 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 IOLINK-SH-SR PPP router will request Link Quality Protocol monitoring on the link that is established to the peer PPP router.

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 the Multilink header. When set to disabled, the NCP messages are not encapsulated within the Multilink frames.

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 IOLINK-SH-SR 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 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

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 addition/deletion or move occurs, the new location can be manually added to the table or the timer value can be temporarily reduced to learn the new change(s). 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 ISDN 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 ISDN 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 ISDN WAN connection to the remote site.

Location

Internal

These are the STP Multicast and LAN port MAC addresses located (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/routers 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. LAN port             menu         - Define port specific options
 2. STP state           [enabled]     - Enable/disable Spanning Tree Protocol
 3. Bridge priority     [32768]       - Define root bridge selection priority
 4. Forwarding delay    [15 sec]      - Set delay before forwarding begins
 5. Message age timer   [20 sec]      - Receive hello message interval
 6. Hello time          [2 sec]       - Set hello message transmission interval
 7. Show bridge                       - View bridge STP status
 8. 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.

1 - LAN Port

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

> 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
> Maximum age — Option 6
> Hello time — Option 7
>
> If these values are set differently upon start-up, the values set on the bridge/router with the lowest MAC address will prevail.

2 - 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**.

3 - 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.

4 - 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 **default: 28 _ 20**

5 - 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 **default: 28 _ 20**

The following relationship to Hello Time must be maintained:
Max Age _ 2x (Hello Time + 1.0) **default: 20 _ 6**

6 - 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) **default: 20 _ 6**

7 - 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 at each bridge with Options 4, 5, and 6.

** These parameters are defined by the Root bridge.

*** 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.)

8 - 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.

LAN Port Menu

```
                              LAN PORT MENU

    Option       Value          Description
 1. State       [enabled]     - Enable/disable LAN 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 PORT MENU** allows the management of the port's 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 either 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.

IP Routing Set-Up Menu

```
                          IP ROUTING SET-UP MENU

    Option                  Value                 Description
 1. IP routes               menu                - Modify/view routes
 2. IP routing             [enabled]            - Enable/disable IP router
 3. IP forwarding          [enabled]            - Enable/disable IP routing
 4. LAN routing protocol   [rip1_compatible]    - Define routing protocol
 5. LAN RIP mode           [both]               - Define RIP send/receive mode
 6. LAN route cost         [0]                  - Cost added to route learned
 7. 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 - IP Routing

The IP Routing option enables or disables the IP routing functions of the router.

Default: [disabled]

Considerations:

When IP Routing is disabled, all learned RIP routes will be cleared from the routing table.

3 - 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: [disabled]

4 - LAN Routing Protocol

The LAN Routing Protocol option defines the type of IP routing protocol to be used on the LAN interface. The IOLINK-SH-SR 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 IOLINK-SH-SR 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 IOLINK-SH-SR 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 IOLINK-SH-SR 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 IOLINK-SH-SR will operate as a RIP2 IP router. All routing information will be sent via multiast RIP2 packets. Routing information may be received as broadcast RIP2 or multicast RIP2.

Default: [rip1_compatible]

Choices: none, rip1, rip1_compatible, rip2

5 - LAN RIP Mode

The LAN RIP Mode option defines how this IOLINK-SH-SR will participate in RIP IP routing messages on the LAN.

When the RIP mode is set to both, the IOLINK-SH-SR will send and receive RIP routing messages on the LAN.

When the RIP mode is set to send_only, the IOLINK-SH-SR will only send and not receive RIP routing messages on the LAN.

When the RIP mode is set to receive_only, the IOLINK-SH-SR will only receive and not send RIP routing messages on the LAN.

Default: [both]

Choices: both, send_only, receive_only

6 - LAN Route Cost

The LAN Route Cost option defines the amount of extra routing cost to add to routes learned from the LAN.

Default: [0]

7 - ARP Proxy

The IOLINK-SH-SR Ethernet router will respond to ARP requests destined for other networks, from its local network, when this option is enabled. The IOLINK-SH-SR will reply to any matching route in the routing table. The IOLINK-SH-SR 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. Show all routes                      - Display the route table
 3. Show static routes                   - Display only static routes
 4. 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 - 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 : 9
Destination      Mask    Next Hop       Remote Site                    Route
IP Address       Size   IP Address     Config Connect   Cost  Age     Type
--Start of table--
default route      0  198.168.1.1           -       -     1     0   LOCAL
+default route     0  192.168.95.190        -       -    16    74   OTHER
190.190.190.0     25  190.190.190.190       -       -     1     0   LOCAL
192.168.95.176    28  192.168.95.190        -       2     2     0   RIP
192.168.95.190    32  192.168.95.190        2       2     2     0   CONNECT
198.169.1.0       24  198.169.1.150       LAN     LAN     1     0   DIRECT
198.169.1.150     32  198.169.1.150       INT     INT     1     0   DIRECT
--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.
Remote Site Config:	Remote site profile ID number configured to use for this route. When a remote site profile is used as the next hop in a static route, the ID number will be

displayed here and the remote site profile alias will be displayed in the next hop IP address field. LAN indicates that this route is on the local LAN.

Remote Site Connect: Remote site ID number that this route is currently using. LAN indicates that this route is on the local LAN.

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.
LOCAL is used for static routes.
CONNECT indicates the route is on a connected peer IP router on an unnumbered link.
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.

3 - Show Static Routes

The Show Static Routes option displays all of the static routes currently in use by the router.

Static IP Routes

Destination IP Address	Mask Size	Next Hop IP Address	Remote Site Config	Remote Site Connect	Cost	Age	Route Type
--Start of table--							
default route	0	198.168.1.1	-	-	1	0	LOCAL
190.190.190.0	25	190.190.190.190	-	-	1	0	LOCAL
192.168.95.190	32	192.168.95.190	2	2	2	0	CONNECT
198.169.1.0	24	198.169.1.150	LAN	LAN	1	0	DIRECT
198.169.1.150	32	198.169.1.150	INT	INT	1	0	DIRECT
--End of table--							

4 - Clear Static Routes

The Clear Static Routes option clears all of the static routes from the routing table.

Edit Route Menu

```
                          EDIT ROUTE MENU

    Option          Value          Description
 1. Network mask  *[        ]   - The network mask for the route
 2. Status        *[        ]   - Is the address in the table
 3. Remote site   *[        ]   - Remote site alias of the next hop
 4. Next hop      *[        ]   - IP address of the next hop
 5. Type          *[        ]   - Type of route
 6. Cost           [        ]   - Cost to reach destination in hops
 7. Private        [        ]   - Do not advertise route
 8. Remove                      - Remove address from 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 192.3.44.0 / 24 199.2.5.12 MENU

    Option          Value               Description
 1. Network mask  *"255.255.255.0"   - The network mask for the route
 2. Status        *"Added"           - Is the address in the table
 3. Remote site   *"none"            - Remote site alias of the next hop
 4. Next hop      *"199.2.5.12"      - IP address of the next hop
 5. Type          *"LOCAL"           - Type of route
 6. Cost           [1]               - Cost to reach destination in hops
 7. Private        [disabled]        - Do not advertise route
 8. Remove                           - Remove address from 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 - 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.

2 - 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]

3 - Remote Site

The Remote Site option defines the remote site profile ID or alias of the remote site router to be used to reach the destination IP address.

4 - Next Hop

The Next Hop option defines the IP address of the next-hop router to be used to reach the destination IP address.

5 - 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.

6 - Cost

The Cost option defines the number of hops required to reach the destination IP address.

Default: [1]

Range: 1 - 15

7 - Private

The Private option when set to enabled causes the IOLINK-SH-SR to not advertise this route in the RIP messages.

Default: [disabled]

8 - Remove

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.

IPX Routing Set-Up Menu

```
                          IPX ROUTING SET-UP MENU

    Option                    Value         Description
 1. Static routes             menu        - Edit/display static routes
 2. Static services           menu        - Edit/display static services
 3. Configure LAN networks    menu        - Configure LAN network numbers
 4. IPX routing              [enabled]    - Enable/disable IPX router
 5. IPX forwarding           [enabled]    - Enable/disable IPX routing
 6. Local networks                        - Display local network connections.
 7. Show routes                           - Display the route table
 8. Show services                         - Display the service table
 9. Help                                  - Description of IPX routing



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

>
```

The **IPX ROUTING SET-UP MENU** allows the display and configuration of the IPX Routing parameters for the router.

1 - Static Routes

The Static Routes option directs you to the Static Routes Menu, where user defined IPX static routes are maintained.

2 - Static Services

The Static Services option directs you to the Static Services Menu, where user defined IPX static services are maintained.

3 - Configure LAN Networks

The Configure LAN Networks option directs you to the Configure LAN Networks Menu, where network numbers may be assigned for the four frame types supported by this router.

4 - IPX Routing

The IPX Routing option enables or disables the IPX routing functions of the router.

Default: [enabled]

Considerations:

Routing information (RIP) will only be transmitted across the WAN to the partner router according to the state of the IPX DMR Enabled option within the IPX Parameters menu of the remote site profile used to establish a PPP connection. If demand RIP is enabled, RIP messages will only be transmitted when there is a change.

When IPX Routing is disabled, all learned RIP routes will be cleared from the routing table.

5 - IPX Forwarding

The IPX Forwarding option enables or disables the forwarding of IPX traffic when IPX routing is enabled. When the IPX forwarding option is disabled, IPX traffic across the WAN links will be blocked

Default: [enabled]

Considerations:

When IPX Forwarding is disabled all learned RIP routes will be cleared from the routing table.

6 - Local Networks

The Local Networks option displays all of the IPX network numbers currently in use by the router on each of its interfaces.

```
                  LOCAL IPX NETWORKS

LAN Interface:
    Ethernet II          51524
    Raw 802.3            0
    IEEE 802.2           0
    802.2 Snap           0

WAN Interface:
    SITE2                14526
```

7 - Show Routes

The Show Routes option displays all of the learned IPX routes currently in use by the router.

There is a maximum of 512 route entries allowed in the table.

```
                        IPX Routes
Total entries : 7

 Network   Interface          Next Hop      Hops    Ticks
-------------------------------------------------------
 51524     local                local         0         1
 126       lan              205204239749     2        50
 14526     SITE2            992400423941     2        50
```

Network: IPX Network Address of the remote network.

Interface: Interface that the IPX network is located on; either local, LAN or remote site router.

Next Hop: IPX address of the next-hop router to use to reach the Destination IPX Network.

Hops: Number of hops to reach the Destination IPX Network.

Ticks: Number of ticks to reach the Destination IPX Network.

Considerations:

A 9600-bps link on this router has a tick value of 5.

8 - Show Services

The Show Services option displays all of the Servers currently seen by the router. The Services table is created from information received by this router in SAP (Server Advertising Protocol) packets generated by Novell Servers.

There is a maximum of 512 server entries allowed in the table.

```
                        IPX Services
Total entries : 3
 Type      Server Address         Hops  Server Name
-------------------------------------------------
 0004  00000311:0000ff3a4001:0451   2  SQA_SERVER_311
 0004  00000312:00004ac38445:0451   6  NOVELL312
 0004  00000401:000e03448a32:0451   2  NOVELL_401
```

Type:	Novell Server types. Some possible Server types are:

Unknown	0
Print Queue	3
File Server	4
Job Server	5
Print Server	7
Archive Server	9
Remote Bridge Server	24
Advertising Print Server	47

Server Address:	IPX address of the Server.
Hops:	Number of hops to reach the Server from this router.
Server Name:	Name of the Server.

9 - Help

The Help option offers a brief description of the IPX routing options.

Static IPX Routes Menu

```
                          STATIC ROUTES MENU

    Option                Value          Description
 1. Edit route            menu         - Modify a route in the table
 2. Convert route                      - Make a learned route static
 3. Show static routes                 - Display static routes
 4. Clear static routes                - Remove groups of static routes









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

>
```

The **STATIC IPX ROUTES MENU** allows the display and configuration of the static IPX routing tables.

1 - Edit Route

The Edit Route option directs you to the Edit Route Menu where the static IPX routing table entries are modified. A maximum of 50 static IPX routes may be defined.

2 - Convert Route

The Convert Route option is used to convert one of the currently learned IPX routes into an IPX static route. Enter the IPX network number of the learned route when prompted and then enter a static route id number. The learned IPX route will become a static IPX route.

```
Enter:
  network number

>


Enter:
  static route entry id
>
```

3 - Show Static Routes

The Show Static Routes option displays all of the static IPX routes currently in use by the router.

```
                              IPX Static Routes
 Total entries : 2

 ID   Network   Interface         Next Hop      Hops  Ticks
-------------------------------------------------------------
 1    00000012  lan               000000012345   1        1
 2    00004143  SITE2             n/a            1        1
```

ID:	Entry number in the static IPX routes table.
Network:	IPX Network Address of the remote network.
Interface:	Interface that the IPX network is located on, either LAN or remote site router.
Next Hop:	IPX address of the next-hop router to use to reach the Destination IPX Network.
Hops:	Number of hops to reach the Destination IPX Network.
Ticks:	Number of ticks to reach the Destination IPX Network.

4 - Clear Static Routes

The Clear Static Routes option clears the specified static IPX routes from the routing table.

```
Enter:
  all, lan, remote site id or alias (up to 16 characters)
>
```

Edit Static IPX Route Menu

```
                              EDIT ROUTE MENU

    Option        Value          Description
 1. Status      *[         ]   - Is entry in static route table
 2. Network      [         ]   - Destination network number
 3. Interface    [         ]   - Interface to destination network
 4. Hops         [         ]   - Hops to destination network
 5. Ticks        [         ]   - Ticks to destination network









Enter:
    entry id (from 1 to 50)


> 1
```

The above display is the first level of the **EDIT ROUTE MENU**. The table id number must be entered to proceed to the next level.

The menu title will change to indicate the table id number that is being edited.

```
                           EDIT ROUTE 1 MENU

    Option        Value             Description
 1. Status      *"Not Present"    - Is entry in static route table
 2. Network      "0"              - Destination network number
 3. Interface    ""               - Interface to destination network
 4. Hops         [1]              - Hops to destination network
 5. Ticks        [1]              - Ticks to destination network









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


>
```

NOTE: A Static Route will **NOT** be replaced with a RIP route, even if the hop and tick count is lower.

1 - Status

The Status option tells whether the static route is "Present" or "Not Present" in the Routing Table. When the route entry is first entered, "Not Present" is the Status value. The * beside the value indicates that this value is changed automatically as an entry is added or deleted and cannot be manually redefined.

Default: * [Not Present]

2 - Network

The Network option defines the destination IPX network address of the static route.

3 - Interface

The Interface option defines the interface, either LAN or remote site device, that the destination IPX network is located on. A value of LAN indicates that another IPX router located on the locally connected LAN is to be used to access the destination IPX network. When the interface is set to LAN, the option Next Hop will be available to define the MAC address of the router located on the locally connected LAN.

A value of a remote site profile name or id indicates that the destination IPX network is located on the remote site IPX router. The Next Hop option is not required and therefore not available when a remote site profile is defined for the interface.

4 - Next Hop

The Next Hop option defines the MAC address of the next-hop IPX router on the locally connected LAN to be used to reach the destination IPX network. The next-hop router must be on the local IPX network.

5 - Hops

The Hops option defines the number of hops to reach the destination IPX network.

Default: [1]

Range: 1 - 15

6 - Ticks

The Ticks option defines the number of ticks to reach the destination IPX network.

Default: [1]

Range: 1 - 64000

7 - Remove

The Remove option removes the IPX static route from the routing table.

Static IPX Services Menu

```
                          STATIC SERVICES MENU

    Option                    Value          Description
 1. Edit service              menu         - Edit a static service
 2. Convert service                        - Make a learned service static
 3. Show static services                   - Display the service table
 4. Clear static services                  - Remove groups of static services









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

>
```

The **STATIC IPX SERVICES MENU** allows the display and configuration of the static IPX services.

1 - Edit Service

The Edit Service option directs you to the Edit Service Menu where the static IPX service entries are modified. A maximum of 50 static IPX services may be defined.

2 - Convert Service

The Convert Service option is used to convert one of the currently learned IPX services into an IPX static service. Enter the server name and service type of the learned service when prompted and then enter a static service id number. The learned IPX service will become a static IPX service.

```
Enter:
  server name

>


Enter:
  hex service type
>


Enter:
  static service entry id
>
```

3 - Show Static Services

The Show Static Services option displays all of the static IPX services currently in use by the router.

```
                              IPX Static Services
 Total entries : 2

 ID Interface        Type Server Address             Hops Server Name
-------------------------------------------------------------------------
  1 lan              0017 00000002:000000015223:0000  0   Mars
```

ID:	Entry number in the static IPX services table.
Interface:	Interface that the IPX service is located on, either LAN or remote site router.
Type:	Hex value of the type of IPX service.
Server Address:	IPX Address of the server.
Hops:	Number of hops to reach the server.
Server Name:	Name of the server.

4 - Clear Static Services

The Clear Static Services option clears the specified static IPX services from the table.

```
Enter:
  all, lan, remote site id or alias (up to 16 characters)
>
```

Edit Static IPX Service Menu

```
                          EDIT SERVICE MENU

    Option          Value          Description
 1. Status        *[        ]   - Is entry in static route table
 2. Server name    [        ]   - Novell server name
 3. Service type   [        ]   - Novell service type
 4. Interface      [        ]   - Interface to service
 5. Network        [        ]   - Server's network number
 6. Node           [        ]   - Server's node number
 7. Socket         [        ]   - Service's socket number
 8. Hops           [        ]   - Hops to server


Enter:
    entry id (from 1 to 50)


> 1
```

The above display is the first level of the **EDIT SERVICE MENU**. The table id number must be entered to proceed to the next level.

The menu title will change to indicate the table id number that is being edited.

```
                       EDIT SERVICE 1 MENU

    Option          Value                   Description
 1. Status        *"Not Present"          - Is entry in static route table
 2. Server name    ""                     - Novell server name
 3. Service type   [0]                    - Novell service type
 4. Interface      ""                     - Interface to service
 5. Network        "0"                    - Server's network number
 6. Node           "00-00-00-00-00-00"    - Server's node number
 7. Socket         [0]                    - Service's socket number
 8. Hops           [0]                    - Hops to server



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


>
```

NOTE: A Static Service will **NOT** be replaced with a SAP learned service, even if the hop count is lower.

1 - Status

The Status option tells whether the static service is "Present" or "Not Present" in the Table. When the service entry is first entered, "Not Present" is the Status value. The * beside the value indicates that this value is changed automatically as an entry is added or deleted and cannot be manually redefined.

Default: * [Not Present]

2 - Server Name

The Server Name option defines the IPX server name of the static service.

3 - Service Type

The Service Type option defines the type of IPX service as a hex value.

Default: [0]

Range: 0 - ffff

4 - Interface

The Interface option defines the interface, either LAN or remote site device, which the IPX service is located on. A value of LAN indicates that the service is located on the locally connected LAN.

A value of a remote site profile name or id indicates that the service is located on the remote site IPX router's network.

5 - Network

The Network option defines the IPX network address of the static service.

6 - Node

The Node option defines the IPX node address of the static service.

7 - Socket

The Socket option defines the socket number of the static service if applicable.

8 - Hops

The Hops option defines the number of hops to reach the IPX service.

Default: [0]

Range: 0 - 15

Configure LAN Networks Menu

```
                        CONFIGURE LAN NETWORKS MENU

   Option               Value          Description
 1. Ethernet-II frames  "0"          - IPX network number
 2. RAW 802.3 frames    "0"          - IPX network number
 3. IEEE 802.2 frames   "0"          - IPX network number
 4. 802.2 SNAP frames   "0"          - IPX network number
 5. Auto Learn          [enabled]    - Auto learn IPX network numbers
 6. Help                             - Description of IPX frame types



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

>
```

The **CONFIGURE LAN NETWORKS MENU** allows the configuration of the IPX network numbers on this router for each IPX frame type on the local LAN.

1 - Ethernet-II Frames
2 - RAW 802.3 Frames
3 - IEEE 802.2 Frames
4 - 802.2 SNAP Frames

A value of "0" indicates that the router will learn the network number associated with this frame type upon receiving the first IPX frame of this frame type.

Default: [0]

Range: 0 to FFFFFFFF hex

Considerations:

Once an IPX network number is defined or learned, all further IPX frames of that frame type will use the network number. If a different network number is found for that frame type, the first network number defined or learned will continue to be used.

5 - Auto Learn

Enables or disables the auto learning of IPX network numbers for this IPX router. All IPX network numbers will be taken from the user defined values within options 1 through 4 in this menu.

Default: [enabled]

6 - Help

The Help option offers a brief description of the IPX frame types and network numbers.

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
 4. IPX router pattern filters  menu        - Define IPX 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.

4 - IPX Router Pattern Filter

The IPX Router Pattern Filter takes you to the IPX Router Pattern Filter Menu, where you can create IPX 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.

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  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
```

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 IOLINK-SH-SR bridge/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 [enable]. 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.
```

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


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

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)

IPX Router Pattern Filter Menu

```
                    IPX 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 **IPX 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 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.

```
                    IPX Router Filter Pattern Aliases

 1. NETBIOS    - 5-14
```

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 IPX Pattern Filters
Id    Pattern
--    ----------------------------
1     12-600x
3     LAT
```

Vancouver (Remote Site alias)

```
                        IPX Pattern Filters to Vancouver
Id    Pattern
--    ----------------------------
2     0-010203040506&12-809B
```

all

```
                    Summary of all IPX 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)
> 9-600x

Enter:
  pattern ID number (from 1 to 64)
> 2
```

A **global** filter pattern will be applied to all IPX routed data.

A **LAN** filter pattern will be applied to all IPX routed data being sent to the local LAN.

A **Remote Site Id or Alias** filter pattern will be applied to all IPX 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)

Statistics Menu

```
                              STATISTICS MENU

    Option                Value          Description
 1. Statistics set-up     menu         - Define statistics operation
 2. LAN statistics        menu         - Access LAN statistics
 3. WAN statistics        menu         - Access WAN statistics









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


>
```

The **STATISTICS MENU** provides paths to Menus for access to complete router statistics.

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 - LAN Statistics

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

3 - WAN Statistics

The WAN Statistics option takes you to the WAN Statistics Menu, where statistics can be examined to evaluate WAN performance.

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], the following statistics displays are unavailable:
- **Frame Size**, LAN Statistics Menu

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).
- **IPX 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.

LAN Statistics Menu

```
                          LAN STATISTICS MENU

   Option                      Description
 1. Bridged traffic        - Summary of Bridge traffic
 2. IP traffic             - Summary of IP Router traffic
 3. IPX traffic            - Summary of IPX Router traffic
 4. Total LAN traffic      - Summary of LAN traffic
 5. LAN error              - View LAN errors history
 6. Frame size             - View frame size history
 7. Clear LAN statistics   - Reset LAN statistics
 8. 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.

3 - IPX Traffic

The IPX Traffic option displays a summary of IPX Router LAN traffic since the statistics were last reset.

4 - Total LAN Traffic

The Total LAN Traffic option displays a summary of Total LAN traffic since the statistics were last reset.

5 - LAN Error

The LAN Error option displays a summary of LAN and router errors since the statistics were last reset.

6 - Frame Size

The Frame Size option displays a summary of the distribution of LAN Frame Sizes since the statistics were last reset.

Considerations:

This option is available only if Extended Stats in the Statistics Set-Up Menu is Enabled.

7 - Clear LAN Statistics

The Clear LAN Statistics option clears all statistic fields in the LAN statistics to zero.

8 - 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


                                        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

Frames to LAN              4215689          221         416         441
Bytes to LAN             269806208        14171       26667       28236

Frames from WAN            4169752          219         416         441
Bytes from WAN           268464916        14024       26667       28250
Frames  filtered from WAN        0            0           0           0

Frames to WAN               215689          121         416         441
Bytes to WAN               2696208        14171       26667       28236




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

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 local LAN.
Bytes from LAN	All bridge data bytes successfully received from the local LAN.
Frames filtered from LAN	All bridge data frames received from the local 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 local LAN.
Bytes to LAN	All bridge data bytes successfully placed upon the local LAN.
Frames from WAN	All bridge data frames successfully received from partner routers.
Bytes from WAN	All bridge data bytes successfully received from partner routers.
Frames filtered from WAN	All bridge data frames received from the partner routers 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 WAN	All bridge data frames successfully sent to partner routers.
Bytes to WAN	All bridge data bytes successfully sent to partner routers.

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.

```
                    LAN Tokyo Routed 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
Frames to LAN            4169752        219        416        441
Bytes to LAN           268464916      14024      26667      28250

Frames from WAN          9802916      14024      26667      28250
Bytes from WAN           4169752        219        416        441
Frames filtered from WAN    1982          6          0        840
Frames to WAN                269         14         27         28
Bytes to WAN                 270         15         28         29

ARP Discards                   0          0          0          0
Redirect Sent                269         14         27         28
Unreachable Sent               0          0          0          0


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

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 local LAN.
Bytes from LAN	All IP bytes successfully received from the local LAN.
Frames filtered from LAN	All IP frames received from the local 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 local LAN.
Bytes to LAN	All IP bytes successfully received from partner routers and placed upon the local LAN.
Frames from WAN	All IP frames successfully received from the local LAN and forwarded to partner routers.
Bytes from WAN	All IP bytes successfully received from the local LAN and forwarded to partner routers.
Frames filtered from WAN	All IP frames received from partner routers 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 WAN	All IP frames successfully forwarded to partner routers.
Bytes to WAN	All IP bytes successfully forwarded to partner routers.
ARP Discards	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	The number of ICMP Redirect messages generated.
Unreachable Sent	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.

IPX Traffic Summary Display (Option 3)

This screen displays IPX Routed LAN traffic statistics gathered since the statistics were last reset and reports statistics generated within the current statistics interval.

```
                        LAN Tokyo IPX 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
Congestion discards from LAN      0            0           0           0

Frames to LAN              269806208        14171       26667       28236
Bytes to LAN                 4169752          219         416         441

Frames from WAN            268464916        14024       26667       28250
Bytes from WAN               4169752          219         416         441
Frames filtered from WAN        1982            6           0         840

Frames to WAN                    269           14          27          28
Bytes to WAN                     270           15          28          29

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

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 bridge/router occurred.

IPX Traffic Summary Statistics Definitions	
Frames from LAN	All IPX frames successfully received from the local LAN.
Bytes from LAN	All IPX bytes successfully received from the local LAN.
Frames filtered from LAN	All IPX frames received from the local LAN and filtered by the router. This includes IPX frames filtered because the frame meets pattern filtering criteria or the frame was unsuccessfully received because of an error.
Congestion Discards from LAN	IPX Data frames discarded because of internal congestion between the LAN and the IPX module
Frames to LAN	All IPX frames successfully placed upon the local LAN.
Bytes to LAN	All IPX bytes successfully placed upon the local LAN.
Frames from WAN	All IPX frames successfully received from partner routers.
Bytes from WAN	All IPX bytes successfully received from partner routers.
Frames filtered from WAN	All IPX frames received from partner routers and filtered by the router. This includes IPX frames filtered because the frame meets pattern filtering criteria or the frame was unsuccessfully received because of an error.
Frames to WAN	All IPX frames successfully forwarded to partner routers.
Bytes to WAN	All IPX bytes successfully forwarded to partner routers.

Total LAN Traffic Summary Display (Option 4)

This screen displays statistics gathered since the statistics were last reset and reports statistics generated within the current statistics interval.

```
                    LAN Tokyo Total 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
Congestion Discards to WAN       0        0           0           0

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.
```

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.
Congestion Discards to WAN	This occurs when the router has to discard frames destined for the WAN because too many frames are waiting for processing inside the router and buffer space is unavailable.
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 5)

```
                        LAN Calgary Error Summary

Bridge Errors                              LAN Errors
-------------------------------------------------------------------------
Loss of Carrier           : 0              CRC Errors                : 0
Underflow Errors          : 0              Framing Errors            : 0
Overflow Errors           : 0              Single Collision          : 0
Receive Buffer Congest    : 0              Multiple Collisions       : 0
Receiver Misses           : 0              Transmit Retry Failures   : 0
Transmit Buffer Errors    : 0              Late Collisions           : 0
Memory Errors             : 0              Heartbeat Failure         : 0


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

Bridge 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.
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. Some faulty transceiver 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.

Frame Size Display (Option 6)

```
                    LAN Calgary Frame Size Distribution

  Range             From LAN        Forwarded              To LAN
-------------------------------------------------------------------
64 - 127              111331           111331               99980
128 - 255                  0                0                   0
256 - 383                  0                0                   0
384 - 511                  0                0                   0
512 - 639                  0                0                   0
640 - 767                  0                0                   0
768 - 895                  0                0                   0
896 - 1023                 0                0                   0
1024 - 1151                0                0                   0
1152 - 1279                0                0                   0
1280 - 1407                0                0                   0
1408 - 1518                0                0                   0
1519 and up                0                0                   0


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

This screen displays a breakdown of the sizes of the frames processed by the router for the indicated LAN since the statistics were last reset.

The first column is the range of frame sizes in bytes;
The second, frames received from the local LAN;
The third, frames forwarded across the router to the other LAN;
The fourth, frames received from the other LAN.

WAN Statistics Menu

```
                          WAN STATISTICS MENU

   Option                    Value         Description
 1. Remote site status       menu        - Display remote site statistics
 2. Display Summary                      - Display summary of remote sites
 3. Clear remote site stats              - Reset remote site statistics
 4. Link status                          - View status of link
 5. Clear link statistics                - Reset link statistics









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


>
```

1 - Remote Site Status

The Remote Site Status option takes you to the Remote Site Status Menu, where statistics for a particular remote site can be examined.

2 - Display Summary

The Display Summary option gives a display of the parameters in the Remote Sites Table.

```
               * - Up   E - Enabled   D - Disabled   NA - Not Available
 Id  Alias             FR  AC MP   Pri/Sec   DLCI  BRG IP IPX CCP CMCP BACP
 --  ----------------  --- -- -- ---------- ----  --- -- --- --- ---- ----
  1  Aukland           RAW  D  E   LINK2/ISDN NA    E   E  E   D   D    NA
 41  INITIAL_PROFILE   D    D  E   none/ISDN  NA    E   E  E   E   D    E
 42  DIRECTDIAL1       D    D  E   none/ISDN  NA    E   E  E   E   D    E
 43  LEASED2           D    D  E   none/ISDN  NA    E   E  E   E   D    E
 44  INCOMING1         D    D  E   none/ISDN  NA    E   E  E   E   D    E
 45  INCOMING2         D    D  E   none/ISDN  NA    E   E  E   E   D    E
```

3 - Clear Remote Site Statistics

The Clear Remote Site Statistics option clears all fields in all of the remote site statistics displays to zero.

4 - Link Status

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

Please refer to the following pages for more detailed information.

5 - Clear Link Statistics

The Clear Link Statistics option clears all fields in the Link statistics to zero.

Link Status Display (Option 4)

```
Enter:
   Link to display (1)
```

Link 1 Status

```
                                Link  1 Status
State: Disabled, Idle
LMI State: Down

Interface State          Frame Counts  (Rcv/Xmt)        Frame Errors
Speed : 64000 bps        Bytes :      47648/47639       Cgt disc   : 0
Type  : V.35             Frames:       3536/3536        CRC        : 0
DTR   : down                                            Rcv abort  : 0
CD    : up                                              Overrun    : 0
RTS   : down                                            Rcv miss   : 0
DSR   : up                                              Too large  : 0
CTS   : up                                              Misaligned : 0
RI    : up                                              Underrun   : 0
                              Throughput
Rcv   0%       0.0 KB |
Xmt   0%       0.0 KB |
                      |----|----|----|----|----|----|----|----|----|----|
                     0   10   20   30   40   50   60   70   80   90  100%

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

State :

This displays the current state of the circuit: Enabled/Disabled, Idle / Opening / Up, Initial / Starting / Closed / Stopped / Closing / Stopping / Req Sent / Ack Rcvd / Ack Sent / Opened.

Remote Site :

The name of the current remote site that this link is connected to.

Speed :

The speed of the connection. If the call is disconnected, no speed (0) will be shown.

Type :

The interface type is identified in this display (V.35).

DTR :

Data Terminal Ready state (up or down).

CD :

Carrier Detect state (up or down).

RTS :

Request To Send state (up or down).

DSR :

Data set ready state (up or down).

CTS :

Clear To Send state (up or down).

RI :

RIng (call indicator) state (up or down).

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.

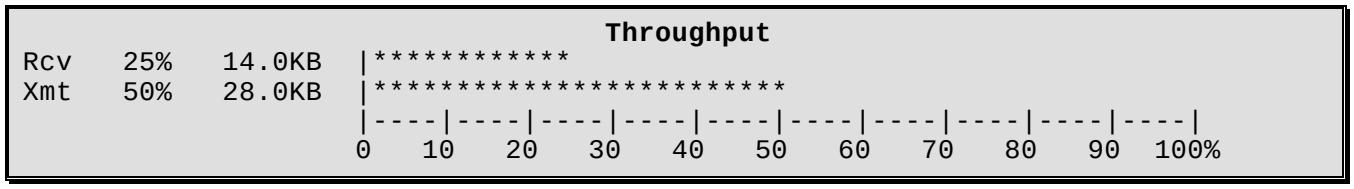
Frame Errors

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 bytes received or sent (including protocol overhead) divided by the total bytes possible based on the call speed. For each statistic, the numerical percentage is printed along with its equivalent baud rate and the bar graph.



Remote Site Statistics Menu

```
                          REMOTE SITE STATUS MENU

    Option                    Value          Description

 1. Usage information                    - Display usage information




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

> two
```

The above display is the first level of the **REMOTE SITE STATUS MENU** . Once the remote site id is entered, the id specified is added to the menu title bar and the Options are as shown below:

```
                       REMOTE SITE STATUS amsterdam MENU

    Option                     Value          Description
 1. Protocol status            menu         - Display protocol statistics
 2. Frame relay status                      - Display frame relay status values
 3. Primary call status                     - Display primary call statistics
 4. Primary call quality                    - Display primary link quality data









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

>
```

1 - Protocol Status

The Protocol Status option takes you to the Remote Site - Protocol Status Menu, where the protocol statistics for this remote site can be examined.

2 – Frame Relay Status

The Frame Relay Status option displays statistics for the PVC connection to this remote site.

3 - Primary Call Status

The Primary Call Status option displays a summary of the LCP parameters and the frame counts and errors for the chosen remote site since the statistics were last reset.

The Primary Call Status option is not available when PPP Encapsulation is disabled for this remote site.

4 - Primary Call Quality

The Primary Call Quality option displays a summary of the Circuit Quality parameters for the chosen remote site since the statistics were last reset.

The Primary Call Quality option is not available when PPP Encapsulation is disabled for this remote site.

Frame Relay Status (Option 2)

```
                              Frame Relay              Remote Site  2-
amsterdam
PVC State : Enabled, Idle
Link: 0, DLCI: 16, CIR: 0Kbps, EIR: 0Kbps

   Frame Counts          (Rcv/Xmt)                 Frame Errors
   Bridge Frames :          0/0                    Total Discards  :     0/0
   BPDU Frames   :          0/0                    Invalid Frames  :     0/0
   IP Frames     :          0/0                    Total Discards  :     0/0
   IPX Frames    :          0/0                    Rcv FECNs       :     0
   PPP Frames    :          0/0                    Rcv BECNs       :     0
   Total Frames  :          0/0


                             Throughput
Rcv   0%       0.0 KB |
Xmt   0%       0.0 KB |
                      |----|----|----|----|----|----|----|----|----|----|
                     0   10   20   30   40   50   60   70   80   90  100%
```

PVC State :

Enabled/Disabled, Idle/Up/Down/Starting/Stopping, Compressing/NonCompressing, Bursting_Enabled/Bursting_Disabled.

Link :

This displays the link number this PVC to this remote site is on.

DLCI :

This displays the DLCI number being used by the PVC to this remote site.

CIR :

This displays the Committed Information Rate (CIR) value being used by the PVC to this remote site.

EIR :

The Excess Information Rate (CIR) value being used by the PVC to this remote site.

Frame Counts

Bridge Frames :

The total number of Bridge frames received/transmitted across the link.

Note: This item is only displayed with PPP encapsulation disabled.

BPDU Frames :

The total number of BPDU (Bridge Protocol Data Unit) frames received/transmitted across the link. If this device is not running STP and receives STP frames from the peer device, the BPDU frames will be counted as received and then silently discarded.

Note: This item is only displayed with PPP encapsulation disabled.

IP Frames :

The total number of IP frames received/transmitted across the link.

Note: This item is only displayed with PPP encapsulation disabled.

IPX Frames :

The total number of IPX frames received/transmitted across the link.

Note: This item is only displayed with PPP encapsulation disabled.

PPP Frames :

The total number of PPP frames received/transmitted across the link.

Note: This item is only displayed with PPP encapsulation enabled.

Total Frames :

The total number of frames received/transmitted across the link. .

Frame Errors

Unknown Protocol:

The number of frames of unknown protocol received over this link.

Total Discards :

The total number of frames discarded across this link.

Invalid Frames :

The number of invalid frames received across this link.

Rcv FECNs :

This indicates the total number of frames received that had the FECN bit set in the Frame Relay header. The FECN bit is used to indicate to the receiving end-system that the frames it receives have encountered congested resources.

Rcv BECNs :

This indicates the total number of frames received that had the BECN bit set in the Frame Relay header. The BECN bit is used to indicate to the receiving end-system that the frames it transmits may encounter congested resources.

Throughput

Both the receive and transmit PVC 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 PVC's configured bandwidth of CIR + EIR. For each statistic, the numerical percentage is printed along with its equivalent baud rate and the bar graph.

To calculate the amount of bursting for this PVC simply use the Xmt KB number from the display and subtract the CIR value. This will result in the amount of excess data that was transmitted over the PVC. Note that when the EIR is set to 0 the Xmt KB value will not exceed the CIR value.

The throughput indicates the actual data throughput on the PVC. When the PVC is compressing, the throughput indicates the compressed data on the PVC.

The KB values indicate the amount of data received and transmitted in Kbits/second.

Primary Call Status (Option 3)

```
                                    Circuit          Remote Site  2-amsterdam
Multilink: Enabled, Link: 1, DLCI: 52
Operational Status: Network, Opened
                    Local LCP          Remote LCP
MRU            :      1500               1500
ACCM           :      0x00000000         0x00000000
Quality        :      none               none
Quality Period :      0                  0
Magic Number   :      0                  0
PFC            :      disabled           disabled
ACFC           :      enabled            enabled
FCS size       :      16-bit FCS         16-bit FCS
SDP            :      0                  0

      Frame Counts   (Rcv/Xmt)          Frame Errors
      Bytes  :      61917/61961         Header       : 0
      Frames :       4229/4229          Rcv Discards : 0
      LCP    :       4016/4016          Pad          : 0
      LQR    :          0/0             Unknown Prot : 0
      PAP    :          0/0
      CHAP   :          0/0
      MP     :        210/210
Type: [s] to redraw, [=] main menu, any other key to end.
```

Multilink :

This displays the current state of Multilink operation for this remote site connection: Enabled / Disabled.

Link :

This displays the link number this PVC to this remote site is on.

DLCI :

This displays the DLCI number being used by the PVC to this remote site.

Operational Status :

This displays the current state of the PPP LCP module for this link of the remote site connection: Dead / Establish / Authenticate / Network / Terminate, Initial / Starting / Closed / Stopped / Closing / Stopping / Req Sent / Ack Rcvd / Ack Sent / Opened.

MRU :

This displays the negotiated MRU (Maximum Receive Unit) value for this end of the link connection as well as the MRU value for the remote end.

ACCM :

This displays the negotiated ACCM (Asynchronous-Control Character-Map) Configuration value for this end of the link connection as well as the ACCM value for the remote end.

Quality :

This displays the negotiated quality protocol type for this end of the link connection as well as the quality protocol type for the remote end.

Quality Period :

This displays the negotiated quality period for this end of the link connection as well as the quality period for the remote end.

Magic Number :

This displays the negotiated magic number value for this end of the link connection as well as the magic number value for the remote end.

PFC :

This displays the negotiated PFC (Protocol Field Compression) state for this end of the link connection as well as the PFC state for the remote end.

ACFC :

This displays the negotiated ACFC (Access and Control Field Compression) state for this end of the link connection as well as the ACFC state for the remote end.

FCS Size :

This displays the negotiated FCS size (Frame Check Sequence) for this end of the link connection as well as the FCS size for the remote end.

SDP :

This displays the negotiated SDP value (Self-Describing-Padding) for this end of the link connection as well as the SDP value for the remote end. A value of 0 indicates no padding is being added.

Frame Counts

Bytes :

This indicates the total number of bytes received/transmitted across this link.

Frames :

This indicates the total number of frames received/transmitted across this link.

LCP :

This indicates the total number of LCP (Link Control Protocol) negotiation frames received/transmitted across this link.

LQR :

This indicates the total number of LQR (Link Quality Report) frames received/transmitted across this link.

PAP :

This indicates the total number of PAP (Password Authentication Protocol) frames received/transmitted across this link.

CHAP :

This indicates the total number of CHAP (Challenge-Handshake Authentication Protocol) frames received/transmitted across this link.

MP :

This indicates the total number of MP (Multilink Protocol) frames received/transmitted across this link.

Frame Errors

Header :

This is generated when an incoming frame is discarded due to a bad header.

Rcv Discards :

This is generated when an incoming frame is discarded due to the frame being destined for a bundle before this link has been bound to a bundle.

Pad :

This is generated when an incoming frame is discarded due to a problem trimming off the SDP padding.

Unknown Prot :

Unknown Protocol — This is generated when an incoming frame is discarded due to the frame being an unknown or unacceptable protocol type, i.e. BDP or IPXCP.

Primary Call Quality (Option 4)

```
                        Circuit Quality              Remote Site  2-amsterdam
Multilink: Enabled

                    Local LQM          Remote LQM
 LQM            :      none               none
 Quality Period :      0                  0

  Recent              (Rcv/Xmt)        LQR
  Lost Packets:          0/0           Lost Outbound LQRs        : 0
  Lost Octets :          0/0           Outbound LQRs in Pipeline : 0
  Total                                Change in Peer InDiscards : 0
  Lost Packets:          0/0           Change in Peer InErrors   : 0
  Lost Octets :          0/0
  LQRs        :          0/0

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

Multilink :

This displays the current state of Multilink operation for this remote site connection: Enabled / Disabled.

LQM :

This displays the negotiated LQM (Link Quality Mode) for this end of the link connection as well as the LQM for the remote end: LQR / none.

Quality Period :

This displays the negotiated quality period value for this end of the link connection as well as the quality period value for the remote end.

Recent Counts

Lost Packets :

This indicates the number of packets lost while receiving / transmitting across this link during the previous quality period.

Lost Octets :

This indicates the number of octets lost while receiving / transmitting across this link during the previous quality period.

Total Counts

Lost Packets :

This indicates the total number of packets lost while receiving / transmitting across this link.

Lost Octets :

This indicates the total number of octets lost while receiving / transmitting across this link.

LQRs :

This indicates the total number of LQR packets received / transmitted across this link.

LQR

Lost Outbound LQRs :

This indicates the total number of LQR packets sent to the remote site that have been lost.

Outbound LQRs in Pipeline :

This indicates the total number of LQR packets sent to the remote site that have not been received by the remote site.

Change in Peer InDiscards:

This indicates the number of times the remote site has discarded packets due to congestion.

Change in Peer InErrors :

This indicates the number of times the remote site has discarded packets due to invalid packets.

Remote Site Statistics - Protocol Status Menu

```
                REMOTE SITE STATUS two PROTOCOL STATUS MENU

   Option              Description
 1. BCP status        - Display BCP status values
 2. IPCP status       - Display IPCP status values
 3. IPXCP status      - Display IPXCP status values
 4. CCP status        - Display CCP status values


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

>
```

The **REMOTE SITE - PROTOCOL STATUS MENU** allows the display of the status of each LCP module.

1 - BCP Status

Displays a summary of BCP (Bridge Control Protocol) parameters for the chosen remote site since the statistics were last reset.

2 - IPCP Status

Displays a summary of IPCP (Internet Protocol Control Protocol) parameters for the chosen remote site since the statistics were last reset.

3 - IPXCP Status

Displays a summary of IPXCP (Internet Packet Exchange Control Protocol) parameters for the chosen remote site since the statistics were last reset.

4 - CCP Status

Displays a summary of CCP (Compression Control Protocol) parameters for the chosen remote site since the statistics were last reset.

This option is only displayed if PPP encapsulation is enabled

BCP Status Display (Option 1)

```
                                  BCP                    Remote Site  2-amsterdam
Multilink: disabled, Bundle state: Idle
Operational status: Initial

                        Local BCP                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

   Frame Counts        (Rcv/Xmt)                Frame Errors
   BCP         :          0/0                   Rcv BPDU Discards : 0
   BPDU        :          0/0                   Xmt BPDU Discards : 0
   Bridge      :          0/0                   Rcv Brg Discards  : 0
                                                Xmt Brg Discards  : 0









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

Multilink :

This displays the current state of Multilink operation for this remote site connection: Enabled / Disabled.

Bundle State :

This displays the current state of the PPP link bundle: Idle / Opening / Up / Stopping / Closing.

Operational Status :

This displays the current state of the PPP IPCP protocol module for this remote site connection: Initial / Starting / Closed / Stopped / Closing / Stopping / Req Sent / Ack Rcvd / Ack Sent / Opened.

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.

Frame Counts

BCP :

This indicates the total number of BCP frames received/transmitted across the link.

BPDU :

This indicates the total number of BPDU (Bridge Protocol Data Unit) frames received/transmitted across the link. If this device is not running STP and receives STP frames from the peer device, the BPDU frames will be counted as received and then silently discarded.

Bridge:

This indicates the total number of non-compressed bridge frames received/transmitted across the link.

Frame Errors

Rcv BPDU Discards :

This is generated when an incoming BPDU frame is discarded due to congestion or BCP not being open.

Xmt BPDU Discards :

This is generated when an outgoing BPDU frame is discarded due to congestion.

Rcv Brg Discards :

This is generated when an incoming bridge frame is discarded due to congestion.

Xmt Brg Discards :

This is generated when an outgoing bridge frame is discarded due to congestion.

IPCP Status Display (Option 2)

```
                              IPCP                          Remote Site  2-amsterdam
Multilink: Enabled, Bundle state: Up
Operational status : Opened

                     Local IPCP                  Remote IPCP
IP Address       :   198.169.3.1                 198.169.3.2
Subnet Mask size :   24                          24
Link IP type     :   unNumbered
VJ Compression   :   VJ TCP                     VJ TCP
Max slot id      :   15                          15
Slot id Comp     :   enabled                     enabled

   Frame Counts        (Rcv/Xmt)                Frame Errors
   IPCP         :         3/2                   VJ      : 0
   IP           :        15/16                  Rcv Discards : 0
   VJ Comp      :         0/0                   Xmt Discards : 0
   VJ Uncomp    :         0/0



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

Multilink :

This displays the current state of Multilink operation for this remote site connection: Enabled / Disabled.

Bundle State :

This displays the current state of the PPP link bundle: Idle / Opening / Up / Stopping / Closing.

Operational Status :

This displays the current state of the PPP IPCP protocol module for this remote site connection: Initial / Starting / Closed / Stopped / Closing / Stopping / Req Sent / Ack Rcvd / Ack Sent / Opened.

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 IOLINK-SH-SR 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.

Frame Counts

IPCP :

This indicates the total number of IPCP frames received/transmitted across the link.

IP :

This indicates the total number of non-compressed IP frames received/transmitted across the link.

VJ Comp :

This indicates the total number of compressed TCP frames received/transmitted across the link.

VJ Uncomp :

This indicates the total number of uncompressed TCP frames received/transmitted across the link.

Frame Errors

VJ :

VJ — This is generated when an incoming compressed TCP frame is discarded, possibly due to error detection.

Rcv Discards :

This is generated when an incoming IP frame is discarded due to congestion.

Xmt Discards :

This is generated when an outgoing IP frame is discarded due to congestion.

IPXCP Status Display (Option 3)

```
                              IPXCP                          Remote Site  2-amsterdam
Multilink: Disabled, Bundle state: Up
Operational status: Opened


IPX Routing Protocol: RIP/SAP
Force RIP Updates   : disabled
IPX Network Number  : 0
IPX Node Number
    Local           : 00-00-00-00-00-00
    Remote          : 00-00-00-00-00-00


   Frame Counts        (Rcv/Xmt)                 Frame Errors
   IPXCP       :         10/33                   Rcv Discards : 0
   IPX         :        423/553                  Xmt Discards : 0




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

Multilink :

This displays the current state of Multilink operation for this remote site connection: Enabled / Disabled.

Bundle State :

This displays the current state of the PPP link bundle: Idle / Opening / Up / Stopping / Closing.

Operational Status :

This displays the current state of the PPP IPCP protocol module for this remote site connection: Initial / Starting / Closed / Stopped / Closing / Stopping / Req Sent / Ack Rcvd / Ack Sent / Opened.

IPX Routing Protocol:

This displays the IPX routing protocol negotiated over the link. The possible routing protocols are RIP/SAP, Static, Demand RIP/SAP.

Force RIP Updates:

This displays the state of the force RIP updates option on the link connection. This display is only applicable when the IPX Routing Protocol is RIP/SAP.

IPX Network Number:

This displays the IPX network number negotiated for the link. The network number will be 0 if the interface is unnumbered.

IPX Node Number:

Local :

This indicates the IPX node number negotiated for this end of the link. The node number will be 0 if the interface is unnumbered.

Remote :

This indicates the IPX node number negotiated for the remote site end of the link. The node number will be 0 if the interface is unnumbered.

Frame Counts

IPXCP :

This indicates the total number of IPXCP frames received/transmitted across the link.

IPX :

This indicates the total number of IPX frames received/transmitted across the link.

Frame Errors

Rcv Discards :

This is generated when an incoming IPX frame is discarded due to congestion.

Xmt Discards :

This is generated when an outgoing IPX frame is discarded due to congestion.

CCP Status Display (Option 4)

```
                          CCP                              Remote Site  2-amsterdam
Multilink: disabled, Bundle state: Idle
Operational status: Initial, Compression: enabled

                     Local CCP                  Remote CCP
Protocol        :    Stac LZS (17)              Stac LZS (17)
Histories       :    1                          1
Check mode      :    Sequence Number            Sequence Number
Restarts        :    0
Resyncs         :    0

   Frame Counts         (Rcv/Xmt)                 Frame Errors
   CCP          :          2/1                    Compress     : 0
   Reset Req    :          0/0                    Decompress   : 0
   Reset Ack    :          0/0                    Rcv Discards : 0
   Comp Frames :       73647/172408              Zero pad     : 0
   Raw Bytes    :    3536850/8277384
   Comp Bytes   :    1397743/3274734
   Comp Ratio   :      2.5:1 / 2.5:1
   Recent Ratio:      4.1:1 / 6.7:1


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

Multilink :

This displays the current state of Multilink operation for this remote site connection: Enabled / Disabled.

Compression :

This displays the current state of compression status for this remote site connection: Enabled / Disabled.

Bundle State :

This displays the current state of the PPP link bundle: Idle / Opening / Up / Stopping / Closing.

Operational Status :

This displays the current state of the PPP CCP protocol module for this remote site connection: Initial / Starting / Closed / Stopped / Closing / Stopping / Req Sent / Ack Rcvd / Ack Sent / Opened.

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.

Restarts :

This displays the number of times that compression has been restarted by renegotiating CCP on the connection.

Resyncs :

This displays the number of times that CCP has been successfully resynchronized on the connection.

Frame Counts

CCP :

This indicates the total number of CCP frames received/transmitted across the link.

Reset Req :

This indicates the total number of Reset Requests received/transmitted across this link.

Reset Ack :

This indicates the total number of Reset Acknowledgments received/transmitted across this link.

Comp Frames :

This indicates the total number of compressed frames received/transmitted across this link.

Raw Bytes :

This indicates the total number of bytes before compression received/transmitted across this link.

Comp Bytes :

This indicates the total number of compressed bytes received/transmitted across this link.

Comp Ratio :

This indicates the received/transmitted average compression ratio since the last time statistics were cleared.

Recent Ratio :

This indicates the received/transmitted compression ratio in the last display period.

Frame Errors

Compress :

This is generated when an error occurred during compression.

Decompress :

This is generated when an error occurred during decompression or a compression sequence number was not received.

Rcv Discards :

The number of discards due to an incorrect compression sequence number or discards when a compressed frame is received before the Ack is received.

Zero Pad :

This number indicates the number of frames with zero pad compression received. This acts as a flag for frames received which have been compressed with an unsupported compression technique.

Diagnostics Menu

```
                          DIAGNOSTICS MENU

   Option             Value          Description
 1. WAN diagnostics    menu         - Access WAN diagnostic tools
 2. Heartbeat         [enabled]     - Report transceiver heartbeat failures
 3. Soft reset                      - Reset device (retain configuration)
 4. Full reset                      - Reset device (use factory defaults)




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

>
```

1 - WAN diagnostics

The WAN diagnostics option takes you to the WAN Diagnostics Menu, where trace and link operations may be accessed.

2 - 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.)

3 - Soft Reset

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

Note that a hardware (and software) reset may be performed by toggling the switch behind the small access hole at the bottom of the faceplate on the right side.

4 - 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.

WAN Diagnostics Menu

```
                          WAN DIAGNOSTICS MENU

   Option                Value          Description
 1. Trace                menu         - View link frames
 2. Link 1 diagnostics   menu         - Access link 1 diagnostic tools









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

>
```

1 - Trace

Takes you to the Trace Menu, where options can be [enabled] or [disabled] for each link in order to evaluate link performance.

2 - Link 1 Diagnostics

Takes you to the Link 1 Diagnostics Menu, where loopback tests may be performed in order to evaluate link performance.

Trace Menu

```
                                TRACE MENU

    Option          Value                  Description
 1. Trace 1        [disabled]             - View link 1 frames
 2. Real time      [disabled]             - Display frames in real-time
 3. Capture        [disabled]             - Capture frames in buffer
 4. Allocate       [0 kbytes]             - Set capture buffer size
 5. End            [disabled]             - End capture at link down
 6. Data display   [hex] [single_line]    - Set frame display format
 7. Time           [disabled]             - Add time to display
 8. Show                                  - View capture buffer




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


>
```

The **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 1

[Enable] the trace for either or both links 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 "3" 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 9, Show, to display the capture.

4 - Allocate

Use this option to set the size of the buffer used to store captured frames. The buffer size is 3 to 20 KB. Once the buffer size is set, it can be adjusted only within the range given.

5 - 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].

6 - 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
>
```

7 - 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.

8 - 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 Information

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 Receiver Ready

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. An **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 transmission of a **SABM** statistic indicates the clearance of a busy condition that was reported by the earlier transmission of an **RNR** frame and statistic by that same bridge/router.

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. The transmission of a **UA** response indicates the clearance of a busy condition that was reported by the earlier transmission of an **RNR** frame by that same bridge/router.

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.

Link 1 Diagnostics Menu

```
                          LINK 1 DIAGNOSTICS MENU

   Option                      Value         Description
 1. Link state                [enabled]    - Allow link to operate
 2. External loopback                      - Generate/verify loopback data
 3. Help                                   - Description of link diagnostics









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


>
```

The **LINK DIAGNOSTICS MENU** allows loopback testing to be performed for this link.

1 - Link State

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

Considerations:

Disabling the link will cause the control signals to be dropped and the link connection to be disconnected.

2 - External Loopback

Enabling this option causes a test pattern to be generated and transmitted by this link module. This external loopback test requires that somewhere along the WAN link connection, there is a loopback to send the test pattern back to the bridge/router. The loopback may be a hardware loopback or an internal loopback on a remote modem.

```
LINK 1 - EXTERNAL LOOPBACK

Link Interface Type:  V.35
Sample Description :  256 Byte Frame

Total Frames Xmt   :              513
Total Frames Rcv   :              513
Good  Frames Rcv   :              253
Error Frames Rcv   :                0
Xmt Failures       :                0









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

Total Frames Xmt: The total number of frames transmitted by the link module.

Total Frames Rcv: The total number of frames received by the link module.

Good Frames Rcv: The total number of good frames received by the link module. A good frame is a frame with a correct CRC, is correctly aligned, etc.

Error Frames Rcv: The total number of error frames received by the link module. An error frame is a frame with a bad CRC, unaligned, contains an abort sequence, etc.

Xmt Failures: The number of times the bridge/router attempted to transmit a test frame and failed. This is due to the absence of a transmit link clock signal. This will indicate that the connection to the link module is faulty.

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 resumption log    - View resume event log
 7. Clear resumption 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 and Security Logs are listed and explained in the Reference Manual file on the accompanying disks.

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 200 most recent ALARMs since the router was last powered up or Cleared with Option 3.

```
#1   94/12/22 13: 39: 05   SNMP is running
#2   94/12/22 13: 39: 06 * IP Routing is enabled
#3   94/12/22 13: 39: 07   Configuration restored
#4   94/12/22 13: 39: 08   Running in OPERATIONAL mode
#5   94/12/22 13: 39: 09 * LAN connection established
#6   94/12/22 13: 39: 35 * LAN started forwarding
time is 94/12/22 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 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.

3 - Clear Events

The Clear Events option removes all ALARMs from the table.

4 - Show Security Log

The Show Security Log option displays the 36 most recent ISDN security logs since the router was last powered up or Cleared with Option 5.

```
#1   96/05/16 16:26:53   Link 1 PAP failed for one (5551313)
#2   96/05/16 16:28:19   Link 1 CHAP failed for one (5551313)
time is 96/05/16 16:28:19, 2 items since last clear.

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

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.

5 - Clear Security Log

The Clear Security Log option removes all ISDN security logs from the table.

6 - Show Resumption Log

The Show Resumption Log option displays the 36 most recent connection management link resumption logs since the router was last powered up or Cleared with Option 7. The entries in the log indicate the device that the call was resumed to, the protocol that caused the resumption, the source and destination addresses within the frame that caused the resumption, and a hex dump of the frame that caused the resumption. The hex dump of the frame may be used for debugging purposes when the link is being resumed incorrectly.

```
#1   97/06/18 14:53:27   Resume event to DEV000d05 (IPX)
#2   97/06/18 14:53:27   Dst 0000411b:000000000001:0451 Src
                        + 00001515:00001b02446b:4003
#3   97/06/18 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   97/06/18 15:06:10   Resume event to DEV000d05 (IP)
#5   97/06/18 15:06:10   Dst 192.168.95.196 Src 198.169.1.149
#6   97/06/18 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 97/06/18 15:06:16, 9 items since last clear.

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

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 Resumption Log

The Clear Resumption Log option removes all connection management link resumption logs from the table.