DI-1133
Ethernet Bridge/Router

PPP Menus

Reference Manual

Issue 2

Software Version 2DG1.5.X

1/97

Part # 168-26306

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

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

Initial Router & Management Console Power-Up

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

```
Self tests in progress...
Proc A ROM, local RAM, Common RAM, Address PROM
System startup
Loopback completes normally.

Terminals supported:

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

Enter terminal type:
```

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

Select your terminal if listed and enter its name in lower case at the prompt, or choose the terminal type **teletype** if your terminal is not listed. This 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.

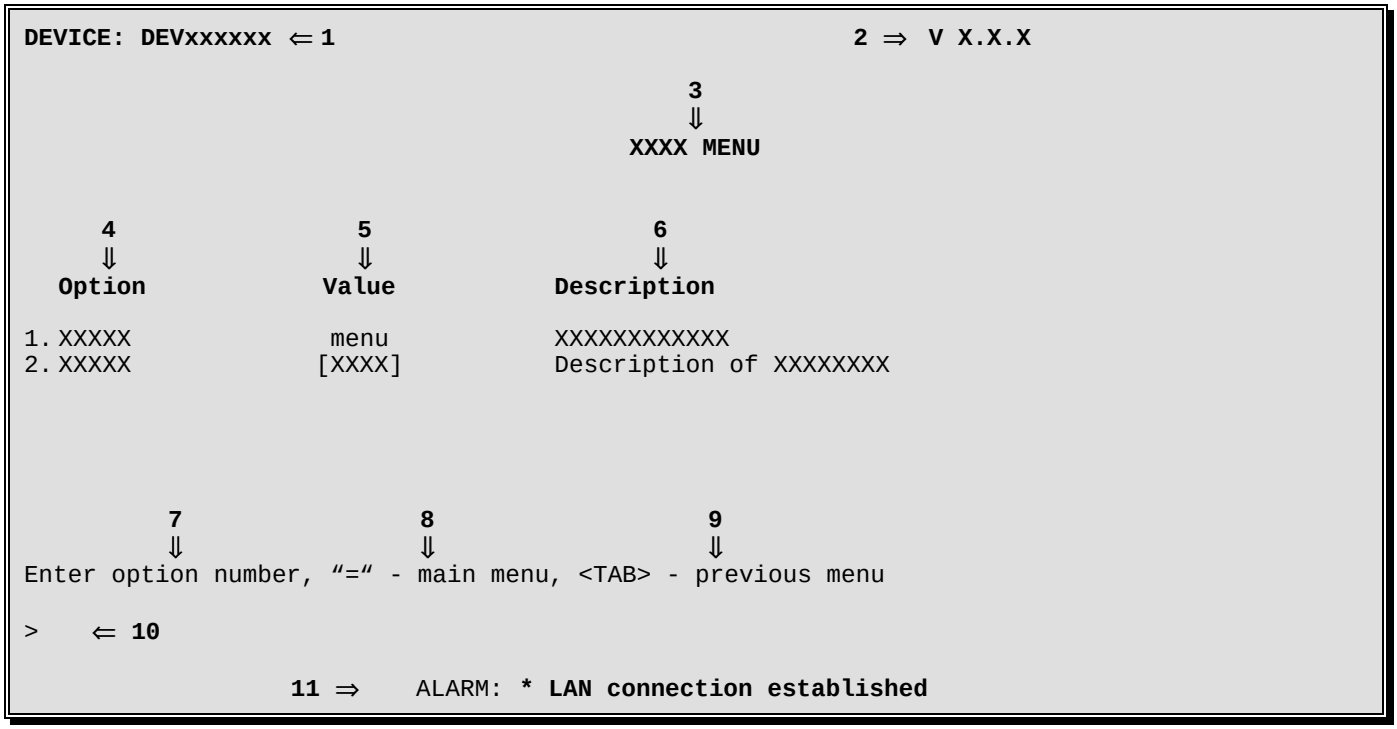
The DI-1133 Ethernet router uses a “hotkey “ Menu. A menu option is chosen by selection of the desired option number.

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 DI-1133 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**
   Selection is made by choosing the number for the Option. 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.

Main (Login) Menu

```
                                LOGIN MENU

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









Enter option number


>
```

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

1 - Login

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

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

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

2 - Configuration

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

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

4 - Diagnostics

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

5 - Network Events

Takes you to the Network Events Menu, where the 42 latest Alarms can be examined.

6 - Save Configuration

Performs an immediate save of the configuration to flash memory.

7 - Logout

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

Provides a brief, one-screen description of menu format and usage.

Quick Start Menu

```
                          QUICK START MENU

   Option              Value         Description
 1. Direct dial         menu        - Make a manual ISDN call
 2. Directory number   [none]       - Set directory number
 3. Switch type        [NET3]       - Set switch type
 4. IP address         [none]       - Define IP address and mask
 5. Default gateway    [none]       - Define default gateway
 6. Security                        - Define outgoing security
 7. Force disconnect                - Disconnect a call
 8. Link status                     - View status of link
 9. Soft reset                      - Reset device (retain configuration)



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

>
```

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

1 - Direct Dial Menu

Takes you to the Direct Dial Menu, where a directly dialed PPP connection may be established to a remote site PPP router. This direct dial functionality may be used to test the connectivity to a remote site router before a remote site profile is created.

2 - Directory Number / Link Set-Up Menu

When the ISDN switch type is set to NET3, 5ESS, KDD, NTT, and TPH1962, this option will be set to Directory Number. Enter the ISDN number assigned to this B-channel. The ISDN number is available from the ISDN circuit provider.

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

When this option is Link Set-Up Menu it will take you to the Link Set-Up Menu, where directory numbers and Service Profile Identifiers are defined for the ISDN B-channels.

3 - Switch Type

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

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

Default: [NET3]

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

4 - IP Address

Allows the definition of an Internet Protocol (IP) address and corresponding subnet size for the router. An IP address is required by the router.

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 Size variable partitions the host field of an IP address into two parts: a *subnet number* and a *host number*. This is used when a site uses multiple logical networks within a single IP network address. The subnet size must be the same as the subnet mask used on the subnet this router is connected to. The subnet mask is defined as a series of contiguous bit locations from the start of the IP address.

Default: [none]

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

Enter :
    size of subnet mask (from 2 to 30)
>
```

5 - Default Gateway

Allows the identification of a local default gateway (i.e. *router*). Messages destined for hosts not on this (sub-)network are forwarded to the default gateway.

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

Default: [none]

6 - Security

This option defines the user name, PAP password, and CHAP secret that this DI-1133 PPP router will use when responding to authentication requests from a remote site PPP router.

The outgoing user name is case sensitive and may consist of 1 to 16 alphanumeric characters. Use the underscore character instead of a space character.

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

Enter :
    PAP password (up to 16 characters), none
>

Enter :
    CHAP secret (up to 16 characters), none
>
```

7 - Force Disconnect

This option will cause the chosen link to be disconnected.

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

8 - Link Status

Displays the status of the links, either individually (more statistics), or together (provides overview).

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

9 - Soft Reset

Selecting this 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.

Direct Dial Menu

```
                              DIRECT DIAL MENU

    Option              Value                Description
 1. BCP enabled         [enabled]          - Enable BCP negotiations
 2. IPCP enabled        [enabled]          - Enable IPCP negotiations
 3. Local IP address    "0.0.0.0" [none]   - Define local IP address
 4. Peer IP address     "0.0.0.0"          - Define peer IP address
 5. IPXCP enabled       [enabled]          - Enable IPXCP negotiations
 6. Manual dial                            - Make the ISDN call









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


>
```

The **DIRECT DIAL MENU** allows a directly dialed PPP connection to be established to a remote site PPP router without having to define a remote site profile first. The direct dial function may be used to test a PPP connection before a remote site profile is created. When configuring a direct dial connection, the link types may only be numbered for an IP connection and unnumbered for an IPX connection. To establish a different type of connection simply define a remote site profile for the particular remote site PPP router and then establish a manual call from the Remote Site menu using the newly defined remote site parameters.

1 - BCP Enabled

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

Default: [enabled]

2 - IPCP Enabled

The IPCP Enabled option enables or disables the Internet Protocol Control Protocol negotiations for this direct dial connection. When the direct dial connection does not require IP routing, this option may be disabled causing IPCP not to be negotiated.

Default: [enabled]

3 - Local IP Address

Allows the definition of an Internet Protocol (IP) address and corresponding subnet size for the link of this router.

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 Size variable partitions the host field of an IP address into two parts: a *subnet number* and a *host number*. The subnet mask is defined as a series of contiguous bit locations from the start of the IP address.

Default: [none]

```
Enter :
    IP address (up to 15 characters)
>
Enter :
    subnet mask size(from 2 to 30)
>
```

4 - Peer IP Address

Allows the definition of an Internet Protocol (IP) address and corresponding subnet size for link side of the PPP 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.

Default: [none]

```
Enter :
    IP address (up to 15 characters)
>
```

5 - IPXCP Enabled

The IPXCP Enabled option enables or disables the Internet Packet Exchange Control Protocol negotiations for this direct dial connection. When the direct dial connection does not require IPX routing, this option may be disabled causing IPXCP not to be negotiated.

Default: [enabled]

6 - Manual Dial

This option is used to establish a manual Direct Dial ISDN PPP call to a remote site PPP router. Once the IP and IPX configuration has been performed using the above parameters, a direct dial connection may be made by entering the ISDN phone number of the remote site PPP router.

When a Direct Dial is made from the Direct Dial menu, any call parameters that are not specified when the call is made will be taken from the "INITIAL_PROFILE" remote site profile. These options include LCP (Link Control Protocol) parameters such as Multilink status.

If the Direct Dial results in a connection to a valid remote site that has already been configured, once the authentication process is finished, the BCP, IPCP, IPXCP, and CCP (Compression) parameters will be used from the configured remote site and not from the "INITIAL_PROFILE" remote site profile.

Please refer to the Remote Site Set-Up Menu for more information on configuring remote site profiles.

```
Enter :
    ISDN_number (up to 35 characters)
>
```

Link Set-Up Menu

```
                          LINK SET-UP MENU

    Option                Value          Description
 1. Directory number 1    [none]       - Link 1 directory number
 2. Directory number 2    [none]       - Link 2 directory number
 3. SPID 1                [none]       - Link 1 Service Profile Identifier
 4. SPID 2                [none]       - Link 2 Service Profile Identifier




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

>
```

The **LINK SET-UP MENU** allows the configuration of the Directory Numbers and Service Profile Identifiers of the B-channels on the ISDN interface of this DI-1133.

This menu is not required and therefore not available when the ISDN switch type is set to NET3, 5ESS, KDD, NTT, and TPH1962. This menu will be replaced with the Directory Number option.

1 - Directory Number 1

Enter the ISDN number assigned to this B-channel. The ISDN number is available from the ISDN circuit provider.

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

2 - Directory Number 2

Enter the ISDN number assigned to this B-channel. The ISDN number is available from the ISDN circuit provider.

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

3 - SPID 1

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

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

4 - SPID 2

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

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

Configuration Menu

```
                          CONFIGURATION MENU

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

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

Takes you to the Internet Set-Up Menu, where the parameters for the Internet configuration are selected.

3 - WAN Set-Up

Takes you to the WAN Set-Up Menu, where the Wide Area Network links are configured and controlled.

4 - Bridging Set-Up

Takes you to the Bridging Set-Up Menu, where the parameters for bridging are selected.

5 - IP Routing Set-Up

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.

6 - IPX Routing Set-Up

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.

7 - SNMP Set-Up

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, authentication failure).

8 - Filter Set-Up

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 access      menu         - Establish remote communications
 4. Upgrade device     menu         - Perform feature upgrade
 5. Load FLASH set-up  menu         - Prepare for software update
 6. TFTP restore      [disabled]    - Permit network configuration load
 7. Hardware status                 - Display hardware information
 8. Dump                            - Back-up configuration from console
 9. 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

Takes you to the Terminal Set-Up Menu, where the terminal parameters used for the router console are selected.

2 - Device Set-Up

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

3 - Telnet Access

Takes you to the Telnet Access Menu, where you can connect to another router in the network of routers.

4 - Upgrade Device

Takes you to the Upgrade Device Menu, where you can upgrade this device to use dual WAN links. This menu option does not appear on Dual-link routers.

5 - Load FLASH Set-Up

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.

6 - TFTP Restore

Determines whether a remote LAN device will be allowed to make a TFTP connection to this router to dump or restore 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 - Hardware Status

Displays the current status of the router hardware.

```
                        Hardware Status

MAC address           : 02-03-04-05-06-07
MAC check code        : 23d4a6
Service reference     : 0/0
LAN interface type    : 10Base5
Link 1 interface type : BRI ST
Link 2 interface type : BRI ST
ROM size              : 1MB
Full management       : enabled
```

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 in the link 1 position of this router.
Link 2 Interface Type	The type of link interface in the link 2 position of this router.
ROM Size	Indicates the size of the FLASH EEPROM installed.
Full Management	Indicates whether the current management level is Full or Limited.

8 - Dump

Lists the configuration so it may be captured and stored to a disk on a PC running a terminal-emulation package. This is an important step after configuration of the router, since the configuration would be lost in the event of battery failure or replacement.

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 to be 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.
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).

9 - Restore

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

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

Displays all terminal definitions. This listing may be of use if you need to create a custom terminal definition.

3 - Add

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

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

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

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

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

2 - Device Name

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 upper left-hand corner of the screen and the Value column will show a prefix of DEV, and will be 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

Allows you to view the current date and time.

4 - Set Time

Use this option to set the date and 24-hour Time Clock. Note that if your network uses the Bandwidth-On-Demand features of the DI-1133 Ethernet router across time zones, you must standardize on one time zone on the routers.

```
Enter:
  Date in format yy/mm/dd, no_change
93/07/27

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

Telnet Access Menu

```
                          TELNET ACCESS MENU

    Option          Value          Description
 1. Telnet        [enabled]     - Allow incoming Telnet connection
 2. Connect                     - Control remote device
 3. Show names                  - Display known remote devices
 4. Add name                    - Name remote devices
 5. Remove name                 - Delete remote device name









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

>
```

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

1 - Telnet

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 - Connect

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

The router being controlled may be identified by noting the Device name at the top left of each Menu.

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 - Show Names

```
Device Name   LAN name    MAC Address         IP Address   Notes
-----------   ---------   -----------------   ----------   --------------
Tokyo         LAN006005   00-00-d0-00-60-05   92.0.0.1     current device
Kyoto         LAN006045   00-00-d0-00-60-45   92.0.0.2     on link 1
Amsterdam     LAN00a007   00-00-d0-00-a0-07   92.0.0.5     on link 2

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

4 - Add Name

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

```
Enter:
  Device name (up to 10 characters)
>


Enter:
  IP address
>


Enter:
  Notes
>
```

5 - Remove Name

Allows you to remove a selected name. Note that the removal of a name also automatically removes the IP address and any notes associated with the name.

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

Upgrade Device Menu

```
                          UPGRADE DEVICE MENU

   Option                 Description
 1. Bridge              - Upgrade to support bridging
 2. IP router           - Upgrade to IP router capability
 3. IP RIP              - Upgrade to support IP RIP
 4. IPX router          - Upgrade to IPX router capability
 5. SNMP                - Upgrade to support SNMP
 6. Activate upgrade    - Enable the upgrade









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


>
```

From the **UPGRADE DEVICE MENU,** the DI-1133 may be upgraded to include IP router support, IPX router support, SNMP support, and others.

This menu will not appear on devices having all options enabled.

1 - Bridge

This option prompts you for an activation key to upgrade this device to support bridging.

The upgrade key is available from your local representative. Each upgrade key is unique for each device, and cannot be used to upgrade more than one device.

Once the upgrade key is correctly entered, the option will no longer be available and the Activate Upgrade option will become available. This allows more than one activation key to be entered before the device is reset and restarted.

2 - IP Router

This option prompts you for an activation key to upgrade this device to support IP routing.

The upgrade key is available from your local representative. Each upgrade key is unique for each device, and cannot be used to upgrade more than one device.

Once the upgrade key is correctly entered, the option will no longer be available and the Activate Upgrade option will become available. This allows more than one activation key to be entered before the device is reset and restarted.

3 - IP RIP

This option prompts you for an activation key to upgrade this device to support RIP in IP routing.

The upgrade key is available from your local representative. Each upgrade key is unique for each device, and cannot be used to upgrade more than one device.

Once the upgrade key is correctly entered, the option will no longer be available and the Activate Upgrade option will become available. This allows more than one activation key to be entered before the device is reset and restarted.

4 - IPX Router

This option prompts you for an activation key to upgrade this device to support IPX routing.

The upgrade key is available from your local representative. Each upgrade key is unique for each device, and cannot be used to upgrade more than one device.

Once the upgrade key is correctly entered, the option will no longer be available and the Activate Upgrade option will become available. This allows more than one activation key to be entered before the device is reset and restarted.

5 - SNMP

This option prompts you for an activation key to upgrade this device to support SNMP.

The upgrade key is available from your local representative. Each upgrade key is unique for each device, and cannot be used to upgrade more than one device.

Once the upgrade key is correctly entered, the option will no longer be available and the Activate Upgrade option will become available. This allows more than one activation key to be entered before the device is reset and restarted.

6 - Activate Upgrade

This option becomes available when at least one upgrade activation key has been successfully entered. This option will cause the device to be reset and then restart with the new features enabled.

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.

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.

1 - Console (ZMODEM)

Resets the router and places it in Console load mode. Once the router is in Console load mode, the “flash.lda” and “flash.fcs” files 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) Execute the Console (ZMODEM) command from the Load FLASH Set-Up menu. Confirmation is required. Enter "yes" to proceed.

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

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

3) Start the ZMODEM transfer and send the files "flash.lda" and "flash.fcs" from the Operational Code diskette.

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

   On the rare occasion that during the programming of the FLASH something happens to the bridge/router (power hit or hardware reset), causing the FLASH to become corrupted, the bridge/router will restart in ZMODEM receive mode only. If the bridge/router does not start in ZMODEM receive mode, power down the bridge/router, remove the case cover, remove the jumper on pins 3-7 of strap W9, power up the bridge/router, power down the bridge/router, re-install jumper on W9 pins 3-7, replace the case cover and power up the bridge/router. The bridge/router should now restart and be in ZMODEM receive mode.

The Load Flash operation may be aborted (before, during, and after the loading of the file "flash.lda", but not during the loading of the file "flash.fcs") 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 both WAN interfaces will be disabled. The router will only accept information from the console management port.

The BOOT code of the DI-1133 may be upgraded by performing a load of the "flash.lda" and "flash.fcs" files from the BOOT Code diskette. Upgrading the BOOT code will allow the DI-1133 to load compressed system code in future upgrades.

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.

This option must be confirmed before operation by typing "yes" when prompted.

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

2) 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.)

3) Put the file "flash.lda" to the router from the Operational Code diskette.
   (Any router not in Network Load BOOT mode will respond with an access violation error.)

4) Put the file "flash.fcs" to the router from the Operational Code diskette.

5) The router will verify the file "flash.lda" 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, and Password), 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 period.

   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: either the mode and version if no errors have occurred, or an error message.

   On the rare occasion that during the programming of the FLASH something happens to the bridge/router (power hit or hardware reset), causing the FLASH to become corrupted, the bridge/router will restart in ZMODEM receive mode only. If the bridge/router does not start in ZMODEM receive mode, power down the bridge/router, remove the case cover, remove the jumper on pins 3-7 of strap W9, power up the bridge/router, power down the bridge/router, re-install jumper on W9 pins 3-7, replace the case cover and power up the bridge/router. The bridge/router should now restart and be in ZMODEM receive mode.

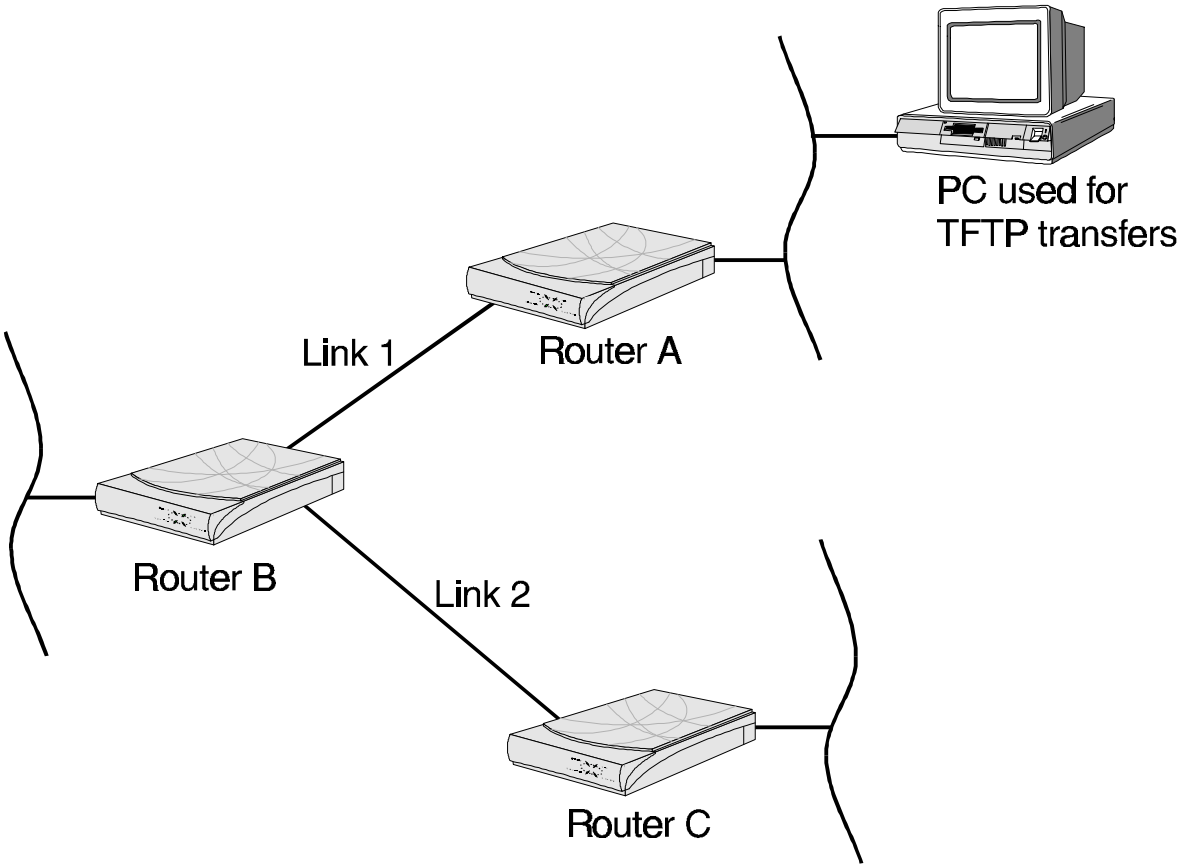
The Load Flash operation may be aborted (before, during, and after the loading of the file "flash.lda", but not during the loading of the file "flash.fcs") by re-connecting to the console of the router and choosing the Abort Load option from the Load FLASH Set-Up menu. This will cause the router to reset and return to normal operations operating from the existing software.

Considerations:

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

When performing a TFTP software download to a remote DI-1133 and that remote DI-1133 router had been configured to make an automatic ISDN call to another device, this call will not be made. A manual ISDN call must be placed to the DI-1133 and then the TFTP transfer may proceed.

In the following diagram, when performing a TFTP software load to router "Router C", an ISDN call must be placed from "Router B" and once the link has been established, the TFTP transfer may proceed. When upgrading the three DI-1133 routers in the diagram, the upgrade order should be "Router C', then "Router B", and finally "Router A".



When the DI-1133 restarts in network load mode, the security settings will be at the default values. When upgrading DI-1133s via TFTP in a network that is using security it may be easier to use one of the DI-1133s to initiate the manual ISDN call to the remote DI-1133s one at a time. Disable security on the DI-1133 that is chosen to establish the manual calls. After each remote DI-1133 is upgraded, the configuration may be restored and security may be started. Upgrading in this method should reduce any security holes that may appear if security is disabled for the entire network of DI-1133s and then the upgrades performed.

Internet Set-Up Menu

```
                          INTERNET SET-UP MENU

   Option                 Value          Description
 1. ARP set-up            menu         - Configure ARP operation
 2. Firewall set-up       menu         - Define firewall parameters
 3. Firewall support      [enabled]    - Activate firewall support
 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. Help                               - Description of IP applications




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

Directs you to the ARP Set-Up Menu, where the ARP timers may be set and the ARP table may be viewed.

2 - Firewall Set-Up

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.

3 - Firewall Support

This option enables or disables the IP Firewall functions of this DI-1133. When enabled, the DI-1133 will filter **all IP traffic** from the Wide Area Network (WAN) connection. That is, all IP traffic from the remote site routers connected on the links.

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

Default: [disabled]

4 - Nonstandard Subnets

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 22. 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 an all ones in the subnet portion of the address, this is not allowable with standard subnet masks.

Default: [enabled]

5 - IP Address

Allows the definition of an Internet Protocol (IP) address and corresponding subnet size for the router. An IP address is required by the router.

The DI-1133 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 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 Size variable partitions the host field of an IP address into two parts: a *subnet number* and a *host number*. This is used when a site uses multiple logical networks within a single IP network address. The subnet size must be the same as the subnet mask used on the subnet this router is connected to. The subnet mask is defined as a series of contiguous bit locations from the start of the IP address.

Default: [none]

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

Enter :
    size of subnet mask (from 2 to 30)
>
```

6 - Default Gateway

Allows the identification of a local default gateway (i.e. *router*). Messages destined for hosts not on this (sub-)network are forwarded to the default gateway.

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.

Default: [none]

7 - Time To Live

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 DI-1133 Ethernet router will have their time-to-live value decremented by two.

Default: [32]

Range: 1 - 255

8 - Help

Offers a brief description of the purpose and format of the IP address and subnet size.

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. 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

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

Sets the time-out value after which an ARP message will be resent.

Default: [2 sec]

Range: 1 - 20 seconds

3 - Show ARP Table

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).

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. Block src IP spoofing   [disabled]  - Discard WAN pkts with local src IP
 4. Firewall statistics                 - View firewall statistics
 5. Show firewall entries               - Display firewall entries
 6. Remove entry                        - Remove a firewall entry




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 IP traffic** from connected remote sites is blocked by default. 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.

1 - Designated Servers

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 allowed to be accessed 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

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 - Block Source IP Spoofing

When this 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 remote site network from attempting to gain access to the local network by using a local IP address as their source address. The DI-1133 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]

4 - Firewall Statistics

Displays a summary of the number of frames discarded by the firewall function.

```
                          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.

5 - Show Firewall Entries

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. Either 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.

6 - Remove Entry

Deletes individual entries or all of the entries from the Firewall table.

```
Enter :
    all, index number (from 1 to 15)

>
```

Designated Servers Menu

```
                          DESIGNATED SERVERS MENU

    Option                      Value         Description
 1. E-mail (SMTP) server      [none]       - Specify E-Mail server IP address
 2. POP 2/3 server            [none]       - Specify E-Mail POP server address
 3. FTP server                [none]       - Specify FTP server IP address
 4. WWW (HTTP) server         [none]       - Specify WWW server IP address
 5. Telnet server             [none]       - Specify Telnet IP address
 6. Domain Name Server(DNS)   [none]       - Specify DNS IP address
 7. 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

This 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

This 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

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

Default: [none]

4 - WWW (HTTP) Server

This 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

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

Default: [none]

6 - Domain Name Server (DNS)

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

Default: [none]

7 - Gopher Server

This 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









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           [1]           - Last port in range









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

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 octets and is represented by 4 fields separated by periods ("**.**"), where each field is specified by a decimal number (e.g. 92.3.1.10). Each decimal number must be less than or equal to 255, that is the maximum value of each 8-bit field.

Default: [none]

2 - Destination Mask

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

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 octets and is represented by 4 fields separated by periods ("**.**"), where each field is specified by a decimal number (e.g. 92.3.1.10). Each decimal number must be less than or equal to 255, that is the maximum value of each 8-bit field.

Default: [all]

4 - Source Mask

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

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

Defines the starting port number to be allowed through the firewall for this entry.

Default: [1]

Range: 1 to 65535

7 - Last Port

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

WAN Set-Up Menu

```
                              WAN SET-UP MENU

    Option                Value         Description
 1. ISDN set-up           menu        - Configure ISDN
 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
 6. IP address connect    menu        - Configure IP address connect




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


>
```

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

1 - ISDN Set-Up

The ISDN Set-Up Menu allows you to set ISDN switch types and other ISDN parameters.

2 - Link Set-Up

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

3 - Remote Site Set-Up

Takes you to the Remote Site Set-Up Menu, where configuration parameters required to establish PPP ISDN connections to remote devices are maintained.

4 - Security Set-Up

Takes you to the Security Set-Up Menu, where PPP security options are maintained.

5 - PPP Set-Up

Takes you to the PPP Set-Up Menu, where general PPP options are maintained.

6 - IP Address Connect

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

ISDN Set-Up Menu

```
                              ISDN SET-UP MENU

    Option                   Value          Description
 1. Switch type             [NET3]       - Set switch type
 2. Dial prefix             [none]       - Set dial prefix
 3. Force 56K               [disabled]   - Force 56K rate adaption
 4. Phantom power detect    [disabled]   - Detect phantom power




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


>
```

The **ISDN SET-UP MENU** provides for stored ISDN number set-up, ISDN call security set-up, and ISDN switch type definition.

1 - Switch Type

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

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

Default: [NET3]

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

Considerations:

The 5ESS switch types are split into two versions: 5ESS-PP (point to point) and 5ESS-MP (multipoint). In ISDN, point to point means that one device (phone, computer, DI-1133) is connected to the phone line, so if an ISDN call comes in, it's for that device. Multipoint means that several devices can be connected to the line, so there may be a phone, computer, fax machine, and DI-1133, all connected to the same line, and when an ISDN call comes in, the call type will determine which machine will answer (voice means the phone picks it up, fax means the fax machine, etc.).

2 - Dial Prefix

This option is used when the ISDN DI-1133 is attached to an ISDN PBX. If a dialing prefix is required before an outside line is obtained, the dialing prefix must be entered here.

Default: [none]

3 - Force 56K

This option forces both B-channels on this DI-1133 router to use V.110 rate adaption for all incoming and outgoing calls.

If the path to a destination number passes through a 56 Kbps digital circuit or the destination itself is a 56 K switched digital service, V.110 rate adaption must be performed to allow the data to be sent at 56 K on the 64 K ISDN lines. When an ISDN call is placed, the local ISDN service must be informed that V.110 rate adaption is required to fully complete this connection. Adding a percent symbol "%" in the ISDN number will cause the DI-1133 to send a message to the local ISDN service requesting V.110 rate adaption.

Default: [disabled]

4 - Phantom Power Detect

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

If the DI-1133 is having difficulty obtaining a connection to the NT-1, this option should be disabled.

Default: [disabled]

Considerations:

This option is not required and therefore not available when the ISDN switch type is set to NET3, KDD, NTT, and TPH1962.

Link Set-Up Menu

```
                          LINK SET-UP MENU

   Option                Value          Description
 1. Link 1 operation     [enabled]    - Allow link 1 to communicate
 2. Link 2 operation     [enabled]    - Allow link 2 to communicate
 3. Directory number 1   [none]       - Link 1 directory number
 4. Directory number 2   [none]       - Link 2 directory number
 5. SPID 1               [none]       - Link 1 Service Profile Identifier
 6. SPID 2               [none]       - Link 2 Service Profile Identifier









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

>
```

The **LINK SET-UP MENU** allows the configuration of the Directory Numbers and Service Profile Identifiers of the B-channels on the ISDN interface of this DI-1133.

1 - Link 1 Operation

Toggles between [enabled] and [disabled] to allow ISDN link 1 to be used for ISDN connections.

Default: [enabled]

2 - Link 2 Operation

Toggles between [enabled] and [disabled] to allow ISDN link 2 to be used for ISDN connections.

Default: [enabled]

3 - Directory Number 1

Enter the ISDN number assigned to this B-channel. The ISDN number is available from the ISDN circuit provider.

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

4 - Directory Number 2

Enter the ISDN number assigned to this B-channel. The ISDN number is available from the ISDN circuit provider.

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

Considerations:

This option is not required and therefore not available when the ISDN switch type is set to NET3, 5ESS, KDD, NTT, and TPH1962.

5 - SPID 1

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

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

Considerations:

This option is not required and therefore not available when the ISDN switch type is set to NET3, 5ESS-PP, KDD, NTT, and TPH1962.

6 - SPID 2

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

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

Considerations:

This option is not required and therefore not available when the ISDN switch type is set to NET3, 5ESS-PP, KDD, NTT, and TPH1962.

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. Show remote site      menu         - Display remote site configuration
 3. Display summary                    - Display summary of all remote sites
 4. Remove remote site                 - Delete remote site entry
 5. Manual call                        - Make a manual call to a remote site
 6. Force disconnect                   - Disconnect a call to a remote site




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

>
```

The **REMOTE SITE SET-UP MENU** allows the display, configuration, and creation of remote site profiles. Remote site profiles are used to establish PPP connections to other PPP IP/IPX routers.

Important: When configuring this DI-1133 to be the originator of PPP ISDN calls, always define a remote site for each of the possible remote partner IP/IPX routers that this DI-1133 may connect to. Each of the remote sites created store all of the configuration information required to properly maintain the PPP connection to that remote PPP router. The remote site alias is used to match against the incoming user name during authentication. If an authenticated user name is the same as one of the configured remote site profiles, that ISDN call will use the configuration defined within the remote site profile.

A remote site profile named "INITIAL_PROFILE" is used to define the Multilink state, the compression parameters, the bridging parameters, and the IP & IPX parameters for the two Direct Dial (ISDN) and the two Incoming remote site profiles.

When an ISDN Direct Dial is made from the Quick Start menu, the Multilink status is taken from the "INITIAL_PROFILE" remote site profile. If the Direct Dial results in a connection to a valid remote site that has already been configured, once the authentication process is finished, the BCP, IPCP, IPXCP, and CCP parameters will be used from the configured remote site profile and not from the "INITIAL_PROFILE" remote site profile.

When the DI-1133 receives an incoming ISDN call, the Multilink state is taken from the "INITIAL_PROFILE" remote site profile. After the authentication process is finished, if the remote site is a valid remote site that has already been configured, the remaining call parameters are taken from the configured remote site profile. If the remote site does not match one of the configured remote site profiles, then the remaining call parameters will be taken from the "INITIAL_PROFILE" remote site profile.

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

There are 40 configurable remote sites available. Each of these remote sites will have a remote site alias associated with them. When an ISDN call is made to a particular remote site, the call will be attached to that remote site profile after the connection has been established. For viewing the statistics for that ISDN call, you must view the statistics for that particular remote site profile alias.

There are five internal system remote sites that are used during the connection process. A cross-reference of these internal remote sites is described here:

Remote Site ID	Remote Site Alias	Description
1	INITIAL_PROFILE	Remote site profile used for incoming calls. Multilink state is taken from this profile. If the incoming user name matches the name of one of the configured remote sites, the remaining call parameters will be negotiated from the values defined for that remote site. If the incoming user name does not match any of the remote sites defined, the connection is attached to one of the INCOMING profiles. The remaining negotiating parameters, such as BCP, IPCP, IPXCP, and CCP, will be taken from the INITIAL_PROFILE settings.
2 - 41	(user configurable)	Remote site used for outgoing calls to these specific remote sites. Configuration parameters for the outgoing call are taken completely from the parameters defined in the remote site. Remote site profile used for incoming calls that have been authenticated and the incoming user name matches the name of one of the configured remote sites.
42	DIRECTDIAL1	Remote site used when a direct dial ISDN call is placed from the Quick Start menu. LCP parameters are taken from the INITIAL_PROFILE remote site for negotiations. If the remote site authenticates and matches one of the user configurable remote sites, then the BCP, IPCP, IPXCP, CCP, and remaining parameters will be taken from the remote site configuration. If the remote site authenticates and does not match one of the user configurable remote sites, the BCP, IPCP, IPXCP, CCP, and remaining parameters will be taken from the INITIAL_PROFILE remote site configuration. When viewing statistics for an ISDN call that has been attached to the DIRECTDIAL1 remote site, you may either specify the name DIRECTDIAL1 or the id 42.
43	DIRECTDIAL2	This remote site functions the same as DIRECTDIAL1 and is used for the second ISDN call available for connections.
44	INCOMING1	Remote site used when an incoming call is established to this DI-1133 PPP router and the user name reported by the remote PPP router during the authentication process does not match one of the configured remote sites. When viewing statistics for an ISDN call that has been attached to the INCOMING1 remote site, you may either specify the name INCOMING1 or the id 44.
45	INCOMING2	This remote site functions the same as INCOMING1 and is used for the second ISDN call that may be established to this DI-1133 PPP router.

1 - Edit Remote Site

Directs you to the Edit Remote Site Menu where the remote site profiles are maintained.

A total of 40 remote sites may be defined.

2 - Show Remote Site

Directs you to the Show Remote Site Menu where the remote site configuration and activation schedule may be viewed.

3 - Display Summary

```
                          Primary         Alternate
 Id  Alias               ISDN Number     ISDN Number
 --  ----------------  ---------------  ---------------
  1  INITIAL_PROFILE   none             none
  2  Vancouver         555-1234         555-2343
 42  DIRECTDIAL1       none             none
 43  DIRECTDIAL2       none             none
 44  INCOMING1         none             none
 45  INCOMING2         none             none


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

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.
Primary ISDN Number:	Primary ISDN number of the remote partner ISDN PPP router.
Alternate ISDN Number:	Alternate ISDN number of the remote partner ISDN PPP router.

4 - Remove Remote Site

Deletes individual entries or all of the entries from the Remote Site table.

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

5 - Manual Call

This option is used to establish a manual PPP call to a configured remote site.

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

6 - Force Disconnect

This option will cause the chosen remote site ISDN connection to be disconnected.

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

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. Secondary activation  menu         - Configure secondary activation
 4. Bridge parameters     menu         - Configure bridge parameters
 5. IP parameters         menu         - Configure IP parameters
 6. IPX parameters        menu         - Configure IPX parameters
 7. CCP parameters        menu         - Configure CCP parameters
 8. Remote site alias     [        ]   - Alias of remote site entry
 9. Multilink operation   [        ]   - Allows multilink operation



Enter:
    Remote site id (from 1 to 41)

> 1
```

The above display is the first level of the **EDIT REMOTE SITE 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:

When creating a new remote site entry, the DI-1133 will prompt you for a remote site id number as well as an alias for the remote site. The menu will then be updated with the id number and the alias name and the parameters may be modified.

```
                        EDIT REMOTE SITE 1 MENU

    Option                Value               Description
 1. Circuit set-up        menu              - Configure circuits
 2. Primary activation    menu              - Configure primary activation
 3. Secondary activation  menu              - Configure secondary activation
 4. Bridge parameters     menu              - Configure bridge parameters
 5. IP parameters         menu              - Configure IP parameters
 6. IPX parameters        menu              - Configure IPX parameters
 7. CCP parameters        menu              - Configure CCP parameters
 8. Remote site alias    *"INITIAL_PROFILE"  - Alias of remote site entry
 9. Multilink operation   [disabled]         - Allows multilink operation




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

>
```

1 - Circuit Set-Up

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. ISDN dialing parameters as well as the Auto-Call values are set within this menu.

2 - Primary Activation

Takes you to the Primary Activation menu for the chosen remote site, where activation conditions are defined for the main ISDN call that is made to this remote site. The activation conditions for the primary ISDN call consist of the activation schedule which determines when the ISDN call may be operational.

3 - Secondary Activation

Takes you to the Secondary Activation menu for the chosen remote site, where activation conditions are defined for the second ISDN call that is made to this remote site when the connection to the remote site is using Multilink protocol. The activation conditions for the secondary ISDN call consist of Bandwidth-on-Demand settings as well as the activation schedule.

This option is only available if Multilink Operation is set to enabled.

4 - Bridge Parameters

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

5 - IP Parameters

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. Both local and peer IP addresses are defined here as well.

6 - IPX Parameters

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.

7 - CCP Parameters

Takes you to the CCP Parameters menu for the chosen remote site, where the CCP parameters are configured.

8 - Remote Site Alias

This 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 ISDN call will use the configuration defined within the corresponding remote site profile.

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

9 - Multilink Operation

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

Default: [disabled]

Considerations:

When a PPP DI-1133 with Multilink disabled attempts to establish an ISDN connection to an Ascend router with Multilink enabled, the Ascend router will shut down the ISDN call. Simply set the Multilink values on each of the routers to be the same value and then establish the ISDN connection.

Circuit Set-Up Menu

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

   Option              Value          Description
 1. ISDN call set-up    menu         - Configure ISDN calls
 2. Auto-call          [enabled]     - 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 ISDN call establishment to the remote site PPP router.

1 - ISDN Call Set-Up

Takes you to the ISDN Call Set-Up Menu for the chosen remote site. Here you set parameters such as ISDN numbers and redial timers that pertain to ISDN circuit activation.

2 - Auto-Call

The Auto-Call option is used to define this remote site as one that the DI-1133 will attempt to establish a connection to at all times. Each time the DI-1133 is powered up an ISDN connection will be attempted to this remote site.

Default: [disabled]

ISDN Call Set-Up Menu

```
                EDIT REMOTE SITE 1 ISDN CALL SET-UP MENU

   Option                  Value         Description
 1. ISDN number            [none]       - Set ISDN number
 2. Alternate ISDN number  [none]       - Set alternate ISDN number
 3. Call you               [none]       - Set Call You prefix
 4. Redial timer           [10 sec]     - Time to wait until redial
 5. Redial count           [5]          - Number of redials to try




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

>
```

The **REMOTE SITE ISDN CALL SET-UP MENU** allows the setting of parameters used for ISDN call establishment to the remote site PPP router.

1 - ISDN Number

Defines the ISDN number to be called to establish a connection to the remote partner PPP router.

Default: [none]

2 - Alternate ISDN Number

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

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

Default: [none]

3 - Call You

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

Default: [none]

4 - Redial Timer

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

Default: [10 sec]

Range: 4 to 255 seconds

Considerations:

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

5 - Redial Count

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

Default: [5] redials

Range: 0 to 255 redials

Auto-Call Considerations:

When two ISDN numbers are defined in the ISDN Call Set-Up menu of the remote site entry, the DI-1133 will alternate between the two numbers when re-dialing.

When the DI-1133 attempts to establish an Auto-Call ISDN call and the PPP router at the remote site does not respond, the DI-1133 will try up to the number of times defined in the Redial Count to establish the ISDN call. The interval between the successive attempts is defined by the Redial Timer. If after the defined number of redials the DI-1133 cannot establish a call to the remote partner, the DI-1133 will wait for one minute and then try to establish the ISDN call again using the Redial Count and the Redial Timer values. If the call is not established after these attempts, the DI-1133 will wait for 2 minutes and then try again. The DI-1133 will keep trying to establish the call (according to Redial Count & Redial Time) in blocks with the time intervals: 4 minutes, 8 minutes, 15 minutes, 15 minutes, etc.) until the remote partner answers the call.

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

When the Redial Count is set to zero (0), the DI-1133 will redial the remote partner indefinitely using the defined ISDN numbers for the remote site according to the redial blocks explained earlier. The DI-1133 will alternate between the two defined ISDN numbers for the partner in blocks of #1, #2 with a time between the two ISDN numbers of 4 seconds.

Address Connect Considerations:

When the DI-1133 attempts to establish an Address Connect ISDN call and the remote partner does not respond, the DI-1133 will not attempt to redial the remote partner until the next Address Connect connection is required.

If two ISDN numbers are defined in the ISDN Call Set-Up menu of the remote site entry, the DI-1133 will dial the alternate ISDN number after waiting 4 seconds if the first ISDN number does not respond.

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 (ISDN call) to be used to connect to the remote site PPP router.

1 - Activation Schedule

Defines the times that the primary link (ISDN call) 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. 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.
```

3 - Display Time

Displays the current router time and date.

4 - Conditional Operation

This option determines if the Activation Schedule will take effect for the primary link (ISDN call) 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]

Secondary Activation Menu

```
                EDIT REMOTE SITE 1 SECONDARY 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
 5. Traffic level          [disabled]   - Activate upon primary call saturation
 6. Up threshold           [80 %]       - Set activation traffic level
 7. Up stability timer     [5 min]      - Define up level steady state time
 8. Down threshold         [60 %]       - Set deactivation traffic level
 9. Down stability timer   [10 min]     - Define down level steady state time


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

>
```

The **SECONDARY ACTIVATION MENU** allows the setting of the activation schedule for the secondary link (ISDN call) to be used to connect to the remote site PPP router. Traffic activation levels may also be set that allows the secondary link to be used when the throughput of the primary link exceeds the defined levels.

1 - Activation Schedule

Defines the times that the secondary link (ISDN call) 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. 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 2 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.
```

3 - Display Time

Displays the current router time and date.

4 - Conditional Operation

This option determines if the Activation Schedule or traffic level conditions will take effect for the secondary link (ISDN call) to the remote site PPP router. When enabled, the secondary link may only be established and active during the times defined within the activation schedule and/or the traffic levels set.

Default: [disabled]

5 - Traffic Level

This option enables or disables the ability to activate this secondary link according to the traffic levels of the primary link to the remote site PPP router.

When this option is disabled, the traffic level definition options are not available.

Default: [disabled]

6 - Up Threshold

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

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

7 - Up Stability Timer

To prevent the unnecessary activation of the secondary link if the Up Threshold is only reached for a brief period of time, the Up Stability Timer is used. It defines how long the primary link's throughput must be at or above the Up Threshold before the secondary call is activated. Using the default values, if an Up Threshold of 80% is maintained on the primary link for a period of 5 min. (length of time the secondary link is "held inactive"), then the secondary link will be activated.

```
Enter:
  time in minutes when link is down (from 1 to 60)
> 5
```

8 - Down Threshold

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

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

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

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

9 - Down Stability Timer

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

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

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

Bridge Parameters Menu

```
                EDIT REMOTE SITE 1 BRIDGE PARAMETERS MENU

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









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

>
```

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

1 - STP Parameters

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

This 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

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

When set to disabled, this DI-1133 will not send the FCS on bridge frames sent to the remote site PPP partner.

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

Default: [enabled]

STP Parameters Menu

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

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









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

>
```

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

1 - State

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

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 tie-breakers.

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

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 IP PARAMETERS MENU

    Option              Value                Description
 1. IPCP enabled       [enabled]           - Enable IPCP negotiations
 2. Link IP type       [numbered]          - Define numbered link
 3. Local IP address   "0.0.0.0" [none]    - Define local IP address
 4. Peer IP address    "0.0.0.0"           - Define peer IP address
 5. VJ compression     [disabled]          - Enable VJ header compression









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


>
```

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

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

1 - IPCP Enabled

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

Default: [enabled]

2 - Link IP Type

This option defines the type of link connection that will be established with the remote site PPP router. The link may be numbered, in which both sides of the WAN connection have IP addresses assigned; or unnumbered, in which the peer (remote partner PPP router) and the calling router use their device IP address.

When operating in unnumbered mode, each of the two IP routers operate as half of a complete router. The WAN connection is considered to be 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

3 - Local IP Address

Allows the definition of an Internet Protocol (IP) address and corresponding subnet size for the link of this router.

When the link IP type is set to unnumbered, the Local IP Address option is not available. For an unnumbered link the local IP address is taken from the IP address assigned to this router in the Internet Set-Up menu.

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

The Subnet Size variable partitions the host field of an IP address into two parts: a *subnet number* and a *host number*. The subnet mask is defined as a series of contiguous bit locations from the start of the IP address.

Default: [none]

```
Enter :
    IP address (up to 15 characters)
>

Enter :
    subnet mask size(from 2 to 30)
>
```

4 - Peer IP Address

Allows the definition of an Internet Protocol (IP) address and corresponding subnet size for link side of the PPP 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 2 to 30)
>
```

5 - VJ Compression

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

Default: [disabled]

IPX Parameters Menu

```
                    EDIT REMOTE SITE 1 IPX PARAMETERS MENU

    Option              Value                  Description
 1. IPXCP enabled       [enabled]            - Enable IPXCP negotiations
 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 PPP router. The parameters defined here are used by the IPXCP (Internet Packet Exchange Control Protocol) functions of the router for negotiating IPX routing during call establishment.

1 - IPXCP Enabled

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

Default: [enabled]

2 - Link IPX Type

This option defines the type of link connection that will be established with the remote site PPP router. The link may be numbered, this is where both sides of the WAN connection have IPX node addresses assigned and the WAN connection also has it's own IPX network number, or unnumbered, this is where the local and peer (remote partner PPP router) routers use their internal LAN side IPX node numbers.

When operating in unnumbered mode, each of the two IPX routers operate as half of a complete router. The WAN connection is considered to be 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 PPP routers.

Default: [unnumbered]

Choices: numbered, unnumbered

3 - IPX Net

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 PPP router.

Default: [0]

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

4 - Local IPX Node

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

Allows the definition of an Internet Packet Exchange (IPX) node address for the link side of the PPP 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)
>
```

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]

7 - IPX DMR Enabled

The IPX DMR Enabled option enables 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.

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]

8 - Force RIP Update

The Force RIP Update option determines if the DI-1133 will send a RIP update request to the WAN peer IPX router when a local LAN RIP update is sent. When operating under normal RIP update times, this 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 DI-1133 performs data compression at the bundle level and not at the link level. Link based compression will be rejected. The DI-1133 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.

Show Remote Site Menu

```
                          SHOW REMOTE SITE MENU

    Option                          Description
 1. Call configuration          - Remote site call configuration
 2. Protocol configuration      - Remote site protocol configuration
 3. Primary schedule            - Display primary activation schedule
 4. Secondary schedule          - Display secondary activation schedule









Enter:
    id or alias to display (1 to 16 characters)

> 1
```

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

```
                        SHOW REMOTE SITE 1 MENU

    Option                          Description
 1. Call configuration          - Remote site call configuration
 2. Protocol configuration      - Remote site protocol configuration
 3. Primary schedule            - Display primary activation schedule
 4. Secondary schedule          - Display secondary activation schedule









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

>
```

1 - Call Configuration

Displays an overview of the call configuration parameters for the chosen remote site.

```
                        REMOTE SITE 2 CALL CONFIGURATION

 General
 Alias                : Vancouver
 MP Operation         : enabled
 Auto-call            : enabled



 Conditional Operation                    ISDN
 Primary              : Disabled          ISDN Number      : 555-1212
 Secondary            : Enabled           Alt. ISDN Number : none
 Traffic Level        : Enabled           Call You Number  : none
 Up Threshold         : 50 %              Redial Timer     : 10
 Up Stability Timer   : 5 min             Redial Count     : 0
 Down Threshold       : 40 %
 Down Stability Timer : 10 min



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

2 - Protocol Configuration

Displays an overview of the LCP (Link Control Protocol) configuration parameters for the chosen remote site.

```
                     REMOTE SITE 2 PROTOCOL CONFIGURATION

 Bridge Parameters                        IP Parameters
 BCP                : enabled             IPCP               : enabled
 Tinygram           : disabled            Link IP Type       : numbered
 FCS Preservation   : enabled             Local IP Address   : 0.0.0.0/0
 STP                : none                Local Subnet Mask  : none
 STP Port State     : enabled             Peer IP Address    : 0.0.0.0/0
 STP Port Path Cost : 100                 Peer Subnet Mask   : none
 STP Port Priority  : 128                 VJ Compression     : disabled


 IPX Parameters                           CCP Parameters
 IPXCP              : enabled             CCP                : disabled
 Link IPX Type      : unnumbered          Protocol           : Stac LZS (17)
 IPX Network Number : 0                   Histories          : 1
 Local IPX Node     : 00-00-00-00-00-00   Check Mode         : Sequence Number
 Peer IPX Node      : 00-00-00-00-00-00   Extended Sequence  : disabled
 IPX Demand RIP     : disabled


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

3 - Primary Schedule

Displays the activation time schedule for the primary link for the chosen remote site.

```
                    Remote Site 1 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.
```

4 - Secondary Schedule

Displays the activation time schedule for the secondary link for the chosen remote site. This option is only available when Multilink is enabled for this remote site.

```
                    Remote Site 1 Call 2 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.
```

Security Set-Up Menu

```
                          SECURITY SET-UP MENU

    Option                  Value          Description
 1. Edit security entry      menu         - Modify/add security entry
 2. Security level          [none]        - Security protocol for calls
 3. Outgoing user name      "DEV050607"   - Outgoing user name
 4. Outgoing PAP password   "*"           - Outgoing PAP password
 5. Outgoing CHAP secret    "*"           - Outgoing CHAP secret
 6. CHAP challenges         [once]        - CHAP Authentication
 7. Show security database                - Display security list
 8. Remove security entry                 - Delete security entries




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 PPP security options for this router.

1 - Edit Security Entry

Takes you to the Edit Security Entry Menu. Here you set the authentication passwords and user names in the incoming security database.

2 - Security Level

This option defines the type of PPP security to use for incoming ISDN calls.

When a security level is set, the DI-1133 will always require authentication on incoming ISDN calls.

The DI-1133 will ask for authentication on all outgoing calls when a security level is set.

Default: [none]

Choices: none, PAP, CHAP

3 - Outgoing User Name

This option defines the user name that this DI-1133 PPP router will use when responding to authentication requests from a remote site PPP router.

The outgoing user name is case sensitive and may consist of 1 to 16 alphanumeric characters. Use the underscore character instead of a space character.

Default: [*] Default device name.

4 - Outgoing PAP Password

This option defines the PAP password that this DI-1133 PPP router will use when responding to authentication requests from a remote site PPP router.

Default: [BRIDGE]

5 - Outgoing CHAP Secret

This option defines the CHAP secret that this DI-1133 PPP router will use when responding to authentication requests from a remote site PPP router.

Default: [BRIDGE]

6 - CHAP Challenges

This option defines the frequency of CHAP challenges that this DI-1133 PPP router will require when authenticating a remote site PPP router.

Default: [once]

Choices: once, continuous

7 - Show Security Database

```
    Identifier     User Name           PAP Password     CHAP Secret
    ----------     ----------------    ------------     -----------
         1         Vancouver           *                none
         2         Denver              none             *
         3         Paris               *                *
```

8 - Remove Security Entry

Allows you to remove a selected user name and passwords from the security database. The user names may be removed individually by using the index number or all at once.

```
Enter :
    all, Security entry index

>
```

Edit Security Entry Menu

```
                        EDIT SECURITY ENTRY MENU

    Option          Value          Description
 1. User name      [        ]   - Security entry user name
 2. PAP password   [        ]   - Security entry PAP password
 3. CHAP secret    [        ]   - Security entry CHAP secret









Enter:
    security entry index (from 1 to 41)


> 1
```

The above display is the first level of the **EDIT SECURITY ENTRY MENU**. Once the security entry index number is entered, the number specified is added to the menu title bar and the Options are as shown below:

When creating a new security entry, the DI-1133 will prompt you for a security entry id number as well as a user name for the security entry. The menu will then be updated with the id number and the user name and the parameters may be modified.

```
                      EDIT SECURITY ENTRY 1 MENU

    Option          Value          Description
 1. User name      [Vancouver]   - Security entry user name
 2. PAP password   [none]        - Security entry PAP password
 3. CHAP secret    [none]        - Security entry CHAP secret









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


>
```

1 - User Name

This option defines the user name that the remote site PPP router will be sending to this DI-1133 PPP router when responding to authentication requests from this DI-1133 PPP router.

The user name must be defined the same as the user name defined on the remote site router.

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.

Default: [none]

2 - PAP Password

This option defines the PAP password that the remote site PPP router will use when responding to authentication requests from this DI-1133 PPP router.

The PAP password must be defined the same as the PAP password defined on the remote site router.

Default: [none]

3 - CHAP Secret

This option defines the CHAP secret that the remote site PPP router will use when responding to authentication requests from this DI-1133 PPP router.

The CHAP secret must be defined the same as the CHAP secret defined on the remote site router.

Default: [none]

PPP Set-Up Menu

```
                              PPP SET-UP MENU

   Option                 Value          Description
 1. Advanced PPP set-up    menu         - Configure advanced PPP parameters
 2. Restart timer         [3000 msec]   - Set restart timer
 3. Configure count       [10]          - Set configure count
 4. Failure count         [5]           - Set failure count
 5. Terminate count       [2]           - Set terminate count









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

>
```

The **PPP SET-UP MENU** 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 DI-1133 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 DI-1133 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

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 sequencing       [normal]        - Set multilink sequence numbers
 7. MP discriminator    [MAC_address]   - Set multilink endpoint discriminator
 8. 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 DI-1133 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 DI-1133 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 DI-1133 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 DI-1133 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 DI-1133 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 DI-1133 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 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.

7 - MP Discriminator

The MP Discriminator option specifies the type of identification used to identify this DI-1133 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

8 - 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

IP Address Connect Menu

```
                          IP ADDRESS CONNECT MENU

    Option                    Value         Description
 1. Edit IP address entry                   - Modify/add IP address entry
 2. IP address connect       [disabled]     - Activate IP address connect
 3. IP inactivity timer      [60 sec]       - Set traffic inactivity timer
 4. Show IP address entries                 - Display IP address entries
 5. Remove IP address entry                 - Delete IP address entry









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

>
```

The **IP ADDRESS CONNECT MENU** allows the display and configuration of the IP Address Connect table entries. IP Address Connect is used to establish ISDN calls to specific remote sites based on specific destination IP addresses.

1 - Edit IP Address Entry

Allows the definition of an entry in the IP Address Connect table allowing this DI-1133 to establish a PPP ISDN call to a specific remote site PPP router when IP traffic destined for a specific IP network is received from the local LAN. The IP addresses in the table are searched sequentially according to entry id number.

An entry of the IP address 0.0.0.0 causes any IP traffic to initiate a call to the specified remote site. Adding one of these default entries to the end of the table, id number 40, causes all IP traffic for destinations not listed in the address connect table to be sent to this default entry.

To change any of the values of an entry that already exists, simply re-enter the values and substitute the new values where appropriate.

```
Enter :
    Set the IP address connect entry id (from 1 to 40)

>

Enter :
    Set the IP Address (up to 15 characters)

>

Enter :
    Size of subnet mask (from 1 to 32)

>

Enter :
    Remote site alias or id (up to 16 characters), none

>
```

2 - IP Address Connect

This option enables or disables the IP Address connect operation of the router. When IP Address Connect is enabled, all IP traffic on the local LAN is checked against the IP routing table. If the IP address is not present in the IP routing table, the address is checked in the IP Address Connect table.

Default: [disabled]

3 - IP Inactivity Timer

This option defines the IP Inactivity Timer that is used to determine when the ISDN to the remote site will be disconnected.

When the IP Inactivity Timer is set to none, this DI-1133 will not disconnect ISDN calls that have been established due to IP address connect.

Default: [60 sec]

Range: none, 20 to 3600 seconds

4 - Show IP Address Entries

Displays all of the IP addresses and their corresponding remote site profile alias currently in the IP Address connect table. There may be up to 40 IP network addresses defined in the table.

```
  ID   IP Address        Subnet Mask Size   Subnet Mask       Remote Site
  --   --------------    ----------------   ---------------   ----------------
   1   12.12.12.12               1          128.0.0.0         Vancouver

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

ID:	Entry number in the IP Address Connect table.
IP Address:	Network IP address of the remote network or device.
Subnet Mask Size:	IP address mask size defined
Subnet Mask:	IP address mask created from the mask size defined. The mask is used to allow all IP addresses of a destination IP network to apply to the Address connect function.
Remote Site:	Remote site profile entry to be used to call a remote partner DI-1133 when IP traffic destined for the IP address is seen on the local LAN.

5 - Remove IP Address Entry

Allows you to remove a selected IP Address Connect entry from the database. The entries may be removed individually by using the index number or all at once.

```
Enter :
    all, id
>
```

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

Directs you to the Spanning Tree Menu, where parameters of the Spanning Tree Protocol for this bridge are set and viewed.

2 - Bridge Forwarding

This option enables or disables the frame forwarding operation of the bridge.

Default: [enabled]

3 - Bridge Aging Timer

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 value 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 value 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

Displays all addresses in the Bridge Filter Table, identifies the active/inactive and permanent/non-permanent addresses, identifies addresses to be filtered if they are a source and/or destination, describes their location, and gives the total number of address table entries.

```
                          ALL Known MAC Addresses
Total entries : 20
                             Filter If
Address            Active Perm Src  Dest Location
Start of table
01-80-c2-00-00-01           *         *  Internal
01-80-c2-00-00-02           *         *  Internal
01-80-c2-00-00-03           *         *  Internal
01-80-c2-00-00-04           *         *  Internal
01-80-c2-00-00-05           *         *  Internal
01-80-c2-00-00-06           *         *  Internal
01-80-c2-00-00-07           *         *  Internal
01-80-c2-00-00-08           *         *  Internal
01-80-c2-00-00-09           *         *  Internal
01-80-c2-00-00-0a           *         *  Internal
01-80-c2-00-00-0b           *         *  Internal
01-80-c2-00-00-0c           *         *  Internal
01-80-c2-00-00-0d           *         *  Internal
01-80-c2-00-00-0e           *         *  Internal
01-80-c2-00-00-0f           *         *  Internal
ff-ff-ff-ff-ff-ff           *            Internal
12-34-56-78-99-99     *     *   *     *     LAN050607(fixed)
11-11-11-11-11-11                   *  unknown
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 third last 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 second last 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 last 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.

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 or is one of the three internal addresses of the bridge. 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.)

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.

LANxxxxxx (unknown)

These are addresses that 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

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
Address            Active Perm Src  Dest Location
Start of table
12-34-56-78-99-99     *     *    *    *     LAN050607(fixed)
End of table
```

6 - Clear Bridging Table

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

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

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**.

When STP is changed from enabled to disabled, all WAN connections will be dropped.

3 - Bridge Priority

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, this 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

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

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. (Basically 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

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

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

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

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 tie-breakers.

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

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. Routing protocol         [rip]        - Define routing protocol
 3. IP routing               [enabled]    - Enable/disable IP router
 4. IP forwarding            [disabled]   - Enable/disable IP routing
 5. ARP proxy                [disabled]   - Support proxy-ARP









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


>
```

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

1 - IP Routes

Directs you to the IP Routes Menu, where the routing tables are displayed and changed.

2 - Routing Protocol

This option allows the IP routing protocol to be defined as RIP or none. When defined as RIP, the DI-1133 will operate as a RIP IP router. When defined as none, the DI-1133 will operate as an IP router but will NOT participate in the exchange of RIP messages between the other IP routers in the network.

When the routing protocol is defined as none, 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.

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: [rip]

Choices: rip, none

3 - IP Routing

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.

4 - IP Forwarding

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]

5 - ARP Proxy

The DI-1133 Ethernet router will respond to ARP requests destined for another subnet, from its local subnet, when this option is enabled. This option applies only to subnets.

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

Directs you to the Edit Route Menu where the routing tables are modified.

2 - Show All Routes

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 are a maximum of 512 route entries allowed in the table.

```
                              All IP Routes
Total entries : 3
Destination   Subnet                          Next Hop                    Route
 IP Address     Size     Subnet Mask          IP Address      Cost  Age  Type
 --Start of table--
198.169.2.0       0      255.255.255.0        198.169.1.23      1     0  LOCAL
198.223.112.0     0      255.255.255.0        198.169.1.22      3     4  RIP
218.199.12.0      0      255.255.255.0        198.169.1.22      5     10 RIP
----End of table
```

Destination IP Address:	Network IP address of the remote network.
Mask Size:	Subnet mask size defined for the route.
Subnet Mask:	Subnet Mask used for the route.
Next Hop IP Address:	IP address of the next hop router to use to reach the Destination IP Address.
Cost:	Number of hops to reach the Destination IP Address.
Age:	Actual cost to reach the Destination IP Address.
Route Type:	Type of route used, either RIP or LOCAL. LOCAL is used for static routes.

3 - Show Static Routes

Displays all of the static routes currently in use by the router.

```
                                Static IP Routes
Destination   Mask                            Next Hop                    Route
 IP Address     Size     Subnet Mask          IP Address      Cost  Age   Type
 --Start of table--
198.169.2.0       0      255.255.255.0        198.169.1.23      1     0  LOCAL
198.169.3.0       0      255.255.255.0        198.169.1.23      1     0  LOCAL
 ----End of table
```

4 - Clear Static Routes

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. Next hop       [        ]   - IP address of the next hop
 4. Cost           [        ]   - Cost to reach destination in hops
 5. Type          *[        ]   - Type of route
 6. 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.

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 MENU

    Option          Value                Description
 1. Network mask  *"255.255.255.0"   - The network mask for the route
 2. Status        *"Not Present"     - Is the address in the table
 3. Next hop       ""                - IP address of the next hop
 4. Cost           [1]               - Cost to reach destination in hops
 5. Type          *""                - Type of route
 6. 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

Tells whether the address is "Present" or "Not Present" in the Routing Table. When the address is first entered, "Not Present" 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 - Next Hop

Defines the IP address of the next-hop router to be used to reach the destination IP address. The next-hop router must be on the local network or sub-network.

4 - Cost

Defines the number of hops required to reach the destination IP address.

Default: [1]

Range: 1 - 15

5 - Type

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 - Remove

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

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

2 - Static Services

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

3 - Configure LAN Networks

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

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

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

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

Displays all of the learned IPX routes currently in use by the router.

There are 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 which 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

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 are 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

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

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

This 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

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 which 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

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

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

Defines the destination IPX network address of the static route.

3 - Interface

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

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

Defines the number of hops to reach the destination IPX network.

Default: [1]

Range: 1 - 15

6 - Ticks

Defines the number of ticks to reach the destination IPX network.

Default: [1]

Range: 1 - 64000

7 - Remove

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

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

This 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

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 which 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

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
 9. Remove                      - Remove entry from table



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

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

Defines the IPX server name of the static service.

3 - Service Type

Defines the type of IPX service as a hex value.

Default: [0]

Range: 0 - ffff

4 - Interface

Defines the interface, either LAN or remote site device, that 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

Defines the IPX network address of the static service.

6 - Node

Defines the IPX node address of the static service.

7 - Socket

Defines the socket number of the static service if applicable.

8 - Hops

Defines the number of hops to reach the IPX service.

Default: [0]

Range: 0 - 15

9 - Remove

Removes the IPX static service from the table.

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. 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 - Help

Offers a brief description of the IPX frame types and network numbers.

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 DI-1133s compliance with the SNMP MIBs and details of the proprietary MIB, please refer to the MIB diskette included with the unit.

1 - Edit Community

Takes you to the Define Community Menu, where the router's agent and NMS are brought under a management community.

2 - Message Size

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

Displays the defined SNMP communities.

```
SNMP Communities

Number of defined communities  :  2

Community Name      Write Access      NMS Addresses     Trap Addresses
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

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 that only alphanumeric characters and the underscore ("_") character may be used in the community name. Also, 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

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

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

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

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

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

Offers a brief description of the address list's purpose and format.

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

Takes you to the MAC Address Filters Menu, where you can define parameters for Source MAC Filters.

2 - Bridge Pattern Filter

Takes you to the Bridge Pattern Filter Menu, where you can create bridge filters based on custom specifications.

3 - IP Router Pattern Filter

Takes you to the IP Router Pattern Filter Menu, where you can create IP filters based on custom specifications.

4 - 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

Takes you to the Edit MAC Address Filter Menu, where the MAC Address Filters are modified.

2 - Filter Operation

This 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

This 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

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.

```
Device: DEV050607
ALL Known MAC Addresses
Total entries : 20
                              Filter If
Address            Active Perm Src  Dest Location
Start of table
01-80-c2-00-00-01           *         *  Internal
01-80-c2-00-00-02           *         *  Internal
01-80-c2-00-00-03           *         *  Internal
01-80-c2-00-00-04           *         *  Internal
01-80-c2-00-00-05           *         *  Internal
01-80-c2-00-00-06           *         *  Internal
01-80-c2-00-00-07           *         *  Internal
01-80-c2-00-00-08           *         *  Internal
01-80-c2-00-00-09           *         *  Internal
01-80-c2-00-00-0a           *         *  Internal
01-80-c2-00-00-0b           *         *  Internal
01-80-c2-00-00-0c           *         *  Internal
01-80-c2-00-00-0d           *         *  Internal
01-80-c2-00-00-0e           *         *  Internal
01-80-c2-00-00-0f           *         *  Internal
ff-ff-ff-ff-ff-ff           *            Internal
12-34-56-78-99-99     *     *   *     *    LAN050607(fixed)
11-11-11-11-11-11                   *  unknown
end of table
```

Refer to the Show Bridging Table option of the Bridging Set-up menu for more details.

5 - Show Permanent Table

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
Address            Active Perm If Src  Location
Start of table
12-34-56-78-99-99     *     *    *     LAN050607(fixed)
End of table
```

6 - Clear Bridging Table

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

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

Identifies the location of the MAC address. The location will either be "unknown" or the LAN name of one of the partner connected DI-1133 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

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

Toggles between Enabling and Disabling of the Destination Filtering feature for the specified address.

Default: [disabled]

Considerations:

When the Filter Operation is set to positive, enabling this option will prevent access to this address from another LAN station located across the bridge/router. Once Filter if Destination is chosen, the Permanent value is set to [enabled]. This may be toggled back to [disabled] if a non-permanent entry is desired.

When the Filter Operation is set to negative, enabling this option will allow access to this address from another LAN station located across the bridge/router. Once Forward if Destination is chosen, the Permanent value is set to [enabled]. This may be toggled back to [disabled] if a non-permanent entry is desired.

5 - Permanent

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 this option if removal of the specified address (permanent or non-permanent) is desired. 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

Displays all 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

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

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

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

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

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

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

Displays all 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

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

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

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

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

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

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

Displays all existing default Aliases and those created with the Add Alias option.

```
                    IPX Router Filter Pattern Aliases
 1. NETBIOS    - 5-14
```

2 - Add Alias

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

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

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

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

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

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

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

Takes you to the LAN Statistics Menu, where statistics can be examined to evaluate LAN performance.

3 - WAN Statistics

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 this 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

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

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

Displays a summary of Bridged LAN traffic since the statistics were last reset.

2 - IP Traffic

Displays a summary of IP Router LAN traffic since the statistics were last reset.

3 - IPX Traffic

Displays a summary of IPX Router LAN traffic since the statistics were last reset.

4 - Total LAN Traffic

Displays a summary of Total LAN traffic since the statistics were last reset.

5 - LAN Error

Displays a summary of LAN and router errors since the statistics were last reset.

6 - Frame Size

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

Clears all statistic fields in the LAN statistics to zero.

8 - Clear LAN Errors

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 LAN            4169752          219         416         441
Bytes from LAN           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 Forwarded          4215689         221         416         441
Bytes Forwarded         269806208       14171       26667       28236

Frames to LAN             4169752         219         416         441
Bytes to LAN            268464916       14024       26667       28250
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 forwarded	All IP frames successfully received from the local LAN and forwarded to partner routers.
Bytes forwarded	All IP bytes successfully received from the local LAN and forwarded to partner routers.
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.
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

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.
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. Clear remote site stats               - Reset remote site statistics
 3. Link status                           - View status of link
 4. Clear link statistics                 - Reset link statistics









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


>
```

1 - Remote Site Status

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

2 - Clear Remote Site Statistics

Clears all fields in all of the remote site statistics displays to zero.

3 - Link Status

Displays the status of the links, either individually (more statistics), or together (provides overview).

Please refer to the following pages for more detailed information.

4 - Clear Link Statistics

Clears all fields in the Link statistics to zero.

Link Status Display (Option 3)

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

all (Multilink)

```
                                  Link  1 Status
State: Enabled, Up, Network, Opened
Remote Site: two
Speed: 64000 bps, BRI

                                  Link  2 Status
State: Enabled, Up, Network, Opened
Remote Site: two
Speed: 64000 bps, BRI

                          Combined 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.
```

The Link Status may be displayed individually for more detailed information:

Link 1 Status

```
                                Link  1 Status
State: Enabled, Up, Network, Opened
Remote Site: two

Interface State         Frame Counts  (Rcv/Xmt)       Frame Errors
Speed   : 64000 bps     Bytes :      47648/47639      Cgt disc   : 0
Type    : BRI           Frames:       3536/3536       CRC        : 0
Circuit : Outgoing                                    Rcv abort  : 0
State   : Active                                      Overrun    : 0
                                                      Rcv miss   : 0
Partner Number:                                       Too large  : 0
5551212                                               Misaligned : 0
                                                      Underrun   : 0
                                Throughput
Rcv   0%       0.0 KB |
Xmt   0%       0.0 KB |
                      |----|----|----|----|----|----|----|----|----|----|
                     0   10   20   30   40   50   60   70   80   90  100%

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

State :

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

Remote Site :

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

Speed :

This displays the speed of the ISDN call. The speed will be as set by the ISDN connection. The speed displayed may either be 56000 or 64000 depending on the ISDN service the router is connected to. If the ISDN call is disconnected, no speed (0) will be shown.

The DI-1133 will perform V.110 rate adaption when required to complete an ISDN call.

Type :

The interface type is identified in this display (BRI DTE).

Circuit :

This identifies the type of ISDN call. The call may be “Incoming, Outgoing, or Cleared”.

State :

This identifies the current state of the ISDN call. The state may be one of “Null, Proceeding, Disconnecting, or Active”.

Partner Number :

This identifies the ISDN number of the remotely connected PPP ISDN router.

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.

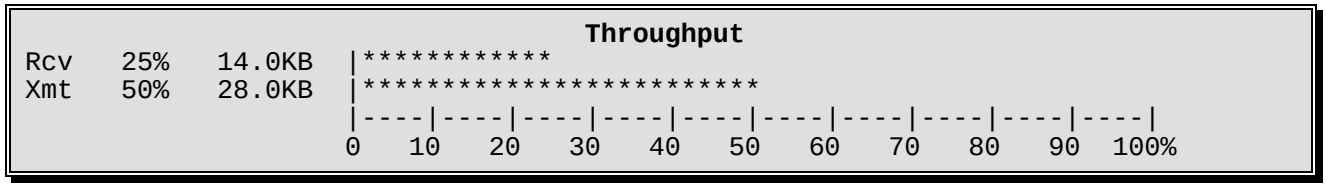
Too large This reports that an incoming frame has been discarded because the frame exceeded the maximum length. This may be caused by a frame being overrun by another frame on the link, so that the router thinks both frames are one frame.

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 the 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                          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
 5. Primary call status          - Display primary call statistics
 6. Secondary call status        - Display secondary call statistics
 7. Primary call quality         - Display primary link quality data
 8. Secondary call quality       - Display secondary link quality data
 9. Multilink statistics         - Display multilink statistics




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 two 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
 5. Primary call status          - Display primary call statistics
 6. Secondary call status        - Display secondary call statistics
 7. Primary call quality         - Display primary link quality data
 8. Secondary call quality       - Display secondary link quality data
 9. Multilink statistics         - Display multilink statistics




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


>
```

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.

5 - Primary Call Status

Displays a summary of the LCP parameters and the frame counts and errors for the primary ISDN call for the chosen remote site since the statistics were last reset.

6 - Secondary Call Status

Displays a summary of the LCP parameters and the frame counts and errors for the secondary ISDN call in a Multilink configuration for the chosen remote site since the statistics were last reset.

7 - Primary Call Quality

Displays a summary of the Call Quality parameters for the primary ISDN call for the chosen remote site since the statistics were last reset.

8 - Secondary Call Quality

Displays a summary of the Call Quality parameters for the secondary ISDN call in a Multilink configuration for the chosen remote site since the statistics were last reset.

9 - Multilink Statistics

Displays a summary of the Multilink statistics for the chosen remote site since the statistics were last reset.

BCP Status Display (Option 1)

```
                                        BCP                    Remote Site  2-two
Multilink: disabled, Auto-call: 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.

Auto-Call :

This displays the current state of Auto-Call 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 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-two
Multilink: Enabled,  Auto-call: 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
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.

Auto-Call :

This displays the current state of Auto-Call 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 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.

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-two
Multilink: Disabled, Auto-call: 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.

Auto-Call :

This displays the current state of Auto-Call 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 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-two
Multilink: Disabled, Auto-call: Disabled, Compression: Enabled
Bundle state: Up, Operational status: Opened

                      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
   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.

Auto-Call :

This displays the current state of Auto-Call status 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.

Primary Call Status (Option 5)

```
                              Primary   Call                  Remote Site  2-two
Multilink: Enabled,  Auto-call: Disabled,  Link: 1
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.

Auto-Call :

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

Link :

This displays the link number being used by the primary call 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.

Secondary Call Status (Option 6)

```
                              Secondary  Call                  Remote Site  2-two
Multilink: Enabled,  Auto-call: Disabled,  Link: 2
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        :      1                   1
SDP             :      0                   0

      Frame Counts   (Rcv/Xmt)          Frame Errors
      Bytes  :      61917/61961         Header       : 0
      Frames :       4229/4229          Discard      : 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.
```

The displayed values and statistics shown here are described under the Primary Call Status option on the preceding pages. All of the values in this display are for the secondary ISDN call to the chosen remote site when in Multilink mode.

Primary Call Quality (Option 7)

```
                          Primary   Call Quality              Remote Site  2-two
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.

Secondary Call Quality (Option 8)

```
                        Secondary Call Quality              Remote Site  2-two
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.
```

The displayed values and statistics shown here are described under the Primary Call Quality option on the preceding pages. All of the values in this display are for the secondary ISDN call to the chosen remote site when in Multilink mode.

Multilink Statistics (Option 9)

```
                                  Multilink                  Remote Site  2-two
Multilink: Enabled,  Auto-call: Disabled, Bundle state: Up, Links: 2

         Local MP                          Remote MP
 MRRU  : 1600                              1600
 SSNHF : normal                            normal
 EPD   : class MAC 02-03-04-05-06-07       class MAC 02-03-04-05-06-08

         Frame Counts                      Fragment Counts
         Rcv              : 220            Rcv              : 437
         Xmt              : 220            Xmt              : 436

         Header Error     : 0              Header Error     : 0
         Discard          : 0              Discard          : 0
         Unknown Protocol : 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.

Auto-Call :

This displays the current state of Auto-Call 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.

Links :

This displays the number of links currently in use by this connection to the chosen remote site.

MRRU :

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

SSNHF :

This displays the negotiated SSNHF (Short Sequence Number Header Format) value for this end of the link connection as well as the SSNHF value for the remote end: normal / short.

EPD :

This displays the negotiated EPD (End Point Discriminator) value for this end of the link connection as well as the EPD value for the remote end.

Frame Counts

Rcv :

Receive — This indicates the number of MP frames that have been received. This is counted after reconstruction of the Multilink frame.

Xmt :

Transmit — This indicates the number of MP frames that have been transmitted. This is counted after reconstruction of the Multilink frame.

Header Error :

This indicates the number of MP frames that have been discarded due to an error in the header. This is counted after reconstruction of the Multilink frame.

Discard :

This indicates the number of MP frames that have been silently discarded due to the frame not belonging within a MP frame, i.e. LCP frames. This is counted after reconstruction of the Multilink frame.

Unknown Protocol :

This indicates the number of MP frames that have been discarded due to the frame being an unknown or unsupported protocol type, i.e. IPXCP or BDP. This is counted after reconstruction of the Multilink frame.

Fragment Counts

Rcv :

Receive — This indicates the number of MP frame fragments that have been received. This is counted before reconstruction of the Multilink frame.

Xmt :

Transmit — This indicates the number of MP frame fragments that have been transmitted. This is counted before reconstruction of the Multilink frame.

Header Error :

This indicates the number of MP frame fragments that have been discarded due to an error in the header. This is counted before reconstruction of the Multilink frame.

Discard :

This indicates the number of MP frame fragments that have been discarded due to the remaining portion of the MP frame not being received.

Diagnostics Menu

```
                              DIAGNOSTICS MENU

    Option              Value          Description
 1. Trace               menu         - View link frames
 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 - Trace

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

2 - Heartbeat

Enables/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 this 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 this 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.

Trace Menu

```
                                TRACE MENU

    Option          Value                   Description
 1. Trace 1         [disabled]              - View link 1 frames
 2. Trace 2         [disabled]              - View link 2 frames
 3. Real time       [disabled]              - Display frames in real-time
 4. Capture         [disabled]              - Capture frames in buffer
 5. Allocate        [0 kbytes]              - Set capture buffer size
 6. End             [disabled]              - End capture at link down
 7. Data display    [hex] [single_line]     - Set frame display format
 8. Time            [disabled]              - Add time to display
 9. 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 router; therefore, the tracing functions should only be [enabled] when needed.

1 - Trace Link 1
2 - Trace Link 2

[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.

3 - 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).

4 - Capture

Enabling this option allows for frame capture and display after the buffer is allocated. Use Option 9, Show, to display the capture.

5 - 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.

6 - 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].

7 - 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
>
```

8 - 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.

9 - Show

This option appears once the buffers are allocated and 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 Router**	**Partner 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 router requesting the connection.

SUPERVISORY FRAMES:

RR — Receiver Ready

A Receive Ready (**RR**) supervisory frame is sent by the 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 router.

RNR — Receiver Not Ready

The **RNR** statistic is generated by either remote 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 — REJect

The **REJ** supervisory frame is generated when a remote 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 router.

UNNUMBERED FRAMES:

SABM — Set Asynchronous Balanced Mode

The **SABM** unnumbered command is generated to place the addressed 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 router.

The receiving 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 DISConnect

The **DISC** statistic is generated when the router sending the **DISC** informs the other router that it (the sending router) is suspending its own operation.

Before the **DISC** is acted upon, the router receiving the **DISC** confirms its acceptance of the **DISC** command by the transmission of a **UA** response. The 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 Unnumbered Acknowledgment

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 router.

DM Disconnected Mode

The **DM** unnumbered response and statistic is generated to report a status where the router is logically disconnected from the link, and is in the disconnected phase.

1) The **DM** may be sent to indicate that the 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 router(s) that this router is still in the disconnected phase and cannot execute the Set Mode command.

A 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 FRaMe Reject

The **FRMR** statistic is generated by the router to report an error condition not recoverable by the re-transmission of an identical frame. This may result from at least one of the following conditions:

1) the receipt of a command or response control field that is undefined or not implemented;

2) the receipt of an I frame with an information field that exceeds the maximum established length;

3) the receipt of an invalid N(R); or

4) the receipt of a frame with an information field that is not permitted or the receipt of a supervisory or unnumbered frame with incorrect length.

An undefined or not implemented control field is any control field encoding not identified in Table 5, LAPB commands and responses.

A valid N(R) must be within the range from the lowest send sequence number N(S) of the still unacknowledged frame(s) to the current logical DCE send state variable, inclusive.

An information field that immediately follows the control field, and consists of 3 to 5 octets, is returned with the FRMR and provides the reason for the FRMR response.

Network Events Menu

```
                          NETWORK EVENTS MENU

    Option                  Description
 1. Acknowledge alarm      - Clear alarm status display
 2. Show events            - View event history
 3. Clear events           - Clear event history
 4. Show security log      - View security failure log
 5. Clear security log     - Clear security failure log









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

This option clears the screen ALARM display for the current alarm.

2 - Show Events

Displays the 42 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

Removes all ALARMs from the table.

4 - Show Security Log

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

Removes all ISDN security logs from the table.