DI-1133
Ethernet Bridge/Router

ISDN Menus

Reference Manual

Issue 1

Software Versions 2SR.07.08.X

 9/96

Part # 168-26205

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

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

Initial Bridge/Router & Management Console Power-Up

The following screen information will be seen on the console connected to the bridge/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 bridge/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.

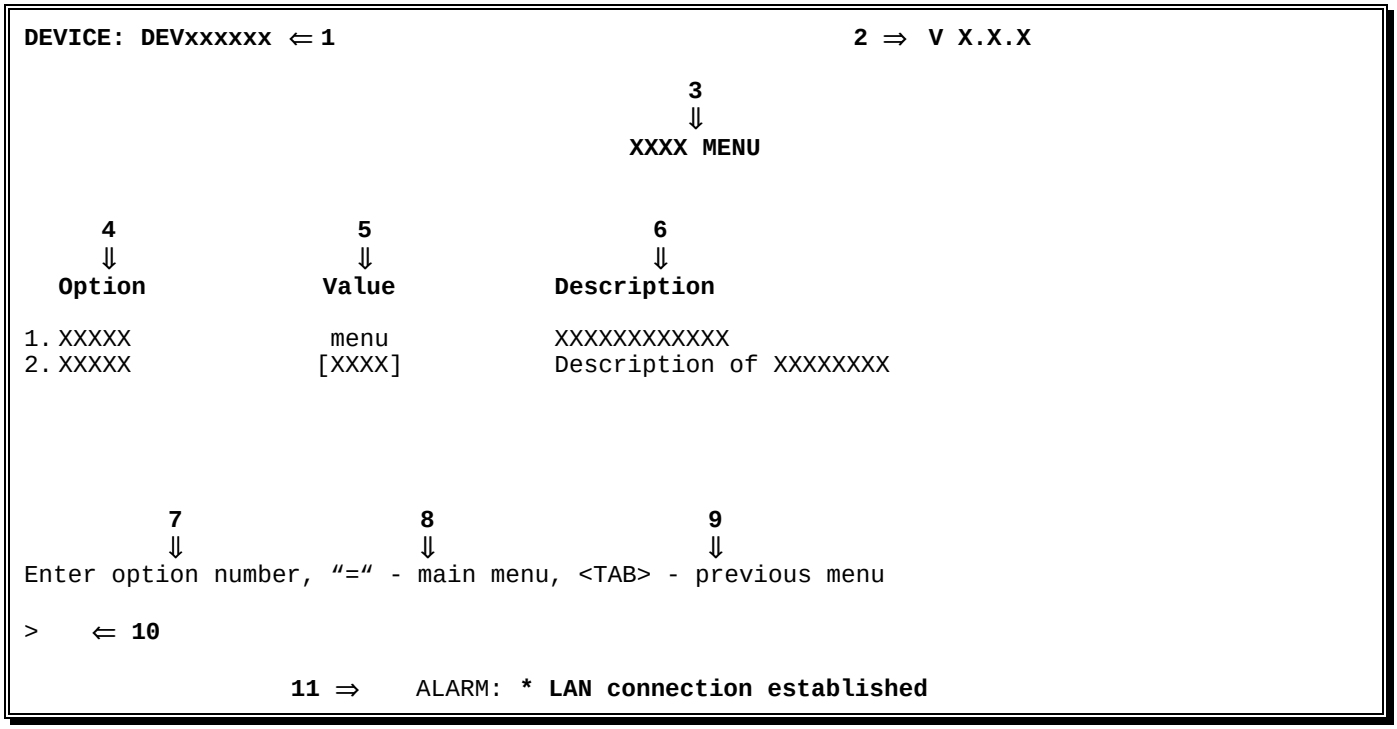
The DI-1133 Ethernet bridge/router uses a “hotkey “ Menu. A menu option is chosen by selection of the desired option number.

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 bridge/router. (xxxxxx are the last 6 digits of the MAC address of the bridge/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 bridge/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. Two of the Menus have their names updated as information is added: - the Address Filters Menu, which adds the Ethernet Address specified, and the Define SNMP Community Menu, which adds the name given by the bridge/router manager.

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 bridge/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 bridge/router.

Login - Option 1

Allows entry of the password for the bridge/router. The default password is "password" (in CAPITAL LETTERS); change it if security is desired. See the Installation & Applications Guide for information on restoring the default password to the bridge/router.

Action to Take:

Choose the Login Option and use the default password "password." 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 bridge/router management features.

Help - Option 2

Provides a brief description of menu format and usage.

Main Menu

```
                                MAIN MENU

    Option              Value          Description
 1. Configuration       menu         - Define operating parameters
 2. Statistics          menu         - Device LAN and WAN statistics
 3. Diagnostics         menu         - Access troubleshooting tools
 4. Network events      menu         - View network event history
 5. Logout                           - End operator session
 6. Help                             - Read menu introduction









Enter option number

>
```

The **MAIN MENU** is a starting and ending point for management of the bridge/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 "=".

Configuration - Option 1

Takes you to the Configuration Menu, where all the various bridge/router parameters can be defined. Take this path to define the operating parameters of the terminal used for the bridge/router console.

Statistics - Option 2

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

Diagnostics - Option 3

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

Network Events - Option 4

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

Logout - Option 5

Terminates your session and secures the bridge/router. The next user must log in and enter the correct password to view or change the bridge/router configuration.

Help - Option 6

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

Configuration Menu

```
                          CONFIGURATION MENU

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




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


>
```

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

Access Set-Up - Option 1

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 bridge/router configuration and connect to another bridge/router in the network of bridge/routers.

WAN Set-Up - Option 2

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

Bridging Set-Up - Option 3

Takes you to the Bridging Set-Up Menu, where the parameters for bridging are selected. The Spanning Tree Protocol (STP) may also be managed from this menu.

Internet Set-Up - Option 4

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

IP Routing Set-Up - Option 5

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.

IPX Routing Set-Up - Option 6

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.

SNMP Set-Up - Option 7

Takes you to the SNMP Set-Up Menu, where you to define the parameters necessary to allow the bridge/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 bridge/router to the NMS to inform it of a significant event (cold start, warm start, link up, link down, authentication failure).

Filter Set-Up - Option 8

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




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


>
```

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

Terminal Set-Up - Option 1

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

Device Set-Up - Option 2

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

Remote Access - Option 3

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

Load FLASH Set-Up - Option 4

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.

TFTP Restore - Option 5

Determines whether a remote LAN device will be allowed to make a TFTP connection to this bridge/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 bridge/router.
   (The IP address of the bridge/router may be found in the Internet Set-Up menu.)

2) Get the file "config.txt" from the bridge/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 bridge/router.
   (The IP address of the bridge/router may be found in the Internet Set-Up menu.)

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

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

Hardware Status - Option 6

Displays the current status of the bridge/router hardware.

```
                        Hardware Status

MAC address           : 02-03-04-05-06-07
MAC check code        : 23d4a6
Service reference     : 0/0
LAN interface type    : 10BaseT
Link 1 interface type : BRI ST
Link 2 interface type : BRI ST
ROM size              : 500KB
Full management       : enabled


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

MAC Address	The MAC Address of the LAN port for this bridge/router.
MAC Check Code	Check code used for feature upgrades.
Service Reference	Internal factory reference number.
LAN Interface Type	The LAN interface currently in use.
Link 1 Interface Type	The type of link interface for link 1.
Link 2 Interface Type	The type of link interface for link 2.
ROM Size	Indicates the size of the FLASH EEPROM installed.
Full Management	Indicates whether the current management level is Full or Limited.

Dump - Option 7

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 bridge/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 bridge/router.

The command "Configuration Access_Set-Up erase_config", is used at the time the dumped configuration is loaded back into the bridge/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).

Restore - Option 8

Restores a configuration to the bridge/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 bridge/router. This may be done through the setting of a delay timer (character or line pacing) or a wait for the echo of the character before transmitting the next character.

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

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

Procedures for performing a Configuration Load:

1) Prepare the PC to transfer the configuration file.
2) Execute the Load command.
   Confirmation is required. Enter "yes" to proceed.
3) Send the file from the PC disk.
4) When the transfer is complete, the configuration will have been restored to the bridge/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 bridge/router console is defined. A custom definition can be added if the terminal to be used is not presently supported by the bridge/router.

Terminal - Option 1

Defines the terminal type to be used for the bridge/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 bridge/router.

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

Show - Option 2

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

Add - Option 3

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.

Remove - Option 4

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. Remote password   [enabled]      - Password protect remote connections
 3. Device name       "DEV050607"    - Name this device
 4. LAN name          "LAN050607"    - Name the local LAN
 5. Show time                        - Display current date and time
 6. 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 and LAN names, and a password to control local/remote access to the bridge/router management console. You can also set the real-time clock and date. Note that the clock is a 24-hour real-time clock.

Password - Option 1

Allows you to change the bridge/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
```

Remote Password - Option 2

Default: [enabled]

With the ability to connect to other bridge/routers comes the possibility that someone might try to get access to the current or another bridge/router and alter its operating parameters. With this option enabled, any attempt to connect to the bridge/router will be allowed only if the correct password is entered as defined on the bridge/router for which the connection is attempted.

Device Name - Option 3

Allows you to name (or re-name) this device for identification purposes. The bridge/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 bridge/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 10 characters)
> Bridge5
```

LAN Name - Option 4

This option allows a name to be given to the LAN that the DI-1133 Ethernet bridge/router is attached to. The default uses the last 6 characters of the bridge/router's LAN port MAC address with a prefix of LAN (e.g. LAN006045).

```
Enter:
  LAN name string (up to 10 characters)
> Purchasing
```

Show Time - Option 5

Allows you to view the current date and time.

Set Time - Option 6

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 bridge/router across time zones, you must standardize on one time zone on the bridge/routers.

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

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

Remote Access Menu

```
                          REMOTE 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 **REMOTE ACCESS MENU** allows telnet connections to be made to other bridge/routers in the network.

Telnet - Option 1

Allows LAN devices to make Telnet connections to this bridge/router for management. Once the connection is established, the LAN device will be presented with the menu interface for configuration management and statistics viewing.

The Remote Password option of the Device Set-Up menu on page 15 determines if the LAN device initiating the Telnet connection will be prompted for a password in order to complete the connection to this bridge/router.

Default: [enabled]

Considerations:

When a Telnet connection is made to a bridge/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.

Connect - Option 2

Choosing this option, and specifying the name or IP address of the bridge/router you wish to connect to, connects to the other bridge/router for configuration purposes and viewing of statistics. To disconnect from the bridge/router being controlled, enter Control-C (**^C**).

The bridge/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.

Considerations:

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

Show Names - Option 3

```
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
Yokohama      LAN00a047   00-00-d0-00-a0-47   92.0.0.3     on link 1
Taipei        LAN00903d   00-00-d0-00-90-3d   92.0.0.4     on link 1
Amsterdam     LAN00a007   00-00-d0-00-a0-07   92.0.0.5     on link 2
London        LAN00a067   00-00-d0-00-a0-67   92.0.0.6     on link 2
New York      LAN00905d   00-00-d0-00-90-5d   92.0.0.7     on link 2


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

Add Name - Option 4

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
>
```

Remove Name - Option 5

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

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

Load FLASH Set-Up Menu

```
                          LOAD FLASH SET-UP MENU

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









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


>
```

From the **LOAD FLASH SET-UP MENU,** the software in the bridge/router may be updated to the latest version.

When installing a new version of operating software in a bridge/router, ensure that the current configuration is backed up before the installation process is started.

Console (ZMODEM) - Option 1

Resets the bridge/router and places it in Console load mode. Once the bridge/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 bridge/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 bridge/router:

1) Execute the Console (ZMODEM) command from the Load FLASH Set-Up menu. Confirmation is required. Enter "yes" to proceed.

2) After the bridge/router restarts, the bridge/router will be in a receive ZMODEM mode. The bridge/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 bridge/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 bridge/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. Refer to the Changing Link Interfaces section in the Installation & Applications Guide for information on removing and inserting the WAN modules.

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 bridge/router will display a limited menu system. Choose the Abort Load option from the Load FLASH Set-Up menu. This will cause the bridge/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 bridge/router is placed in Console load BOOT mode, the LAN and WAN interface will be disabled. The bridge/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.

Network (TFTP) - Option 2

Resets the bridge/router and places it in Network Load mode. Once the bridge/router is in Network Load mode, a TFTP connection may be made to the bridge/router to upgrade to a new version of software. Make sure to disconnect any telnet sessions to the bridge/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 bridge/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 bridge/router.
   (The IP address of the bridge/router may be found in the Internet Set-Up menu.)

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

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

5) The bridge/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, Switch Type, Directory Numbers, SPIDs, and Password), and then reset. After the reset, the bridge/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 bridge/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 bridge/router's current state during this process, get the file "status.txt" from the bridge/router. This file will report the bridge/router's state: either the mode and version if no errors have occurred, or an error message.

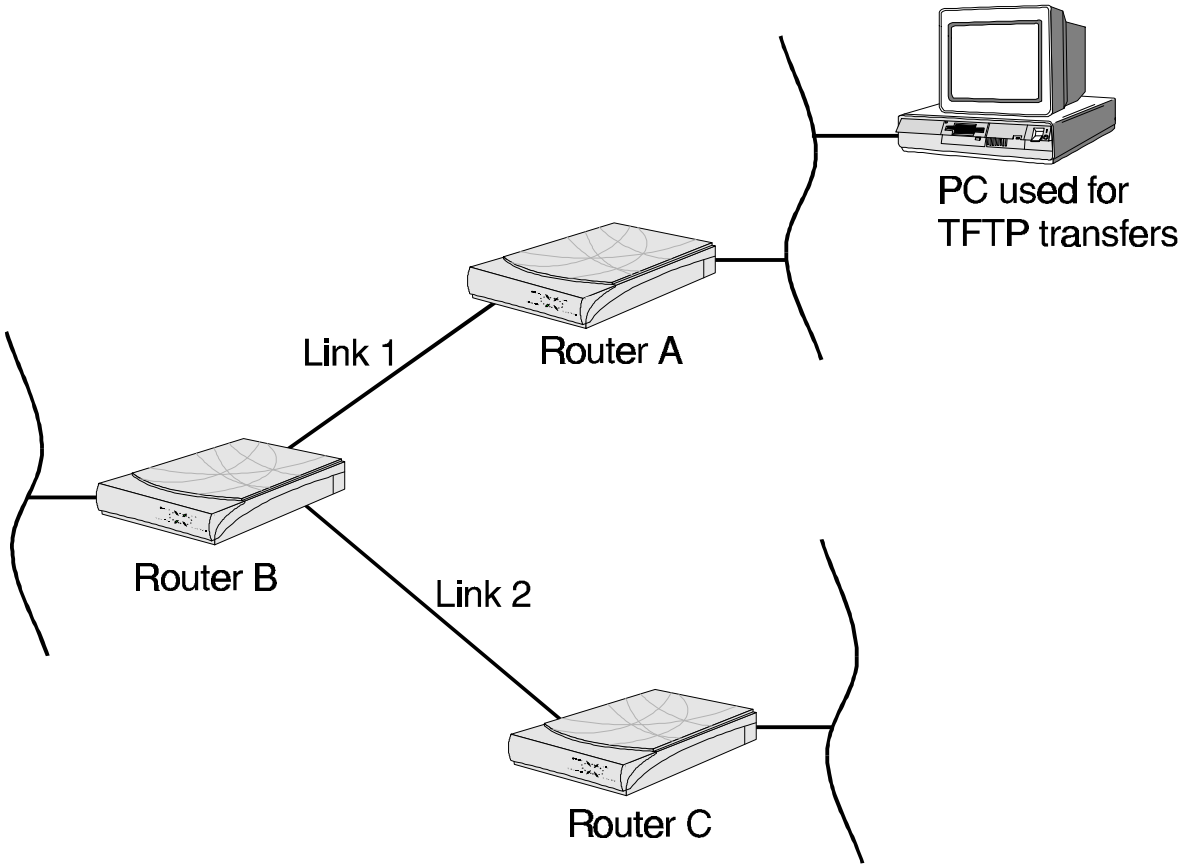
   On the rare occasion that during the programming of the FLASH something happens to the bridge/router (power hit or hardware reset), causing the FLASH to become corrupted, the bridge/router will restart in ZMODEM receive mode only. If the bridge/router does not start in ZMODEM receive mode, power down 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 the 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. Refer to the Changing Link Interfaces section in the Installation & Applications Guide for information on removing and inserting the WAN modules.

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 bridge/router and choosing the Abort Load option from the Load FLASH Set-Up menu. This will cause the bridge/router to reset and return to normal operations operating from the existing software.

Considerations:

When the bridge/router is placed in Network (TFTP) load BOOT mode, the bridge/router will restart and establish its LAN and WAN connections. In this state, bridge traffic is passed normally, the IPX router is not operational, and the IP router will only route IP traffic that is received from the LAN.

When performing a TFTP software download to a remote DI-1133, it is recommended that any unused WAN links be disabled before the DI-1133 is placed in Network load (TFTP) mode. In the following diagram, when performing a TFTP software load to bridge/router "Router B", the WAN link labeled "Link 2" should be disabled before the TFTP transfer is started.



WAN Set-Up Menu

```
                              WAN SET-UP MENU

    Option                 Value            Description
 1. ISDN set-up            menu           - Configure ISDN
 2. Circuit 1 set-up       menu           - Configure circuit 1
 3. Circuit 2 set-up       menu           - Configure circuit 2
 4. IP address connect     menu           - Configure IP address connect
 5. Connection Mgmt        menu           - Configure connection mgmt
 6. Extended routing      [disabled]      - Set extended routing
 7. WAN environment       [multipoint]    - Set operational mode




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


>
```

The **WAN SET-UP MENU** allows the definition of the ISDN link operation for the bridge/router. This menu also directs you to the desired ISDN Circuit Set-Up Menus.

ISDN Set-Up - Option 1

The ISDN Set-Up Menu allows you to set ISDN switch types and configure stored numbers.

Circuit 1 (2) Set-Up - Options 2 & 3

The Circuit Set-Up Menus allow you to set ISDN call configuration parameters for each of the two ISDN circuits available for connections to partner DI-1133 bridge/routers.

IP Address Connect - Option 4

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

Considerations:

The IP Address Connect menu option is only available when IP Routing is enabled.

Connection Management - Option 5

The Connection Management Menu allows you to configure the ISDN Connection Management options. Connection Management allows the ISDN calls to be suspended during periods of inactivity and then resumed when needed.

Extended Routing - Option 6

This option defines the DI-1133 WAN routing timer that is used. With Extended Routing disabled, the WAN routing timer is set to one tenth the default value. Extended Routing disabled will cause ISDN connection time to be substantially reduced.

If more than 3 DI-1133s are being used in a multipoint WAN set-up, Extended Routing must be set to enabled to allow for the increased WAN routing information required in a multi-DI-1133 configuration.

Default: [disabled]

Considerations:

If Extended Routing is set to disabled in a multipoint WAN set-up consisting of more than 3 DI-1133s, the ISDN links may not be maintained due to inadequate time for WAN routing information to be passed between the DI-1133s.

WAN Environment - Option 7

With the ISDN bridge/router, both ISDN links can pass data between the same two LANs in a Point-to-Point topology; or they can connect to other DI-1133 Ethernet bridge/routers located on two different LANs in a Multipoint topology.

(In this instance only the first letter is required as command-completion can be used):

```
Enter:
  multipoint, point_to_point
> p
```

Considerations:

When changing the WAN Environment, both ISDN links will perform a reset.

When changing from Multipoint to Point-to-Point, both ISDN links on this bridge/router will return to the default Compression state of Enabled. If the compression mode is not desired in the Point to Point configuration, you must change the Compression option to Disabled.

On **Single Active Link** ISDN DI-1133 Bridge/Routers, when the WAN Environment is set to Multipoint, only ISDN circuit 1 is available; ISDN circuit 2 is disabled. A Single Active Link ISDN DI-1133 will be able to use both ISDN calls to connect in a Point-to-Point topology to another ISDN DI-1133.

ISDN Set-Up Menu

```
                          ISDN SET-UP MENU

   Option                  Value         Description
 1. Stored number set-up    menu        - Configure stored numbers
 2. Security set-up         menu        - Configure security
 3. ISDN interface set-up   menu        - Configure ISDN interface
 4. Switch type            [NET3]       - Set switch type
 5. Dial prefix            [none]       - Set dial prefix
 6. Force 56K              [disabled]   - Force 56K rate adaption
 7. Phantom power detect   [disabled]   - Detect phantom power
 8. ISDN password                       - Set outgoing call password



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.

Stored Number Set-Up - Option 1

Takes you to the Stored Number Set-Up Menu, where ISDN numbers may be stored with optional aliases for ease of use when initiating a call.

Security Set-Up - Option 2

Takes you to the Security Set-Up Menu, where passwords may be defined for remote DI-1133 devices. When security is enabled, each remote DI-1133 calling this DI-1133 will be required to send the correct password before the WAN link is established.

ISDN Interface Set-Up - Option 3

Takes you to the ISDN Interface Set-Up Menu, where directory numbers and Service Profile Identifiers are defined for the ISDN B-channels.

Switch Type - Option 4

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

When the Switch Type is changed, a **Soft Reset** must be performed for this to take effect. This allows the bridge/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.).

Dial Prefix - Option 5

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]

Force 56K - Option 6

This option forces both B-channels on this DI-1133 bridge/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]

Phantom Power Detect - Option 7

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.

ISDN Password - Option 8

This option defines the ISDN password that is used by this DI-1133 when attempting to establish an ISDN connection to another DI-1133 with security enabled.

This DI-1133's device name and password must be defined on all remote DI-1133s within their respective security databases. If the passwords do not match, an ISDN WAN link connection will not be established.

Stored Number Set-Up Menu

```
                          STORED NUMBER SET-UP MENU

    Option                        Value    Description
 1. Edit stored number item       menu   - Modify stored number entry
 2. Show stored numbers                  - Display stored numbers
 3. Delete                               - Delete stored number item









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


>
```

The **STORED NUMBER SET-UP MENU** allows the display and configuration of the ISDN stored numbers for the ISDN bridge/router. The ISDN stored numbers are used to conveniently store the ISDN numbers of the partner ISDN DI-1133 bridge/routers in a single table.

The Stored Number table is used when Connection Management is enabled in order to determine the correct ISDN number to use when re-dialing a suspended ISDN call to a remote partner. All possible partner ISDN DI-1133 bridge/routers **must** be configured in the Stored Number table in order for Connection Management to operate.

Edit Stored Number Item - Option 1

Directs you to the Edit Stored Number Item Menu where the ISDN numbers of partner DI-1133 bridge/routers are maintained.

The index number or alias of the stored ISDN numbers are used in the other ISDN options: Auto-Call Number and IP Address Connect. The index number (@1 for ISDN stored number 1) or the alias may be used in these options.

A total of 40 entries are allowed in the Stored Number table.

Show Stored Numbers - Option 2

```
  Index Call You   ISDN Number1 ISDN Number2 Call Me    Alias
  ----- --------   ------------ ------------ -------    -----
    1   1303       555-2353     555-2354     1306       DENVER
    2   011441     14635                     34223      LONDON
    4   1403       245-7923     245-7933     1306       CALGARY
    5   1514       468-0234     345-3564     1306       TORONTO

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

Index: Entry number in the Stored Number table. The Index number may be used to reference this entry in the Auto-Call Number option or in the IP Address Connect table.

Call You: Dialing prefix used to make the ISDN call to the remote partner ISDN DI-1133.

ISDN Number 1: ISDN number of the remote partner ISDN DI-1133. This is the Directory Number 1 entry defined on the partner DI-1133.

ISDN Number 2: ISDN number of the remote partner ISDN DI-1133. This is the Directory Number 2 entry defined on the partner DI-1133.

Call Me: Dialing prefix used by the remote partner DI-1133 to make an ISDN call to this DI-1133. When Connection Management is enabled, this ISDN DI-1133 will pass its Directory Numbers as well as the Call Me dialing prefix to the remote partner ISDN DI-1133. This allows the remote partner ISDN DI-1133 to correctly dial this DI-1133 when the ISDN circuit needs to be resumed.

Alias: Text name used to easily reference this entry in the table. The Alias may be used to reference this entry in the Auto-Call Number option or in the IP Address Connect table.

Delete - Option 3

Deletes individual entries or all of the entries from the Stored Number table. When deleting an entry by indicating the index number, remember to use a "@" before the index number. For example: to delete index number 2 you would enter @2 when deleting the entry.

```
Enter:
   all, index or alias
>
```

Edit Stored Number Item Menu

```
                        EDIT STORED NUMBER ITEM MENU

    Option                Value          Description
 1. Call you              [        ]   - Set Call You prefix
 2. ISDN number           [        ]   - Set ISDN Number
 3. Second ISDN number    [        ]   - Set 2nd ISDN Number
 4. Call me               [        ]   - Set Call Me prefix
 5. Alias                 [        ]   - Set Alias




Enter:
    Set the index number (from 1 to 40)

>
```

The above display is the first level of the **EDIT STORED NUMBER ITEM MENU**. Once the index is entered, the index specified is added to the menu title bar and the Options are as shown below:

```
                      EDIT STORED NUMBER ITEM 1 MENU

    Option               Value      Description
 1. Call you             [none]   - Set Call You prefix
 2. ISDN number          [none]   - Set ISDN Number
 3. Second ISDN number   [none]   - Set 2nd ISDN Number
 4. Call me              [none]   - Set Call Me prefix
 5. Alias                [none]   - Set Alias









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

>
```

The "#" and "*" characters are valid for use in the Call You and Call Me dialing prefixes as well as the ISDN numbers.

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 "%" within the Call You dialing prefix or the ISDN numbers will cause the DI-1133 to send a message to the local ISDN service requesting V.110 rate adaption.

Adding a percent symbol "%" within the Call Me dialing prefix will cause the remote partner DI-1133 to initiate a rate adaption call when attempting to resume a suspended call to this ISDN DI-1133.

Call You - Option 1

Dialing prefix used to make the ISDN call to the remote partner ISDN DI-1133. 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 partner ISDN DI-1133.

Default: [none]

ISDN Number - Option 2

Defines the ISDN number called to establish a connection to the remote partner ISDN DI-1133.

When in Point-to-Point WAN mode, this ISDN Number **must** be the same as the Directory Number 1 defined on the remote partner ISDN DI-1133.

When three ISDN DI-1133s are set-up in a Multipoint WAN environment, the first remote ISDN DI-1133 should have the Directory Number 1 of the local DI-1133 as the ISDN Number in the Stored Number entry. The second remote ISDN DI-1133 should have the Directory Number 2 of the local DI-1133 as the ISDN Number in the Stored Number entry. This configuration allows each of the two remote ISDN DI-1133s to establish a connection to the local DI-1133.

Default: [none]

Second ISDN Number - Option 3

The second ISDN number is used for two different situations when in Point-to-Point WAN mode.

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. When the ISDN circuit is 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 Second ISDN Number will be used to place the second ISDN call according to the Bandwidth on Demand options defined.
2. ISDN number called when the ISDN circuit is set to unconditional and an Auto-Call or IP Address Connect call is placed. This will cause both ISDN calls to be placed to the remote DI-1133 bridge/router.

When in Point-to-Point WAN mode, this Second ISDN Number **must** be the same as the Directory Number 2 defined on the remote partner ISDN DI-1133.

Default: [none]

Call Me - Option 4

Dialing prefix used by the remote partner DI-1133 to make an ISDN call to this DI-1133. When Connection Management is enabled, this ISDN DI-1133 will pass its directory numbers as well as the Call Me dialing prefix to the remote partner ISDN DI-1133. This allows the remote partner ISDN DI-1133 to correctly dial this DI-1133 when the ISDN circuit needs to be resumed.

The Call Me dialing prefix is used to define the area codes, country codes, long distance dialing prefixes, or any other information required for the remote partner ISDN DI-1133 to establish an ISDN call to this ISDN DI-1133.

Default: [none]

Alias - Option 5

Text name used to easily reference this entry in the table. The Alias may be used to reference this entry in the Auto-Call Number option or in the IP Address Connect table.

Security Set-Up Menu

```
                          SECURITY SET-UP MENU

   Option                   Value          Description
 1. Password security       [disabled]   - Activate password security
 2. Add security entry                   - Configure a security entry
 3. Show security database               - Display security list
 4. Remove security entry                - Remove a security entry









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


>
```

The **SECURITY SET-UP MENU** allows the display and configuration of the security database which lists ISDN DI-1133 devices requiring passwords to make connections to this DI-1133.

Password Security - Option 1

This option enables or disables the requirements for security on incoming ISDN calls to this DI-1133. When password security is enabled, each remote DI-1133 that attempts to make an ISDN connection to this DI-1133 must provide the proper password before the WAN link is established. When password security is disabled, all incoming ISDN calls are allowed.

The passwords associated with remote devices are maintained within the security database.

Default: [disabled]

Considerations:

If password security is enabled on one DI-1133, it must also be enabled on each DI-1133 that may be connected via an ISDN call.

Add Security Entry - Option 2

Use this option to add a device name and password to the security database. The security database may contain up to 36 entries. The password is not displayed when it is entered, but is visible in the dump file.

```
Enter :
    Index number (from 1 to 36)

> 1


Enter :
    Device Name

> Chicago1a


Enter :
    new password (up to 8 characters)

> remote1


Enter :
    Verification of new password (up to 8 characters)

> remote1
```

Show Security Database - Option 3

```
  Index   Device Name    Password        Index   Device Name    Password
  -----   -----------    --------        -----   -----------    --------
    1      Chicago1a        *               2      DEV060605        *
    3      Chicago1b        *

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

Remove Security Entry - Option 4

Allows you to remove a selected device name and password. The device names may be removed individually by using the index number or all at once.

```
Enter :
    all, Security entry index

>
```

ISDN Interface Set-Up Menu

```
                        ISDN INTERFACE SET-UP MENU

   Option                Value          Description
 1. Directory number 1   [none]       - Set directory number
 2. SPID 1               [none]       - Set service profile identifier
 3. Directory number 2   [none]       - Set directory number 2
 4. SPID 2               [none]       - Set service profile identifier 2









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


>
```

The **ISDN INTERFACE 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.

Directory Number 1 - Option 1

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

The Directory Number 1 **must** be configured in order for Connection Management to function. The Directory Number is used by the DI-1133 during Connection Management in order to communicate to partner ISDN DI-1133 bridge/routers the ISDN number to use to re-connect a suspended call.

When adding entries to the Stored Number table on remote partner ISDN DI-1133 bridge/routers, this Directory Number 1 must be entered in the ISDN Number section in the table on the remote DI-1133.

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

SPID 1 - Option 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 bridge/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.

Directory Number 2 - Option 3

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

The Directory Number 2 **must** be configured in order for Connection Management to function. The Directory Number is used by the DI-1133 during Connection Management in order to communicate to partner ISDN DI-1133 bridge/routers the ISDN number to use to re-connect a suspended call.

When adding entries to the Stored Number table on remote partner ISDN DI-1133 bridge/routers, this Directory Number 2 must be entered in the Second ISDN Number section in the table on the remote DI-1133.

When the Directory Number is changed, a **Soft Reset** must be performed for this to take effect. The bridge/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.

SPID 2 - Option 4

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 bridge/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.

Circuit 1 (2) Set-Up Menu

```
                          CIRCUIT 1 SET-UP MENU

    Option                        Value          Description
 1. HDLC operating parameters     menu         - Define low level settings
 2. ISDN operating parameters     menu         - Define ISDN settings
 3. Activation conditions         menu         - Set activation criteria
 4. Conditional operation        [disabled]    - Use activation conditions
 5. State                        [enabled]     - Enable/disable circuit
 6. Circuit status                             - Show circuit status/statistics
 7. Manual call                                - Initiate a manual call
 8. Force disconnect                           - Disconnect a call




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


>
```

The **CIRCUIT SET-UP MENU** provides for ISDN call set-up and monitoring functions.

HDLC Operating Parameters - Option 1

Takes you to the HDLC Operating Parameters Menu for the chosen circuit. Here you set parameters such as compression, retry timers, and extended buffering that pertain to the low level settings of the ISDN circuit.

ISDN Operating Parameters - Option 2

Takes you to the ISDN Operating Parameters Menu for the chosen circuit. Here you set parameters such as redial timers, and auto-call numbers that pertain to ISDN circuit activation.

Activation Conditions - Option 3

Takes you to the Activation Conditions menu, where parameters are defined to activate the Bandwidth-On-Demand features of the ISDN bridge/router.

When operating two ISDN bridge/routers in a Point-to-Point configuration, set the activation conditions on only one of the bridge/routers.

Conditional Operation - Option 4

This option determines if the Activation Schedule or Activation Conditions will take effect for this ISDN circuit.

Default: [disabled]

State - Option 5

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

Default: [enabled]

Circuit Status - Option 6

Choosing this option displays the ISDN circuit status and statistics for the link.

Multipoint Circuit Status Display

```
Device: DEV050607              Circuit 1 Status
State   : Multipoint, Enabled, OPEN, Compressing, Unconditional
Link State   : Up

Interface State        Frame Counts (Rcv/Xmt)        Frame Errors
Speed   : 64000 bps    Bytes :     200544/177535     Invalid    : 0
Type    : BRI ST DTE   I     :       5987/8972       CRC        : 0
Circuit : Outgoing     RR    :      18898/20653      Rcv abort  : 0
State   : Active       RNR   :          0/0          Overrun    : 0
Redials left: 0        SABM  :          0/0          Rcv miss   : 0
                       DM    :          0/0          Too large  : 0
Partner Number         UA    :          0/0          Misaligned : 0
3069333300             DISC  :          0/0          Re-Xmt     : 0
                       REJ   :          0/0          Underrun   : 0
                       FRMR  :          0/0

                             Throughput
Rcv   25%   16.0KB  |************
Xmt   50%   32.0KB  |************************
                    |----|----|----|----|----|----|----|----|----|----|
                   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: Multipoint or Point_to_Point, Enabled/Disabled, OPEN/CLOSED/SUSPENDING/SUSPENDED/RESUMING, Compressing/NonCompressing, Conditional/Unconditional.

Link State :

This displays the current state of the ISDN call: Up/Down/Starting/Stopping

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 bridge/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".

Redials Left:

This identifies the number of redial attempts left to be made to the ISDN number configured for this call. This counter starts at the redial count value and counts down to zero.

Partner Number :

This identifies the ISDN number of the remotely connected DI-1133. The ISDN number is taken from the number provided by the partner DI-1133 when establishing a connection.

Frame Counts

Bytes :

This indicates the total number of bytes (including HDLC link overhead) received/transmitted across the link. The number displayed here when the link is compressing is the amount of compressed data received/transmitted across the link. To determine the amount of uncompressed (before sent across the link) data being sent, you must refer to the Link Traffic option of the WAN Statistics Menu on page 128.

These Level 2 frames are considered valid:

I	Information	**SABM**	Set Asynchronous Balance Mode
RR	Receiver Ready	**UA**	Unnumbered Acknowledgment
RNR	Receiver Not Ready	**DISC**	Disconnect
REJ	Reject	**DM**	Disconnect Mode
		FRMR	Frame Reject

These frames are considered **valid** because they are generated by one bridge/router to another to indicate an operational status of the link.

An **I** frame and statistic is sent in response to an **RR**. The **RR** indicates that the receiver is ready (**RR**) to receive **I** Information frames. This is the usual condition. When the link is inactive, periodic **RR**s are passed between bridge/routers to ensure the link is up.

RNR, REJ, SABM, UA, DISC, DM and **FRMR** statistics indicate an unusual condition that should be evaluated. (Refer to the Trace Menu on page 138 for further information.)

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 bridge/router.

Invalid This is generated when a frame is either too short or too long. This often indicates a problem with the transmitting hardware and/or communications line (a modem, noisy line, bridge/router link problem).

CRC Cyclic Redundancy Check — This often indicates a problem with the transmitting hardware and/or communications line (a modem, noisy line, bridge/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 bridge/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 bridge/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 bridge/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.

Re-Xmt Retransmit — This results when the frame transmission time-out expires (essentially, the T1 timer in the HDLC frame of reference) and a re-transmission of a frame is made.

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 bridge/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.

The throughput indicates the actual data throughput on the link. When the link is compressing, the throughput indicates the compressed data on the link. To determine the amount of uncompressed data being sent; use the Link Traffic option of the WAN Statistics Menu on page 128.

```
                                    Throughput
Rcv   25%   14.0KB  |************
Xmt   50%   28.0KB  |************************
                    |----|----|----|----|----|----|----|----|----|----|
                   0   10   20   30   40   50   60   70   80   90  100%
```

Keep in mind that the link speed relates to the clocking rate of the ISDN call. Since each link supports transmit/receive simultaneously at the ISDN call speed, the aggregate throughput at 100% link utilization would actually be double the ISDN call speed (128-Kbps for a 64-Kbps link).

Point-to-Point Circuit Status Display

```
Device: DEV050607              Circuit 1 Status
State: Point_to_Point, Enabled, OPEN, Compressing, UnConditional
Link  1 State : Up
Speed         : 64000 bps, BRI DTE


Link  2 State : Up
Speed         : 64000 bps, BRI DTE


                         Combined Throughput
Rcv   25%   16.0KB  |************
Xmt   50%   32.0KB  |************************
                    |----|----|----|----|----|----|----|----|----|----|
                   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: Multipoint or Point_to_Point, Enabled/Disabled, OPEN/CLOSED/SUSPENDING/SUSPENDED/RESUMING, Compressing/NonCompressing, Conditional/Unconditional.

Link State :

This displays the current state of the ISDN call: Up/Down/Starting/Stopping

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 bridge/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.

Combined 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.

The throughput indicates the actual data throughput on the link. When the link is compressing, the throughput indicates the compressed data on the link. To determine the amount of uncompressed data being sent; use the Link Traffic option of the WAN Statistics Menu on page 128.

```
                          Combined Throughput
Rcv   25%   14.0KB  |************
Xmt   50%   28.0KB  |************************
                    |----|----|----|----|----|----|----|----|----|----|
                   0   10   20   30   40   50   60   70   80   90  100%
```

Keep in mind that the link speed relates to the clocking rate of the ISDN call. Since each link supports transmit/receive simultaneously at the ISDN call speed, the aggregate throughput at 100% link utilization would actually be double the ISDN call speed (128-Kbps for a 64-Kbps link).

Manual Call - Option 7

This option is used to establish a manual ISDN call to another ISDN bridge/router.

The ISDN number to be called may be entered in one of three ways: enter the complete ISDN number, enter the stored number index e.g. @3, or enter the stored number alias e.g. PARIS. The manual call ISDN number must be a stored number index or alias in order for Connection Management to operate during the manual call.

The “#” and “*” characters are valid for use in an ISDN number.

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.

A forced manual call may be placed to an ISDN DI-1133 bridge/router that does not support Connection Management by placing a greater than symbol “>“ before the ISDN number.

```
Enter :
    ISDN Number (up to 20 characters)
>
```

Force Disconnect - Option 8

This option will cause the current ISDN circuit to be dropped and all ISDN calls associated with this circuit to be disconnected.

Circuit 1 (2) HDLC Operating Parameters Menu

```
                    CIRCUIT 1 HDLC OPERATING PARAMETERS MENU

   Option               Value          Description
 1. Retry timer         [5000 msec]   - Wait before frame considered lost
 2. Retry count         [3]           - Resend unacked frame [x] times
 3. Extended buffering  [disabled]    - Increase link buffering
 4. Compression         [enabled]     - Activate data compression









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


>
```

The **CIRCUIT 1 (2) HDLC OPERATING PARAMETERS MENU** allows the setting of various parameters used for the low level ISDN link configuration.

Retry Timer - Option 1

When a frame is sent, an acknowledgment is expected. If an acknowledgment is not received within the retry time-out interval, the frame is retransmitted. This continues up to the limit of the retry count (Option 2). If all the retries are unsuccessful, the ISDN call is considered down.

Default: [600 msec]

Range: 50 to 20000 milliseconds

Considerations:

For most installations, the default setting of 600 ms is adequate. However, if ISDN lines are noisy and CRC and other errors are encountered, it may be advantageous to set the value lower.

Retry Count - Option 2

When the ISDN call is coming up, or if a problem is encountered, the Retry Count specifies the number of times the bridge/router will try to bring the ISDN call up. In a case where the retry time-out is expiring, this setting—known as N2 in Recommendation X.25—specifies the number of retries before the ISDN call is declared down.

Default: [5] retries

Range: 2 to 20 retries

Extended Buffering - Option 3

By default, the DI-1133 allocates an internal buffer to be used for link transmissions. This buffer allows for buffering up to one seconds worth of data at the given link speed. Some devices will attempt to transmit more data than the DI-1133 has buffer space for, this will cause frames to be discarded internally before the link buffer is flushed out, and the remote device will retransmit the data possibly causing more discards.

Enabling this option increases the link buffers to approximately 8 times the default buffer size to help buffer the link data sufficiently and help to reduce retransmissions.

Default: [disabled]

Compression - Option 4

The Compression option enables or disables data compression on this ISDN call. This option will **not** be present if the compression module is not installed.

If either end of the link connection has Compression disabled, no compression will be done.

Default: [enabled]

Considerations:

When changing the WAN Environment from Multipoint to Point-to-Point, both links on this bridge/router will return to the default Compression state of Enabled. If the compression mode is not desired in the Point-to-Point configuration, you must change the Compression option to Disabled.

In Point-to-Point configurations, **both links** will operate in the same Compression mode, either enabled or disabled.

The bridge/routers must re-negotiate the link parameters in order to change the compression mode from enabled to disabled or disabled to enabled. **Both** ISDN calls must be disconnected and then re-established for this to take effect.

When changing from non-compression to compression on a link, the WAN statistics should be cleared. Otherwise the existing statistic numbers will make the compression ratios incorrect.

Circuit 1 (2) ISDN Operating Parameters Menu

```
                    CIRCUIT 1 ISDN OPERATING PARAMETERS MENU

    Option              Value          Description
 1. Redial timer       [10 sec]      - Time to wait until redial
 2. Redial count       [0]           - Number of redials to try
 3. Auto-call number   [none]        - Set auto-call number
 4. Auto-call enable   [disabled]    - Activate auto-call









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


>
```

The **CIRCUIT 1 (2) ISDN OPERATING PARAMETERS MENU** allows the setting of parameters used for call establishment.

Redial Timer - Option 1

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

Default: [10 sec]

Range: 4 to 255 seconds

Considerations:

In a Point-to-Point configuration, when the Address Connect feature is used in Answer/Originate mode on each bridge/router, the Redial Timer should be set differently on each bridge/router to avoid the possibility of each bridge/router trying to initiate a call to each other at the same time.

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

Redial Count - Option 2

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

Default: [0] redials

Range: 0 to 255 redials

Auto-Call Considerations:

When two ISDN numbers are defined in the Stored Number entry assigned in the Auto-Call, the DI-1133 will alternate between the two numbers when re-dialing.

When the Redial Count is set to zero (0), the DI-1133 will redial the remote partner indefinitely each time the Redial Timer expires. The DI-1133 will alternate between the two defined ISDN numbers for the partner in blocks of #1, #2 with the Redial Timer used to determine the time between #1 and #2. The time between blocks is 4 seconds.

When the DI-1133 attempts to establish an Auto-Call ISDN call and the remote partner 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 the time intervals: 4 minutes, 8 minutes, 15 minutes, 15 minutes, etc.) until the remote partner answers the call.

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.

Auto-Call Number - Option 3

The Auto-Call Number is an ISDN number that is automatically called when the bridge/router needs to use this link. When this call is set as unconditional (Conditional Operation - disabled), the bridge/router will attempt to establish an ISDN call to this number right after powering up.

The Auto-Call Number must be an entry in the Stored Number table. The entry may be referenced by index number "@12" or by alias "DENVER".

This call (link) may be activated by any of the Activation Conditions when conditional operation is enabled for this call.

Considerations:

For IPX configurations with one side of the connection having only IPX clients and the other side having both clients and servers, any defined Auto-Call number should be defined on the client side only. This allows any client initiated communications to prompt the DI-1133 to restart the ISDN call should the call be dropped for any reason.

Auto-Call Enable - Option 4

The Auto-Call Enable option is used to disable the Auto-Call feature without having to remove and then re-enter the Auto-Call Number. This may be useful when a series of manual calls are to be made and the Auto-Call function is to be temporarily disabled.

Default: [disabled]

Considerations:

When the DI-1133 is in Point-to-Point WAN mode, IP Address Connect and Auto-Call should not be enabled at the same time. Only one automatic call option should be enabled at once.

Circuit 1 (2) Activation Conditions Menu

```
                    CIRCUIT 1 ACTIVATION CONDITIONS MENU

   Option                 Value          Description
 1. Activation schedule    menu         - Timetable of call operation
 2. Traffic level         [disabled]    - Activate upon main call saturation
 3. Up threshold          [80 %]        - Set activation traffic level
 4. Up stability timer    [5 min]       - Define up level steady state time
 5. Down threshold        [60 %]        - Set deactivation traffic level
 6. Down stability timer  [10 min]      - Define down level steady state time




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


>
```

An **ISDN** bridge/router uses this Circuit Activation Conditions menu for each ISDN call.

When operating two ISDN bridge/routers in a Point-to-Point configuration, set the activation conditions on only one of the bridge/routers.

The Traffic Level option is only available when the WAN Environment is set to Point-to-Point.

When the **Traffic Level** option is enabled, the (*Up Threshold, Up Stability Timer, Down Threshold, & Down Stability Timer*) options of the traffic level feature become available.

Activation Schedule - Option 1

This option takes you to the Activation Schedule Menu for this call. The Activation Schedule determines what times of the day this call will operate.

Traffic Level - Option 2

This option enables or disables the ability to activate this ISDN call according to the traffic levels of the partner ISDN call on this bridge/router.

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

Default: [disabled]

Up Threshold - Option 3

The Up Threshold value determines the percentage of main ISDN call's capacity that will cause the secondary ISDN call to be activated. The main ISDN call 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 ISDN call to be activated.

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

Up Stability Timer - Option 4

To prevent the unnecessary activation of the secondary ISDN call if the Up Threshold is only reached for a brief period of time, the Up Stability Timer is used. It defines how long the main ISDN calls 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 main ISDN call for a period of 5 min. (length of time the secondary ISDN call is "held inactive"), then the secondary ISDN call will be activated.

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

Down Threshold - Option 5

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

After the secondary ISDN call comes on-line, it will begin to share the load that would have gone across the main ISDN call. For example, if the main ISDN call brings the secondary ISDN call 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 ISDN call will be brought down. The total throughput is a percentage of the main ISDN calls bandwidth; when the total throughput drops below the Down Threshold, the second ISDN call will be dropped.

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

Down Stability Timer - Option 6

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

For example, if the total throughput of the ISDN calls drop below 60% of the main ISDN calls bandwidth (64 Kbps) for a period of 10 minutes, the secondary ISDN call will be disconnected.

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

Circuit 1 (2) Activation Schedule Menu

```
                    CIRCUIT 1 ACTIVATION SCHEDULE MENU

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









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


>
```

ISDN Bridge/Routers will use the Activation Time Schedule to determine when each of the circuits will be active. The Activation Time Schedule is checked in conjunction with the other conditional states set for a particular ISDN call. If the Activation Time Schedule is configured to disallow circuit operation and one of the other conditional states wishes to enable the circuit , the ISDN call will not be allowed.

Activation Time Schedule - Option 1

Defines the times that this ISDN circuit will be activated or deactivated.

Set ISDN circuit 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 ISDN 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
```

Display Activation Time Schedule - Option 2

```
 Device: DEV050607       Call 1 (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.
```

Display Time - Option 3

Displays the current bridge/router time and date.

IP Address Connect Menu

```
                          IP ADDRESS CONNECT MENU

   Option                          Value          Description
 1. Edit address connect item      menu         - Modify address connect entry
 2. IP address connect            [disabled]    - Activate IP address connect
 3. Show address connect table                  - Display IP addr connect table
 4. Clear address connect table                 - Delete all addr connect items









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 based on specific destination IP addresses.

Edit Address Connect Item - Option 1

Directs you to the Edit Address Connect Item Menu where the ISDN numbers to call for specific destination IP addresses are defined. An IP address may be in the table only once.

IP Address Connect - Option 2

This option enables or disables the IP Address connect operation of the bridge/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]

Considerations:

When the DI-1133 is in Point-to-Point WAN mode, IP Address Connect and Auto-Call may not be enabled at the same time. Only one automatic call option may be enabled at once.

If the WAN topology is multipoint and IP Address Connect is enabled along with auto-call being enabled for any ISDN call, and the topology is changed to point-to-point, IP Address connect will be disabled and auto-call on each ISDN call will be disabled.

Show Address Connect Table - Option 3

Displays all of the IP addresses and their corresponding ISDN numbers (Stored Number table entries) currently in the IP Address connect table. There may be up to 40 IP network addresses defined in the table.

```
 ID  IP Address      Mask             ISDN Number
 --  ----------      ----             -------------
  1  195.145.55.0    255.255.255.0    DENVER
  2  192.169.34.0    255.255.255.0    @5
  3  192.169.3.3                      PARIS


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.
Mask:	IP address mask used against the IP address. The mask is used to allow all IP addresses of a destination IP network to apply to the Address connect function.
ISDN Number:	Stored Number table entry to be used to call a remote partner ISDN DI-1133 when IP traffic destined for the IP address is seen on the local LAN.

Clear Address Connect Table - Option 4

Clears all of the IP addresses and ISDN numbers from the IP Address Connect table.

Edit Address Connect Item Menu

```
                        EDIT ADDRESS CONNECT ITEM MENU

    Option                Value          Description
 1. Status              *[        ]   - Is the address in the table?
 2. IP address           [        ]   - Set IP address
 3. Number table entry   [        ]   - Set number table entry
 4. Address mask         [        ]   - Set mask for network address
 5. Remove                            - Delete IP address connect entry









Enter:
    Set the index number (from 1 to 40)

>
```

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

```
                      EDIT ADDRESS CONNECT ITEM 2 MENU

    Option                Value             Description
 1. Status              *"Not Present"    - Is the address in the table?
 2. IP address           [none]           - Set IP address
 3. Number table entry   [none]           - Set number table entry
 4. Address mask         [none]           - Set mask for network address
 5. Remove                                - Delete IP Address connect entry









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

>
```

Status - Option 1

Tells whether the IP address is "Present" or "Not Present" in the IP Address Connect 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]

IP Address - Option 2

Defines the IP address of the remote IP network or device. A complete IP address may be used to indicate an individual device on a remote LAN. A network IP address may be used to indicate a remote network. When a network IP address is defined, the Address Mask option **must** be configured.

Number Table Entry - Option 3

The entry in the Stored Number table to used to establish an ISDN call to a remote partner ISDN DI-1133 bridge/router. The entry may be specified by index number "@3" or by alias "ROME".

Address Mask - Option 4

IP address mask used against the IP address. The mask is used to allow all IP addresses of a destination IP network to apply to the Address connect function.

When an address mask is defined, ensure that the mask is applicable to the IP address.

Remove - Option 5

Removes the IP address and ISDN numbers from the IP Address connect table.

Connection Management Menu

```
                          CONNECTION MGMT MENU

   Option                  Value         Description
 1. Connection mgmt        [disabled]   - Perform connection management
 2. Ignore bridge traffic  [enabled]    - Traffic not used in connection mgmt
 3. Ignore IPX type20      [enabled]    - Traffic not used in connection mgmt
 4. Idle timer             [60 sec]     - Set idle time
 5. TCP keepalive          [120 min]    - Set TCP keepalive wait timer
 6. IPX watchdog interval  [59 sec]     - Time between IPX watchdog frames









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


>
```

The **CONNECTION MANAGEMENT MENU** allows the configuration of the Connection Management options for this ISDN DI-1133 bridge/router.

Refer to the **DI-1133 ISDN Connection Management** section of the Reference Manual file for more information.

Connection Management - Option 1

This option determines the state of the Connection Management system for the ISDN calls used to communicate to partner ISDN DI-1133 bridge/routers.

Connection Management is used to minimize the amount of connection time used when connected to partner DI-1133s.

When Connection Management is enabled, the active ISDN calls are monitored for “Interesting Traffic” and suspended and resumed when required to transfer user data between DI-1133s.

Default: [disabled]

Considerations:

Connection Management must be enabled on the DI-1133s on both ends of the ISDN call in order to operate properly.

Two types of Wide Area Network (WAN) topologies are supported with Connection Management

1. Two DI-1133 Bridge/Routers connected.
2. Three DI-1133 Bridge/Routers connected in a star configuration.

Connection Management is not functional when DI-1133 Bridge/Routers are connected in a ring.

Ignore Bridge Traffic - Option 2

This option enables or disables the bridge frame forwarding functions of the ISDN bridge while Connection Management is enabled.

When the ISDN bridge is ignoring bridge traffic, the bridge traffic received from the LAN will not be used to resume a suspended ISDN call or to keep an existing ISDN call up.

Default: [enabled]

Ignore IPX Type20 - Option 3

While this option and Connection Management are enabled, this IPX router will ignore IPX type 20 packets and not re-transmit them to partner routers on the WAN.

When the ISDN bridge is ignoring IPX type 20 packets, the type 20 packets received from the LAN will not be used to resume a suspended ISDN call or to keep an existing ISDN call up.

Default: [enabled]

Idle Timer - Option 4

This option defines the Connection Management Idle Timer that is used to determine when an ISDN call will be suspended.

When the Idle Timer is set to 0, this DI-1133 will not suspend the ISDN call. This may be used to allow only one of the DI-1133s to suspend the ISDN call.

Default: [60 sec]

Range: 0, 20 to 3600 seconds

TCP Keepalive - Option 5

Defines the time period between successive TCP keepalive frames generated by this ISDN DI-1133 when Connection Management is enabled.

Default: [120 min]

Range: 1 - 240 minutes

IPX Watchdog Interval - Option 6

Defines the time period between successive IPX watchdog frames generated by this ISDN DI-1133 when Connection Management is enabled.

Default: [59 sec]

Range: 1 - 623 seconds

Bridging Set-Up Menu

```
                          BRIDGING SET-UP MENU

   Option                  Value          Description
 1. Spanning tree          menu         - Configure STP communications
 2. Bridge forwarding     [enabled]     - Enable/disable LAN frame 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.

Spanning Tree - Option 1

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

Bridge Forwarding - Option 2

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

Default: [enabled]

Considerations:

STP operation will not be affected when bridge forwarding is disabled. STP should be disabled when this bridge should not participate with other STP devices on the LAN.

Bridge Aging Timer - Option 3

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.

Show Bridging Table - Option 4

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-c2-00-00-00           *         *  Internal
00-00-d0-00-20-21           *            Internal
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

In the above table, two addresses are shown as Permanent with a Location of Internal. The first of these (01-80-c2-00-00-00) is the STP Multicast address that is common to all bridges using the Spanning Tree Protocol. This STP address appears only when the STP is enabled. The next Internal address is the MAC addresses of the LAN port. These two Internal addresses cannot be removed nor altered.

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.

Show Permanent Table - Option 5

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









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

Clear Bridging Table - Option 6

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. Device priority    [32]        - Define device selection priority
 4. Bridge priority    [32768]     - Define root bridge selection priority
 5. Forwarding delay   [15 sec]    - Set delay before forwarding begins
 6. Message age timer  [20 sec]    - Receive hello message interval
 7. Hello time         [2 sec]     - Set hello message transmission interval
 8. Show bridge                    - View bridge STP status
 9. Topology status                - View network 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.

LAN Port - Option 1

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 4
> Forwarding delay — Option 5
> 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.

STP State - Option 2

Toggles between the [enabled] / [disabled] states of the Spanning Tree Protocol for the bridge.

Considerations:

The 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 Connection Management is enabled, the STP state will be changed to disabled.

Device Priority - Option 3

Specifies the devices priority for becoming the control bridge within the WAN connected devices. The bridge with the lowest device priority is selected to be the control bridge. When two WAN connected devices have the same device priority, the device with the lowest MAC address shall become the control bridge.

The control bridge is used to administer STP among the WAN connected devices.

Default: [32]

Range: 17 to 32

Considerations:

The devices should be configured so that the device at the most central location within the WAN topology becomes the control bridge.

Bridge Priority - Option 4

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. (Refer to Option 4, Show Port, in the LAN PORT MENU for a description of the *designated bridge*).

Forwarding Delay - Option 5

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

Message Age Timer - Option 6

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**

Hello Time - Option 7

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**

Show Bridge - Option 8

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.)

Topology Status - Option 9

Displays the status of this bridge's LAN ports, identifies the Designated Bridge and its designated LAN Ports, and flags any changes in the topology.

```
Port Status Summary

                          Designated  Designated  Topology
                          Bridge            Port              Change
Name        State   Id    Pri   Cost  Address     Pri   Id    Pri   Cost  Acked
LANXXXXXX  Forward  1     128   100   self        self              0
LANXXXXXX


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

Name

The **Name** column shows either the default LAN name (e.g. LANxxxxxx) or the name assigned through Menu naming options.

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.

Port Priorities

The Port Priorities are in decimal format (default 128).

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 as shown in the 0x80NN display in the LAN PORT MENU, Option 4, Show Port, display.

Priority

This is the priority of the Designated Port.

Cost

If this is the Root Port, the priority is 0.

Topology Changed Acked

If the topology is stable this value is 0.
If the topology is changing this value is 1.

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
 4. Show port                - View port STP status









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


>
```

The **LAN PORT MENU** allows the management of the port's state, path cost, and priority. The display of the STP port status for the port is available through this Menu.

State - Option 1

Toggles between Enabling and Disabling of the Spanning Tree Protocol for the port.

Considerations:

When the port is [enabled] the states are reported as either Listen(ing), Learn(ing), Forward(ing) or Block(ing) in the Show Port, Option 4, display. If the port is disconnected, "Disabled" is shown in the Show Port, Option 4, 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.

Path Cost - Option 2

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.

Priority - Option 3

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) hex (80) - Refer to "Show Port"

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.

Show Port - Option 4

Displays the STP status of the port. The screen below shows a bridge that is not the Root:

```
Port Status

Bridge ID    :     32768-0000d0006005
Port ID :     0x8001
Port state   :     Forward
Path cost    :     100
Designated Root    :     32768-0000d000e034
Designated bridge  :     32768-0000d0006005
Designated port    :     0x8002
Designated cost    :     100
Topology change acknowledged   :     0



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

In the above display, the parameters not discussed previously are the relationships between Designated bridge, Designated port, and Designated cost.

Designated bridge

This indicates the bridge in the forwarding state, perhaps winning an STP redundant bridge case (but not necessarily in that situation), receiving protocol messages for/from the Root bridge coming from/to the LAN *X* indicated in the Port Status display. If the designated bridge's MAC address (here shown as 32768-0000d0006005) matches the MAC address for this bridge, then this bridge is the Designated bridge for LAN *X*.

Designated port

The Designated port is attached to the Designated bridge for the LAN. It is the port attached to the LAN which receives messages for/from the Root bridge coming from/to the attached LAN.

Designated cost

This value indicates the total path cost to reach the LAN that the Root bridge is attached to. For the Root bridge's Designated port, the cost is 0. The cost increases as each additional LAN is crossed according to the path cost of each Designated bridge's Designated port. Note that a Root port does not have a Designated cost. When displaying the Port Status of a Root port attached to a LAN, the Designated port (and the designated cost) for this LAN is found on another bridge.

Internet Set-Up Menu

```
                          INTERNET SET-UP MENU

   Option                  Value          Description
 1. ARP set-up              menu         - Configure ARP operation
 2. IP address             [none]        - Define internet address
 3. Nonstandard subnets    [disabled]    - Allow subnet zero
 4. Subnet size            [none]        - Define subnet field size
 5. Network mask          *"none"        - Subnet mask used
 6. Default gateway        [none]        - Define default gateway
 7. BSD type broadcast     [disabled]    - Use '0' as broadcast bit
 8. Time to live           [32]          - Router hops allowed
 9. Help                                 - Description of IP applications




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


>
```

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

ARP Set-Up - Option 1

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

IP Address - Option 2

Allows the definition of an Internet Protocol (IP) address for the bridge/router. An IP address is required by the bridge/router in order to become an IP Router.

The DI-1133 Ethernet bridge/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 bridge/routers across the LAN by using Telnet (for example, from a remote bridge/router to a local bridge).

If "none" is given (the default value), the bridge/router's IP Routing function and SNMP agent are disabled, and the bridge/router cannot be reached from another bridge/router or an NMS. (Directly linked remote partners can still control each other.)

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.

IP Routing must be disabled before the IP Address may be modified.

Default: [none]

Nonstandard Subnets - Option 3

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: [disabled]

Subnet Size - Option 3

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 bridge/router is connected to. The subnet mask is defined as a series of contiguous bit locations immediately following the network portion of the IP address.

In the following example, three bits of the host portion of the address will be used for the subnet portion. The value of the subnet size will be 3 in this case.

Example: Network portion of address ⇨ ⇦ Host portion of address

NNNNNNNN.NNNNNNNN.HHHHHHHH.HHHHHHHH

| ⇔ | This portion of the Host address will be used for the subnetting.

The subnet size must be at least 2 bits long. The size of the subnet may only be in the ranges shown here:

Class A networks - 2 to 22
Class B networks - 2 to 14
Class C networks - 2 to 6.

The position of the subnet mask will vary depending on the network class being used. For example: a class A network with an 8-bit mask will have a mask of 255.255.0.0, while a class B network with an 8-bit mask will have a mask of 255.255.255.0.

Class A network 8-bit mask: 255.255.000.000
|-8-|

Class B network 8-bit mask: 255.255.255.000
|-8-|

Class C network 3-bit mask: 255.255.255.224
|-3-|

Default: [none]

```
Enter :
    none, size of subnet mask (from 2 to 22)
>
```

Network Mask - Option 5

Displays the subnet mask that the DI-1133 is currently using. The subnet mask is calculated automatically from the IP address assigned to the DI-1133 and from the subnet size defined. This value is a display only value and may not be modified.

Default Gateway - Option 6

Allows the identification of a local default gateway (i.e. *router*). The "Default gateway" must reside on the same network, and subnet (if used), as defined by the IP address for the bridge/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 bridge/router that points to the best route gateway. In this manner, the bridge/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]

BSD Type Broadcast - Option 7

Determines whether all zeros or ones will be used as the broadcast address for internally generated broadcasts. IP specifies that all ones are used, while BSD 4.2 UNIX uses all zeros. With the option disabled, the broadcast address will be all ones.

Default: [disabled]

Considerations:

All interconnected subnets should use the same representation in order to understand a broadcast packet that is being routed.

Time To Live - Option 8

Sets the maximum number of router hops that an IP packet generated by the bridge/router is allowed before being discarded.

IP packets that are being routed through the DI-1133 Ethernet bridge/router will have their time-to-live value decremented by two.

Default: [32]

Range: 1 - 255

Help - Option 9

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.

ARP Aging Timer - Option 1

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)

ARP Retry Timer - Option 2

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

Default: [2 sec]

Range: 1 - 20 seconds

Show ARP Table - Option 3

Displays all of the devices that have responded to ARP requests from this bridge/router and the devices that this bridge/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         164.44.25.53          00-00-d0-00-28-24  dynamic
 Link 1         164.44.25.86          00-00-d0-00-29-24  dynamic
 Link 1         164.44.25.24          00-00-d0-00-30-24  dynamic
 Link 2         164.44.25.76          00-00-d0-00-23-25  dynamic
 Link 2         164.44.25.111         00-00-d0-00-23-26  dynamic
 Link 2         164.44.25.54          00-00-d0-00-23-27  dynamic
 Link 2         164.44.25.244         00-00-d0-00-23-28  dynamic

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

Interface:	Interface on which the ARP mapping applies. When this bridge/router is configured as an IP router, all entries will be from the LAN interface only because the rest of the entries are in the routing tables (on partner routers).
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).

IP Routing Set-Up Menu

```
                          IP ROUTING SET-UP MENU

    Option                      Value          Description
 1. IP routes                   menu         - Modify/view routes
 2. Routing protocol           *[rip]        - Active 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
 6. Source quench generation    [enabled]    - ICMP source quench
 7. Help                                     - Description of IP routing




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 bridge/router. Options 4 through 6 are only available when Option 3, IP Routing, is enabled.

IP Routes - Option 1

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

Routing Protocol - Option 2

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 DI-1133 routers connected on the WAN do not need to have their IP routing protocols set to the same values. An DI-1133 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 DI-1133s at the remote sites would have their routing protocol set to none.

Default: [rip]

Choices: rip, none

Considerations:

The routing protocol may not be changed unless IP routing has been disabled.

IP Routing - Option 3

Enables or disables the IP routing functions of the bridge/router. With IP routing disabled, all IP traffic will be bridged.

Options 4 through 6 are available only when this option is enabled.

Default: [disabled]

Considerations:

An IP address must be defined for the bridge/router before IP routing will be allowed.

If one or more bridge/routers connected to the same WAN have IP Routing disabled, IP Routing will only take place between the bridge/routers that have IP Routing enabled. All bridge/routers in that WAN network with IP Routing disabled will become bridges only.

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

IP Forwarding - Option 4

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]

ARP Proxy - Option 5

The DI-1133 Ethernet bridge/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]

Source Quench Generation - Option 6

Enables or disables the generation of Source Quench messages. Source Quench messages will be sent out for the first discarded frame from the station and approximately every fifth discarded frame after that, provided that the discarded frame is the first portion of a fragmented frame and not an ICMP frame.

Default: [enabled]

Help - Option 7

Offers a brief description of the IP routing options.

IP Routes Menu

```
                              IP ROUTES MENU

   Option                Value          Description
 1. Show all routes                   - Display the route table
 2. Show static routes                - Display only static routes
 3. Edit route           menu         - Modify a route in the table
 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.

Show All Routes - Option 1

Displays all of the routes currently in use by the bridge/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
198.169.3.0       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.
Subnet 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.

Show Static Routes - Option 2

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

```
                              Static IP Routes
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
198.169.3.0       0      255.255.255.0       198.169.1.23       1     0  LOCAL
 ----End of table
```

Edit Route - Option 3

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

Clear Static Routes - Option 4

Clears all of the static routes from the routing table.

Edit Route Menu

```
                              EDIT ROUTE MENU

    Option          Value          Description
 1. Subnet size   *[        ]   - The subnet field size for this route
 2. Subnet mask   *[        ]   - The network mask for the route
 3. Status        *[        ]   - Is the address in the table
 4. Next hop       [        ]   - IP address of the next hop
 5. Cost           [        ]   - Cost to reach destination in hops
 6. Metric         [        ]   - Actual cost to reach destination
 7. Type          *[        ]   - Type of route
 8. Remove                      - Remove address from table



Enter:
    destination IP address (up to 15 characters)

> 192.3.44.0
```

The above display is the first level of the **EDIT ROUTE MENU**.

NOTE: The ability to define the IP routing protocol is currently only available on ISDN versions of the DI-1133.

Options 1 & 2 are only valid when the IP routing protocol has been set to none. When the routing protocol is set to none, the subnet size to use to mask the destination IP network address is specifiable along with the destination IP network address.

When defining static routes with the routing protocol set to RIP, the network IP address must be specified. Once the network IP address is entered, the address specified is added to the menu title bar and the Options are as shown below:

When defining static routes with the routing protocol set to none, the network IP address and the subnet size must be specified. Once the network IP address is entered, the address specified is added to the menu title bar and the Options are as shown below:

```
                          EDIT ROUTE 192.3.44.0 MENU

    Option          Value                Description
 1. Subnet size    *[0]                - The subnet field size for this route
 2. Subnet mask    *"255.255.255.0"    - The network mask for the route
 3. Status        *"Not Present"       - Is the address in the table
 4. Next hop       ""                  - IP address of the next hop
 5. Cost           [1]                 - Cost to reach destination in hops
 6. Metric        *[16]                - Actual cost to reach destination
 7. Type          *""                  - Type of route
 8. Remove                             - Remove address from table



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

>
```

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

Subnet Size - Option 1

When the IP routing protocol is set to none, the subnet size must be specified when defining the static route entry. The subnet size value entered will be displayed here.

A value of 0 indicates that there is no subnet mask associated with this route.

Subnet Mask - Option 2

When the IP routing protocol is set to none, 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.

Status - Option 3

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]

Next Hop - Option 4

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.

Cost - Option 5

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

Default: [1]

Range: 1 - 15

Metric - Option 6

Displays the current cost to actually reach this network. This display only option will either show the operator-entered cost value, or 16 if the next hop gateway cannot be reached at this time.

Type - Option 7

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 bridge/router.

Remove - Option 8

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. Show interconnect                 - Display the linked networks
 2. Network numbers      menu         - Define networks for frame types
 3. IPX routing         [enabled]     - Enable/disable IPX router
 4. IPX forwarding      [enabled]     - Enable/disable IPX routing
 5. Show routes                       - Display the route table
 6. Show services                     - Display the service table
 7. 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 bridge/router.

Show Interconnect - Option 1

Displays the IPX networks for each frame type on the LANs of each of the partner bridge/routers.

```
Interconnected IPX Networks
Device Name     MAC address      Routing    Frame      Network
                                 Enabled    Type       Number
-------------------------------------------------------------
 BRG008a72   00-00-d0-00-8a-72     Yes    Ethernet-II  00000000
                                         raw 802.3    08023311
                                         802.2        08022311
                                         802.2-SNAP   00000000

 BRG008a32   00-00-d0-00-8a-32     Yes    Ethernet-II  00000000
                                         raw 802.3    00802312
                                         802.2        08022312
                                         802.2-SNAP   00000000

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

Network Numbers - Option 2

Directs you to the Network Numbers Menu, where network numbers may be assigned for the four frame types supported by this bridge/router.

IPX Routing - Option 3

Enables or disables the IPX routing functions of the bridge/router. With IPX routing disabled, all IPX traffic will be bridged.

Default: [enabled]

Considerations:

Routing will take place only if all partner bridge/routers (connected to the same WAN) have IPX Routing enabled. If one or more bridge/routers have IPX Routing disabled, all bridge/routers in that WAN network will become bridges only.

Routing information packets will only be transmitted across the WAN to partner bridge/routers when the links are first brought up and when there is a change in the routing information.

When IPX Routing is disabled, all learned RIP routes will be cleared from the routing table. All IPX traffic will be bridged. This may cause problems within the network, because the IPX Networks that were previously isolated will now be directly connected together. The Servers on each network will see different network numbers on the same LAN. Remember that a bridged network creates one logical LAN.

IPX Forwarding - Option 4

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: [disabled]

Considerations:

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

Show Routes - Option 5

Displays all of the routes currently in use by the bridge/router.

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

```
IPX Routes
Total entries : 7
 Destination    Next Hop
 IPX Network   IPX Address          Hops    Ticks
-----------------------------------------------------
Start of Table
 08023311          local              0         1
 00000311      0000c023655b           1         2
 08022311          local              0         1
 00802312      0000d0008a32           1         2
 08022312      0000d0008a32           1         2
 00000312      0000d0008a32           2         3
 00000401      0000d0008a32           2         3
End of Table


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

Destination IPX Network:	IPX Network Address of the remote network.
Next Hop IPX Address:	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 bridge/router has a tick value of 5.

Show Services - Option 6

Displays all of the Servers currently seen by the bridge/router. The Services table is created from information received by this bridge/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
        Network     Node   Socket
-------------------------------------------------
Start of Table
 0004  00000311 0000ff3a4001 0451   2  SQA_SERVER_311
 0004  00000312 00004ac38445 0451   6  NOVELL312
 0004  00000401 000e03448a32 0451   2  NOVELL_401
End of Table


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

Type:	Novell Server types. 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 bridge/router.
Server Name:	Name of the Server.

Help - Option 7

Offers a brief description of the IPX routing options.

Network Numbers Menu

```
                          NETWORK NUMBERS 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 **NETWORK NUMBERS MENU** allows the display and configuration of the IPX network numbers on this bridge/router for each IPX frame type on the local LAN.

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

Displays the IPX network number currently in use on this bridge/router's LAN for this IPX frame type. A value of "0" indicates that a frame of this type has not been received from the LAN; the bridge/router will learn the network number associated with this frame type upon receiving the first IPX frame of this frame type.

Network numbers may be pre-defined by the operator only when IPX Routing is disabled.

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.

Help - Option 5

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 SNMP community       menu          - Modify SNMP community
 2. SNMP message size        [1472 bytes]   - Define maximum message size
 3. Show SNMP communities                   - View SNMP communities
 4. Remove SNMP 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 bridge/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.

Edit SNMP Community - Option 1

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

SNMP Message Size - Option 2

Allows the setting of the maximum message size sent by the bridge/router's SNMP agent.

Default: [1472 bytes]

Range: 484 to 1472 bytes

Considerations:

The message size sent by the bridge/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.

Show SNMP Communities - Option 3

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.
```

Remove SNMP Community - Option 4

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 SNMP Community Menu

```
                          EDIT SNMP 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 SNMP 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:

>
```

Write Access - Option 1

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 bridge/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).

Show Addresses - Option 2

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
```

Add NMS Address - Option 3

Up to five NMS addresses may be added to the NMS address list. If the address list is empty, the bridge/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 bridge/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).

Add Trap Address - Option 4

Allows the addition of up to five trap addresses to the trap address list. When a trap is generated by the bridge/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.

Remove NMS Address - Option 5

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.)

Remove Trap Address - Option 6

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.)

Help - Option 7

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 filter    menu        - Define IP pattern filters
 4. IPX router pattern filter   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.

MAC Address Filters - Option 1

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

Bridge Pattern Filters - Option 2

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

IP Router Pattern Filter - Option 3

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

IPX Router Pattern Filter - Option 4

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 bridge/router.

Edit MAC Address Filter - Option 1

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

Filter Operation - Option 2

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.

Broadcast Address - Option 3

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]

Show Bridging Table - Option 4

Displays all addresses in the Bridge Filter Table, identifies the active/inactive and permanent/non-permanent addresses, identifies addresses to be filtered or forwarded 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-c2-00-00-00           *         *  Internal
00-00-d0-00-20-21           *            Internal
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
Type: [s] to redraw, [=] main menu, any other key to end.
```

Address

In the above table, two addresses are shown as Permanent with a Location of Internal. The first of these (01-80-c2-00-00-00) is the STP Multicast address that is common to all bridges using the Spanning Tree Protocol. This STP address appears only when the STP is enabled. The next Internal address is the MAC addresses of the LAN port. These two Internal addresses cannot be removed nor altered.

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/router is connected to.

The second-last address (12-34-56-78-99-99) is an active, permanent address on LAN050607 (in this example, this is the LAN the bridge/router is attached to). Frames to and from this address will not cross the bridge/router as 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/router, as 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/router manager or is one of the three internal addresses of the bridge/router. Permanent addresses are not subject to the aging timer, but will be reported as active if they are encountered.

Filter (or Forward) if Src

This indicates that a bridge/router manager has specified that this address be filtered (or forwarded) if it is found as a source address.

Filter (or Forward) if Dest

This indicates that a bridge/router manager has specified that this address be filtered (or forwarded) if it is found as a destination address.

Filter (or Forward) if Src / Dest

This indicates that a bridge/router manager has specified that this address be filtered (or forwarded) if it is found either as a source or as a destination address. (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.

Show Permanent Table - Option 5

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
```

Clear Bridging Table - Option 6

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)


>
```

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









>
```

Status - Option 1

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]

Location - Option 2

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]

Filter *(Forward)* If Source - Option 3

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.

Filter *(Forward)* If Destination - Option 4

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.

Permanent - Option 5

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.

Remove - Option 6

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.

Bridge pattern filters are checked against all bridge data from the local LAN only.

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.

Show Alias - Option 1

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.
```

Add Alias - Option 2

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
```

Remove Alias - Option 3

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).

Show Pattern - Option 4

Displays the filter masks that have been defined with the Add Pattern option:

```
Bridge Filter Patterns
Id    Pattern
--    ---------------------------
1     12-600x
2     0-010203040506&12-809B
```

Considerations:

When operating in a Multipoint environment with 3 or more bridge/routers connected in the WAN network, the Show Pattern option appears differently. It will prompt for "global," "Destination LAN name," or "all."

```
Enter:
  global, Destination LAN name, all
>
```

global

```
Bridge Filter Patterns
Id    Pattern
--    ---------------------------
1     12-600x
3     LAT
```

MARKETING - (Destination LAN name)

```
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
```

Add Pattern - Option 5

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:
  filter pattern (up to 80 characters)
> 12-600x


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

Considerations:

When operating in a Multipoint environment with 3 or more bridge/routers connected in the WAN network, the Define Pattern option appears differently. It will prompt for "global" or "Destination LAN name."

```
Enter:
  global, Destination LAN name or MAC address
>

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 data being sent to other bridge/routers on the same Wide Area Network.

A **Destination LAN name** filter pattern will be applied to all data being sent to the specified LAN name only. The Destination LAN name must be a valid LAN name on the Wide Area Network. LAN names may be displayed by issuing the Show Names command in the Remote Access menu or LAN Statistics menu.

A **MAC Address** filter pattern will be applied to all data being sent to the specified MAC address only. The MAC Address is used to define a remote partner bridge/router that is not currently connected on the Wide Area Network.

Remove Pattern - Option 6

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
```

Considerations:

When operating in a Multipoint environment with 3 or more bridge/routers connected in the WAN network, the Remove Pattern option appears differently. It will prompt for "global," "Destination LAN name," or "all."

```
Enter:
  global, Destination LAN name
>

Enter:
  all, pattern ID number
>
```

Entering **global** will allow the removal of all or specific filter patterns defined as global filter patterns.

Entering **Destination LAN name** will allow the removal of all or specific filter patterns defined for a specific LAN name.

Help - Option 7

Provides three Help screens describing the creation of Filter Masks. The third screen displays some sample Filter Masks.

To move between the three 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.

IP Router pattern filters are checked against all IP data from the local LAN only.

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.

Show Alias - Option 1

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.
```

Add Alias - Option 2

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:

```
IP Router Filter Patterns

ID    Pattern
--    ----------------------------
1     12-600x
2     0-010203040506&12-809B
...
5     bmCast
```

Remove Alias - Option 3

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).

Show Pattern - Option 4

Displays the filter masks that have been defined with the Add Pattern option:

```
IP Router Filter Patterns
Id    Pattern
--    ---------------------------
1     12-600x
2     0-010203040506&12-809B
```

Considerations:

When operating in a Multipoint environment with 3 or more bridge/routers connected in the WAN network, the Show Pattern option appears differently. It will prompt for "global," "Destination LAN name," or "all."

```
Enter:
  global, Destination LAN name, all
>
```

global

```
IP Router Filter Patterns
Id    Pattern
--    ---------------------------
1     12-600x
3     LAT
```

MARKETING (Destination LAN name)

```
IP Router Filter Patterns to MARKETING
Id    Pattern
--    ---------------------------
2     0-010203040506&12-809B
```

all

```
Summary of all IP Router filter patterns
Type      Id    Pattern
--------  --    ---------------------------
Global     1     12-600x
           3     LAT
MARKETING  2     0-010203040506&12-809B
```

Add Pattern - Option 5

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:
  filter pattern (up to 80 characters)
> 12-600x

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

Considerations:

When operating in a Multipoint environment with 3 or more bridge/routers connected in the WAN network, the Define Pattern option appears differently. It will prompt for "global" or "Destination LAN name."

```
Enter:
  global, Destination LAN name
>

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 data being sent to other bridge/routers on the same Wide Area Network.

A **Destination LAN name** filter pattern will be applied to all data being sent to the specified LAN name only. The Destination LAN name must be a valid LAN name on the Wide Area Network. LAN names may be displayed by issuing the Show Names command in the Remote Access menu or LAN Statistics menu.

Remove Pattern - Option 6

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
```

Considerations:

When operating in a Multipoint environment with 3 or more bridge/routers connected in the WAN network, the Remove Pattern option appears differently. It will prompt for "global," "Destination LAN name," or "all."

```
Enter:
  global, Destination LAN name
>

Enter:
  all, pattern ID number
>
```

Entering **global** will allow the removal of all or specific filter patterns defined as global filter patterns.

Entering **Destination LAN name** will allow the removal of all or specific filter patterns defined for a specific LAN name.

Help - Option 7

Provides three Help screens describing the creation of Filter Masks. The third screen displays some sample Filter Masks.

To move between the three 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.

IPX Router pattern filters are checked against all IPX data from the local LAN and the WAN.

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.

Show Alias - Option 1

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

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

Add Alias - Option 2

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:

```
IPX Router Filter Patterns
ID    Pattern
--    ----------------------------
1     12-600x
2     0-010203040506&12-809B
...
5     bmCast
```

Remove Alias - Option 3

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).

Show Pattern - Option 4

Displays the filter masks that have been defined with the Add Pattern option:

```
IPX Router Filter Patterns at LAN050607
Id    Pattern
--    ---------------------------
1     9-600x
2     12-809B
```

Add Pattern - Option 5

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:
  filter pattern (up to 80 characters)
> 9-600x

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

Remove Pattern - Option 6

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
```

Help - Option 7

Provides three Help screens describing the creation of Filter Masks. The third screen displays some sample Filter Masks.

To move between the three 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 bridge/router statistics.

Statistics Set-Up - Option 1

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.

LAN Statistics - Option 2

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

WAN Statistics - Option 3

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


>
```

Extended Statistics - Option 1

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
- **Channels "all"**, WAN Statistics Menu
- **Link Traffic "all"**, WAN Statistics Menu

When extended stats are [disabled], limited information is available from:
- **Link Status**, Link 1 (2) Setup Menu & WAN Statistics Menu (only Link State, Routing to Bridge/Routers, and Interface State are 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 bridge/router performance as additional processing is required. You must confirm a change by entering "yes" at the prompt.

Interval - Option 2

Sets the timer that updates the statistics.

Default: [60 sec]

Range: 10 to 3,600 seconds.

Considerations:

Lowering the time interval will require more bridge/router processing power while increasing the time interval will require less.

Clear All Statistics - Option 3

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. Show names             - Display known remote devices
 8. Clear LAN statistics   - Reset LAN statistics
 9. Clear LAN errors       - Reset LAN errors




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


>
```

Bridged Traffic - Option 1

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

IP Traffic - Option 2

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

IPX Traffic - Option 3

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

Total LAN Traffic - Option 4

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

LAN Error - Option 5

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

Frame Size - Option 6

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.

Show Names - Option 7

This option displays the default names or those specified by the bridge/router manager, and addresses of each Device and its associated LAN.

Clear LAN Statistics - Option 8

Clears all statistic fields in the LAN statistics to zero.

Clear LAN Errors - Option 9

Clears all error fields in the LAN statistics to zero.

(For screen displays of Options 1-6 refer to the pages following this one).

Bridged Traffic Summary Screen 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.

```
                    LAN Tokyo 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             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
```

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 by the Bridge/Router Manager or a re-powering of the bridge/router occurred.

Bridged 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	All frames received from the local LAN and filtered by the bridge/router. This includes frames filtered because the bridge/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.
Frames Forwarded	All frames successfully received from the local LAN and forwarded to partner bridge/routers.
Bytes Forwarded	All bytes successfully received from the local LAN and forwarded to partner bridge/routers.
Frames To LAN	All frames successfully received from partner bridge/routers and placed upon the local LAN.
Bytes To LAN	All bytes successfully received from partner bridge/routers and placed upon the local LAN.

IP Traffic Summary Display (Option 2):

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

LAN Tokyo Routed Traffic Summary

Statistic	Total	Average Rate	Recent Rate	Highest Rate
Frames from LAN	4348699	228	416	840
Bytes from LAN	278317248	14616	26667	53785
Frames Filtered	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
Source Quench Sent	92	2	1	4
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 by the Bridge/Router Manager or a re-powering of the bridge/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	All IP frames received from the local LAN and filtered by the bridge/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 bridge/routers.
Bytes Forwarded	All IP bytes successfully received from the local LAN and forwarded to partner bridge/routers.
Frames To LAN	All IP frames successfully received from partner bridge/router's and placed upon the local LAN.
Bytes To LAN	All IP bytes successfully received from partner bridge/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 bridge/router, but there is no entry in the ARP table for that IP address, and the station does not respond to an ARP request.
Source Quench Sent	The number of ICMP Source Quench messages generated.
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 bridge/router. A properly routed frame will be MAC addressed to the bridge/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               132982            6           0         840

Congestion discards from LAN       0            0           0           0
Frames Forwarded           269806208        14171       26667       28236
Bytes Forwarded              4169752          219         416         441

Frames from WAN            268464916        14024       26667       28250
Bytes from WAN               4169752          219         416         441
Congestion discards from WAN      92            2           1           4

Frames to LAN                    269           14          27          28
Bytes to LAN                     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 by the Bridge/Router Manager 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	All IPX frames received from the local LAN and filtered by the bridge/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 Forwarded	All IPX frames successfully received from the local LAN and forwarded to partner bridge/routers.
Bytes Forwarded	All IPX bytes successfully received from the local LAN and forwarded to partner bridge/routers.
Frames from WAN	All IPX frames successfully received from partner bridge/routers and sent to the IPX module.
Bytes from WAN	All IPX bytes successfully received from partner bridge/routers and sent to the IPX module.
Congestion Discards from WAN	IPX data frames discarded because of internal congestion between the WAN 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.

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

Statistic	Total	Average Rate	Recent Rate	Highest Rate
Frames from LAN	4348699	228	416	840
Bytes from LAN	278317248	14616	26667	53785
Frames Filtered	132982	6	0	840
Adapter Discards	0	0	0	0
Frames Forwarded	4215689	221	416	441
Bytes Forwarded	269806208	14171	26667	28236
WAN Congestion Discards	0	0	0	0
Frames to LAN	4169752	219	416	441
Bytes to LAN	268464916	14024	26667	28250
LAN Congestion Discards	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 by the Bridge/Router Manager or a re-powering of the bridge/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	All frames received from the local LAN and filtered by the bridge/router. This includes frames filtered because the bridge/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 bridge/router, primarily because the bridge/router is engaged in other functions such as filtering.
Frames Forwarded	All frames successfully received from the local LAN and forwarded to partner bridge/routers.
Bytes Forwarded	All bytes successfully received from the local LAN and forwarded to partner bridge/routers.
WAN Congestion Discards	This occurs when the bridge/router has to discard frames destined for partner bridge/routers because too many frames are waiting for processing inside the bridge/router and buffer space is unavailable.
Frames To LAN	All frames successfully received from partner bridge/routers and placed upon the local LAN.
Bytes To LAN	All bytes successfully received from partner bridge/routers and placed upon the local LAN.
LAN Congestion Discards	This occurs when the bridge/router has to discard frames from a partner bridge/router destined for the local LAN because too many frames are waiting for processing inside the bridge/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
Transmit Babble Errors   : 0            Framing Errors            : 0
Underflow Errors         : 0            Single Collision          : 0
Overflow Errors          : 0            Multiple Collisions       : 0
Receive Buffer Congest   : 0            Transmit Retry Failures   : 0
Receiver Misses          : 0            Late Collisions           : 0
Transmit Buffer Errors   : 0            Oversized frames received : 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 Bridge/Router or in the transceiver.
Transmit Babble Errors	The bridge/router transmitted a frame larger than 1518 bytes on the LAN. This error is displayed only when the Filter Large option in the Diagnostic menu is enabled.
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 bridge/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 bridge/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 bridge/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.
Oversize Frames Received	The bridge/router received a frame larger than 1518 bytes from the LAN. This error is displayed only when the Filter Large option in the Diagnostic menu is enabled.
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 bridge/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 bridge/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 bridge/router to the other LAN;
The fourth, frames received from the other LAN.

Show Names Display (Option 7)

If the Bridge/Routers and LANs have not been named, the default names use a prefix of DEV or LAN and end with the MAC address.

The first in the list is the bridge/router attached to. Added to the end of the address of the others is the Link through which the first is able to reach the indicated bridge/router/LAN.

```
Device Name LAN Name   MAC Address       IP Address      Notes
----------- ---------- ----------------- --------------- -----------------
Tokyo       LAN006005  00-00-d0-00-60-05  92.1.0.1       current device
Kyoto       LAN006045  00-00-d0-00-60-45  92.2.0.2       on link 1
Yokohama    LAN00a047  00-00-d0-00-a0-47  92.3.0.3       on link 2
Taipei      LAN00903d  00-00-d0-00-90-3d  92.4.0.4       on link 3
Amsterdam   LAN00a007  00-00-d0-00-a0-07  92.5.0.5       on link 4
London      LAN00a067  00-00-d0-00-a0-67  92.6.0.6       on link 5
New York    LAN00905d  00-00-d0-00-90-5d  92.7.0.7       on link 6


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

WAN Statistics Menu

```
                          WAN STATISTICS MENU

   Option                  Value    Description
 1. Connection time stats  menu   - Accounting
 2. Circuit status                - View status of circuit
 3. Circuit traffic               - View WAN traffic history
 4. Channels                      - View inter-LAN traffic history
 5. Clear WAN statistics          - Reset WAN statistics




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


>
```

Connection Time Stats - Option 1

Takes you to the Connection Time Statistics Menu, where ISDN connection time statistics can be examined.

Circuit Status - Option 2

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

The same display is available from the Circuit 1 (2) Set-Up Menu.

Circuit Traffic - Option 3

Displays a summary of WAN traffic statistics. The statistics are available either individually (more statistics) or together (provides overview).

Considerations:

The "all" selection of this option is available only if Extended Stats in the Statistics Set-Up Menu is Enabled.

Channels - Option 4

The Channels option appears only on a bridge/router that has seen two different bridge/routers on its links when in multipoint mode. Its purpose is to provide an overview of statistics on a LAN-to-LAN basis.

Considerations:

The "all" selection of this option is available only if Extended Stats in the Statistics Set-Up Menu is Enabled.

Clear WAN Statistics - Option 5

Clears all fields in the WAN statistics to zero.

Circuit Status Display (Option 2)

```
Enter:
  Circuit number (1 or 2), all
```

The screen below shows a **multipoint** application, where each circuit goes to a different remote bridge/router.

all (multipoint)

```
 Device: DEV050607          Circuit 1 Status
Link State   : Multipoint, Enabled, Up, Compressing, UnConditional
Speed        : 64000 bps, External clock, BRI ST DTE
Routing cost : 156 (Default: 156, Assigned: auto)

                            Throughput
Rcv  25%      14.0 KB |************
Xmt  50%      28.0 KB |************************
                      |----|----|----|----|----|----|----|----|----|----|
                      0   10   20   30   40   50   60   70   80   90  100%

                            Circuit 2 Status
Link State   : Multipoint, Enabled, Up, Compressing, Conditional
Speed        : 64000 bps, External clock, BRI ST DTE
Routing cost : 156 (Default: 156, Assigned: auto)

                            Throughput
Rcv  32%      17.9KB  |***************
Xmt  40%      22.4KB  |******************
                      |----|----|----|----|----|----|----|----|----|----|
                      0   10   20   30   40   50   60   70   80   90  100%

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

The screen below shows a **point-to-point** application, where each link goes to the same remote bridge/router.

Point-to-Point Circuit Status Display

```
Device: DEV050607              Circuit 1 Status
State: Point_to_Point, Enabled, OPEN, Compressing, UnConditional
Link  1 State : Up
Speed         : 64000 bps, BRI DTE


Link  2 State : Up
Speed         : 64000 bps, BRI DTE


                         Combined Throughput
Rcv   25%   16.0KB  |************
Xmt   50%   32.0KB  |************************
                    |----|----|----|----|----|----|----|----|----|----|
                    0   10   20   30   40   50   60   70   80   90  100%

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

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

Circuit 1 Status

```
Device: DEV050607              Circuit 1 Status
State   : Multipoint, Enabled, OPEN, Compressing, Unconditional
Link State   : Up

Interface State         Frame Counts (Rcv/Xmt)         Frame Errors
Speed   : 64000 bps     Bytes :     200544/177535      Invalid    : 0
Type    : BRI DTE       I     :       5987/8972        CRC        : 0
Circuit : Outgoing      RR    :      18898/20653       Rcv abort  : 0
State   : Active        RNR   :          0/0           Overrun    : 0
Redials left: 0         SABM  :          0/0           Rcv miss   : 0
                        DM    :          0/0           Too large  : 0
Partner Number          UA    :          0/0           Misaligned : 0
3069333300              DISC  :          0/0           Re-Xmt     : 0
                        REJ   :          0/0           Underrun   : 0
                        FRMR  :          0/0

                                Throughput
Rcv   25%   16.0KB  |************
Xmt   50%   32.0KB  |************************
                    |----|----|----|----|----|----|----|----|----|----|
                   0   10   20   30   40   50   60   70   80   90  100%

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

Circuit Traffic Display (Option 3)

```
Enter:
  Circuit number (1 or 2), all
```

Individual Circuit display

```
Device: DEV050607            Circuit 1 Traffic Summary

                                          Average      Recent     Highest
Statistic                        Total       Rate        Rate       Rate
-------------------------------------------------------------------------
Frames to link                 2184436         66         400        409
Bytes to link                139803904       4264       25600      26208
Link Congested Discards            0          0           0          0

Frames from link               3036941         92         200        412
Bytes from link              194437913       5933       12385      24406
Lost frames                        0          0           0          0

Compressed bytes to link      46408933       1416        7953       9056
Compressed bytes from link    63289895       1931        3822       9214
Compression ratio on link          n/a     3.1: 1      3.2: 1     11.8: 1




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

all

```
Device: DEV050607             WAN Traffic Summary

Path    Frames Rcv  Rate  Bytes Rcv   Rate Frames Xmt  Rate  Bytes Xmt   Rate
------  ---------- ----- ---------- ------ ---------- ----- ---------- ------
Link 1     3036941   200  194437913  12385    2184436   400  139803904  25600
Link 2           0     0          0      0          0     0          0      0


                          Compression Traffic Summary

Path       Ratio Rcv   Rate  Bytes Rcv  Rate  Ratio Xmt   Rate Bytes Xmt  Rate
------    ---------- ------ ---------- ------ ---------- ------ ---------- ------
Link 1      3.1: 1  3.2: 1   63289895  3822      3.0: 1  3.2: 1  46408933  7953
Link 2        -: -    -: -          0     0        -: -    -: -         0     0



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

The Rates are the average number of occurrences in the last statistics interval.

NOTE: Compression statistics will be calculated when compression is enabled on a link. When a link has a compression module installed but compression disabled, the compression ratios will be displayed as "-: -." When a link does not have a compression module installed, the compression statistics are not displayed.

NOTE: In a dual-link loadshare configuration, using the display "all" will display all of the statistics on link 1, even if link 1 is down and traffic is passing across link 2. This occurs because the bridge/router considers the WAN as one link when in loadshare mode.

Link Traffic Summary Statistics Definitions	
Frames To Link	All frames successfully transmitted to the link.
Bytes To Link	All bytes successfully transmitted to the link.
Link Congested Discards	This occurs when the bridge/router has to discard frames destined for a partner bridge/router because too many frames are waiting for processing inside the bridge/router and buffer space is unavailable.
Frames From Link	All frames successfully received from the link.
Bytes From Link	All bytes successfully received from the link.
Lost Frames	This occurs when the bridge/router has to discard frames destined for the local LAN from the partner bridge/router because too many frames are waiting for processing inside the bridge/router and buffer space is unavailable.
Compressed Bytes To Link	All compressed bytes successfully transmitted on the link to the partner bridge/router.
Compressed Bytes From Link	All compressed bytes successfully received on the link from the partner bridge/router.
Compression Ratio On Link	The ratio of the bytes sent to the link board to the actual compressed bytes sent out on the link. The compression ratio displayed in the individual link display is the total of the transmit and receive ratio. The individual ratios are shown in the all traffic display.

NOTE: When changing from non-compression to compression on a link, the WAN statistics should be cleared. Otherwise the compression ratios will be incorrect because of the existing statistic numbers.

Channels Display (Option 4):

```
Enter:
  Destination LAN name, all
```

All

```
LAN to LAN STATISTICS

Src Dest   Frame-Fwd Rate  Byte-Fwd Rate  Frame-Rcv Rate  Byte-Rcv Rate
-------------------------------------------------------------------------
LAN00a017
  LAN00a037    65334  112   4200636 7168      47937   55   3150045 3520
  LAN00a077    23515  234   5230636 1476    4793713  152   2233505 9728




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

This screen displays a breakdown of the data being transferred between LANs in the bridge/router network. The numbers shown in each row indicate the data from the Src LAN to the Dest LAN and the data from the Dest LAN to the Src LAN.

The Frame-Fwd / Rate columns	indicate the number of frames sent from the Src LAN to the Dest LAN.
The Byte-Fwd / Rate columns	indicate the number of bytes sent from the Src LAN to the Dest LAN.
The Frame-Rcv / Rate columns	indicate the number of frames sent from the Dest LAN to the Src LAN.
The Byte-Rcv / Rate columns	indicate the number of bytes sent from the Dest LAN to the Src LAN.

Destination LAN Name

```
LAN "LAN050608" to "LAN05060b" STATISTICS

                                        Average      Recent     Highest
Statistic                      Total       Rate        Rate        Rate
-------------------------------------------------------------------------
Frames Forwarded                   9          0           0           0
Bytes Forwarded                  456          1           0           0
Frames Filtered                    0          0           0           0
Congestion Forward Discards        0          0           0           0

Frames from remote device          9          0           0           0
Bytes from remote device         456          1           0           0
Congestion Receive Discards        0          0           0           0


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

This screen displays a breakdown of the data being transferred between the local LAN and the specified remote LAN in the bridge/router network.

Channels Traffic Summary Statistics Definitions	
Frames Forwarded	All frames successfully sent to the other bridge/router.
Bytes Forwarded	All bytes successfully sent to the other bridge/router.
Frames Filtered	All frames destined for the other LAN but filtered by the bridge/router. This includes bridged frames filtered because the bridge/router is in Learn mode, the source address is specified for filtering, the frame meets pattern filtering criteria.
Congestion Forward Discards	All frames destined for the other LAN but discarded because of congestion of the link to that bridge/router.
Frames from Remote Device	All frames successfully received from the other bridge/router.
Bytes from Remote Device	All bytes successfully received from the other bridge/router.
Congestion Forward Discards	All frames from the other bridge/router discarded because of congestion of the local LAN transmitter.

Connection Time Stats Menu

```
                          CONNECTION TIME STATS MENU

    Option              Value          Description
 1. Connection time   *[0]           - Total in seconds
 2. Connections       *[0]           - Count of connections
 3. Clear counts









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


>
```

The **CONNECTION TIME STATS MENU** is available **only** on ISDN DI-1133 bridge/routers and is used to monitor the number and time of the ISDN calls made by this device.

Connection Time - Option 1

The total connection time for the ISDN DI-1133 is shown. The time is indicated in seconds.

Connections - Option 2

The total number of ISDN connections made from this ISDN DI-1133 is shown. Each time one of the ISDN B-channels establishes a connection this count is incremented.

Clear Counts - Option 3

Clears ALL of the Connection Time statistics to zero.

Diagnostics Menu

```
                              DIAGNOSTICS MENU

    Option              Value          Description
 1. Trace               menu         - View link frames
 2. Filter large       [disabled]    - Filter frames larger than 1518 bytes
 3. Heartbeat          [enabled]     - Report transceiver heartbeat failures
 4. Soft reset                       - Reset device (retain configuration)
 5. Full reset                       - Reset device (use factory defaults)









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


>
```

Trace - Option 1

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

Filter Large - Option 2

If you enable this option, frames larger than 1518 bytes will be filtered. This option applies only to bridged frames.

These oversize packet sizes are in violation of the Ethernet maximum frame size, but, they are, in some applications, sent during file transfers from diskless workstations, and SUN\SPARC type machines.

Heartbeat - Option 3

Enables/Disables reporting of transceiver heartbeat failures. This failure is not a bridge/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 bridge/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 bridge/router performance, since additional processing must be done by the bridge/router to report these errors. (Disable for Version 1 Ethernet.)

Soft Reset - Option 4

Selecting this option resets the bridge/router software and restarts the bridge/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.

Full Reset - Option 5

Selecting this option resets the bridge/router configuration to factory default settings and restarts the bridge/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 bridge/router; therefore, the tracing functions should only be [enabled] when needed.

Trace Link 1(2) - Option 1 & 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.

Real Time - Option 3

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).

Capture - Option 4

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

Allocate - Option 5

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.

End - Option 6

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].

Data display - Option 7

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
>
```

Time - Option 8

[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.

Show - Option 9

* Appears once the buffers are allocated *

This option displays the frames captured by the Trace and stored in the capture buffer. (BOB = Beginning of Buffer; EOB = End of Buffer.) The trace shown below is with the data display in the "off" mode.

BOB	**This Bridge/Router**	**Partner Bridge/Router**
rRR 0		expects 0
xI 4,0 122	expects 4, sends 0	gets 0
rRR 1		expects 1
rI 1,4 68	gets 4	still expecting 1, sends 4
xRR 5	expects 5	
rI 1,5 68	gets 5	still expecting 1, sends 5
xI 5,1 122	still expecting 5, sends 1	gets 1
xRR 6	expects 6	
rRR 2		expects 2
xI 6,2 236	still expecting 6, sends 2	gets 2
rRR 3		expects 3
rI 3,6 68	gets 6	still expecting 3, sends 6
xRR 7	expects 7	
rI 3,7 68	gets 7	still expecting 3, sends 7
xI 7,3 144	still expecting 7, sends 3	gets 3
xRR 0	expects 0	
rRR 4		expects 4
xI 0,4 122	still expecting 0, sends 4	gets 4
rRR 5		expects 5
rI 5,0 68	gets 0	still expecting 5, sends 0
xRR 1	expects 1	
rI 5,1 68	gets 1	still expecting 5, sends 1
xI 1,5 122	still expecting 1, sends 5	gets 5
xRR 2	expects 2	
rRR 6		expects 6
xI 2,6 258	still expecting 2, sends 6	gets 6
rRR 7		expects 7
rI 7,2 68	gets 2	still expecting 7, sends 2
xRR 3	expects 3	
rI 7,3 68	gets 3	still expecting 7, sends 3
xI 3,7 68	still expecting 3, sends 7	gets 7
xRR 4	expects 4	
rRR 0		expects 0
EOB		

Format:

Receive frames (r) are indented.
Transmit frames (x) are not.

Valid frames are as follows:

I	-	Information
RR	-	Receiver Ready
RNR	-	Receiver Not Ready
REJ	-	Reject
SABM	-	Set Asynchronous Balance Mode
DM	-	Disconnect Mode
DISC	-	Disconnect
UA	-	Unnumbered Acknowledgment
FRMR	-	Frame Reject

Information (I) Frame traces will be displayed with the following:

Link (L1/L2) (x/r)I N(r), N(s) Data Field Length Data Field (hex)

As much of the Data Field as will fit on one line will be displayed if hex or ASCII format is specified. If **off** is specified, only the Data Field Length is given.

Supervisory (S) frame traces will be displayed with the following:

Link (L1/L2) (x/r)(RR / RNR / REJ) N(r)

Unnumbered (U) frame traces will be displayed with the following:

Link (0/1) (x/r) (SABM / DM / DISC / UA / FRMR)

Any illegal or unknown frame will be completely dumped in hex. Note that any frame with a CRC error will not be displayed and a Level 2 error will be output.

LAPB *control field* formats:

Three types of Link Access Procedures (Balanced) **LAPB** control field formats are used to perform:

1) numbered information transfer (**I** format),
2) numbered supervisory functions (**S** format) and
3) unnumbered control functions (**U** format).

The numbered **I** format is used to perform information transfer.

The numbered **S** format is used to perform data link supervisory control functions such as:
- acknowledge **I** frames,
- request transmission of **I** frames, and
- to request a temporary suspension of **I** frames.

The unnumbered **U** format is used to provide additional data link control functions.

INFORMATION FRAMES:

I Information

The (**I**) statistic indicates a transfer of a sequentially numbered frame containing an (**I**) information field.

To allow the sending of an **I**nformation frame a Receive Ready (**RR**) supervisory frame is sent by the remote bridge/router requesting the connection.

SUPERVISORY FRAMES:

RR — Receiver Ready

A Receive Ready (**RR**) supervisory frame is sent by the bridge/router in order to:

1) indicate that it is ready to receive an **I** frame;
2) acknowledge previously received **I** frames numbered up to and including N(R) - 1.

An **RR** frame may be used to indicate the clearance of a busy condition reported by the earlier transmission of an **RNR** frame by that same bridge/router.

RNR — Receiver Not Ready

The **RNR** statistic is generated by either remote bridge/router to indicate a busy condition. A busy condition essentially indicates a temporary inability to accept incoming **I** frames. **I** frames numbered up to and including N(R) - 1 are acknowledged.

I frame N(R) and any subsequent **I** frames received, are not acknowledged; the acceptance state of these unacknowledged frames will be indicated in subsequent exchanges.

REJ — REJect

The **REJ** supervisory frame is generated when a remote bridge/router requests transmission of **I** frames starting with the frame numbered N(R). **I** frames numbered N(R) - 1 and below are acknowledged. Additional **I** frames (pending initial transmission) may be transmitted following the retransmitted **I** frame(s).

Only one **REJ** exception condition for a given transfer direction may be established at any time. This **REJ** exception condition is reset (cleared) upon the receipt of an **I** frame with an N(S) equal to the N(R) of the **REJ** frame. An **REJ** frame may be used to indicate the clearance of a busy condition that was reported by the earlier transmission of an **RNR** frame by that same bridge/router.

UNNUMBERED FRAMES:

SABM — Set Asynchronous Balanced Mode

The **SABM** unnumbered command is generated to place the addressed bridge/router into an asynchronous balanced mode information-transfer phase, where all command/response control fields will be one octet in length.

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

The receiving bridge/router confirms acceptance of the **SABM** by the transmission, at the first opportunity, of a **UA** response.

Previously transmitted **I** frames that are unacknowledged when a **SABM** command is generated remain unacknowledged. It is the responsibility of a higher level (e.g. TCP, XNS, LAT) to recover from the loss of the contents (packets) of such **I** frames.

DISC — DISConnect

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

Before the **DISC** is acted upon, the bridge/router receiving the **DISC** confirms its acceptance of the **DISC** command by the transmission of a **UA** response. The bridge/router sending the **DISC** enters the disconnected phase when it receives the acknowledged **UA** response.

Previously transmitted **I** frames that are unacknowledged when **DISC** is generated remain unacknowledged. It is the responsibility of a higher-level protocol (e.g. TCP, XNS, LAT) to recover from the possible loss of the contents (packets) of such **I** frames.

UA — **U**nnumbered **A**cknowledgment

A **UA** response and statistic is generated to acknowledge the receipt and acceptance of the mode-setting commands. Received mode-setting commands are not acted upon until the **UA** response is transmitted. The transmission of a **UA** response indicates the clearance of a busy condition that was reported by the earlier transmission of an **RNR** frame by that same bridge/router.

DM — **D**isconnected **M**ode

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

1) The **DM** may be sent to indicate that the bridge/router has entered the disconnected phase without having received a **DISC** command.

2) If sent in response to the reception of a mode-setting command, the **DM** is sent to inform the other bridge/router(s) that this bridge/router is still in the disconnected phase and cannot execute the Set Mode command.

A bridge/router in the **DM** phase will monitor received commands and will react to a **SABM** command. It will send a **DM** response with the F bit set to 1 in response to another command received with the P bit set to 1.

FRMR — **FR**a**M**e **R**eject

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

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

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

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

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

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

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

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

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.

Acknowledge Alarm - Option 1

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

Show Events - Option 2

Displays the 42 most recent ALARMs since the bridge/router was last powered up or Cleared with Option 3.

```
#1   94/12/22 13: 39: 04   IPX routing is enabled
#2   94/12/22 13: 39: 05   STP disabled
#3   94/12/22 13: 39: 05   SNMP is running
#4   94/12/22 13: 39: 06 * IP Routing is enabled
#5   94/12/22 13: 39: 07   Configuration restored
#6   94/12/22 13: 39: 08   Running in OPERATIONAL mode
#7   94/12/22 13: 39: 09 * LAN connection established
#8   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.

Clear Events - Option 3

Removes all ALARMs from the table.

Show Security Log - Option 4

Displays the 36 most recent ISDN security logs since the bridge/router was last powered up or Cleared with Option 5.

A security log is only produced on the called DI-1133 when the security checking has failed on an incoming ISDN call.

```
#1   92/01/11 09: 30: 21     DEV00b433   ascer    9999995797
#2   92/01/11 09: 31: 02     DEV00b433    NONE    9999995797
#3   92/01/11 09: 31: 40   No Device or Password received. CLID 9999995797
time is 92/01/11 09: 40: 48, 3 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.

Clear Security Log - Option 5

Removes all ISDN security logs from the table.