Copyright Statement

Trademarks

D-Link is a registered trademark of D-Link Corporation/D-Link Systems, Inc.

All other trademarks belong to their respective owners.

Limited Warranty

This guide and the accompanying product are each provided “as is,” without warranty as to their performance, merchantability or fitness for any particular purpose. D-Link Corporation and D-Link Systems, Inc. reserve the right to revise this publication and to make changes to its contents at any time, without obligation to notify any person or entity of such revisions or changes.

Table of Contents

Introduction

Congratulations on your purchase of a D-Link DI-106 series remote access router with integrated Ethernet hub. No larger than an ordinary modem, your router offers inexpensive yet complete telecommunications and internetworking solutions for your home or branch office. It is ideal for everything from Internet browsing to receiving calls from Remote Dial-in Users and making LAN-to-LAN connections to Remote Nodes.

Distinguishing features of the DI-106 series include support for a full range of networking protocols such as TCP/IP (Transmission Control Protocol/Internet Protocol, also known as IP), Novell IPX (Internet Packet Exchange), and Transparent Bridging.

- DI-106: ISDN S/T interface, IP routing
- DI-106W: ISDN U interface, IP routing
- DI-106M: ISDN S/T interface, IP/IPX routing, bridging
- DI-106MW: ISDN U interface, IP/IPX routing, bridging

This complete solution also includes remote dial-in user support, an Internet single-user account (Network Address Translation) option, extensive network management capabilities, and solid security features.

NOTE: ***Throughout the remainder of this manual, the term "DI-106" refers to any DI-106 or DI-106W, and the term "DI-106M" refers to any DI-106M or DI-106MW.***

Features

Each DI-106 series router is packed with features that give it the flexibility to provide a complete networking solution for almost any user.

Ease of Installation

Your DI-106 or DI-106M is a self-contained unit that is quick and easy to install. Physically, it resembles an external modem; however, it is a combination ISDN router and 10BASE-T Ethernet hub, and it uses twisted-pair Ethernet cables to connect to the host network.

Built-in Hub

As a 10BASE-T Ethernet hub, your DI-106 or DI-106M provides six ports for connection of standard 10-Mbps Ethernet devices. Five ports are designed for connection of network end nodes—single-user computers, servers, bridges, other routers, etc.—through standard "straight-through" twisted-pair cables; the sixth is wired for making an "uplink" connection to another hub through the same kind of cable for network expansion.

ISDN Basic Rate Interface (BRI)

Using a standard S/T or U Interface (the DI-106 and DI-106M use the S/T interface, while the DI-106W and DI-106MW use the U interface) the DI-106 and DI-106M support a full range of switch types. The switch type depends on the CO (Central Office) switch your ISDN line is connected to. See the *ISDN Switch Types* chapter for more information on North American, European, and Asian ISDN firmware and switch types supported by these routers.

The two B-channels can be used independently for two destinations. Or they can be bundled for one connection to support bandwidth-on-demand.

ISDN Leased Line

If the router is set up for an ISDN leased line (that is, if any option but Switch/Switch or Switch/Unused is selected for the B Channel Usage control in setup menu 2, ISDN Setup, and the Transfer Type control is set to Leased in either setup menu 4, Internet Access Setup, or setup menu 11.1, Remote Node Profile), the router will automatically initialize the leased-line connection each time it is powered up or the settings in setup menu 2, 4, or 11.1 are saved.

The DI-106 and DI-106M implement the PPP echo mechanism for verifying ISDN leased line status. The setting of the Idle Timeout control in setup menu 11.1 will be used as the interval between two LCP_Echo_Req messages. It is supposed that there exists an echo reply corresponding to an echo request. Whenever an echo request is sent, the counter will be incremented by one.

The send counter will be reset to zero after an echo response is received. The leased-line error recovery mechanism will be

triggered after the send counter reaches 4. If the Idle Timeout control is set to zero, the PPP echo mechanism will not be used.

Multiple Networking Protocol Support

The DI-106M is a multi-protocol router. It supports TCP/IP, Novell IPX, and Transparent Bridging.

Standard Phone Jacks

The router is equipped with two standard phone jacks for connecting telephones, fax machines, or modems. This allows the ISDN line to be used for voice calls as well as data calls.

Dial On Demand

The Dial On Demand feature allows a DI-106 or DI-106M to automatically place a call to a Remote Node whenever there is traffic coming from any workstation on the LAN (Local Area Network) to that remote site.

Bandwidth On Demand

Your DI-106 or DI-106M supports bandwidth up to 128 kbps (kilobits—that is, thousands of bits—per second) over a single ISDN BRI line. It incorporates PPP/MP (Point-to-Point Protocol/ Multilink Protocol) to bundle two B channels over a BRI line. In addition, the router dynamically allocates bandwidth between the two B channels, increasing or decreasing bandwidth as needed to allow for greater efficiency in data transfer. It supports BAP (Bandwidth Allocation Protocol) and BACP (Bandwidth Allocation

Control Protocol) to manage the number of links in multilink bundle.

Full Network Management

The DI-106M incorporates SNMP (Simple Network Management Protocol) support and menu-driven network management via an RS-232 or Telnet connection. In addition, both the DI-106 and the DI-106M offer the Call Detail Record (CDR) function to help you analyze and manage your telephone bill.

RADIUS (Remote Authentication Dial In User Service)

The RADIUS feature allows you to use a central external Unix-based server to support thousands of users (DI-106M only).

PPP Security

The DI-106 and DI-106M support PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol).

MS (Microsoft) CHAP

Your DI-106 or DI-106M and a Microsoft Windows 95 or Windows NT server can authenticate each other using Microsoft's proprietary CHAP algorithm. No special setup is needed to support MS CHAP. Everything is done through PPP negotiation between the router and the server.

RIP-1/RIP-2

Your DI-106 or DI-106M supports both RIP-1 and RIP-2 (Routing Information Protocol versions 1 and 2) exchanges with other routers. RIP version controls in setup menus 3.2 (TCP/IP and DHCP Ethernet Setup) and 11.3 (Remote Node Network Layer Options) let you control RIP use, and offer the following version options: RIP-1 (accept and send RIP-1 messages only), RIP-2B (accept RIP-1 and RIP-2 messages, both broadcast and multicast, and send RIP-2 messages in broadcast format), and RIP-2M (accept RIP-1 and RIP-2 messages, both broadcast and multicast, and send RIP-2 messages in multicast format).

(The suggested choice in both menus is RIP-2B, except in environments where there are routers that do not understand RIP-2 packets at all. *Broadcast*, above, means a destination MAC or IP host address consisting of all binary ones; *multicast* means a MAC address of 01:00:5E:00:00:09 hex or an IP destination address of 224.0.0.9.)

DHCP Support (Dynamic Host Configuration Protocol)

DHCP (Dynamic Host Configuration Protocol) allows you to dynamically and automatically assign IP address settings to hosts on your network.

Call Control

Your DI-106 or DI-106M provides budget management for outgoing calls and maintains a “blacklist” of unreachable phone numbers in order to save you the expense of unnecessary charges.

Data Compression

The DI-106 and DI-106M incorporate Stac data compression and CCP (Compression Control Protocol).

Networking Compatibility

The DI-106 and DI-106M are compatible with remote access products from other companies such as Ascend, Cisco, and 3Com. Furthermore, they support Microsoft Windows 95 and Windows NT remote access capability.

Applications For Your DI-106 or DI-106M

Some applications for the DI-106 and DI-106M include:

Internet Access

Your DI-106 or DI-106M supports the TCP/IP protocol, which is the language used for the Internet. It is also compatible with access servers manufactured by major vendors such as Cisco and Ascend.

Internet Single User Account (SUA)

For small office environments, the DI-106 and DI-106M offer a Single User Internet Account (also known as a Network Address Translator, or NAT) from an ISP (Internet Service Provider). This allows multiple users on the LAN to access the Internet concurrently for the cost of a single user.

Single User Account address mapping can also be used for LAN to LAN connections.

Multiprotocol LAN-to-LAN Connection

The DI-106 and DI-106M can dial to or answer calls from another remote access router connected to a different network. The DI-106M supports TCP/IP and Novell IPX, and has the capability to bridge any Ethernet protocol.

Telecommuting Server

The DI-106 and DI-106M allow Remote Dial-in Users to dial in and gain access to your LAN. This feature enables users that have workstations with remote access capabilities, e.g., Windows 95, to dial in using an ISDN terminal adapter (TA) to access the network resources without physically being in the office.

What This Manual Covers

This manual is divided into five parts.

1. Part One, **Getting Started**, is structured as a step-by-step guide to help you connect, install, and set up your DI-106 or DI-106M to operate on your LAN.
2. Part Two, **The Internet**, describes how to configure the router to connect to the Internet.
3. Part Three, **Setting Up Advanced Applications**, describes how to use the router for more advanced applications, such as TCP/IP routing and Bridging.
4. Part Four, **Advanced Management**, provides information on advanced management features for network managers.

5. Part Five, **System Maintenance**, describes maintenance features for checking system status and logging errors.

Regardless of the application, it is important that you follow the steps outlined in Part One to correctly connect your DI-106 or DI-106M to your LAN. You can then refer to other chapters of the manual depending on which applications you wish to use.

What This Manual Doesn't Cover

This manual assumes that you know how to use your computer and are familiar with your communications software. If you have questions about using either one, refer to the manual for the product.

Other Resources

For more information about your DI-106 or DI-106M check the following sources:

- Quick Start Guide.
- Support disk.

Packing List

Before you proceed further, check all items you received with your DI-106 or DI-106M against this list to make sure nothing is missing. The complete package should include:

- One DI-106 or DI-106M ISDN router.
- One power adapter.

- One RS-232 cable.
- One "straight-through" twisted-pair Ethernet cable.
- One Support Disk.
- This *User's Guide*.

Additional Installation Requirements

In addition to the contents of your package, there are other hardware and software requirements you need before you can install and use your router. These requirements include:

- An ISDN telephone line.
- Ethernet connection(s) to your computer(s).
- A computer equipped with an RS-232 port and communications software configured to the following parameters:
  - VT100 terminal emulation.
  - 9600 baud.
  - No parity, 8 data bits, 1 stop bit.

After the router has been successfully connected to your network, you can make future changes to the configuration using a Telnet client application.

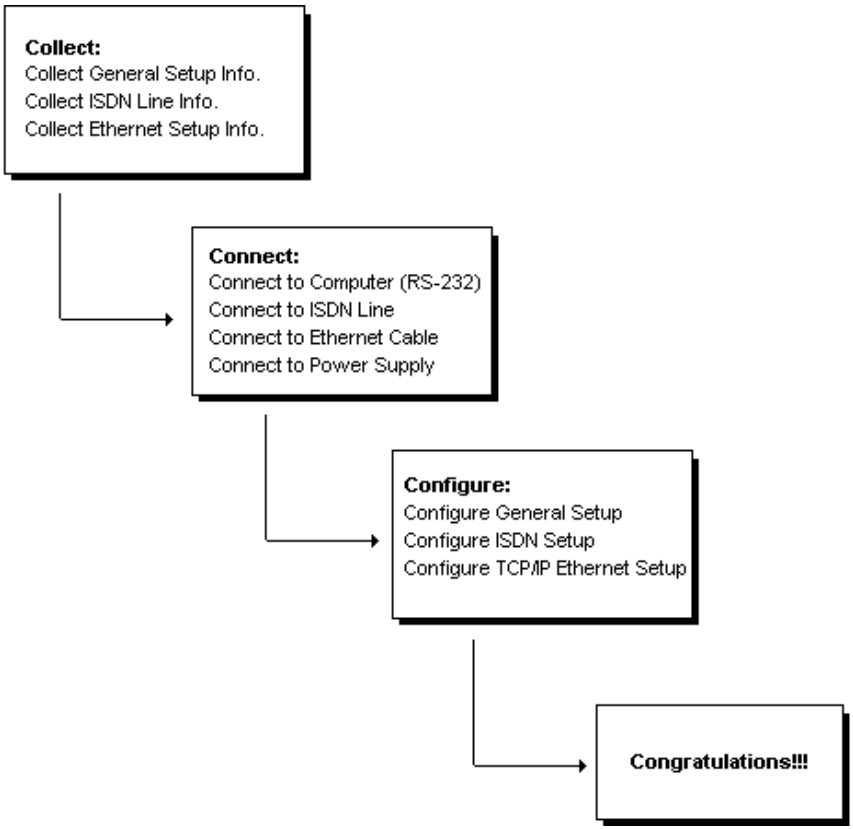
Before You Begin

To ensure successful installation of your DI-106 or DI-106M, we strongly recommend that you carefully follow the steps outlined in the next two chapters. These chapters are designed as a guide for you to collect the necessary information about your ISDN phone line and the LAN which you will be connected to. Once this information has been collected, it will be used to configure your router.

After you have successfully configured your DI-106 or DI-106M, see the appropriate chapters to set up your applications. For Internet Access, see the *Configuring for Internet Access* chapter starting on page 47.

Road Map and Flow

The chart below is provided as a step by step guide to successfully installing your DI-106 or DI-106M.



Completing the Worksheet

Before you continue, locate the worksheet at the end of this chapter. This information worksheet has been provided to help you get through setup and installation of your DI-106 or DI-106M as easily as possible.

Ordering Your ISDN Line

If you do not have the ISDN line installed already, we suggest that you order it from your telephone company as soon as possible to avoid the long waiting period common when ordering a new line. Use the information in this section to place the order (see the *ISDN Switch Types* chapter for information on provisioning your ISDN line). If you have already installed your ISDN line, you can check the following section to make sure that you can use all the features of your DI-106 or DI-106M.

1. Contact your local telephone company's ISDN Ordering Center.
2. Find out what type of ISDN service is available. Refer to the *ISDN Switch Types* chapter to find out the provisioning information for the appropriate switch type and ISDN service. For the U.S., the DI-106W and DI-106MW (U Interface) have been approved by Bellcore and have IOC (ISDN Ordering Code) "S" Capability, EZ-ISDN 1.
3. Provide your telephone company with the proper provisioning information.
4. When the telephone company installs your ISDN line, be sure to obtain the following information:
   - ◊ ISDN switch type.
   - ◊ ISDN telephone number(s).
   - ◊ ISDN Service Profile Identifier (SPID) number(s) (only for North America).

Collecting General Setup Information

Your DI-106 or DI-106M requires the following system information. You can obtain all the pertinent information from your network administrator. Record this information into the worksheet as it becomes available. This worksheet will later be referred to as you configure your router.

- **System Name**—This is the name given to the router for identification purposes. This name should be no more than 8 alphanumeric characters. Spaces are not allowed, but "-" and "_" are accepted. This name can be obtained remotely via the SNMP management protocol and will be displayed as the prompt when the user enters Command Interpreter Mode.
- **Route IP Field**—For Internet access, you will need to enable the Route IP Field. See the *Configuring for Internet Access* chapter starting on page 47 for more details on configuring your router for Internet access. To support Novell IPX, or Bridging, enable the appropriate protocol and reference the related chapters for detailed information.

You have now collected all of the general setup information you need. Make sure that you have entered all the values onto the worksheet before proceeding to the next section.

Collecting ISDN Phone Line Information

After you have successfully installed the ISDN phone line or if you already have one installed, you need to use the ISDN line information to complete the worksheet and configure your router.

Your telephone company can give you the following information to configure the DI-106 or DI-106M:

Switch Type	Geography	No. of Phone #s	No. of SPIDs
AT&T 5ESS NI-1	North America	2	2
AT&T 5ESS Point to Point	North America	1	0
AT&T 5ESS Multipoint	North America	2	2
Northern Telecom NI-1	North America	2	2
Northern Telecom Custom	North America	2	2
DSS1	Europe, Asia	2	N/A
1TR6	Germany	2	N/A

- **Switch Type—**This is the type of switch used by your telephone company. Check with your telephone company and choose the appropriate option on the worksheet. For North America, select your ISDN switch type. For DSS1 and 1TR6, verify this field to make sure that you have the proper firmware loaded.
- **B Channel Usage—**Determine which connection is appropriate for your B channel and check the corresponding option on the worksheet.

  If your DI-106 or DI-106M is the only device using the ISDN line, configure B Channel Usage to **Switch/Switch** so the router device will use both B channels to communicate. If the router is sharing the ISDN line with other devices, configure B Channel Usage to **Switch/Unused**. If your DI-106 or DI-106M is on a leased line, configure B channel usage to **Leased/Leased** or **Leased/Switch**, depending on the setting of the line.
- **Telephone Number(s)**—Record on the worksheet the telephone number(s) given to you by your ISDN provider. Some switch types only have one telephone number. These phone numbers should be in a standard digit format (for

example, 5551212). Note that these fields will only accept digits, so hyphens and spaces will not be accepted.

- **Analog Call**—The router can direct an incoming analog call to standard phone jack 1 or to standard phone jack 2, or treat it as a data call, on the basis of the number being called. On the worksheet, check the way analog calls to each phone number are to be handled.

  The Phone1 setting directs incoming analog calls for the associated number to standard phone jack 1 (also referred to as A/B adapter 1, POTS [Plain Old Telephone System] port 1, and analog port 1). The Phone2 setting directs such calls to standard phone jack 2.

  The DOVBS setting is used for Data Over Voice Bearer Service, also known as Data Over Speech Bearer Service, or DOSBS. This is a service available from some ISDN providers that declares incoming ISDN data calls as analog. Check this setting if your service contract specifies DOVBS on the associated number.

- **SPID Number(s)—**(For North America only) The SPID (Service Profile Identifier) is a number used by a central office switch for identification purposes. With the switch information, see the previous table for the number of SPIDs you must enter.

You have now collected all of the necessary information about your ISDN phone line. Make sure that these values are entered into your worksheet before you continue to the next section. For DSS1 and 1TR6 ISDN, refer to the *Installation* chapter starting on page 23.

Collecting Ethernet Setup Information

This section assumes that you are setting up your router for a TCP/IP connection. If you want to configure the system for other protocols (e.g., IPX), refer to the appropriate chapters.

- **Ethernet Interface**—Your DI-106 or DI-106M is equipped with six Ethernet ports (input/output circuits). The jacks (that is, the connectors) for ports 1 through 5 are wired to let you connect network end nodes—single-user computers, servers, bridges, and other routers, for example—using easily obtained "straight-through" twisted-pair Ethernet cables. The jack for the sixth port is labeled **Uplink** and is wired to let you connect another 10-Mbps Ethernet hub using a straight-through cable, or an end node using a cross-wired cable.
- **IP Address—**An IP Address is required for TCP/IP protocol. The IP Address is a unique 32-bit number assigned to your router. It is written in dotted decimal notation (four 8-bit numbers, between 0 and 255, separated by periods), e.g., 192.68.203.5.

  Record the IP Address into the worksheet as assigned by your network administrator. Note that every machine on a TCP/IP network (the global Internet, for example) must have a unique IP address; do not assign an arbitrary address to any machine.
- **IP Sub-net Mask—**This field is required for TCP/IP protocol. An IP address consists of two parts, the network ID and the host ID. The IP Subnet Mask is used to specify the network ID portion of the address, expressed in dotted decimal notation. Your DI-106 or DI-106M will automatically calculate this mask based on the IP address that

you assign. Unless you have special need for subnetting, use the default mask as calculated by the router.

The table below lists some examples of IP subnet masks and the number of hosts that are allowed. Consult your network administrator if you are unsure of this value.

IP Subnet Mask	Number of Host IDs	Number of Bits
255.255.255.0	254	24
255.255.255.128	126	25
255.255.255.192	62	26
255.255.255.224	30	27
255.255.255.255	1	32

DI-106/DI-106M Setup and Installation Worksheet

General Setup Information

- **System Name (for identification purposes):**

  _____

- **Protocol(s):**

  ___TCP/IP

  ___IPX (DI-106M only)

  ___Bridging (DI-106M only)

ISDN Setup Information

- **Switch Type (check one):**

  ___AT&T 5ESS NI-1

  ___AT&T Point to Point

  ___AT&T 5ESS Multipoint

  ___Northern Telecom NI-1

  ___Northern Telecom Custom

  ___DSS1

  ___1TR6

- **B-Channel Usage (check one):**

  ___Switch/Switch

  ___Switch/Leased

  ___Leased/Switch

  ___Leased/Unused

___Unused/Leased

___Leased/Leased

___Leased128

___Switch/Unused

North American ISDN

- **1st Telephone Number:**

  _____

  Analog Call (check one): __Phone1 __Phone2 __DOVBS

- **1st SPID Number:**

  _____

- **2nd Telephone Number:**

  _____

  Analog Call (check one): __Phone1 __Phone2 __DOVBS

- **2nd SPID Number:**

  _____

DSS1 ISDN

- **ISDN Data Number & Subaddress:**

  _____

- **A/B Adapter 1 Number & Subaddress:**

  _____

- **A/B Adapter 2 Number & Subaddress:**

  _____

- **Outside Line Prefix Number:**

  _____

- **PBX Number (S/T Bus Number):**

  _____

- **Incoming Number Matching:**

  ___MSN

  ___Calling Party Subaddress

  ___Don't Care

- **Analog Call Routing:**

  __A/B #1 __A/B #2 __Ignore

- **Global Analog Call:**

  __Accept __Ignore

1TR6 ISDN:

- **ISDN Data Number:**

  _____

- **A/B Adapter 1 Number:**

  _____

- **A/B Adapter 2 Number:**

  _____

- **Outside Line Prefix Number:**

  _____

- **PBX Number (S/T Bus Number):**

  _____

- **Incoming Number Matching:**

  ___EAZ ___Don't Care

- **Analog Call Routing:**

  __A/B #1 __A/B #2 __Ignore

Ethernet Setup Information

- **IP Address:**

  _____.____.____.____

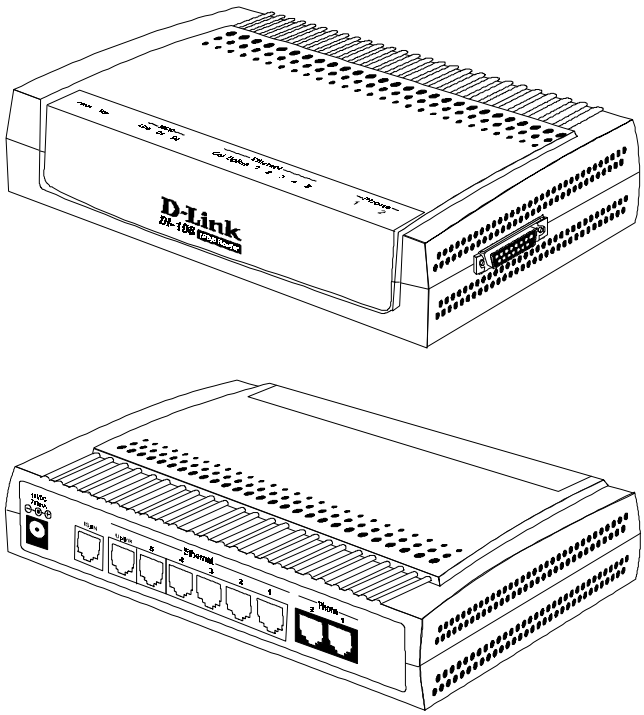
- **IP Subnet Mask:**

  _____.____.____.____

Notes:

Installation

This chapter outlines how to connect your DI-106 or DI-106M to your LAN and ISDN line. Refer to the diagram below to identify all of the ports on your device when you make connections.



A Warning On Connection Cables

ISDN and Ethernet cables are very similar to each other. It is important that you use the correct cable for each connection; otherwise, your router could be damaged.

Before connecting or disconnecting an RS-232 cable between two devices, turn both devices off to avoid any chance of damaging them.

Mounting the Router

The router can be placed on a desktop or mounted on a wall, depending on your needs. Two mounting holes are provided on the bottom of the unit for wall mounting. The recommended mounting position is with the cable jacks facing sideways or downward to help keep dust off the contacts.

Regardless of how you mount the router, make sure its cable jacks are accessible, its LED indicators are visible, and its ventilation holes are never blocked.

Connecting Your Computer and Your DI-106 or DI-106M

For initial setup of your DI-106 or DI-106M, you must use an RS-232 connection, either to a computer running serial communications software or to a serial data terminal.

After the router has been successfully installed, you can modify the configuration through a remote Telnet connection. See the chapter

entitled *Telnet Configuration and Capabilities* for detailed instructions on using Telnet to configure your DI-106 or DI-106M.

Connecting the RS-232 Cable to the Router

An RS-232 cable is included in your package. To connect this cable, plug its nine-pin connector into the DCE port on the router's side panel, then connect the other end to an RS-232 serial port on your computer or data terminal (on IBM-type microcomputers, serial ports are usually labeled COM1, COM2, etc.).

Connecting an ISDN Line to the Router

Plug one end of your ISDN phone line into the socket on the rear panel of the router labeled ISDN and the other end into the ISDN wall jack.

- **S/T interface—**This can only connect to your NT-1 (Network Termination) device.

NOTE: *Do not under any circumstances connect directly to the ISDN wall jack.*

- **U interface—**This allows you to connect directly to your ISDN wall jack.

NOTE: *The ISDN jack is for ISDN line connection only. Connection of a phone line may result in damage to your DI-106 or DI-106M.*

Connecting a Telephone or Fax Machine to the Router

You can connect a regular telephone, fax machine, or modem to your router to be used for analog calls, just as you can do on a conventional telephone line. Note that the router's other functions all work the same whether you connect an analog device or not.

To connect an analog device, just plug one end of the device's line cord into the socket on the back of the router marked PHONE 1 or PHONE 2.

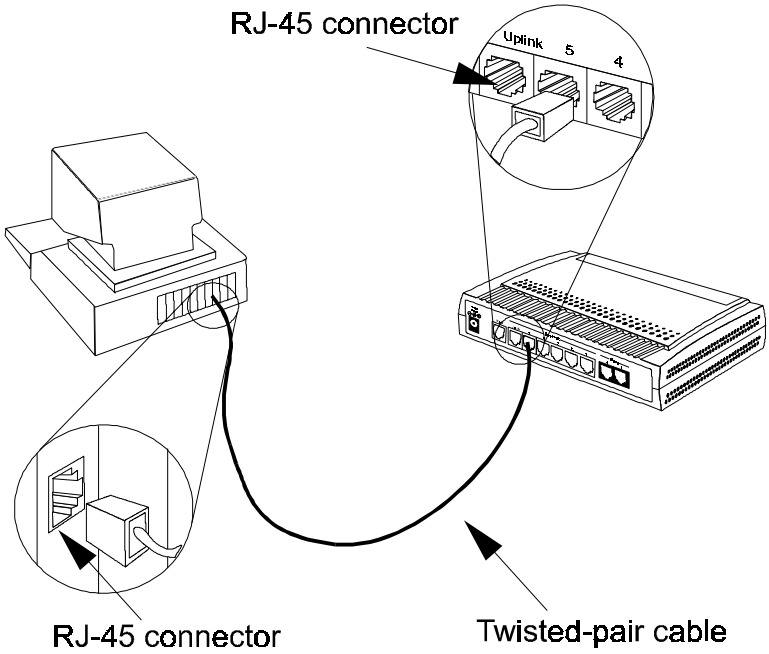
To have incoming calls directed to a device on a PHONE port, you must select Phone1 or Phone2 for the desired telephone number's **Analog Call** control in setup menu 2, ISDN Setup.

Connecting Ethernet Cables to the Router

Your DI-106 or DI-106M has six ports for connecting 10BASE-T Ethernet devices to form a LAN. The jacks for ports 1 through 5 are wired to let you connect network end nodes (single-user computers, servers, bridges, other routers, etc.) using standard "straight-through" EIA (Electronic Industries Association) Category 3 or higher-grade twisted-pair data cables. The jack for the sixth port is labeled **Uplink** and is wired to let you connect another 10-Mbps Ethernet hub using a straight-through cable, or an end node using a cross-wired cable.

The jacks for the router's Ethernet ports are of the type known as EIA RJ-45 (Recommended Jack No. 45). Note that when you make an uplink connection to another hub using a straight-through cable, you must use an uplink-type jack at one end and an end-node-type jack at the other.

The following figure shows how to make an Ethernet connection between the router and a network end node.

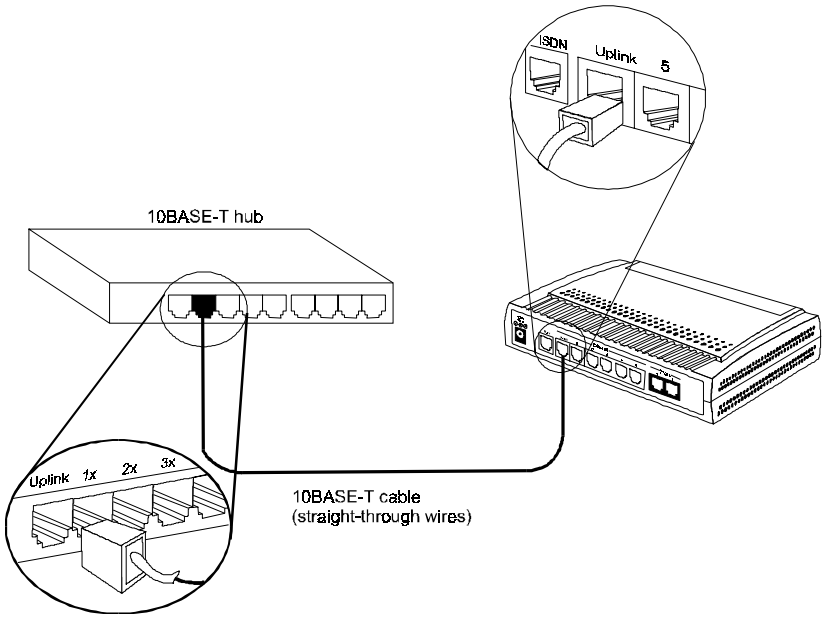


Important Notes on Ethernet Hub Connections

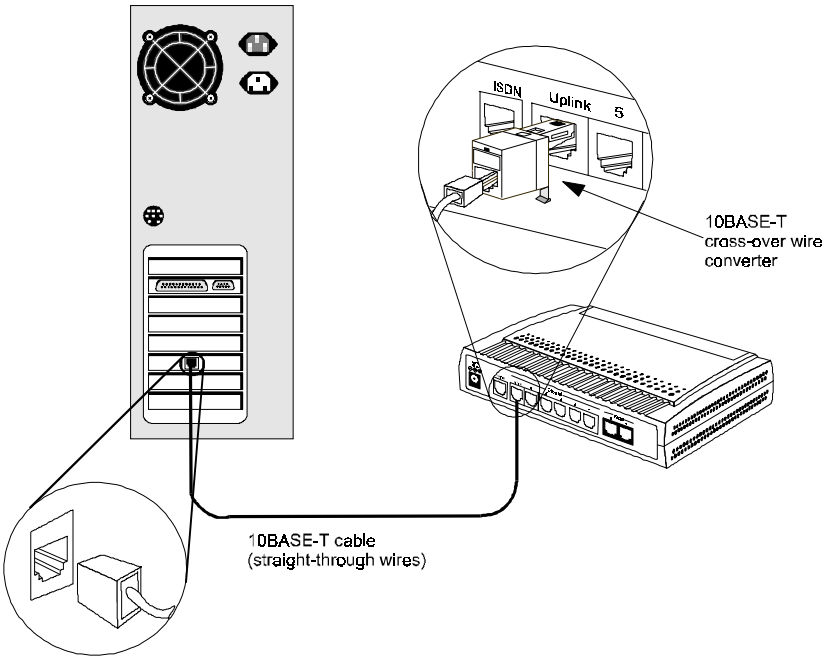
Observe the following rules when connecting devices with twisted-pair Ethernet cables:

- For both end-node and uplink connections, use only EIA Category 3 or higher-grade twisted-pair data cables with RJ-45 plugs. In almost all cases, only standard straight-through cables are needed.
- Make sure no cable is more than 100 meters (328 feet) long.

- When uplinking two hubs together with a straight-through cable, use an uplink-type jack at one end and an end-node-type jack at the other.



Note that you can connect an end node through the Uplink jack, but to do so you must use a cross-wired cable or cable converter.



- If uplinking more than two hubs together, observe the 5-4-3 rule: no signal, in order to go from one end node to another, must ever pass through more than five twisted-pair cables, four repeaters (that is, hubs), and three uplink connections. This is the maximum signal path in twisted-pair Ethernet. Also be sure never to allow a signal loop to form.

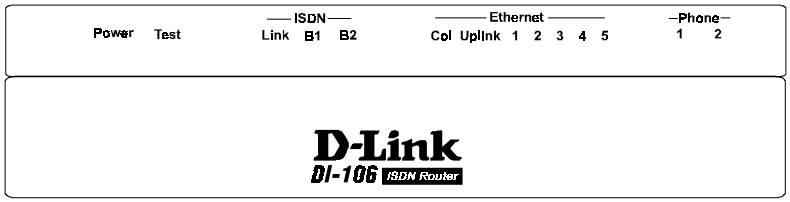
Connecting a Power Adapter to the Router

Plug an 18V DC, 750 mA power adapter into the power jack on the router's rear panel.

At this point, you should have connected the RS-232 cable, the ISDN phone line, one or more Ethernet cables, and the power adapter. You can now power up your DI-106 or DI-106M.

The DI-106 or DI-106M's Front Panel

Names and descriptions of your router's front panel LEDs are given below:



POWER—Comes on as soon as you connect the router to the power adapter and plug the power adapter into a suitable AC outlet.

TEST—Should be blinking if the router is functioning properly.

ISDN – LINK—Indicates that the router has an ISDN line connected to the WAN interface and it has been successfully initialized.

ISDN – B1 and **ISDN – B2**—On if there is an active WAN session on that channel or if that channel is making or receiving a call.

ETHERNET – COL—Shines yellow when a collision occurs on the LAN, that is, when two devices have attempted to transmit at the same time.

ETHERNET – Uplink and **ETHERNET – 1** through **ETHERNET – 5**—Each of these indicators shines green when a connection to an Ethernet device is detected. The indicator blinks when a transmission is received from the device, and shines yellow when the device has been partitioned, that is, temporarily isolated

from the LAN because of excessive collisions (partitioning is a required capability of all Ethernet hubs).

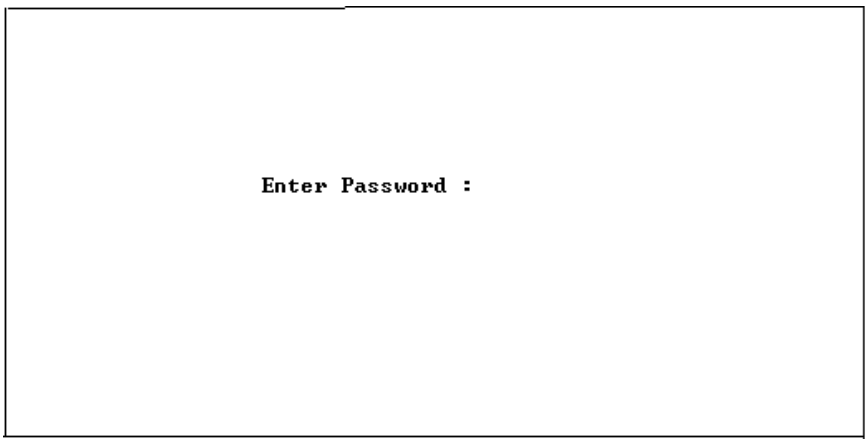
PHONE – 1—Lights up when standard phone port 1 is in use.

PHONE – 2—Lights up when standard phone port 2 is in use..

Powering Up Your DI-106 or DI-106M

When you power up your DI-106 or DI-106M, the router will perform several internal tests and do an ISDN line initialization. After ISDN line initialization, the router will ask you to press **ENTER** to continue.

When you press **ENTER**, the router will display a login screen and ask you to enter the password, as shown below:



Enter the default password, **1234**, to get into the main menu of the System Management Terminal (SMT). Note that once you are in the SMT, if there is no activity for more than 5 minutes, the router

will automatically log you out and display a blank screen. If you see a blank screen, press **ENTER** to bring up the password screen.

Navigating Through the System Management Terminal Interface

The SMT is the interface that you use to configure your DI-106 or DI-106M. Several operations that you should be familiar with before you attempt to modify the configuration of your router are listed below:

- **Moving Forward to Another Menu.** To move forward to a sub-menu below the current one, type in the number of the sub-menu and press **ENTER**.
- **Moving Backward to a Previous Menu.** Press the **Escape** key to move back to the previous menu.
- **Moving the Cursor.** Within a menu, press **ENTER** (carriage return) to move to the next field. You can also use the **Up** and **Down** keys to move to the previous and the next field, respectively.
- **Entering Information.** There are two types of fields that you will need to fill in. The first requires you to type in the appropriate information. The second gives you choices to choose from. In the second case, press the **space bar** to cycle through the available choices.
- **Required Fields.** Some of the fields in the SMT are essential in order to configure the DI-106 or DI-106M. These fields will initially show question marks, indicating that the information must be filled in before that menu can be saved.

- **N/A Fields.** Some of the fields in the SMT will show a N/A. This symbol refers to an option that is not available or not applicable.
- **Saving Your Configuration.** You can save your configuration by pressing **ENTER** at the message 'Press ENTER to confirm or ESC to cancel'. Saving the data on the screen will take you in most cases to the previous menu.

The SMT main menu is shown below.

```
                        D-Link Corporation

                         DI-106M Main Menu

  Getting Started                     Advanced Management
    1. General Setup                    21. Filter Set Configuration
    2. ISDN Setup                       22. SNMP Configuration
    3. Ethernet Setup                   23. System Security
    4. Internet Access Setup            24. System Maintenance

  Advanced Applications
    11. Remote Node Setup
    12. Static Routing Setup
    13. Default Dial-in Setup
    14. Dial-in User Setup              99. Exit



                     Enter Menu Selection Number:
```

System Management Terminal Interface Summary

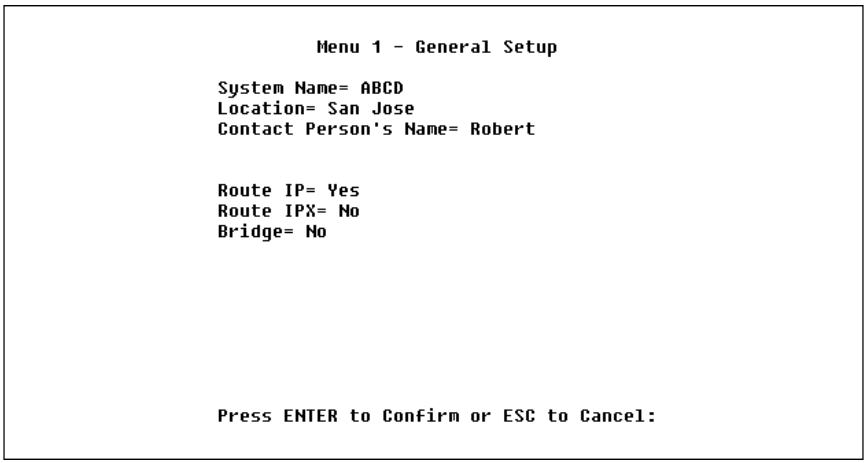
This section summarizes all major SMT menus:

#	Menu Title	Description
1	General Setup	Set up general information and enable routing or bridging of specific protocols
2	ISDN Setup	Set up ISDN configuration
3	Ethernet Setup	Set up Ethernet configuration
4	Internet Access Setup	A quick and easy way to setup Internet connection
11	Remote Node Setup	Set up Remote Node for LAN-to-LAN connection

#	Menu Title	Description
		including Internet connection. A DI-106 or DI-106M can have up to four Remote Nodes.
12	Static Routing Setup	Set up static routes for different protocols. Up to four static routes can be set for each protocol.
13	Default Dial-in Setup	Set up default dial-in parameters such that your DI-106 or DI-106M can be a dial-in server for the Remote Node and Remote Dial-in User.
14	Dial-in User Setup	Set up Remote Dial-in User. Your DI-106 or DI-106M can directly support up to eight Remote Dial-in Users.
21	Filter Set Configuration	Set up filters to be used in menu 3 and menu 11 to provide security, call control, etc.
22	SNMP Configuration	Set up SNMP-related parameters (DI-106M only)
23	System Security	Set up security related parameters
24	System Maintenance	Provide system status, diagnostics, firmware upload, etc.
99	Exit	To exit from SMT and return to the blank screen

General Setup

This menu contains administrative and system-related information. Enter **1** in the main menu to go to menu 1, General Setup.

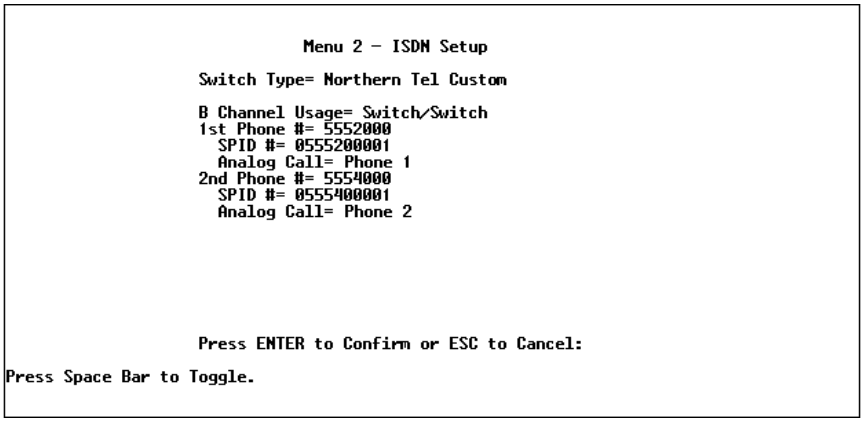


1. **System Name—**Give the router a descriptive name for identification purposes, e.g., **ABCD**. This name should be no more than 8 alphanumeric characters. Spaces are not allowed, but "-" and "_" are accepted. This name can be retrieved remotely via SNMP, used for CHAP authentication, and will be displayed as the prompt in command interpreter mode. See the *Dial-In Configuration* chapter starting on page 68 for more information on CHAP; see the *System Maintenance* chapter starting on page 128 for more information on command interpreter mode.
2. **Location—**Enter the geographic location (up to 31 characters) of your DI-106 or DI-106M, e.g., San Jose.
3. **Contact Person's Name—**Enter the name (up to 8 characters) of the person in charge of the router. The Location and the Contact Person fields are optional.
4. **Protocols—**Turn on or off the individual protocols for your particular application. Unsupported protocols will have a N/A in their fields.

ISDN Setup

Menu 2 is for entering information about your ISDN line. Different telephone companies deploy different types of switches for ISDN service. Depending on the switch for your particular installation, you will have a different number of telephone numbers, and if you are in North America, you may also have SPIDs. Make sure that you have correct and complete telephone numbers and SPIDs. You need to pass the ISDN setup before your system can make an outgoing call or answer an incoming call.

North American ISDN



1. **Switch Type**—Verify the switch type information with your telephone company. For North America, select the type of switch used by your telephone company. If your switch type is not currently shown, press the **space bar** to change to the next switch; repeat until you see the correct switch type. The router will not be able to place or to receive calls if the wrong switch type is specified. If you are not sure, contact your telephone company to confirm the exact switch type.
2. **B Channel Usage—**If you are using one B channel of your router with another device on the S/T bus, then select **Switch/Unused**. If not choose **Switch/Switch**. The following table shows the relationship between the **B Channel Usage** setting and ISDN B channels.

B Channel Usage	B1	B2
Switch/Switch	Switch	Switch
Switch/Leased	Switch	Leased
Leased/Switch	Leased	Switch
Leased/Unused	Leased	N/A
Unused/Leased	N/A	Leased
Leased/Leased*	Leased	Leased

B Channel Usage	B1	B2
Leased128**	Leased	Leased
Switch/Unused	Switch	N/A

*Leased/Leased = B1 and B2 channels connect to different remote nodes.
**Leased128 = B1 and B2 channels connect to the same remote node.

3. **Telephone Number(s)**—Enter the telephone number(s) assigned to your ISDN by your telephone company. Some switch types allow only one telephone number. In North America, each number should be in standard seven-digit format, for example, 5551212. Note that the router accepts only digits; do not include hyphens or spaces in this field. This field should be no longer than 19 digits.

4. **Analog Call**—This tells the router where to direct incoming analog calls for the associated phone number. Set to Phone1 to direct such calls to the PHONE 1 port, Phone2 to direct them to the PHONE 2 port, or DOVBS to have them handled as Data Over Voice Bearer Service (also known as Data Over Speech Bearer Service, or DOSBS) data calls. (The PHONE 1 and PHONE 2 ports are known as Plain Old Telephone Service [POTS] ports in North America and A/B Adapter ports in Europe.)

5. **SPID Number(s)—**SPIDs are numbers used by a switch for identification purposes. Depending on your switch type, you may have zero, one, or two SPIDs assigned to your line. For example, if your switch type is Northern Telecom Custom, you will have to enter two SPID numbers.

DSS1 & 1TR6 ISDN

```
                              Menu 2 - ISDN Setup

          Switch Type: DSS-1(Japan)
          B Channel Usage= Switch/Switch

          ISDN Data     =                     Subaddress=
          A/B Adapter 1 =                     Subaddress=
          A/B Adapter 2 =                     Subaddress=

          Dial Prefix to Access Outside Line=
          PABX Number (Include S/T Bus Number)=
          Incoming Phone Number Matching= Multiple Subscriber Number (MSN)
            Analog Call Routing= N/A
            Global Analog Call= N/A




                    Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

```
                              Menu 2 - ISDN Setup

          Switch Type: 1TR6
          B Channel Usage= Switch/Switch

          ISDN Data     =
          A/B Adapter 1 =
          A/B Adapter 2 =

          Dial Prefix to Access Outside Line=
          PABX Number (Include S/T Bus Number)=
          Incoming Phone Number Matching= Endgeraete Auswahl Ziffer (EAZ)
            Analog Call Routing= N/A




                    Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

1. **Switch Type—**This field is fixed as DSS1 or 1TR6.
2. **B Channel Usage**—This field is fixed as Switch/Switch.

3. **ISDN Data & Subaddress—**Enter the telephone number and subaddress assigned to the ISDN data call for the router. It will be used as the outgoing CGPN (Calling Party Number) setting for ISDN data calls. Note that the router only accepts digits; do not include hyphens or spaces in this field. This field should be no longer than 19 digits for the number and 5 digits for the subaddress. The subaddress is only available for DSS1.
4. **A/B Adapter 1 & Subaddress—**Enter the telephone number and subaddress assigned to analog port 1 (PHONE 1, also known as A/B Adapter 1 and POTS port 1) calls. This setting will be used at the Calling Party Number for outgoing calls made through this port.
5. **A/B Adapter 2 & Subaddress—**Enter the telephone number and subaddress assigned to analog port 2 (PHONE 2, also known as A/B Adapter 2 and POTS port 2) calls. This setting will be used at the Calling Party Number for outgoing calls made through this port.
6. **Dial Prefix to Access Outside Line—**Enter the prefix number if the router is connected to an ISDN PABX. This number will be added to all outgoing calls and should be no longer than 3 digits. Otherwise, leave this field blank.
7. **PABX Number (with S/T Bus Number)**—Enter the S/T bus number if the router is connected to an ISDN PABX. If this field is left as blank then the loopback test will be skipped.
8. **Incoming Phone Number Matching**—The setting of this control determines what incoming calls will be answered. There are three possible settings:
    - ◊ **Multiple Subscriber Number (MSN)**—Digital calls will be answered only when there is a match for the ISDN data number; analog calls will be answered only when there is a

match for the number assigned to an analog phone port, and they will be directed to the port to which the number is assigned (if no number is assigned to analog phone port 1 or 2, analog calls will not be answered). This option is available as EAZ (Endgeraete Auswahl Ziffer) for 1TR6.

◊ **Called Party Sub-Address (CDSA)**— Digital calls will be answered only when there is a match for the ISDN data subaddress; analog calls will be answered only when there is a match for the subaddress assigned to an analog phone port, and they will be directed to the port to which the subaddress is assigned (if no subaddress is assigned to analog phone port 1 or 2, analog calls will not be answered). This option is available only for DSS1.

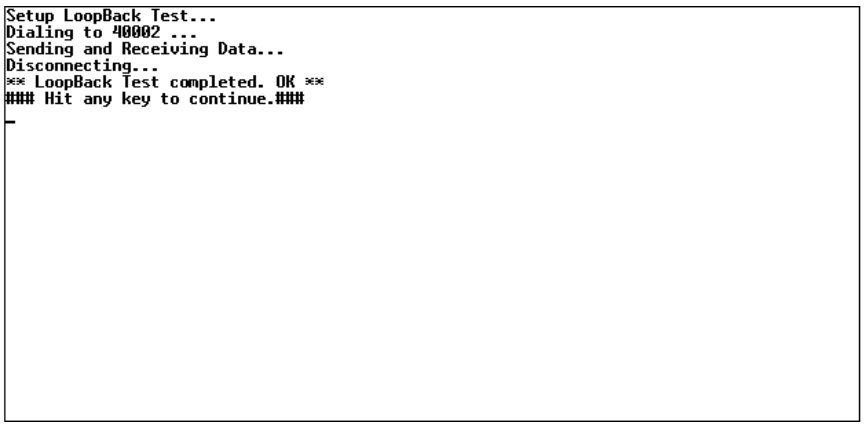
◊ **Don't care – all numbers accepted**—All digital calls to any Called Party Number, including global calls (those without CDPN or CDSA in the call setup), will be answered. All analog calls will be directed to analog port 1 or analog port 2, or (if Analog Call Routing is set to Ignore) not answered.

- **Analog Call Routing**—All analog calls will be directed to analog phone port 1 if the setting is A/B Adapter 1, or to analog phone port 2 if the setting is A/B Adapter 2. If the setting is Ignore, analog calls will not be answered.
- **Global Analog Call**—If the setting is Accept, all analog calls will be answered and directed to analog port 1 or analog port 2, as specified by setting of the **Analog Call Routing** control. If **Global Analog Call** is set to Ignore, no analog calls will be answered.

9. Enter the S/T bus number if the router is connected to an ISDN PABX. If this field is left as blank then the loopback test will be skipped.

When you are finished, press **ENTER** at the message 'Press ENTER to Confirm...' to save your selections, or press **ESC** to cancel. When you press ENTER, the router will use the information that you entered to initialize the ISDN link to the telephone company switch. It should be noted that whenever the switch type is changed, the ISDN initialization will take slightly longer. In addition, if you are using the U-interface, the system will also take slightly longer to initialize.

At this point, you will be asked if you wish to check if your ISDN line has been successfully connected to your router. If you select Yes, the router will perform a loop-back test to check the ISDN line. If the loop-back test fails, note the error message that you receive and take the appropriate troubleshooting action.

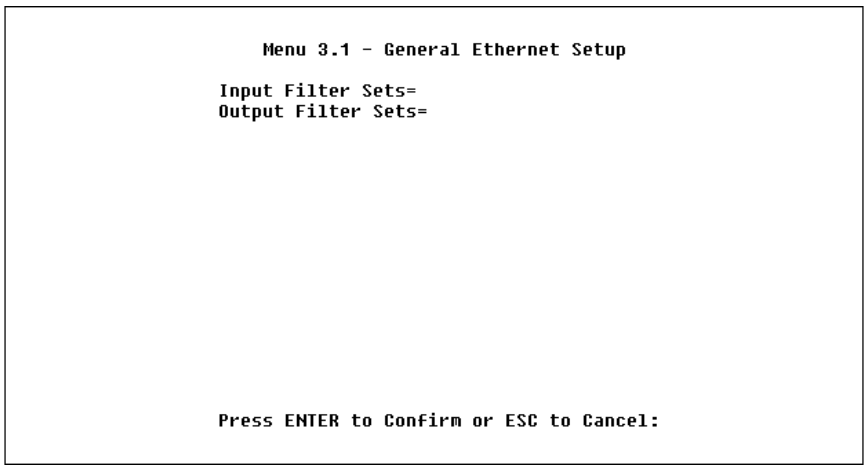


Ethernet Setup

Menu 3 is used to enter Ethernet related information. Depending on the protocols (TCP/IP or IPX) on your LAN, you will need to configure each protocol separately.

General Ethernet Setup

This menu determines the type of Ethernet interface you are using as well as the filter sets you wish to implement to monitor your Ethernet traffic. From menu 3, Ethernet Setup, enter **1** to go to menu 3.1, General Ethernet Setup.

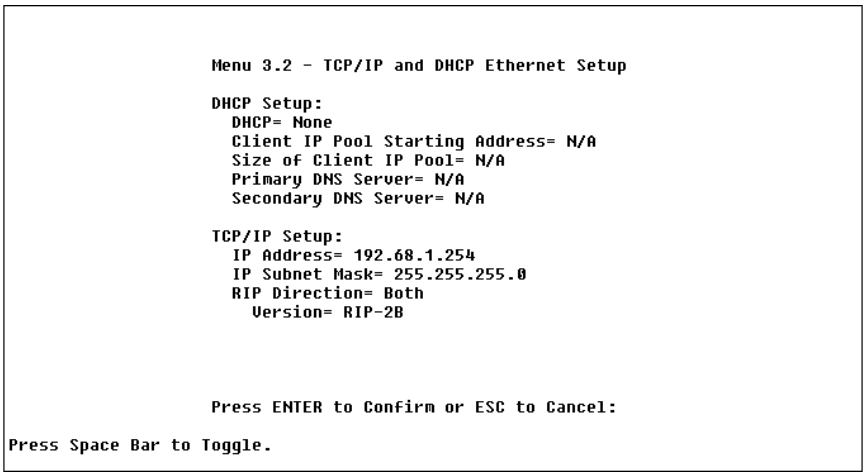


Input and Output Filter Sets—Filter sets are used to block certain packets to reduce traffic and to prevent a security breach. Filtering is a very involved subject, so leave these fields blank for the time being. After you have studied the *Filter Configuration* chapter starting on page 103, come back and define the filter sets.

TCP/IP and DHCP Ethernet Setup

If you are setting up your network for the first time, read the chapter entitled *Configuring for Internet Access* before proceeding. The chapter contains important information on how to assign IP addresses for your network.

From menu 3, Ethernet Setup, enter **2** to go to menu 3.2, TCP/IP and DHCP Ethernet Setup.



1. **DHCP**—This field determines whether the router will act as a DHCP (Dynamic Host Configuration Protocol) server. If this control is set to None, DHCP will not be used. If it is set to Server, the router will act as a DHCP server, capable of automatically assigning IP addresses to Windows 95, Windows NT, and other systems that support the DHCP client. When DHCP is used, the following four items need to be set.

   Do not set this field to Server if there is already a DHCP server on your network.

2. **Client IP Pool Starting Address**—DHCP can assign IP addresses to hosts dynamically instead of requiring that each system have a fixed IP address. IP addresses are allocated from a block of addresses, usually assigned by your Internet provider. The Client IP Pool Starting Address gives the first address in the reserved block, which is also used as the LAN network address of the router itself. This address will also serve as the default gateway for DHCP clients.
3. **Size of Client IP Pool**—Gives the size of the block of addresses reserved for DHCP address assignment. The default is 6 addresses; the maximum is 32. The router itself uses the first address in the block, and the remaining addresses in the pool are assigned to clients.
4. **Primary DNS Server/Secondary DNS Server**—These two fields are used by DHCP clients (such as Windows 95 and Windows NT systems) for Domain Name Servers. Usually your Internet provider will provide one or more name service hosts.
5. **IP Address—**Enter the IP address of the DI-106 or DI-106M in dotted decimal notation (four 8-bit numbers, between 0 and 255, separated by periods), e.g., 192.68.135.5. Note that every machine on the TCP/IP network must have a unique IP address.
6. **IP Subnet Mask—**An IP address consists of two parts, the network ID and the host ID. The IP Subnet Mask is used to specify the network ID portion of the address, expressed in dotted decimal notation. Your DI-106 or DI-106M will automatically calculate this mask based on the IP address that you assign. Unless you have special need for subnetting, use the default subnet mask calculated by the router.
7. **RIP Direction—**This parameter determines how the DI-106 or DI-106M handles RIP (Routing Information Protocol). If set to

Both (default), the router will broadcast its routing table on the LAN, and incorporate RIP broadcasts by other routers into its routing table. If set to In Only**,** the router will not broadcast its routing table on the LAN, if set to Out Only**,** the router will broadcast its routing table but ignore any RIP broadcast packets that it receives. If set to None, the router will not participate in any RIP exchange with other routers.

Usually, you should leave this parameter at its default of Both and let RIP propagate the routing information automatically.

8. **RIP Version**—Determines what versions of the RIP Routing Information Protocol the router accepts. Choices are:

   ◊ **RIP-1** The router will accept and send RIP version 1 messages only.

   ◊ **RIP-2B** The router will accept RIP-1 and RIP-2 messages (both broadcast and multicast), and sends RIP-2 messages in broadcast format.

   ◊ **RIP-2M** The router will accept RIP-1 and RIP-2 messages (both broadcast and multicast), and sends RIP-2 messages in multicast format.

   Unless there are routers in your environment that do not understand RIP-2 packets, you should probably set this field to RIP-2B.

When you are finished, press **ENTER** at the message 'Press ENTER to Confirm...' to save your selections, or press **ESC** at any time to cancel them.

Novell IPX Ethernet Setup

Refer to the chapter on Novell IPX configuration.

Bridge Ethernet Setup

Refer to the chapter on Bridging configuration.

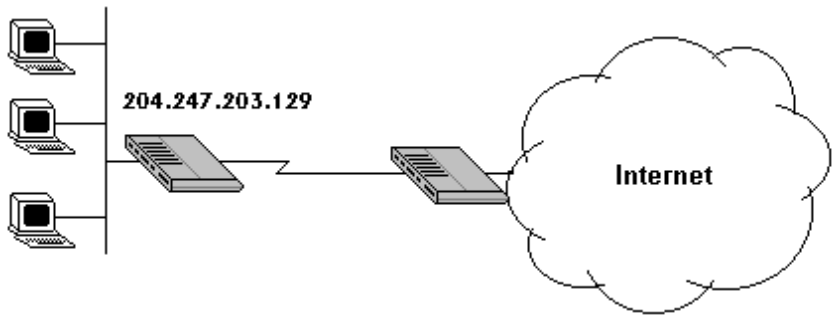
Configuring for Internet Access

Menu 4 of the SMT allows you to configure Internet access on one screen. Before you configure your DI-106 or DI-106M for Internet access, you need to collect the following information from your ISP (Internet Service Provider).

- IP address of the ISP's gateway (optional).
- Telephone number(s) of your ISP.
- Login name.
- Password for ISP authentication

For your Workstation:

- Domain Name Server (DNS)



IP Addresses and the Internet

Conventionally, the Internet (with a capital I) refers the large-scale interconnected networks across the world that was originally

developed by the US Department of Defense. The Internet uses exclusively the TCP/IP suite of protocols. The term “internet” (lower case i), however, refers to any interconnected networks using any protocol. An internet can be as simple as two hosts on a LAN, or it can be as complex as the Internet itself.

Every machine on the Internet must have a unique address within that internet. If your networks are isolated from the Internet, e.g., only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

```
10.0.0.0    – 10.255.255.255
172.16.0.0  – 172.31.255.255
192.168.0.0 – 192.168.255.255
```

For this reason, it is recommended that you choose your network number from the above list.

You can obtain your IP address from the IANA, from an ISP, or assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

NOTE: *Regardless of your particular situation,* ***do not*** *create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, refer to RFC 1597,*

Address Allocation for Private Internets *and RFC 1466,* Guidelines for Management of IP Address Space.

Once you have determined the IP address range for your local network, you may want to use DHCP (Dynamic Host Configuration Protocol) to assign addresses to individual hosts on the network, as an alternative to manually configuring each host's IP settings. See the TCP/IP and DHCP section on page 43 for more information about DHCP.

Internet Access Configuration

This section describes how to configure your DI-106 or DI-106M for Internet access. The information you will need to provide will be indicated in **bold** type.

Note that configuring the router for Internet access will automatically create a new entry in the Remote Node Setup menu (menu 11). Before carrying out the following steps, check the Remote Node Setup menu to make sure there is space for a new entry. In order for you to be able to configure the router for Internet access, there must be no more than three entries in the Remote Node Setup menu before you start.

```
                Menu 4 - Internet Access Setup

          ISP's Name= myisp
          ISP IP Addr= 10.145.233.5
          Pri Phone #= 5551234
          Sec Phone #= 5551235
          My Login= abcd
          My Password= ********
          Single User Account= No
            IP Addr= N/A
            Server IP Addr= N/A
          Telco Option:
            Transfer Type= 64K

          Multilink= Off



          Press ENTER to Confirm or ESC to Cancel:
```

1. From the main menu, enter 4 to go to menu 4, Internet Access Setup. This menu is shown above.
2. **ISP's Name—**Enter the name of your Internet Service Provider, e.g., myisp. This information is for identification purposes only.
3. **ISP IP Addr—**Enter the IP Address of the remote gateway at the ISP's site. If you do not have this data, just leave it blank.
4. **Pri(mary) Phone #** and **Sec(ondary) Phone Number—**Both the Primary and the Secondary Phone number refer to the number that your DI-106 or DI-106M will dial to connect to the ISP. The router will always call your ISP using the Primary Phone number first. If the Primary Phone number is busy or does not answer, the router will call the Secondary Phone number if available. Once connected, the router will use the BACP (Bandwidth Allocation Control Protocol) to establish the second B-channel if PPP/MP is enabled, and the ISP also supports MP and BACP.

5. **My Login Name—**Enter the login name given to you by your ISP.
6. **My Password—**Enter the password associated with the login name above. Note that this login name/password pair is only for the router to connect to the ISP's gateway. When you use TCP/IP applications, e.g., FTP, to access the Internet from your workstation, you will need a separate login name and password for each server.
7. **Single User Account**—See the following section for a more detailed discussion on the Single User Account feature. The default is No.
8. **Telco Options: Transfer Rate—**This field (which only applies to outgoing calls) controls the rate at which the data is transferred between your router and the Internet. The options for this field are:
   - ◊ **64K**—The router will place 64-kbps (kilobits per second) digital data calls.
   - ◊ **56K**—(For the North America only) The router will place 56-kbps digital data calls.
   - ◊ **Lease—**The router will place leased-line calls.
   - ◊ **DOVBS**—This option is for North America only. The router will place 56-kbps Data Over Voice Bearer Service (DOVBS) calls. Some phone companies in North America charge less if calls are made with the DOVBS option.
9. **Multilink**—Determines whether or not Multilink PPP should be used. Available options are:
   - ◊ **Off**—The base transfer rate and maximum transfer rate will be 64 kbps.

- ◊ **BOD** (Bandwidth On Demand)—The base transfer rate will be 64 kbps, and the maximum transfer rate will be 128 kbps.
- ◊ **Always**—Multilink will always be on; both the base transfer rate and maximum transfer rate will be 128 kbps.

10. Press **ENTER** at the message 'Press ENTER to Confirm...' to confirm your selections, or press **ESC** at any time to cancel your selections.

11. At this point, the SMT will ask if you wish to test the Internet connection. If you select Yes, the router will call the ISP to test the Internet connection. If the test fails, note the error message that you receive and take the appropriate troubleshooting steps.

Single User Account

Typically, if there are multiple users on the LAN wanting to concurrently access the Internet, they will have to subscribe to multiple IP addresses or a Class C subnetwork from the ISP. In either case, these two approaches will cost more than a single user account.

The Single User Account (SUA) feature allows customers to have the same benefits as having a Class C address, but still only pay for one IP address, thus saving significantly on subscription fees. (Check with your ISP before you enable this feature).

This feature may also be used to connect to TCP/IP remote nodes other than Internet Service Providers. For example this feature can be used to simplify the allocation of IP addresses when connecting branch offices to the corporate network.

The IP address for the Single User Account can be either fixed or dynamically assigned by the ISP (or other remote node). In addition, you can also configure a server, e.g., a Web server, on your local network and make it accessible by outside users.

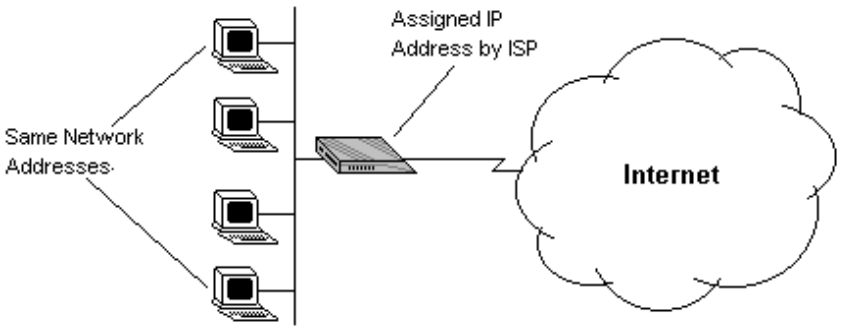
If you do not set a server IP address, SUA offers the additional benefit of firewall protection. This is because if no server is defined, all incoming inquiries will be filtered out by the router even if you do have a server on your network. This can prevent intruders from probing your system.

The router accomplishes this address sharing by translating the internal LAN IP addresses to a single address that is globally unique on the Internet. For more information on IP address translation, refer to RFC 1631, *The IP Network Address Translator (NAT)*.

In summary:

1. SUA is an ideal, cost-effective solution for small offices with less than 20 hosts using a LAN to concurrently access the Internet or other remote TCP/IP network.
2. SUA can provide one server address to be accessed by Remote Dial-in Users, thus controlling the incoming packets.
3. SUA can provide firewall protection if you do not configure a server IP address. All incoming inquiries will be filtered out by the DI-106 or DI-106M. Therefore, servers on your network are protected.
4. UDP and TCP datagrams can be routed. In addition, ICMP echo can also be routed.

The figure below shows an example of a small office connected to the Internet via a Single User Account using a DI-106 or DI-106M. Note that if you enable the Single User Account feature, your local IP address **MUST** be selected from the list of IP addresses for private networks as defined by the IANA.



Configuration for Single User Account

The steps for configuring your DI-106 or DI-106M for Single User Internet Access are identical to conventional Internet Access, with the exception that you need to fill in three extra fields.

Follow steps 1-4 from the previous section, Internet Access Configuration.

1. **Single User Account—**Enter Yes to enable the Single User Account feature. Use the space bar to toggle between Yes and No.

2. **Single User Account: IP Addr—**If your ISP assigns you a dynamic IP address, enter 0.0.0.0 here. If your ISP assigns you a static IP address enter that IP address here.

3. **Single User Account: Server IP Addr—**If you want to make a single server, e.g., a Web server, accessible to outside users, enter that server's IP address here.

   Press **ENTER** at the message 'Press ENTER to Confirm...' to confirm your selections or press **ESC** at any time to cancel your selections.

   At this point, the router will ask if you wish to test the Internet connection. If you select Yes, the router will call the ISP to test the Internet connection. If the test fails, note the error message that you receive and take the appropriate troubleshooting steps.

Configuring Backup ISP Accounts

Sometimes it may be desirable to configure more than one ISP account for backup purposes. The Single User Account feature can be enabled for all of these accounts, making it convenient to switch Internet Service Providers in the event of a failure.

To configure a backup ISP,

1. Configure your primary ISP using menu 4, as described earlier in this chapter.
2. Enter menu 11, then select the number of an unused remote node.
3. In menu 11.1, choose a name for your backup ISP account, set the Active field to No, and enter your outgoing login name, password, and phone number(s). The Remote IP Address field should be set to 1.1.1.1.

4. In menu 11.3, set the remote node's subnet mask to 0.0.0.0, and set RIP to None.

5. Save the new configuration.

Once you have done this, if you need to change from your primary ISP to a backup ISP follow the steps below:

1. Enter menu 11 and select your Primary ISP.

2. In menu 11.1, set the Active field to No.

3. Enter menu 11 again and select your backup ISP.

4. In menu 11.1, set the Active field to Yes.

You will now be able to access the Internet through the backup ISP Remote Node.

Remote Node Configuration

A Remote Node represents both a remote gateway and the internet behind it, across an ISDN connection. A Remote Node is required for placing calls to or answering calls from a remote network. Note that when you use menu 4 to configure the Internet, your DI-106 or DI-106M will automatically add a Remote Node for you. Once a Remote Node is configured properly, traffic to the remote LAN will trigger the router to make a call automatically (i.e., Dial On Demand). Similarly, calls from the remote LAN will be answered automatically and security will be checked.

In this chapter, we will discuss the parameters that are protocol independent. The protocol dependent configuration will be covered in subsequent chapters. For TCP/IP, see the *TCP/IP Configuration* chapter on page 79. For IPX, see the *Novell IPX Configuration* chapter on page 87. For bridging, see the *Bridging Configuration* chapter on page 97.

From the main menu, enter **11** to go to menu 11, Remote Node Setup. When in menu 11, enter the number of the Remote Nodes (1 to 4) that you wish to configure as shown below:

```
                Menu 11 - Remote Node Setup

            1. SJHQ
            2. ________
            3. ________
            4. ________




                     Enter Node # to Edit:
```

Enter the Remote Node number to edit and you will go to the next submenu: 11.1, Remote Node Profile, shown below:

```
                    Menu 11.1 - Remote Node Profile

Rem Node Name= SJHQ                  Route= IP
Active= Yes                          Bridge= No
Call Direction= Both
                                     Edit PPP Options= No
Incoming:                            Rem IP Addr= 198.23.34.5
  Rem Login= abcd                    Edit IP/IPX/Bridge= No
  Rem Password= ********             Telco Option:
  Rem CLID=                            Transfer Type= 64K
  Call Back= No                        Allocated Budget(min)= 0
Outgoing:                              Period(hr)= 0
  My Login= wxyz                     Session Options:
  My Password= ********                Input Filter Sets=
  Authen= CHAP/PAP                     Output Filter Sets=
  Pri Phone #= 5551230                 Call Filter Sets=
  Sec Phone #= 5551231                 Idle Timeout(sec)= 300

              Press ENTER to Confirm or ESC to Cancel:
```

1. **Rem Node Name—**This is a required field. Enter a descriptive name for the Remote Node, e.g., SJHQ. The name can be up to

eight characters long, and must be different from any other Remote Node name or Remote Dial-in User name.

2. **Active—**Press the space bar to toggle between Yes and No. When a Remote Node is deactivated, it has no effect on the operation of the router, even though it is still kept in the database, and can be activated in the future. Deactivated nodes are displayed with a minus sign [-] at the beginning of the name in menu 11.

3. **Call Direction—**If this parameter is set to Both, your DI-106 or DI-106M can both place and receive calls to/from this Remote Node. If set to Incoming, the router will not place a call to this Remote Node. If set to Outgoing, the router will drop any call from this Remote Node.

   Several other fields in this menu depend on this parameter. For example, in order to enable Call Back, the Call Direction must be Both.

4. **Incoming: Rem Node Login Name**—Enter the login name that this Remote Node will use when it calls into the router. The login name in this field combined with the Rem Node Password will be used to authenticate the incoming calls from this node.

5. **Incoming: Rem Node Password**—Enter the password used when this Remote Node calls into the router.

6. **Incoming: Rem CLID**—This control is active only if the Call Direction control is set to either Both or Incoming. Otherwise, N/A appears here. This is the Calling Line ID (the telephone number of the calling party) of this Remote Node. If you enable the CLID Authen field in menu 13, Default Dial In, the router will check this number against the CLID in the incoming call. If they do not match and the CLID Authen control is set to Required, the router will reject the call.

7. **Incoming: Call Back**—This field will be valid only if Call Direction is Both. Otherwise, an N/A appears in the field. This field determines whether or not you wish the router to call back after receiving a call from this Remote Node. If this option is enabled, the router will disconnect the initial call from this node and call it back at the Outgoing Primary Phone Number (see below).

8. **Outgoing: My Login Name**—This is a required field if Call Direction is either Both or Out. Enter the login name for the router when it calls this Remote Node. If the login name is longer than 24 characters, only the first 23 will be displayed, with a + displayed at the end.

9. **Outgoing: My Password**—This is a required field if Call Direction is either Both or Out. Enter the password for the router when it calls this Remote Node. If the password is longer than 20 characters then a + will be displayed at the end.

10. **Outgoing: Authen—**This field sets the authentication protocol used for outgoing calls.

    Your DI-106 or DI-106M supports two authentication protocols: PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol).

    ◊ **PAP** sends the user name and password in plain text.

    ◊ **CHAP** scrambles the password before it is sent over the wire.

    Generally speaking, CHAP is more secure than PAP; however, PAP is readily available on more platforms. The recommendation is to use CHAP whenever possible. Turning off the authentication is STRONGLY discouraged.

Options for this field are:

- ◊ **CHAP/PAP**—The router will try CHAP when CHAP is requested by the Remote Node or PAP when PAP is requested by the Remote Node.
- ◊ **CHAP**—use CHAP only.
- ◊ **PAP**—use PAP only.

11. **Outgoing: Pri(mary) Phone Sec(ondary) Phone Number**—Both the Primary Phone number and the Secondary Phone number refer to the number that the router will dial to connect to the Remote Node. The router will always call the Remote Node using the Primary Phone number first. If the Primary Phone number is busy or does not answer, the router will call the Secondary Phone number if available. Once connected, the router will use the BACP (Bandwidth Allocation Control Protocol) to establish the second B-channel if Multilink PPP is enabled, and the Remote Node supports MP and BACP.

    Some areas require dialing # before the phone number for local calls. A # symbol may be included at the beginning of the Primary Phone number or Secondary Phone number.

12. **Route**—This fields determines the protocols that your DI-106 or DI-106M will route. The choices for this field are determined by the features enabled on your router.

13. **Bridge**—Bridging is used (on the DI-106M only) for protocols that are not supported or not turned on in the previous Route field, e.g., SNA. When bridging is enabled, the DI-106M will forward any packet that it does not recognize to this Remote Node; otherwise, the unrecognized packets are discarded. The disadvantage of bridging is that it usually generates large

amounts of traffic. Press the space bar to select either Yes or No.

14. **Edit PPP Options**—To edit the PPP options for this Remote Node, move the cursor to this field, use the space bar to select **Yes** and press **ENTER**. This will bring you to menu 11.2, Remote Node PPP Options. For more information on configuring PPP options, see the section entitled "Editing PPP Options."

15. **IP Addr**—This is a required field if Route is set to IP. Enter the IP address of this Remote Node.

16. **Edit IP/IPX/Bridge Options**—To edit the parameters of the protocols, go to this field, select Yes and press ENTER. This will bring you to menu 11.3, Remote Node Network Layer Options. For more information on filling out this screen, refer to the chapter pertaining to your specific protocol.

17. **Telco Options: Transfer Rate**—This field (which only applies to outgoing calls) controls the rate at which the data is transferred between your router and the Remote Node. The options for this field are:

    ◊ **64K**—The router will place 64-kbps (kilobits per second) digital data calls.

    ◊ **56K**—(For North America only) The router will place 56-kbps digital data calls.

    ◊ **Lease line**—The router will place leased-line calls.

    ◊ **DOVBS**—This option is for North America only. The router will place 56-kbps Data Over Voice Bearer Service (DOVBS) calls. Some phone companies in North America charge less if calls are made with the DOVBS option.

18. **Telco Options: Allocated Budget (min)—**This field will set a budget outgoing call time for the Remote Node. The default for this field is 0 for no budget control.

19. **Telco Options: Period (hr)—**This field will set the time interval to reset the above outgoing call budget control.

20. **Session Option: Input Filter Sets, Output Filter Sets and Call Filter Sets**—In these fields, select which filter set(s) you would like to implement to filter the incoming and outgoing traffic between this Remote Node and the router. You can choose from 12 different filter sets. In addition, you can link up to 4 filter sets together for further customization (e.g., 1, 5, 9, 12). Note that spaces and commas are accepted in this field.

    For more information on customizing your filter sets, see the *Filter Configuration* chapter starting on page 103. The default is blank, i.e., no filters defined.

21. **Session Option: Idle Timeout (sec)—**This value specifies the number of idle seconds that elapses before the Remote Node is automatically disconnected. Idle seconds is the period of time where no data is passed between the Remote Node and your DI-106 or DI-106M. Administrative packets such as RIP are not counted as data. The default is 300 seconds (5 minutes).

Once you have finished filling in menu 11.1, Remote Node Profile, press ENTER at the message 'Press ENTER to Confirm...' to confirm your selections, or press ESC at any time to cancel your selections.

Bandwidth on Demand

The Bandwidth on Demand (BOD) feature allows you to bundle both B channels in one connection. The second channel is added

and subtracted dynamically according to traffic demand. The router uses the Bandwidth Allocation Control Protocol (BACP) and the Multilink Protocol (MP) to implement bandwidth on demand.

The configuration of bandwidth on demand focuses on the Base Transmission Rate (BTR) and the Maximum Transmission Rate (MTR). The relationship between BTR and MTR are shown below:

BTR & MTR Setting	No. of channel(s) used to initiate call	Max No. of channel(s) used	Bandwidth on demand
BTR = 64, MTR = 64	1	1	Off
BTR = 64, MTR = 128	1	2	On
BTR = 128, MTR = 128	2	2	Off

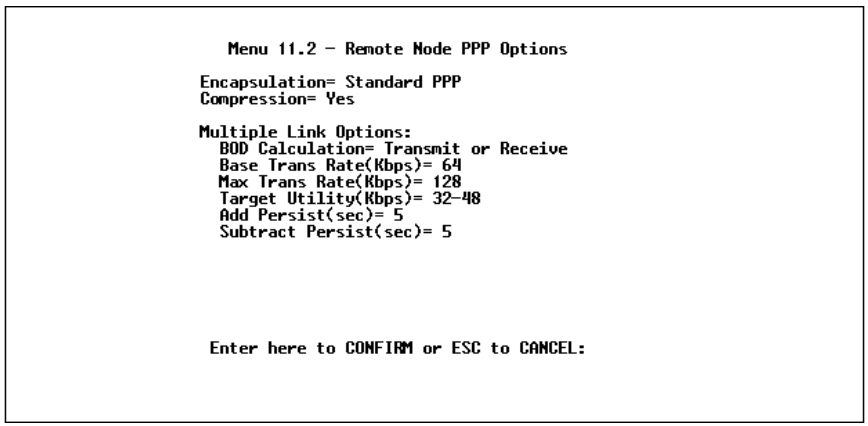
When bandwidth on demand is enabled, a second channel will be brought up if traffic on the initial channel is higher than the high Target Utility number for longer than the specified Add Persist value. Similarly, the second channel will be dropped if the traffic level falls below the low Target Utility number for longer than the Subtract Persist value.

The Target Utility specifies the line utilization range at which you want your DI-106 or DI-106M to add or subtract bandwidth. The range is 30 to 64 kbps (kilobits per second). The parameters are separated by a hyphen [-]. For example, 30-60 means the add threshold is 60 kbps and subtract threshold is 30 kbps. The router will perform bandwidth on demand only if it initiates the call. Addition and subtraction are based on the value set in the BOD Calculation field. If this field is set to Transmit or Receive, then traffic in either direction will be calculated to determine if a link should be added or dropped. Transmit will only use outgoing traffic

to make this determination, and Receive will only use incoming traffic to make this determination.

If, after making the call to bring up a second channel, the second channel does not succeed in joining the Multilink Protocol bundle (because the remote device does not recognize the second call as coming from the same device), the router will hang up the second channel and continue with the first channel alone.

Editing PPP Options



1. **Encapsulation—**Select CCP (Compression Control Protocol) for the PPP or MP link. There are two options in this field.
   - ◊ **Standard PPP**—Standard PPP options will be used.
   - ◊ **CISCO PPP—**Cisco PPP options will be used.
2. **Compression—**Turn on Stac Compression. The default setting for this control is No.

3. **Multiple Link Options: BOD Calculation**—Select the direction of the traffic you wish to calculate in order to determine when to add or subtract a link. The default for this field is Transmit or Receive.

4. **Multiple Link Options: Base Trans Rate**—Select the base data transfer rate for this Remote Node. This parameter is in kbps (kilobits per second). There are two options for this field:

   ◊ **64**—Only one channel will be used.

   ◊ **128**—Two channels will be used when a packet triggers a call.

5. **Multiple Link Options: Max Trans Rate—**Enter the maximum data transfer rate allowed for this Remote Node. This parameter is in kilobits per second. There are two options for this field:

   ◊ **64**—At most one channel can be used.

   ◊ **128**—A maximum of two channels can be used.

6. **Multiple Link Options: Target Utility**—Enter the two thresholds, separated by a hyphen [-], for subtracting and adding the second channel. The default is 32-48.

7. **Multiple Link Options: Add Persist**—This parameter specifies the number of seconds where traffic is above the adding threshold before the router will bring up the second channel. The default is 5 seconds.

8. **Multiple Link Options: Subtract Persist**—This parameter specifies the number of seconds where traffic is below the subtraction threshold before the router drops the second channel. The default is 5 seconds.

Once you have completed menu 11.2, Remote Node PPP Options, press **ENTER** at the message 'Press ENTER to Confirm...' to confirm your selections, or press **ESC** to cancel your selections.

Dial-In Configuration

You can configure your DI-106 or DI-106M to receive calls from Remote Dial-in Users (e.g., telecommuters) and Remote Nodes. There are several differences between Remote Dial-in Users and Remote Nodes:

1. The router can make calls to or answer calls from a Remote Node. However, it will only answer calls from Remote Dial-in Users.
2. Each Remote Node can have its own set of parameters such as Bandwidth On Demand, Protocol, Security, etc., while all Remote Dial-in Users share one common set, as defined in the Default Dial In Setup (menu 13).
3. Generally, Remote Dial-in Users are individual users who dial in to the DI-106 or DI-106M directly from their workstations, while Remote Nodes represent networks and are used for LAN-to-LAN connections.

This chapter discusses how to set up Default Dial-in parameters for both Remote Node and Remote Dial-in Users. The following sections give two examples of how a DI-106 or DI-106M can be configured as a dial-in server for either or both.

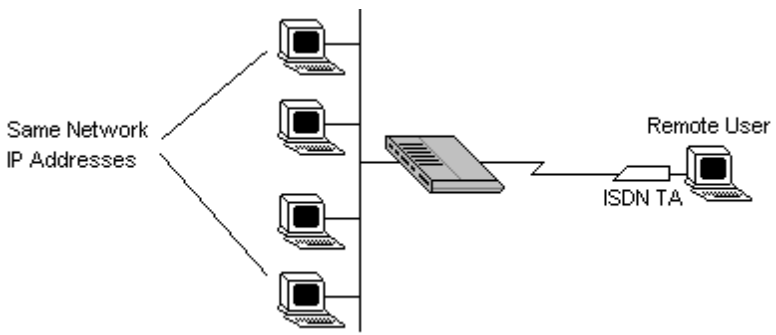
By default, your DI-106 or DI-106M allows information for up to eight users to be kept. To let more than eight remote dial-in users access a DI-106M, you can use a separate RADIUS server to provide remote authentication services. For details on using a

separate RADIUS server, see the *Using RADIUS Authentication* section on page 124.

Telecommuting

Telecommuting enables people to work at remote sites and still have access to the resources in the business office. Typically, a telecommuter will use a client workstation with TCP/IP or IPX and dial-out capabilities, e.g., a Windows 95 PC or a Macintosh and an ISDN Terminal Adapter (TA). For telecommuters to call in to your LAN, you need to configure a Dial-In User Profile for each telecommuter. Additionally, you need to configure the Default Dial-In Setup to set the operational parameters for all dial-in users. You can configure up to eight Remote Dial-in Users for your DI-106 or DI-106M.

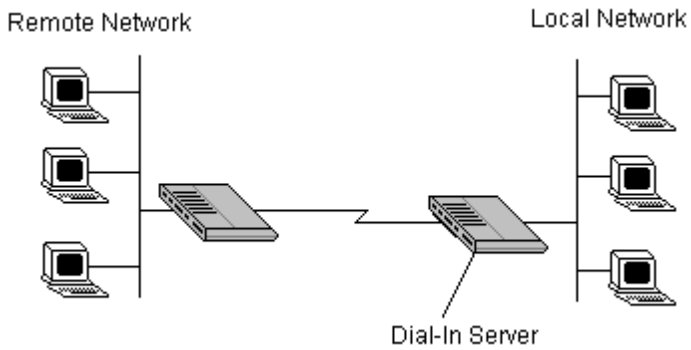
An example of Remote Dial-in User application, telecommuting, is shown below:



Dial-In Server Application

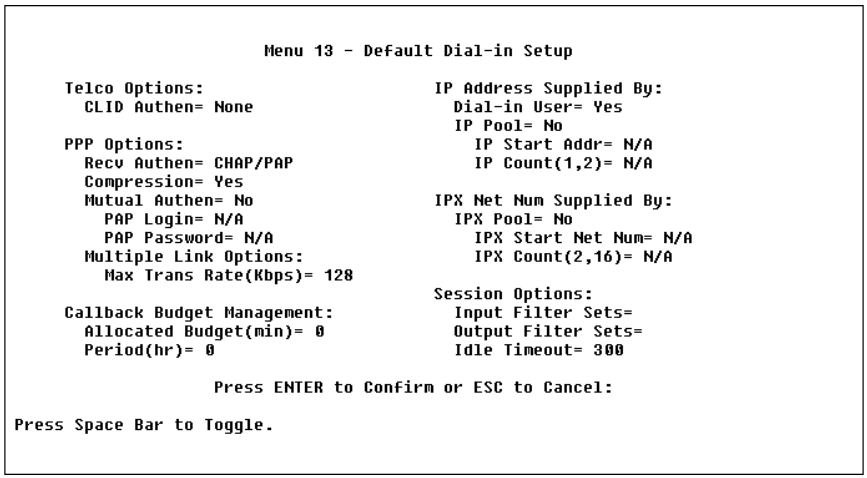
A DI-106 or DI-106M can also be used as a dial-in server. This application allows the router to provide services for

workstations on a remote network. For the router to be set up as a dial-in server, you need to configure the Default Dial-In Setup to set the operational parameters for incoming call. Additionally, you will have to create a Remote Node for the router on the remote network (see the *Remote Node Configuration* chapter starting on page 57). An example of a DI-106 or DI-106M being used as a dial-in server is shown below:



Default Dial-In Setup

This section covers the default dial-in parameters. The parameters in menu 13 affect incoming calls from all Remote Dial-in Users and Remote Nodes before authentication is completed. Once authentication is completed, and if it matches a Remote Node, the router will use parameters from that particular Remote Node.



From the main menu, enter 13 to go to menu 13, Default Dial-in Setup. This section will describe how to configure the protocol-independent fields in this menu. For the protocol-dependent fields, refer to the appropriate chapters.

1. **Telco Options: CLID Authen.**—This field sets the CLID authentication parameter for all incoming calls. There are three options for this field:
   - ◊ **None**—No CLID is required.
   - ◊ **Required**—Must provide CLID, or call is disconnected.
   - ◊ **Preferred**—If the CLID is available then CLID will be used to do authentication. If the CLID is not available the call will continue.
2. **PPP Options: Recv. Authen.—**This field sets the authentication protocol used for incoming calls. User names and passwords are configured in the next section (Remote users/Dial-in Users Setup). Options for this field are:

- ◊ **CHAP/PAP**—The router will try CHAP first, but PAP will be used if CHAP is not available.
- ◊ **CHAP**—Use CHAP only.
- ◊ **None**—No authentication required.

3. **PPP Options: Compression**—The setting in this field determines if Stac compression will be used. The default setting is **Yes**.
4. **PPP Options: Mutual Authen.**—Some vendors, e.g. Cisco, implement a type of mutual authentication. That is, the node that initiates the call will request a user name and password from the far end that they are dialing to. If the Remote Node that is dialing in implements this type of authentication, set this field to Yes.
5. **PAP Login—**This field will only be enabled if the Mutual Authen. field is set to Yes. Enter in the login name to be used to respond to the far end's PAP authentication request. This field does not apply to CHAP authentication.
6. **PAP Password**—This field will only be enabled if the Mutual Authen. field is set to Yes. Enter in the PAP password to be used to respond to the far end's authentication request. This field does not apply to CHAP authentication.
7. **Multiple Link Options: Max Trans Rate—**Enter the maximum data transfer rate between your router and the Remote Dial-in User. The unit is kbps (kilobits per second). There are two options for this field:
   - ◊ **64—**At most, one B channel will be used.
   - ◊ **128—**A maximum of two channels can be used.

When the DI-106 or DI-106M calls back to the Remote Dial-in User the maximum data transfer rate is always 64.

8. **Callback Budget Management: Allocated Budget (min)—** This field will set a budget callback time for all the Remote Dial-in Users. The default for this field is 0 for no budget control.
9. **Callback Budget Management: Period (hr)—**This field will set the time interval to reset the above callback budget control.
10. **Dial-In IP Address Supplied By**: **Dial-in User—**If set to Yes, it tells the DI-106 or DI-106M to allow a remote host to specify its own IP address. This is to prevent the remote host from using an invalid IP address and potentially disrupting the whole network. If set to No, the remote host must use the IP address assigned by the DI-106 or DI-106M from the IP pool, configured below. The default is Yes.
11. **Dial-In IP Address Supplied By: IP Pool—**This field tells your DI-106 or DI-106M to provide the remote host with an IP address from the pool. This field is required if Dial-In IP Address Supplied By: Dial-in User is set to No. You can configure this field even if Dial-in User is set to Yes, in which case the DI-106 or DI-106M will accept the IP address if the remote peer specifies one; otherwise, an IP address is assigned from the pool. If Dial-in User is Yes and this field is No, the remote peer *must* supply its own IP address, or communication will not be possible. The default is No.
12. **IP Pool: IP Start Addr—**This field is active only if you selected Yes in the Dial-In IP Address Supplied By: IP Pool field. The IP pool contains contiguous IP addresses and this field specifies the first one in the pool.
13. **IP Count (1,2)**—In this field, enter the number (1 or 2) of the addresses in the IP Pool. For example, if the starting address is

192.168.135.5 and the count is 2, then the pool will have 192.68.135.5 and 192.68.135.6

14. **Dial-In IPX Net. Num. Supplied By: IPX Pool—**This field tells the DI-106M to provide the remote host with an IPX network number from the pool. Otherwise, the router will generate a random IPX network number. The default is No.

15. **IPX Start Net. Num.—**This field is active only if you selected Yes in the Dial-In IPX Net. Num. Supplied By: IPX Pool field. The IPX pool contains contiguous IPX network numbers and this field specifies the first one in the pool.

16. **IPX Count (1,16)**—In this field, enter the number (1–16) of network numbers in the IPX Pool. For example, if the starting number is 12345678, and the count is 2, then the pool will have 12345678 and 12345679.

17. **Session Options: Input Filter Sets** and **Session Options: Output Filter Sets—**In these fields, you need to select the filter set(s) to filter the incoming and outgoing traffic between your DI-106 or DI-106M and the Remote Dial-in User. Keep in mind that these filter set(s) will only apply to all Remote Dial-in Users but not the Remote Nodes.

    You can choose from 12 different filter sets. In addition, you can link up to 4 filter sets together for further customization (e.g., 1, 5, 9, 12). Note that spaces and commas are accepted in this field. For more information on customizing your filter sets, see the *Filter Configuration* chapter on page 103. The default is blank, i.e., no filters.

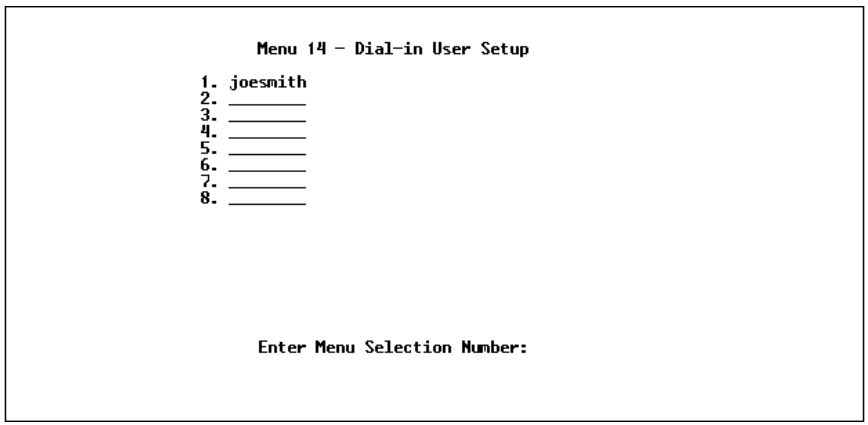
18. **Session Options: Idle Timeout—**This value is the number of idle seconds that elapses before the dial-in user is automatically disconnected. Idle Timeout is the period of time when there is no data traffic between the dial-in user or Remote Node and the

router. This field will only be used if Recv. Authen is set to None and the call is not mapped to any Remote Node or Remote Dial-in User, or the router calls back to the Remote Dial-in User.

Once you are finished filling in menu 13, Default Dial-in Setup, press **ENTER** at the message 'Press ENTER to Confirm...' to save your selections, or press **ESC** at any time to cancel your selections.

Dial-In Users Setup

The following steps describe the setup procedure for adding a Remote Dial-in User. From the main menu, enter 14 to go to menu 14, Dial-in User Setup. This menu is shown below:



Select one of the eight possible users by number. This will bring you to the next screen, menu 14.1, Edit Dial-in User.

```
                Menu 14.1 - Edit Dial-in User

        User #: 1
        User Name= joesmith
        Active= Yes
        Passwd= ********
        Callback= No
          Phone # Supplied by Caller= N/A
          Callback Phone #= N/A
        Rem CLID=
        Idle Timeout= 300




        Press ENTER to Confirm or ESC to Cancel:
```

1. **User Name**—This is a required field. This will be used as the login name for authentication. Choose a descriptive word for login, e.g., kathyg.
2. **Active—**You can disallow dial-in access to this user by setting this field to Inactive. When set to inactive, the user record is still kept in the database for later activation. Deactivated users are displayed with a hyphen [-] at the beginning of the name in menu 14.
3. **Password—**Enter the password for the Remote Dial-in User.
4. **Callback—**This field determines if the DI-106 or DI-106M will allow callback to the Remote Dial-in User upon dial-in. If this control is set to Optional, the router will be able to call back to the Remote Dial-in User if so requested by that user's system; if the control is set to Mandatory, the router will attempt callback in all cases. Callback entails disconnecting the call and dialing the specified callback number (see below). The default setting of this control is No.

5. **Phone # Supplied by Caller—**This control allows the Remote Dial-in User to specify the callback telephone number on a call-by-call basis. This is useful for when the DI-106 or DI-106M returns a callback to a mobile user at different numbers, e.g., a sales rep in a hotel. Note that the default is No, i.e., the router always calls back to the fixed callback number.
6. **Callback Phone #—**If Callback is Yes, then this is a required field. Otherwise, N/A will appear in the field. Enter the telephone number to which the router will call back.
7. **Rem CLID—**If you have enabled the CLID Authen field in menu 13, you need to specify the telephone number from which this Remote Dial-in User calls. The DI-106 or DI-106M will check this number against the CLID in the incoming call. If they do not match and the CLID Authen is Required, the router will reject the call.
8. **Idle Time-out—**Enter the idle time (in seconds). This time-out determines how long the dial-in user can be idle before the DI-106 or DI-106M disconnects the call. Idle time is defined as the period of time where there is no data traffic between the dial-in user and the router. The default is 300 seconds (5 minutes).

More on CLID

CLID allows your DI-106 or DI-106M to authenticate the caller before a call is answered, thus saving the cost of a connection. The router uses the caller ID in the ISDN call setup message to match against the CLID in the database.

However, CLID may not be available due to your switch configuration.

Besides authentication, another application of CLID is to *combine* it with callback. For instance, your company pays for the connection charges for telecommuting employees, and you are using the DI-106 or DI-106M as the dial-in server. You can turn on both the CLID authentication and callback options for the dial-in users. By doing so, all usage are charged to the company instead of the employees, and your accounting department can avoid the hassles of accountability and reimbursement.

Once you are finished filling in menu 14.1, Edit Dial-in User, press **ENTER** at the message 'Press ENTER to Confirm...' to save your selections, or press **ESC** at any time to cancel your selections.

TCP/IP Configuration

This chapter shows you how to configure your DI-106 or DI-106M for TCP/IP. Depending on your particular applications, you will need to configure different menus. For instance, Internet access is the most common application of TCP/IP. For this application, you should configure menu 4. We will illustrate the configuration for other applications in the following sections.

IP Subnet Mask

A subnet mask is a 32-bit quantity that, when logically ANDed with an IP address, yields the network number. For instance, the subnet masks for class A, B and C networks without subnetting are 255.0.0.0, 255.255.0.0 and 255.255.255.0, respectively.

To create more network numbers, you shift some bits from the host ID to the network ID. For instance, to partition a class C network number 192.68.135.0 into two, you shift 1 bit from the host ID to the network ID. Thus the new subnet mask will be 255.255.255.128; the first subnet will have network number 192.68.135.0 with hosts 192.68.135.1 to 129.68.135.126 and the second subnet will have network number 192.68.135.128 with hosts 192.68.135.129 to 192.68.135.254.

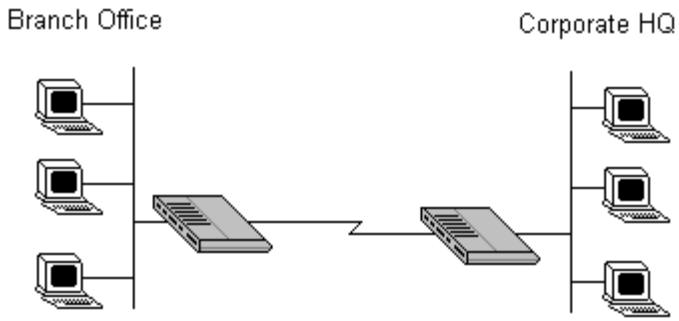
It is recommended that you use the same subnet mask for all physical networks that share an IP network number. The table below lists the additional subnet mask bits in dot decimal notations. To use to following table, write down the original subnet mask and substitute the higher order 0s with the dot decimal of the additional

subnet bits. For instance, to partition your class C network 204.247.203.0 with subnet mask 255.255.255.0 into 16 subnets (4 bits), the new subnet mask becomes 255.255.255.240.

Number of Bits	Dot Decimal
1	128
2	192
3	224
4	240
5	248
6	252
7	254
8	255

LAN-to-LAN Application

A typical LAN-to-LAN application is to use the DI-106 or DI-106M to call from a branch office to the headquarters, as depicted in the following diagram.



For the branch office, you need to configure a Remote Node in order to dial out to the headquarters. Additionally, you may also need to configure Static Routes if some services reside beyond the immediate remote LAN.

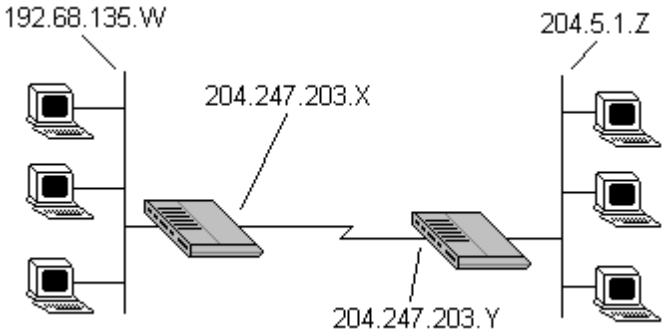
Remote Node Setup

Follow the procedure in the *Remote Node Configuration* chapter starting on page 57 to fill the protocol-independent parameters in menu 11, Remote Node Profile. For the protocol-dependent parameters, follow the instructions below. If you are configuring the router to receive an incoming call, you also need to set the default dial-in parameters in menu 13 (see the chapter entitled *Dial-In Configuration*, starting on page 68).

1. **Route**—Make sure IP is among the protocols in the Route field.
2. **IP Address**—Enter the IP address of the gateway at the remote site (in this case, headquarters). If the remote router is using a different IP address than the one entered here, your DI-106 or DI-106M will drop the call.
3. **Edit IP/IPX/Bridge**—Press the space bar to change the setting to Yes and press Enter to go to menu 11.3, Remote Node Network Layer Options. This menu is shown below:

```
                Menu 11.3 - Remote Node Network Layer Options

    IP Options:                          IPX Options:
      Rem IP Addr:                         Dial-On-Query= Yes
      Rem Subnet Mask= N/A                 Rem LAN Net #= 01001234
      My WAN Addr= N/A                     My WAN Net #= 00000000
      Single User Account= N/A             Hop Count= 1
        Server IP Addr= N/A                Tick Count= 2
      Metric= N/A                          W/D Spoofing(min)= 3
      Private= N/A                         SAP/RIP Timeout(min)= 3
      RIP Direction= N/A
        Version= N/A                     Bridge Options:
                                           Dial-On-Broadcast= N/A
                                           Ethernet Addr Timeout(min)= N/A




                    Enter here to CONFIRM or ESC to CANCEL:

Press Space Bar to Toggle.
```

1. **Rem IP Address**—This will show the IP address you entered for this Remote Node in the previous menu.
2. **Rem IP Subnet Mask**—Enter the subnet mask for the remote network.
3. **My WAN Addr**—Some implementations, especially the UNIX derivatives, require hosts on both ends of the ISDN link to have separate addresses from the LAN, and that the addresses must have the same network number. If this is the case, enter the IP address assigned to the WAN port of your DI-106 or DI-106M. Note that this is the address assigned to the local DI-106 or DI-106M, not the remote router.



1. **Single User Account—**This field should be set to yes to enable the Single User Account (Network Address Translator) feature for this site. Use the space bar to toggle between yes and no. See page 52 for more information on the Single User Account feature.
2. **Server IP address—**If you are using the Single User Account feature and you want to make a server accessible on your LAN, e.g., a web server, accessible to outside users, enter that servers IP address here.

3. **Metric**—The metric represents the "cost" of transmission for routing purpose. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 16. In practice, 2 or 3 is usually a good number.

4. **Private**—This parameter determines if your DI-106 or DI-106M will include the route to this Remote Node in its RIP broadcasts. If set to yes, this route is kept private and not included in RIP broadcasts. If no, the route to this Remote Node will be propagated to other hosts through RIP broadcasts.

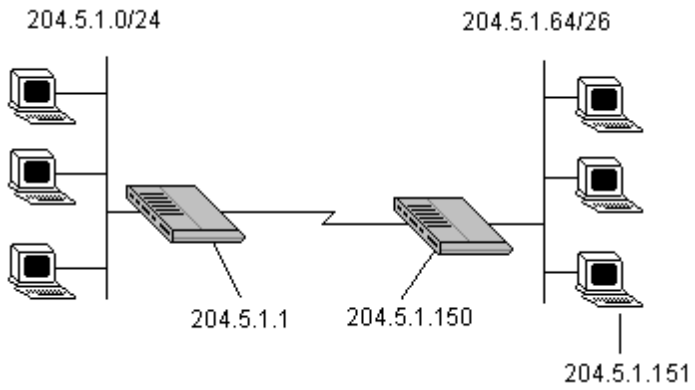
5. **RIP**—This parameter determines how your DI-106 or DI-106M handles RIP (Routing Information Protocol), and the default is Both. If set to Both, your router will broadcast its routing table on the WAN and incorporate RIP broadcasts from the other router into its routing table. If set to In Only, your router will not broadcast its routing table on the WAN; if set to Out Only, it will broadcast its routing table but ignore any RIP broadcast packets that it receives. If set to None, your DI-106 or DI-106M will not participate in any RIP exchange with other routers. Usually, you should leave this parameter at its default of Both and let RIP propagate the routing information automatically.

Once you have completed filling in the Network Layer Options menu, press **ENTER** to return to menu 11. Press ENTER at the message 'Press ENTER to Confirm...' to save your selections, or press **ESC** at any time to cancel your selections.

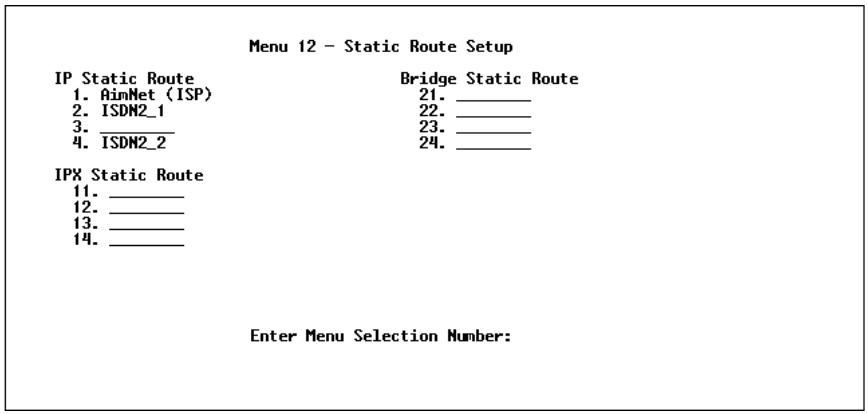
Static Route Setup

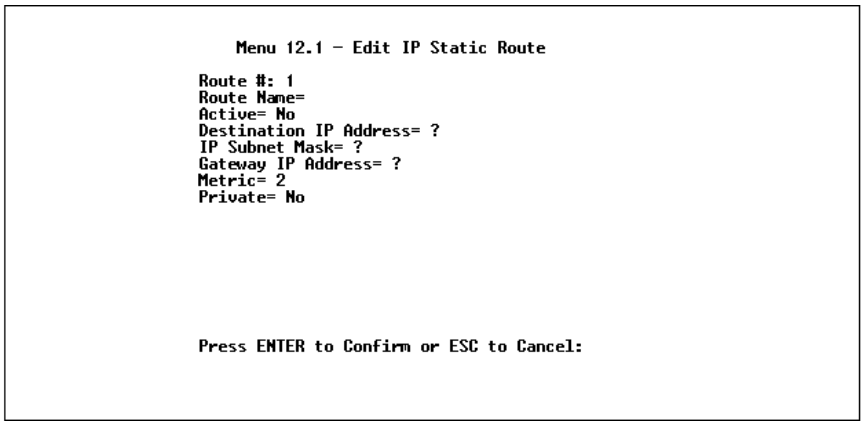
On a directly connected internet, RIP usually handles the routing automatically. However, RIP cannot propagate across isolated

networks, as in the case before a connection is made between the two subnetworks using one Class C IP address. Without a route, no packets can be forwarded to their destinations. A static route is used to resolve this problem by providing the DI-106 or DI-106M with some static routing information. As a matter of fact, when you configure the Internet Access or a Remote Node, a static route is implicitly created. An example is given below. In the example, stations on the 204.5.1.0/24 subnetwork can access the remote stations using the static route. The route will have a destination of 204.5.1.64/26 with the gateway address being that of the Remote Node (204.5.1.150).



Note that in normal circumstances, your DI-106 or DI-106M will have adequate routing information after you configure it for Internet access and Remote Nodes; you do not need to configure additional static routes. You will need to configure static routes only for unusual cases, e.g., subnetting. To create additional static routes for IP, use menu 12, Static Route Setup, as shown below:





1. **Route Name**—Enter a descriptive name for this route. This is for identification purpose only.
2. **Active**—This fields allows you to activate/deactivate this static route.
3. **Destination IP Address**—This parameter specifies the IP *network* address of the final destination. Routing is always based

on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.

4. **IP Subnet Mask**—Enter the subnet mask for this destination. Follow the discussion on IP subnet mask in this chapter.

5. **Gateway IP Address**—Enter the IP address of the gateway. The gateway is an *immediate* neighbor of the DI-106 or DI-106M that will forward packets to the destination. On the LAN, the gateway must be a router on the same segment as the DI-106 or DI-106M; over ISDN, the gateway must be the IP address of one of the Remote Nodes.

6. The **Metric** and the **Private** parameters have the same meaning as those in the Remote Node Setup.

Once you are finished filling in the menu, press **ENTER** at the message 'Press ENTER to Confirm...' to save your selections, or press **ESC** at any time to cancel your selections.

Novell IPX Configuration

This chapter shows you how to configure the DI-106M for IPX. Depending on your particular applications, you will need to configure different menus. We will illustrate the configuration for some applications in the following sections.

IPX Network Environment

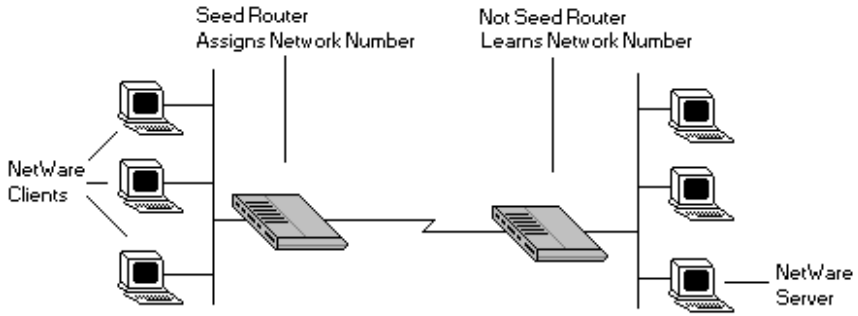
Frame Type

The stations on an IPX network (both clients and servers) can run on four different frame types existing on one physical Ethernet cable. These frame types are 802.2, 802.3, Ethernet II (DIX), and SNAP.

Network Numbers

Whenever you are setting up an IPX routing environment, it is important to correctly configure the network numbers on the LAN. On any IPX network, there is an external network number, that is, the number associated with the frame type on the Ethernet cable to which the stations on the network are joined. In addition to this external network number, each NetWare server has its own internal network number. It is important to remember that every network number has to be unique for that entire internetwork. So if a server station has an internal network number of 00000011, there must be no other network number (internal or external) of 00000011 anywhere on the entire network.

There are two different scenarios in which you would connect your DI-106M to a LAN: one with a server (server side), and one without a server (client side).



DI-106M on LAN with Server

If the DI-106M will be connected to a LAN with an existing NetWare server, you will not need to configure the DI-106M as a seed router, and hence there will be no need for a network number parameter in the Ethernet Setup menu for the DI-106M. Rather, the DI-106M will learn the network number of the network it is attached to through the regular RIP broadcasts sent by the server, and it will add this route to its routing table.

DI-106M on LAN without Server

If the DI-106M is connected to a LAN without an existing NetWare server station, then it needs to create a unique external network number to apply to that frame on the LAN. This DI-106M must then be configured as a Seed Router, and the network number can be configured in the Ethernet Setup menu.

The network number must be unique and not used anywhere else on the entire internetwork.

IPX Spoofing

The DI-106M comes with several pre-defined call filters designed to prevent certain IPX packets from triggering a call to a Remote Node. These filters should inform your DI-106M which packets should be ignored as traffic.

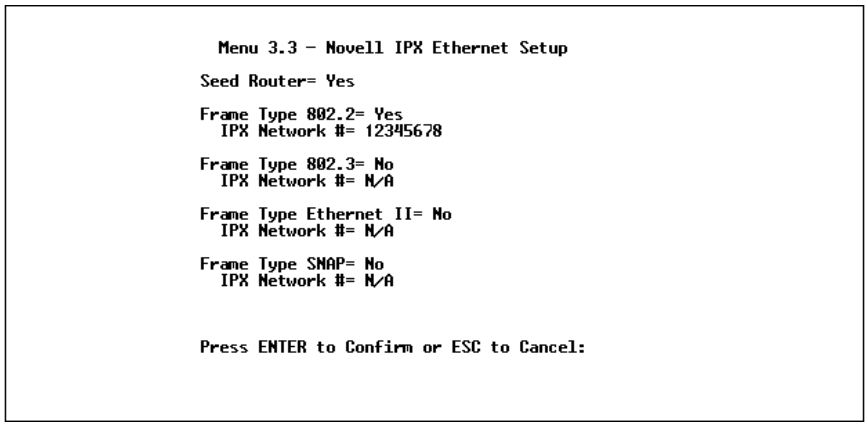
When you are routing IPX packets, the default call filters are defined as follows:

- Block periodical SAP and RIP response messages.
- Block NetWare serialization packets.
- Allow SAP and RIP inquiry packets.

These call filters prevent the DI-106M from making a call to the Remote Node, thus preventing the expense of an unnecessary phone call.

IPX Ethernet Setup

The first step is to set up the DI-106M on the LAN. From menu 3, select option 3 to go to menu 3.3, Novell IPX Ethernet Setup. This menu is shown below:



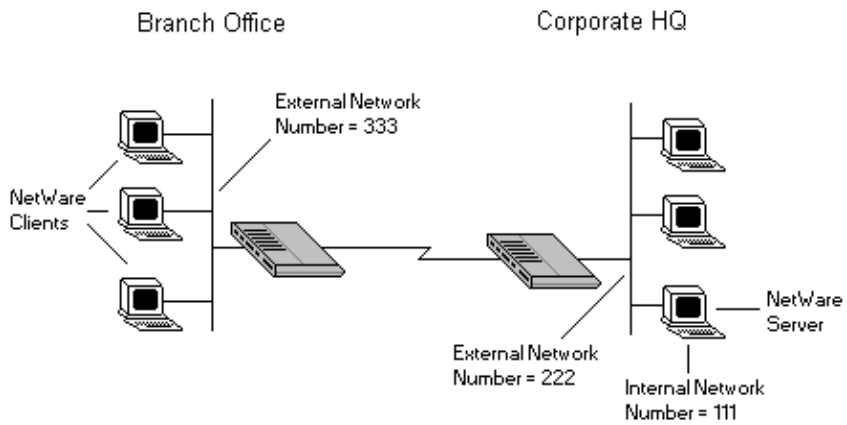
1. **Seed Router**—Determine if the DI-106M is to act as a seed router. This value depends on the existing network. If there is a NetWare server providing the network number, select No. If there is no NetWare server providing the network number, select Yes.
2. **Frame Type**—For every frame type that the DI-106M needs to support, you need to set the corresponding field to Yes. The frame type(s) selected here must be the same frame type(s) as the server or client stations on that network. Otherwise, the devices will not be able to communicate. You can select one or more of these four frame types:
   - ◊ 802.2
   - ◊ 802.3
   - ◊ Ethernet II
   - ◊ SNAP
3. **IPX Network #**—If you selected the DI-106M to act as a seed router, you need to provide a unique network number to be

associated with the network that the DI-106M has joined. Keep in mind that this number must not be used anywhere else on the entire internetwork.

Once you are finished filling in menu 3.3, press **ENTER** at the Save message to save your selections, or press **ESC** at any time to cancel your selections.

LAN-to-LAN Application

A typical LAN-to-LAN application is to use the DI-106M to call from a branch office to headquarters such that all of the stations on the branch office network have access to the server at the headquarters, as depicted in the following diagram:

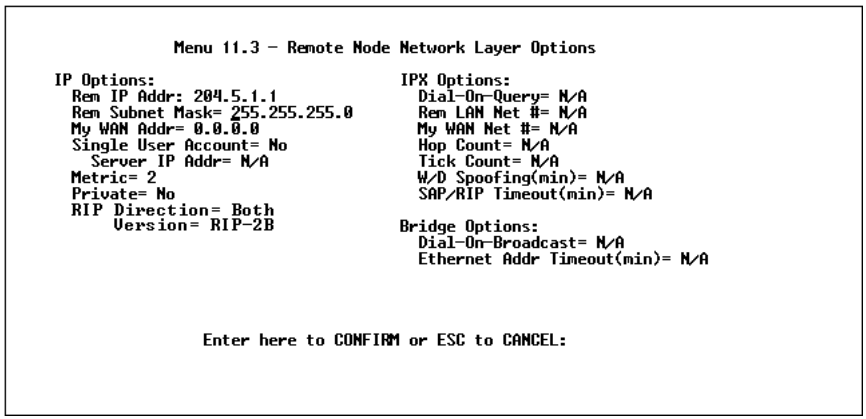


For the branch office, you need to configure a Remote Node in order to dial out to headquarters.

Remote Node Setup

Follow the instructions in the chapter entitled *Remote Node Configuration*, starting on page 57, to fill in the protocol-independent parameters in menu 11, Remote Node Profile. For the protocol-dependent parameters, follow the instructions below. If the DI-106M is configured to receive incoming calls, you can configure the default dial-in parameters in menu 13 (see the chapter entitled *Dial-In Configuration*, starting on page 68).

1. Route—Make sure IPX is among the protocols in the Route field.
2. Edit IP/IPX/Bridge—Press the space bar to change the setting to Yes, then press Enter to go to the Remote Node Network Layer Options menu.



1. **Dial-On-Query**—This field is necessary for the DI-106M on the client side LAN. When set to Yes, any "Get Service" SAP or RIP broadcasts coming from the LAN will trigger the DI-106M

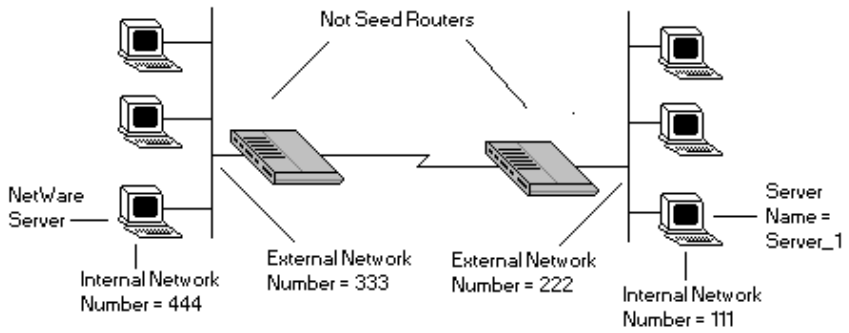
to make a call to that Remote Node. If it is set to No, the DI-106M will not make the outgoing call.

2. **Rem LAN Net #**—In this field, enter the internal network number of the NetWare server on the remote side LAN. The router will create a route to access this server.
3. **My WAN Net #**—In this field, you can enter in the WAN network number of the device that you are connecting to. This number will be used for negotiation between the router and the remote device. If you leave this field as 00000000, the router will select the greater WAN network number between the two devices.
4. **Hop Count**—This field indicates the number of intermediate networks that must be passed through to reach the Remote Node. The default is one (1).
5. **Tick Count**—This field indicates the time-ticks required to reach the Remote Node. The default is two (2).
6. **W/D Spoofing (min)**—This field is used for the router when it is on the server side LAN. The router can spoof a response to a server's watchdog request after the connection is dropped. In this field, enter in the time (number of minutes) that you want the router to spoof the watchdog response.
7. **SAP/RIP Timeout (min)**—This field indicates the amount of time that you want the router to maintain the SAP and RIP entries learned from this Remote Node in its internal tables after the connection has been dropped. If this information is retained, then the router will not have to get the SAP information when the line is brought back up. Enter the time (number of minutes) in this field.

Once you have completed filling in the Network Layer Options menu, press **ENTER** to return to menu 11.1. Press **ENTER** at the message 'Press ENTER to Confirm...' to save your selections, or press **ESC** at any time to cancel your selections.

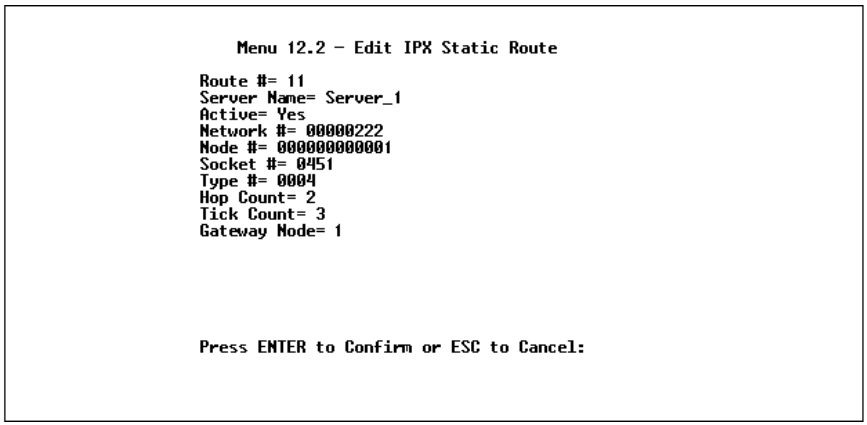
Static Route Setup

If your LAN-to-LAN application has NetWare servers on both sides of the link, then all NetWare client stations will have access to a server on their LAN as shown below:



This may present a problem if you desire your client station to access a server at a remote site. For example, in the above diagram, suppose that a client station on the network on the left wishes to access the NetWare server on the right (internal network number = 111). However, the SAP broadcasts will receive a response from the server on the left (internal network number = 444). A static route is used to resolve this problem by providing the router with some static routing information to access the remote server.

From menu 12, select one of the four possible IPX Static Routes as shown below:



1. **Server Name**—In this field, enter in the name that has been configured for the server. This name must be the *exact* name configured in the NetWare server.
2. **Network #**—This field contains the internal network number of the remote server which you wish to access. Do not use 00000000 or FFFFFFFF for this field.
3. **Node #**—This field contains the address of the node on which the server resides. If you are using a Novell IPX implementation, this value is 000000000001.
4. **Socket #**—This field contains the socket number on which the server will receive service requests. The default for this field is hex 0451.
5. **Type #**—This field identifies the type of service the server provides. The default for this field is hex 0004.

6. **Gateway Node**—In this field, enter the number (1-4) of the Remote Node that is linked to this static route. That is, the Remote Node that you wish to route the packet to.

The Hop Count and Tick Count fields have the same meaning as those in the Remote Node Setup.

Once you have completed filling in the menu, press **ENTER** at the message 'Press ENTER to Confirm...' to save your selections, or press **ESC** at any time to cancel your selections.

Bridging Configuration

This chapter shows you how to configure the Bridging options for the DI-106M. Depending on your particular applications, you will need to configure different menus. We will illustrate the configuration for some applications in the following sections.

IPX Spoofing

The DI-106M comes with several pre-defined call filters designed to prevent certain IPX packets from triggering a call to a Remote Node. These filters should inform your DI-106M which packets should be ignored as traffic.

When you are bridging IPX packets, the default call filters are defined as follows:

- Block periodical SAP and RIP response messages.
- Block SAP and RIP inquiry packets if set to Handle IPX as Server.
- Allow SAP and RIP inquiry packets if set to Handle IPX as Client or None.

These call filters prevent the DI-106M from making a call to the Remote Node, thus preventing the expense of an unnecessary phone call.

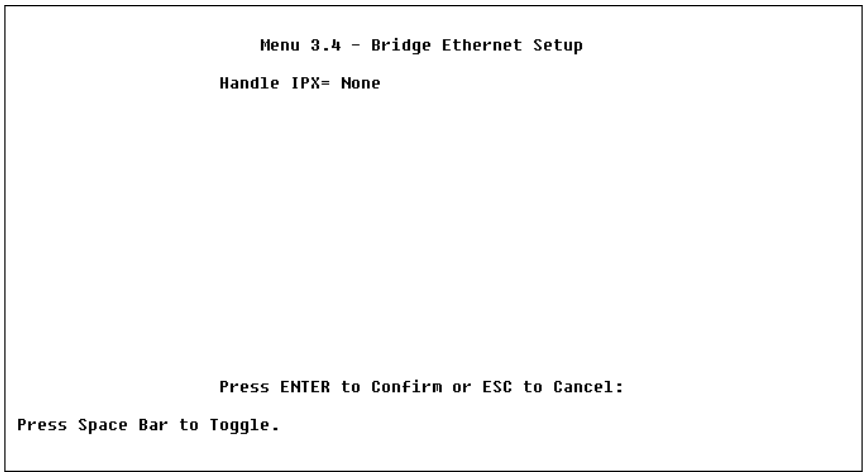
Bridge Ethernet Setup

Bridging is used to forward packets of unsupported protocols whose destination is not on the local Ethernet to the WAN.

Basically, all non-local packets are bridged to the WAN; however, the DI-106M applies special handling for certain IPX packets to reduce the number of calls, depending on the setting of the "Handle IPX" field.

- If this field is set to **None,** nothing is done to IPX traffic.
- If it is set to **Client,** all RIP and SAP (Service Advertising Protocol) periodical response packets will not trigger the call.
- If it is set to **Server,** no RIP or SAP packets will trigger the call. In addition, during the time when the ISDN line is down, the DI-106M will reply to the server's watchdog messages on behalf of remote clients. The period of time that the DI-106M will do this is linked to the *Ethernet Address Timeout* parameter in each Remote Node (see the *Remote Node Configuration* chapter starting on page 57). When a remote Ethernet address is aged out, there is no need to maintain its connection to the IPX server.

From menu 3, Ethernet Setup, enter "4" to go to menu 3.4, Bridge Ethernet Setup, shown below:



- **Handle IPX**—Set this parameter to None if there is no IPX traffic on the LAN or if you do not want to apply any special handling for IPX. Set it to Client if there are only client workstations on the LAN. Set to Server if there are only IPX servers on the LAN.

  If there are both clients and servers on the LAN, then the setting depends on whether the local clients will access the remote servers. If they do, set to **Client** and set Dial-On-Broadcast in menu 11.2 to **Yes** to allow client queries to trigger calls. If they do not, set it to **Server**.

When you are finished, press **ENTER** at the message 'Press ENTER to Confirm...' to save your selections, or press **ESC** at any time to cancel them.

LAN-to-LAN Application

A typical LAN-to-LAN application is to use the DI-106M to call from one office to another office such that stations on one network

have access to stations on the remote side and vice versa. You will need to configure a Remote Node in order to dial out to another office.

Remote Node Setup

Follow the procedure in the *Remote Node Configuration* chapter starting on page 57 to fill the protocol-independent parameters in menu 11, Remote Node Profile. For the protocol-dependent parameters, follow the ensuing instructions:

1. **Bridge**—Make sure this field is set to Yes.
2. **Edit IP/IPX/Bridge**—Press the space bar to change it to Yes and press Enter to go to the network layer options menu as seen below:

```
              Menu 11.3 - Remote Node Network Layer Options

IP Options:                          IPX Options:
  Rem IP Addr:                         Dial-On-Query= N/A
  Rem Subnet Mask= N/A                 Rem LAN Net #= N/A
  My WAN Addr= N/A                     My WAN Net #= N/A
  Single User Account= N/A             Hop Count= N/A
    Server IP Addr= N/A                Tick Count= N/A
  Metric= N/A                          W/D Spoofing(min)= N/A
  Private= N/A                         SAP/RIP Timeout(min)= N/A
  RIP Direction= N/A
    Version= N/A                     Bridge Options:
                                       Dial-On-Broadcast= No
                                       Ethernet Addr Timeout(min)= 0




                Enter here to CONFIRM or ESC to CANCEL:
```

1. **Dial-On-Broadcast**—This field is necessary for the DI-106M on the caller side LAN. When set to Yes, any broadcasts coming from the LAN will trigger the DI-106M to make a call to that

Remote Node. If it is set to No, the DI-106M will not make the outgoing call.

2. **Ethernet Addr Timeout (min)**—In this field, enter the time (number of minutes) that you wish the DI-106M to retain the Ethernet Addr information in its internal tables while the line is down. If this information is retained, the DI-106M will not have to re-negotiate the protocol and recompile the tables when the line is brought back up.

Once you have completed filling in the Network Layer Options menu, press **ENTER** to return to menu 11. Press ENTER at the message 'Press ENTER to Confirm...' to save your selections, or press **ESC** at any time to cancel your selections.

Default Dial-In Setup for Bridge

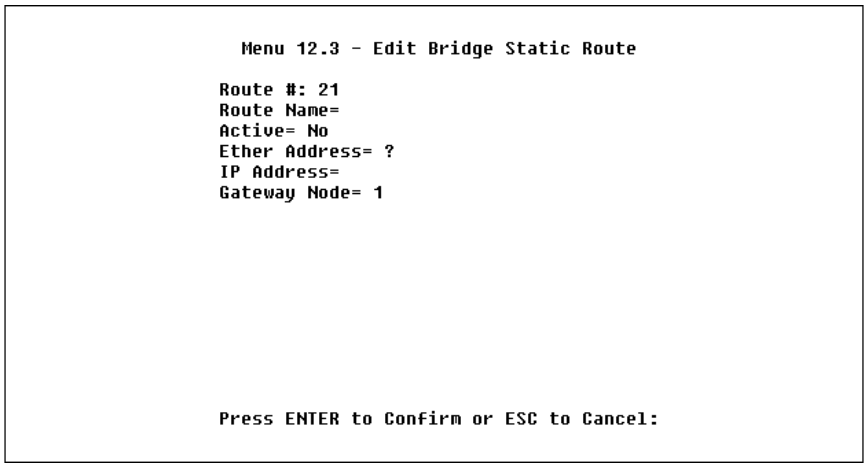
There is only one parameter you need to fill out for Bridging applications.

- **PPP Options: Recv. Authen.**—verify that this field is *not* set to None. Bridging applications must have some sort of authentication turned on in order to match to a Remote Node.

Once you have completed filling in the menu, press ENTER at the message 'Press **ENTER** to Confirm...' to save your selections, or press **ESC** at any time to cancel your selections.

Bridge Static Route Setup

You can configure Bridge static routes for your Bridging applications.



1. **Route Name**—For identification purposes enter a name for the bridge static route.
2. **Active**—Indicates whether the static route is active or not.
3. **Ether Address** -Enter the MAC address of the destination device that you wish to bridge your packets to.
4. **IP Address**—If available, enter the IP address of the destination device that you wish to bridge your packets to.
5. **Gateway Node**—Enter the number (1-4) of the Remote Node that is linked to this static route. When an incoming packet's destination Ether (MAC) address matches the value entered above, then it will trigger a call to this Remote Node.

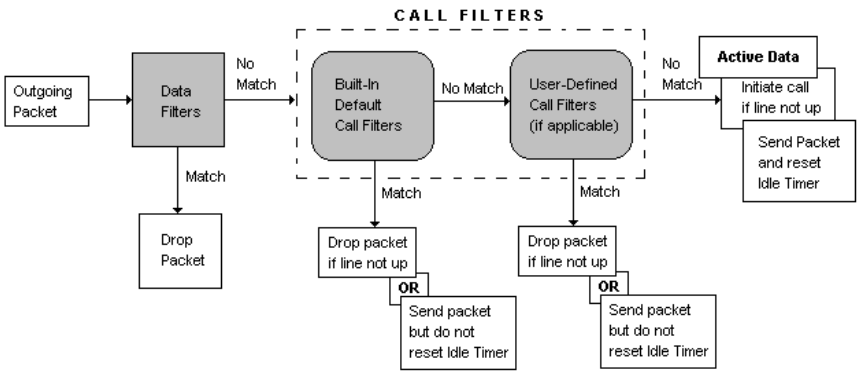
Once you have completed filling in the menu, press **ENTER** at the message 'Press ENTER to Confirm...' to save your selections, or press **ESC** at any time to cancel your selections.

Filter Configuration

About Filtering

Your DI-106 or DI-106M uses filters to decide whether or not to allow passage of a data packet and/or to make a call over the ISDN line. There are three types of filters involved: incoming data filters, outgoing data filters, and call filters. Data filters screen the data to determine if the packet should be allowed to pass. Call filters are used to determine if a call should be placed.

Outgoing packets must pass through the data filters before they encounter the call filters. Call filters are divided into two groups: default call filters and user-defined call filters. The router has default call filters that filter out administrative packets, e.g., RIP and SAP packets. The router applies the default filters first, and then the user-defined call filters if applicable, as shown below:



For incoming packets, your DI-106 or DI-106M applies data filters only. Packets are processed depending upon whether a match is made. The router allows you to customize the filter sets that you wish to use. This following sections describe how to configure the router's filter sets.

DI-106's Filter Structure

You can configure up to twelve filter sets with six rules in each set. Therefore, your DI-106 or DI-106Mallows you to customize up to 72 filter rules (12×6).

When implementing these filter sets, you can link up to four of the filter sets together to screen the data packet. Therefore, with each filter set having up to six rules, you can have a maximum of 24 rules active for a single filtering application.

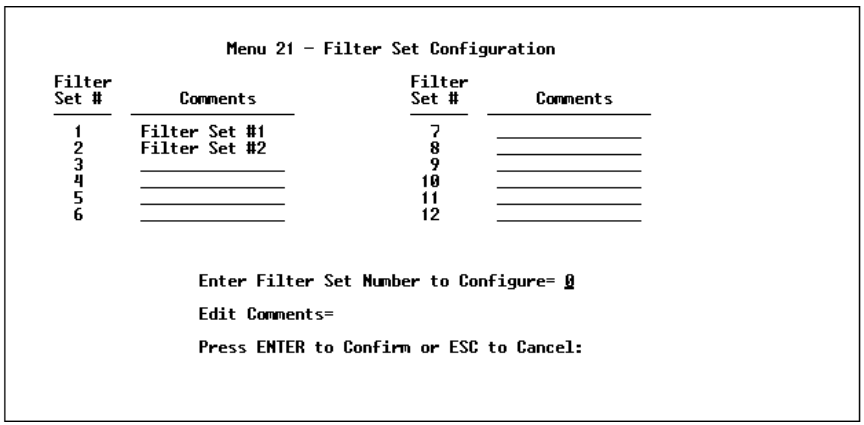
Configuring a Filter Set

In order to distinguish between the 12 filter sets, each filter set should have a name or some comments. You can edit these comments in the following way.

1. From the main menu, select option 21. This will take you to menu 21, Filter Set Configuration.
2. This menu lets you choose from twelve filter sets. Select the filter set you wish to configure (1-12).

This will take you to the **Edit Comments** field. You can edit the comments you wish to use to identify that filter set. The comments for any given filter set can contain up to 15 characters.

Once you have completed filling in **Edit Comments** field, press **ENTER** at the message 'Press ENTER to Confirm...' to confirm your selections, or press **ESC** at any time to cancel your selections. The new information will now be displayed in the read-only section of menu 21, Filter Set Configuration, as shown below:



After you press ENTER, you will be taken to menu 21.1, Filter Rules Summary, as shown below. The information displayed in this menu is read-only. From here, you can examine the parameters of each rule that you have configured for that set. Following are brief descriptions of the column headings in this menu.

- #—Refers to the filter rule number (1-6).
- **A**—Refers to Active. **Y** means the filter rule is active and **N** means the filter rule is inactive.
- **Type**—Refers to the type of filter rule. This can display GEN for generic, IP for TCP/IP, or IPX for Novell IPX.

- **Filter Rules**—The filter rule parameters will be displayed here (see below).
- **M**—Refers to More. **Y** means there are more rules to check, **N** means there aren't.
- **m**—Refers to Action Matched. **F** means to forward the packet, **D** means to drop the packet, and **N** means check the next rule. The Action Matched control has no effect when the More control (see preceding) is set to **Y**.
- **n**—Refers to Action Not Matched. **F** means to forward the packet, **D** means to drop the packet, and **N** means check the next rule. The Action Not Matched control has no effect when the More control is set to **Y**.

```
                    Menu 21.1 - Filter Rules Summary

# A Type                        Filter Rules                          M m n
- - ---- ------------------------------------------------------------ - - -
1 Y IP   Pr=17, SA=204.247.203.2, SP=520, DA=192.68.135.1             N F D
2 Y Gen  Off=4, Len=2, Mask=ffff, Value=0802                         N D N
3 Y IPX  PT=ad, SS<2222, DS!=1111                                    N F N
4 N
5 N
6 N




              Enter Filter Rule Number (1-6) to Configure:
```

If the filter type is IP (TCP/IP), the following abbreviations will be used:

- ◊ **Pr**—Protocol.

- **SA**—Source Address.
- **SP**—Source Port number.
- **DA**—Destination Address.
- **DP**—Destination Port number.

If the filter type is GEN (generic), the following abbreviations will be used:

- **Off**—Offset.
- **Len**—Length.

If the filter type is IPX (Novell IPX), the following abbreviations will be used:

- **PT**—IPX Packet Type.
- **SS—**Source Socket.
- **DS**—Destination Socket.

For more information on configuring the filter rule parameters, refer to the next section.

To configure a specific filter rule, simply select the number of the filter rule (1-6) you wish to configure and press ENTER. This will take you to menu 21.1.1, TCP/IP Filter Rule (next section).

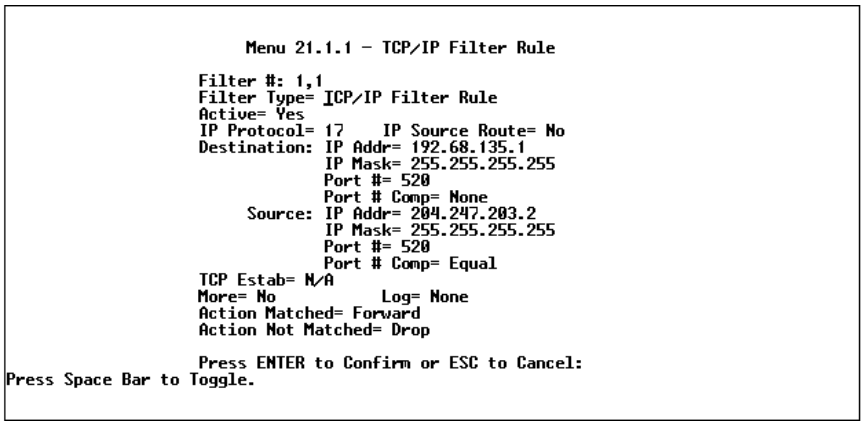
Configuring a Filter Rule

There are three types of filter rules that you can configure. Some of the parameters will differ depending on the type of rule. When you first enter the Filter Rule menu, you will be presented with menu 21.1.1, TCP/IP Filter Rule. If you wish to configure another type of

filter rule, you need to select the appropriate type (by pressing SPACE bar) under the **Filter Type** field and press ENTER. This will bring you to the corresponding menu.

TCP/IP Filter Rule

This section will show you how to configure a TCP/IP filter rule for your outer. The fields in the menu are indicated in **bold** type.



1. **Active**—In this field, you can make the filter rule active or inactive. There are two options:
   - ◊ Yes.
   - ◊ No.
2. **IP Protocol**—Protocol refers to the IP specific number of the protocol. The range for this value should be between 0 and 255. For example, 6 refers to the TCP protocol.

3. **IP Source Route—**Determine, Yes or No, whether to check the source route.
4. **Destination: IP Addr—**In this field, enter the destination IP Address of the packet you wish to filter. The address is usually written in dotted decimal notation such as a.b.c.d where a, b, c, and d are numbers between 0 and 255.
5. **Destination: IP Mask—**In this field, enter the IP mask that will be used to mask the bits of the IP Address given in **Destination: IP Addr**.
6. **Destination: Port #—**Enter the destination port of the packets that you wish to filter. The range of this field is 0 to 65535.
7. **Destination: Port # Comp—**In this field, you can select what comparison quantifier you wish to enable to compare to the value given in **Destination: Port #.** There are five options for this field:
   - ◊ None.
   - ◊ Less.
   - ◊ Greater.
   - ◊ Equal.
   - ◊ Not Equal.
8. **Source: IP Addr—**In this field, enter the source IP Address of the packet you wish to filter. The address is usually written in dotted decimal notation such as a.b.c.d where a, b, c, and d are numbers between 0 and 255.
9. **Source: IP Mask—**In this field, enter the IP mask that will be used to mask the bits of the IP Address given in **Source: IP Addr**.

10. **Source: Port #—**Enter the source port of the packets that you wish to filter. The range of this field is 0 to 65535.
11. **Source: Port # Comp—**In this field, you can select what comparison quantifier you wish to use to compare to the value given in **Source: Port #.** There are five options for this field:
    - ◊ None.
    - ◊ Less.
    - ◊ Greater.
    - ◊ Equal.
    - ◊ Not Equal.
12. **TCP Estab—**This field is dependent upon the IP Protocol field. This field will be inactive (N/A) unless the value in that field is 6 (TCP protocol). In this field you specify what type of TCP packets will be filtered. There are two options:
    - ◊ Yes—filter match only established TCP connections.
    - ◊ No—filter match both initial and established TCP connections.
13. **More**—In this field, you can determine if you want to pass the packet through the next filter rule before an action is taken. There are two options for this field:
    - ◊ Yes.
    - ◊ No.

    If More is Yes, then Action Matched and Action Not Matched will be N/A.
14. **Log—**In this field, you can determine if you wish to log the results of packets attempting to pass the filter rule. These

results will be displayed on the System Log (see the *Log and Trace* section on page 132). There are 4 options for this field:

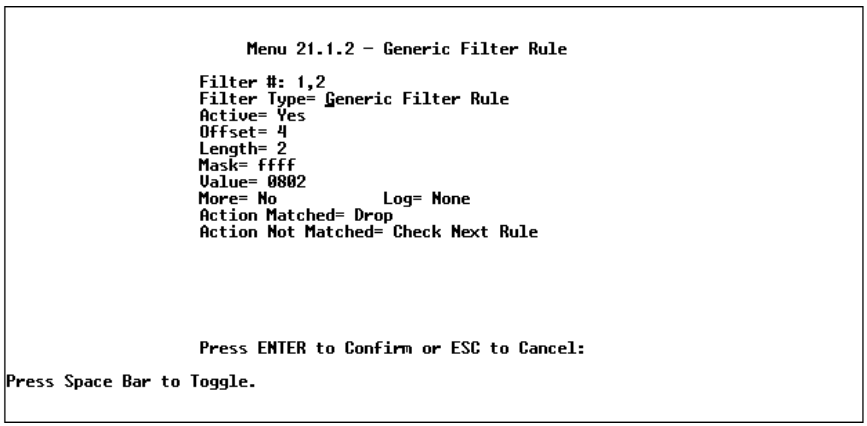
- ◊ **None**—No packets will be logged.
- ◊ **Action Matched**—Only packets that match the rule parameters will be logged.
- ◊ **Action Not Matched**—Only packets that do not match the rule parameters will be logged.
- ◊ **Both**—All packets will be logged.

15. **Action Matched—**If the conditions for the filter rule are met, you can specify what to do with the packet. There are three options for this field:
    - ◊ Check Next Rule.
    - ◊ Forward.
    - ◊ Drop.
16. **Action Not Matched—**If the conditions for the filter rule are not met, you can specify what to do with the packet. There are three options for this field:
    - ◊ Check Next Rule.
    - ◊ Forward.
    - ◊ Drop.

Once you are finished filling in menu 21.1.1, TCP/IP Filter Rule, press **ENTER** at the message 'Press ENTER to Confirm...' to confirm your selections, or press **ESC** at any time to cancel your selections. This data will now be displayed in menu 21.1, Filter Rules Summary.

Generic Filter Rule

This section will show you how to configure the protocol-independent parameters for a Generic filter rule for your DI-106 or DI-106M. For information on the protocol-dependent fields, refer to the previous section, TCP/IP Filter Rule, and the following section, Novell IPX Filter Rule. The fields in the menu are indicated in **bold** type.



1. **Offset—**Offset refers to the value of the byte that you want to use as your starting offset. That is, in the data packet, at what point do you want to begin the comparison. The range for this field is from 0 to 255. *Default = 0*
2. **Length—**This field refers to the length (in bytes) of the data in the packet that the router should use for comparison and masking. The starting point of this data is determined by **Offset**. The range for this field is 0 to 8. *Default = 0*

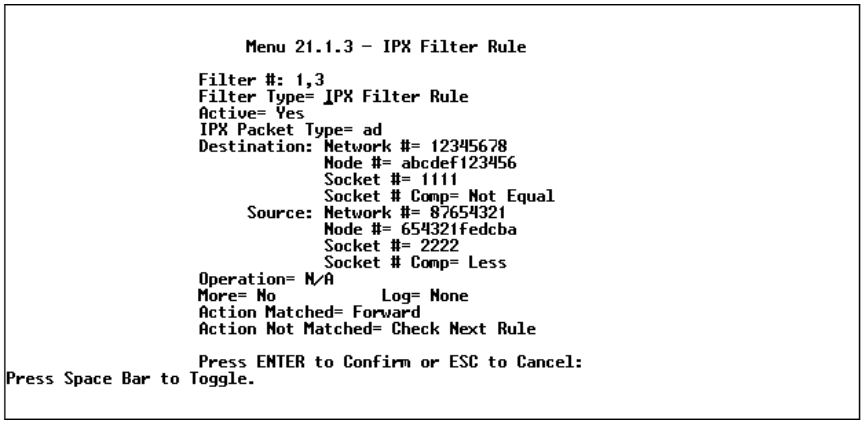
3. **Mask—**In this field, specify (in Hexadecimal) the value that the router should logical-AND with the data in the packet. The mask must have the number of bytes indicated in the **Length** field. For example, if **Length** is 4, one possible **Mask** setting would be 1155ABF8.
4. **Value—**In this field, specify (in Hexadecimal) the value that the router should use to compare with the masked packet. The value should align with **Offset**, and must have the number of bytes indicated in the **Length** field. For example, if **Length** is 4, one possible **Value** setting would be 1155ABF8. If the result from the masked packet matches **Value**, then the packet is considered matched.
5. **Action Matched—**If the conditions for the filter rule are met, you can specify what to do with the packet. There are three options for this field:
   - ◊ Check Next Rule.
   - ◊ Forward.
   - ◊ Drop.
6. **Action Not Matched—**If the conditions for the filter rule are not met, you can specify what to do with the packet. There are three options for this field:
   - ◊ Check Next Rule.
   - ◊ Forward.
   - ◊ Drop.

Once you are finished filling in menu 21.1.1, Generic Filter Rule, press **ENTER** at the message 'Press ENTER to Confirm...' to confirm your selections, or press **ESC** at any time to cancel your

selections. This data will now be displayed in menu 21.1, Filter Rules Summary.

Novell IPX Filter Rule

This section will show you how to configure the protocol-dependent parameters for an IPX filter. The fields in the menu are displayed in **bold** type.



1. **IPX Packet Type**—Enter the IPX packet type value of the packet you wish to filter. This setting should be a one-byte value, expressed in hexadecimal..
2. **Destination/Source Network #**—Enter the four hex-byte destination/source network numbers of the packet that you wish to filter.
3. **Destination/Source Node #—**Enter in the six hex-byte value for the destination/source node number of the packet you wish to filter.

4. **Destination/Source Socket #**—Enter the destination/source socket number of the packets that you wish to filter. This should be a 4-byte hex value.
5. **Destination/Source Socket # Comp—**You can select what comparison quantifier you wish to use to compare to the value given in Destination Socket # and Source Socket #.
6. **Operation**—This field is only active if one of the Socket # fields is 0452 or 0453 indicating SAP and RIP packets. There are seven options for this field which determines the operation for the IPX packet.
   - ◊ None.
   - ◊ RIP Request.
   - ◊ RIP Response.
   - ◊ SAP Request.
   - ◊ SAP Response.
   - ◊ SAP "Get Nearest Server" Request.
   - ◊ SAP "Get Nearest Server" Response.

The **More**, **Log**, **Action Matched**, and **Action Not Matched** controls work as described in the preceding sections.

Once you are finished filling in menu 21.1.3, IPX Filter Rule, press **ENTER** at the message 'Press ENTER to Confirm...' to confirm your selections, or press **ESC** at any time to cancel your selections. This data will now be displayed in menu 21.1, Filter Rules Summary.

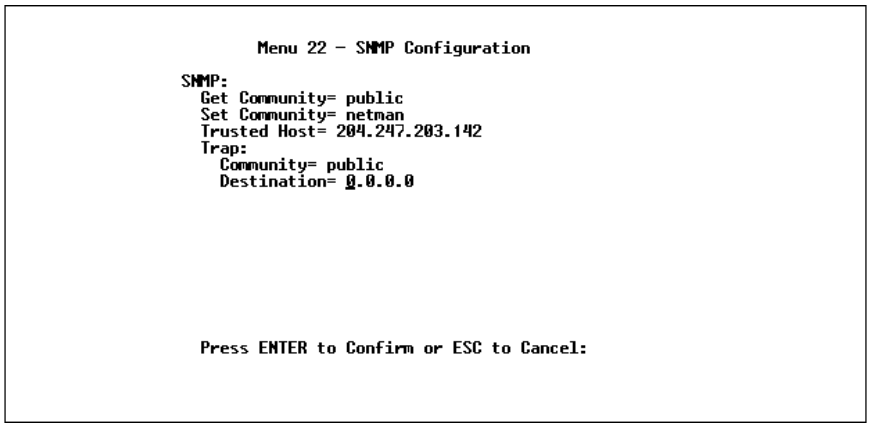
SNMP

About SNMP

The Simple Network Management Protocol (SNMP) is a protocol governing network management and the monitoring of network devices and their functions. The DI-106M supports the use of SNMP to regulate communication between management stations and agent stations on a network. Basically, the DI-106M, when connected to the LAN, acts as an agent station. In this way, a management station on your LAN can monitor the DI-106M as it would another station on the network. Keep in mind that SNMP is only available if TCP/IP is configured on your DI-106M.

Configuring Your DI-106M For SNMP Support

Following is a description of how to configure the DI-106M for SNMP management.



1. From the main menu, select option 22, SNMP Configuration. This will bring you to menu 22, SNMP Configuration, shown above.
2. You will then be prompted to enter the following information. Steps 3 -7 will describe the specific parameters involved in the configuration. The parameters you will have to fill in will be indicated in **bold** type.
3. **Get Community—**From this field, you can determine what the "Get" community is for your DI-106M. The value entered into this field will be used to authenticate the community field for incoming "Get" and "GetNext" requests from the management station. The default is public.
4. **Set Community**—In this field, enter the "Set" community for your DI-106M. The value entered in this field will be used to authenticate the community field for incoming "Set" requests from the management station. The default is public.
5. **Trusted Host**—Enter the IP address of the Trusted Host SNMP management station. If this field is configured, the DI-106M will

only respond to SNMP messages coming from this address. If you leave the field blank (default), the DI-106M will respond to all SNMP messages it receives, regardless of origin.

6. **Trap: Community—**In this field, enter the community name that is sent with each trap to the SNMP manager. This should be treated like a password and must match what the SNMP manager is expecting. The default is public.
7. **Trap: Destination—**This field contains the IP address of the station that you wish to send your SNMP traps to.

Once you have finished filling in menu 22, SNMP Configuration, press **ENTER** to confirm your selections, or press **ESC** to cancel your selections.

If you are unsure how to configure the fields for the SNMP configuration, consult your network administrator.

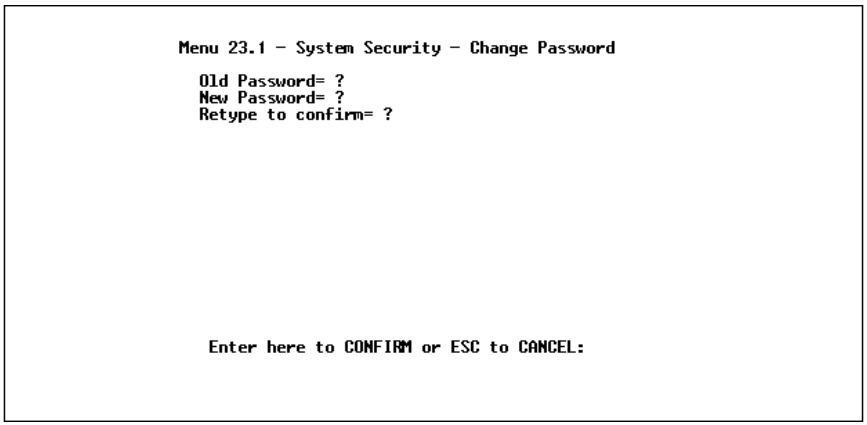
System Security

Your DI-106 or DI-106M incorporates a number of security measures to prevent unauthorized access to your network. For example, it supports both PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol) for authenticating a Remote Node. More information on CHAP and PAP can be found in the *Dial-In Configuration* chapter starting on page 68.

By default, the router can store information about up to eight different users. If more dial-up users are necessary, an external RADIUS (Remote Authentication Dial In User Service) server can be used to provide centralized user security.

In addition, the DI-106 and DI-106M implement a user password to get into the SMT screen. You will have three attempts to enter the correct system password. If you do not do so, the SMT will kick you out. In addition, the router will support only one user in the SMT at one time.

Configuring the SMT Password



The following steps describe a simple setup procedure for configuring the SMT password.

1. From the main menu, select option 23. System Security. This will bring you to menu 23, System Security.
2. From this menu, you can select option 1. Change Password. This will bring you to menu 23.1, System Security – Change Password.
3. Type in your previous system password and press **ENTER**.
4. Type in your new system password and press **ENTER**.
5. Re-type your new system password for confirmation purposes and press **ENTER**.

You will now need to enter in this password when you try to get into the SMT. In addition, this password will also be used when a network administrator attempts to telnet to the router.

Using RADIUS Authentication

In addition to the DI-106M's built-in dial-up user list, which can hold up to eight users, this model also supports an external authentication server which may provide password storage and usage accounting for thousands of users.

Installing a RADIUS Server

To use RADIUS authentication, you will need to have a UNIX-based machine on your network to act as a `radiusd` server, as well as a copy of the `radiusd` server program itself. You can obtain a copy of the RADIUS software, along with documentation for the server, at

http://www.livingston.com/Tech/FTP/pub-le-radius.shtml

or at

ftp://ftp.livingston.com/pub/le/radius/

Follow the included instructions to install the RADIUS software on your server.

Once you have installed the server, you will need to edit the `dictionary` file in the RADIUS configuration directory (which will usually be `/etc/raddb`). Using any text editor, add the following lines to the `dictionary` file:

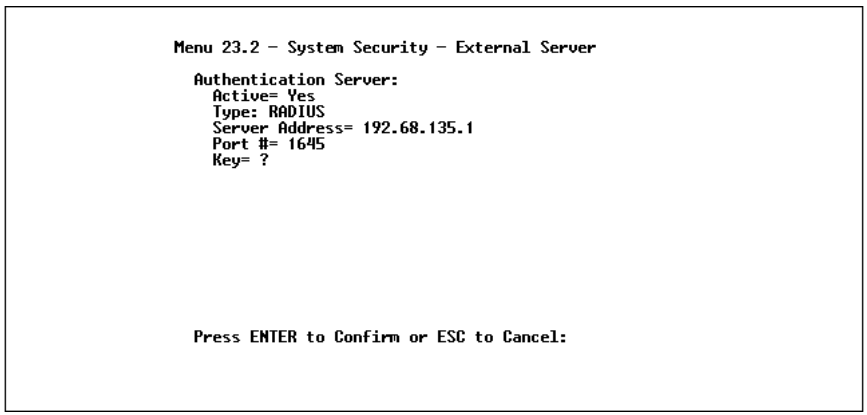
```
# D-Link proprietary attributes
```

```
ATTRIBUTE D-Link-Callback-Option   192 integer
VALUE     D-Link-Callback-Option   None        0
VALUE     D-Link-Callback-Option   Optional    1
VALUE     D-Link-Callback-Option   Mandatory   2

#   Callback phone number source
ATTRIBUTE D-Link-Callback-Phone-Source 193 integer
VALUE     D-Link-Callback-Phone-Source Preconfigured  0
VALUE     D-Link-Callback-Phone-Source User           1
```

These changes allow the RADIUS server to be used with D-Link CLID authentication, as described in the section below.

Configuring the DI-106M for RADIUS Authentication

To configure the DI-106M to use the RADIUS server set up in the previous section, select option 23, System Security, from the main menu. This will bring you to menu 23, System Security. From this menu, select option 2, External Server. This will bring you to menu 23.2, System Security – External Server.



The fields in the System Security – External Server menu are as follows:

1. **Active**—Determines whether the external security facility is enabled. If this field contains No, only the built-in dial-up user list will be used. If this field contains Yes, the built-in dial-up user list will be searched first, then the external authentication server.
2. **Type**—Determines the type of the external authentication server. At present only the RADIUS type is supported.
3. **Server Address**—The IP address of your network's UNIX-based RADIUS server.
4. **Port #—**The IP port address used by the authentication server. The default value of 1645 should be used.
5. **Key**—A "password" used to identify the DI-106M as a valid client of the RADIUS authentication service.

The Key password should be stored in the `client` file in the RADIUS server's `/etc/raddb` directory. Lines of the form

```
# Client Name            Key
#------------------------------
192.168.0.1              1234
```

should be added to the `client` file. The Client Name field in the file gives the IP address of the DI-106M, and the Key field should be the same as the Key field in menu 23.2.

After a RADIUS server has been configured, the DI-106M will use it to authenticate all users that it can't find in its internal Dial-Up User List (menu 14).

Adding Users to the RADIUS Database

The DI-106M only uses the RADIUS database for user authentication; except for `Password`, `Dialback-No`, and the D-Link extensions `D-Link-Callback-Option` and `D-Link-Callback-Phone-Source` (described below), most standard RADIUS attribute fields are ignored by the DI-106M.

To add a user to the RADIUS database, edit the `users` file in the RADIUS server's `/etc/raddb` directory, and add a line similar to the following:

```
joeuser          Password = "joepassword"
```

Each user should have a user name/password record in the `users` database.

Using RADIUS Authentication for CLID

To use RADIUS for CLID authentication, create a user record in the `users` file , where the user name (the first field) is the telephone number, and the password (the second field) is always `D-Link-CLID` (case-sensitive). The regular user name is put in a User-Name field. The following is an example of a CLID user record:

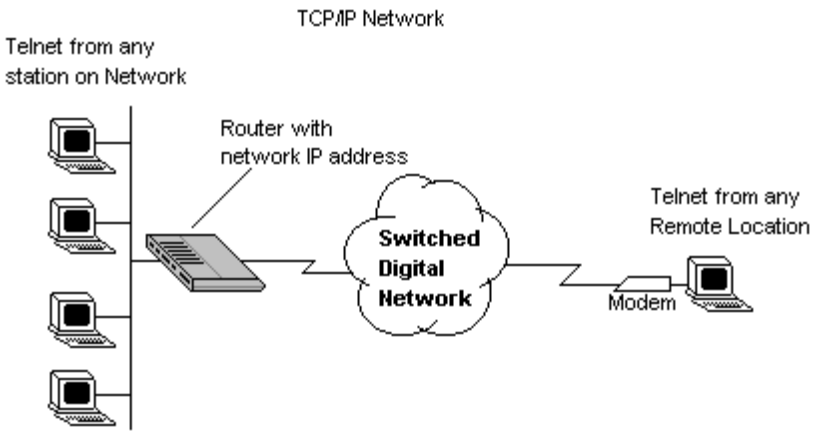
```
5551212    Password = "D-Link-CLID"
             User-Name = "joeuser",
             D-Link-Callback-Option = Mandatory,
             D-Link-Callback-Phone-Source = Preconfigured
             Dialback-No = "5551212"
```

Note that if CLID is turned off in the DI-106M, you still need to have a separate user record for `joeuser` so the regular user name/password mechanism still works.

Telnet Configuration and Capabilities

About Telnet Configuration

When you first configure your DI-106 or DI-106M, it must be done via a computer connected to the RS-232 port. However, once the router has been initially configured, you can use `telnet` to configure it remotely as shown below:



In order to configure your DI-106 or DI-106M in this way, you must first assign it an IP Address and connect it to your network. See the *Configuring for Internet Access* chapter starting on page 47 for more information on assigning an IP Address. Once this is configured, any station on the LAN or remote network that has TCP/IP installed can use `telnet` remote management. If your DI-106M is configured for IPX routing but not IP in menu 1,

`telnet` will still be available provided you assign the router an IP address.

Telnet Capabilities

Single Administrator

To prevent confusion and discrepancy on the configuration, your DI-106 or DI-106M will allow only one terminal connection at any time. The router also gives priority to the RS-232 connection over `telnet`. If you have already connected to the router via `telnet`, you will be logged out if another user is connecting to it via the RS-232 cable. Only after the other administrator has been disconnected will you be able to `telnet` to the router again.

System Timeout

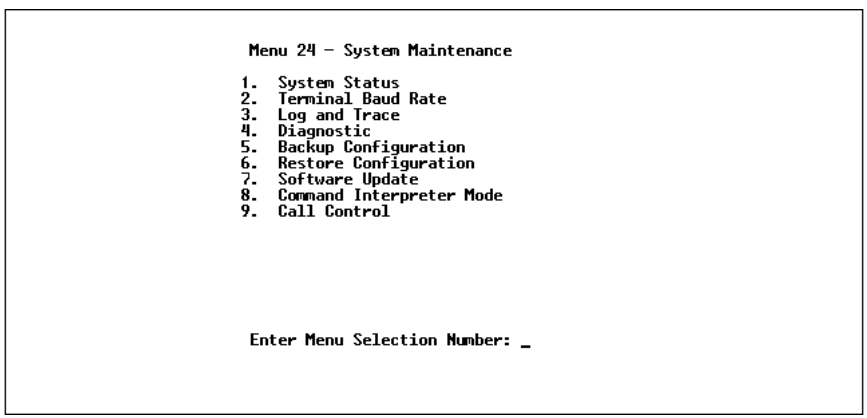
When you are connected to your DI-106 or DI-106M via `telnet`, there is a system timeout of 5 minutes (300 seconds). If you are not configuring the device and leave it inactive for this timeout period, the router will automatically disconnect you.

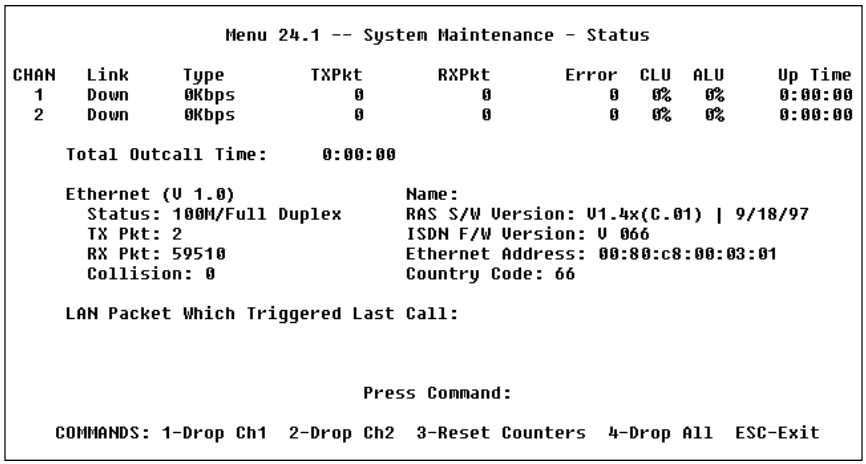
System Maintenance

Your DI-106 or DI-106M provides diagnostic tools that you can use to maintain your device. Some of these tools include updates on system status, ISDN B channel status, log and trace capabilities and upgrades to the system software. This chapter will describe how to use these tools in greater detail.

System Status

System Status is a tool that can be used to monitor your DI-106 or DI-106M. Specifically, it will give you information on the status of your system software version, ISDN telephone line, number of packets sent and number of packets received.



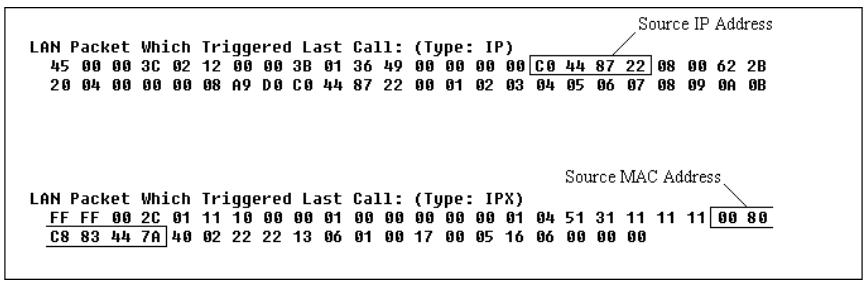


1. To get to the System Status display, select option 24. System Maintenance. This will bring you to menu 24, System Maintenance.
2. From this menu, select option 1, System Status.
3. There are four (4) possible commands in menu 24.1, System Maintenance – Status. Entering **1** will disconnect the current channel 1 call; **2** will disconnect the current channel 2 call; **3** will reset the counters; **4** will disconnect channel 1 and channel 2; and **ESC** will exit the screen.
4. Items 5 through 25 describe the fields present in menu 24.1, System Maintenance – Status. It should be noted that these fields are READ-ONLY and are meant to be used for diagnostic purposes.
5. **CHAN**—shows statistics for channel 1 and channel 2, respectively. Following is the information displayed for each channel:

6. **Link**—shows the Remote Node the channel is currently connected to or the status of the channel (Idle, Calling, Answering, etc.).
7. **Type**—the current connecting speed (56K or 64K).
8. **TXPkt**—the number of transmitted packets on this channel.
9. **RXPkt**—the number of received packets on this channel.
10. **Error**—the number of error packets on this channel.
11. **CLU** (Current Line Utilization)—percentage of current bandwidth used on this channel.
12. **ALU** (Average Line Utilization)—average CLU for this channel.
13. **Up Time**—time this channel has been connected to the current Remote Node.
14. **Total Outgoing call Time**—shows the total outgoing call time for both channel 1 and channel 2 since the system was powered up.
15. **Ethernet**—shows the current status of the LAN connection on your DI-106 or DI-106M.
16. **Status**—shows the LAN's current speed (10 Mbps or 100 Mbps) and manner of data flow (half-duplex or full-duplex).
17. **TX Pkt**—the number of packets transmitted to the LAN.
18. **RX Pkt—**the number of packets received from the LAN.
19. **Collision**—number of collisions.
20. **Name**—displays the system name of your router. This information can be modified in menu 1, General Setup.

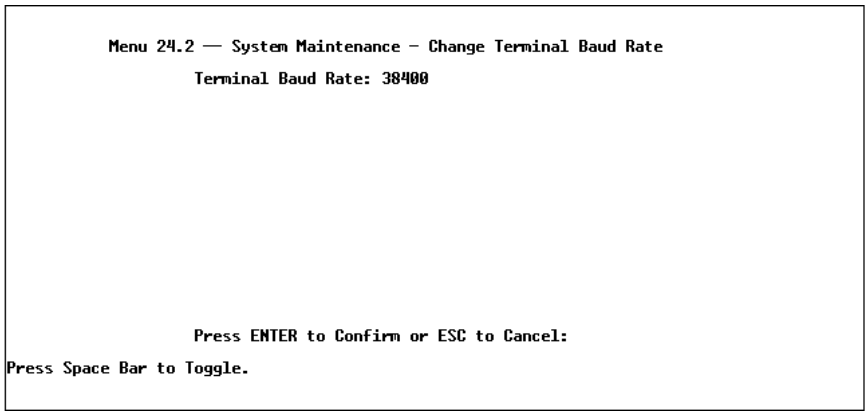
21. **RAS S/W Version**—refers to the version of the current RAS software.
22. **ISDN F/W Version**—refers to the version of the current ISDN firmware.
23. **Ethernet Address**—refers to the Ethernet MAC address assigned to your DI-106 or DI-106M.
24. **Country Code**—refers to the one byte country code value (in decimal notation), e.g., 255 indicates North America.
25. **LAN Packet Which Triggered Last Call**—shows the first 48 octets of the LAN packet that triggered the last outgoing call. There are three different types of packets: IP, IPX, and RAW. By viewing the packet information, you can determine which station has sent a packet to cause the router to make an outgoing call.

Two example figures are shown below. the first of an ICMP Ping packet (Type: IP) triggering the call and the second with a SAP packet (Type: IPX) triggering the call. With this information, you can determine the source IP address of the packet or the source MAC address of the packet.



Terminal Baud Rate

Users can set different baud rates for the RS-232 connection through menu 24.2, System Maintenance – Change Terminal Baud Rate. The router supports 9600 (default), 19200, and 38400 bps for the RS-232 connection.



Log and Trace

Log and trace tools allow users of the DI-106 or DI-106M to view the error logs and trace records to troubleshoot any errors that may occur. The router is also able to generate syslogs to send to other machines.

1. To get to the log and trace tools, select option 24, System Maintenance. This will bring you to menu 24, System Maintenance.

2. From this menu, select option 3, Log and Trace. This will bring you to menu 24.3, System Maintenance – Log and Trace.
3. You will be given two options.
   - ◊ View Error Log.
   - ◊ Syslog and Accounting.

The following list describes the fields involved in the trace and log options:

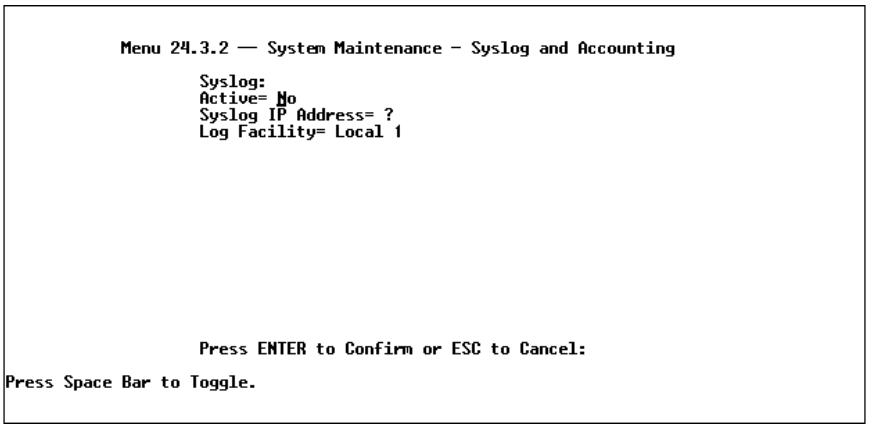
View Error Log

Selecting the first option from menu 24.3, System Maintenance – Log and Trace, will display the system's Error Log. In addition to providing error messages, the Error Log is a valuable source of information about your DI-106 or DI-106M.

You can also clear the Error Log on your DI-106 or DI-106M. After each display, you are prompted with an option to do so. Enter the appropriate choice and press ENTER.

Syslog And Accounting

Syslog and Accounting can be configured in menu 24.3.2, System Maintenance – Syslog and Accounting. This menu configures the router to send UNIX syslogs to another machine.



The User needs to configure the following 3 parameters to activate syslog:

1. **Active**—Use the space bar to turn the syslog option on or off.
2. **Syslog IP Address**—Input the IP Address that you wish to send your syslog to. The address is usually written in dotted decimal notation such as a.b.c.d where a, b, c, and d are numbers between 0 and 255.
3. **Log Facility**—Use the space bar to toggle between the 7 different Local options. This feature is used for UNIX applications.

Your DI-106 or DI-106M will send three different types of syslog messages: Call information messages (i.e. CDR), Error information messages, and Session information messages. Some examples of these messages are shown below:

Call Information Messages:

```
line 1 channel 1, call 41, C01, Incoming Call, 40001
line 1 channel 1, call 41, C01, ANSWER Connected, 64K 40001
line 1 channel 1, call 41, C01, Incoming Call, Call Terminated
```

Error Information Messages:

```
line 1, channel 1, call 44, E01, CLID call refuse
line 1, channel 1, call 45, E02, IP address mismatch
```

Session Information Messages:

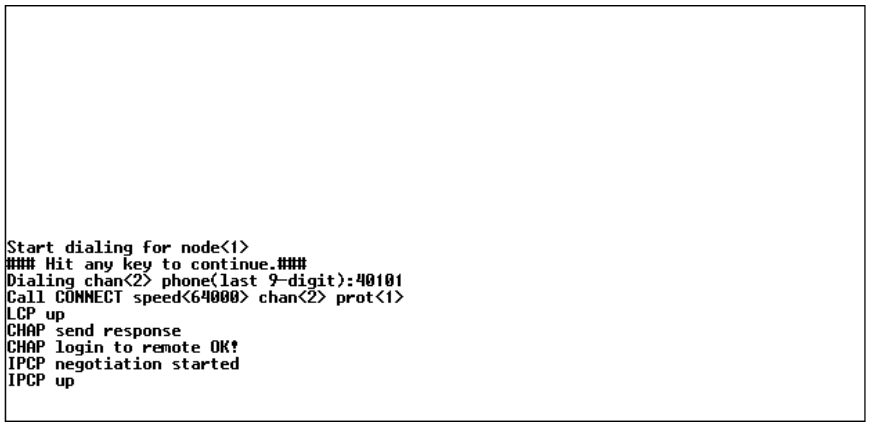
```
line 1, channel 1, call 41, I01, IPCP up, 306L
line 1, channel 1, call 41, I01, IPCP down, 306L
```

Diagnostic

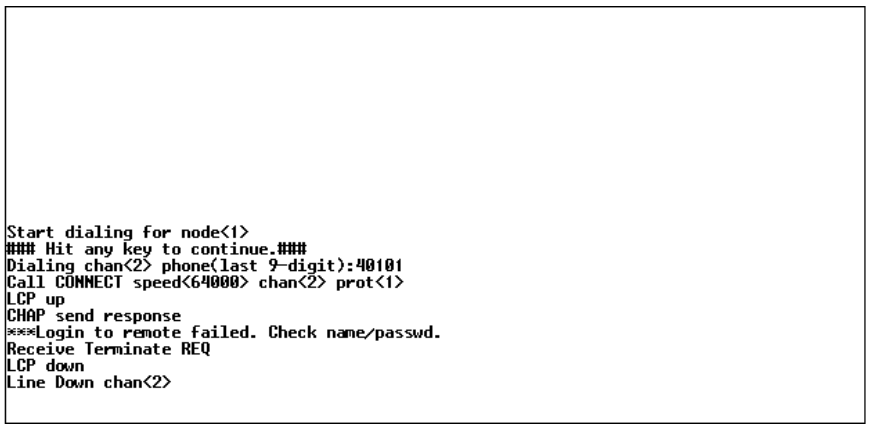
The diagnostic functions on your DI-106 or DI-106M allow you to test aspects of your device to determine if they are working properly. The following list provides a short description to the types of diagnostic tests available to your system.

```
                Menu 24.4 - System Maintenance - Diagnostic

ISDN                                    System
  1.  Hang Up CHAN 1 Call                 21. Reboot System
  2.  Hang Up CHAN 2 Call                 22. Command Mode
  3.  Reset ISDN
  4.  ISDN Connection Test
  5.  Manual Call

TCP/IP
  11. Internet Setup Test
  12. Ping Host


                      Enter Menu Selection Number:

                Manual Call Remote Node= N/A
                Host IP Address= N/A
```

1. From the main menu, select option 24, System Maintenance. This will bring you to menu 24, System Maintenance.
2. From this menu, select option 4, Diagnostic. This will bring you to menu 24.4, System Maintenance – Diagnostic.
3. Items 4–12 will describe the nine (9) options to test your router and its connections.
4. **Hang Up CHAN1 Call**—This tool hangs up the channel 1 line. This will only be useful if the line is currently connected to a Remote Node or a dial-in user.
5. **Hang Up CHAN2 Call**—This tool hangs up the channel 2 line. This will only be useful if the line is currently connected to a Remote Node or a dial-in user.
6. **Reset ISDN**—This command will re-initialize the ISDN link to the telephone company.
7. **ISDN Connection Test**—You can use this command to see if your ISDN line has been successfully connected to your DI-106 or DI-106M. This command will trigger the router to perform a loop-back test to check the functionality of the ISDN line. If your line is working properly, the test will succeed. Otherwise, note the error message that you receive and consult your network administrator.
8. **Manual Call**—This provides a way for the users of the DI-106 or DI-106M to place a manual call to a Remote Node. This tests the connectivity to that Remote Node. When you use this command, you will see traces displayed on the screen showing what is happening during the call setup and protocol negotiation. Below is an example of a successful connection.



Below is an example of a failed Trace Display for a Successful IPCP Connection via Manual Call.



9. **Internet Setup Test**—This test checks to see if your Internet access configuration has been done correctly. When this option is chosen, your DI-106 or DI-106M will PING the Internet IP Address. If everything is working properly, you will receive an appropriate response. Otherwise, note the error message and consult your network administrator.

10. **Ping Host**—This diagnostic test pings the host which determines the functionality of the TCP/IP protocol on your system.
11. **Reboot System**—This option reboots the system. This serves to implement any changes that may have been recently added to your system.
12. **Command Interpreter Mode**—This option allows the user to enter command interpreter mode. This mode allows you to diagnose and test your DI-106 or DI-106M using a specified set of commands.

Backup Configuration

Selecting option 5 from menu 24, Maintenance, will allow you to back up your current DI-106 or DI-106M configuration to disk. Backup is highly recommended once your configuration is functioning.

Backing up a configuration involves downloading configuration information from the router and saving it to disk. Procedures for downloading and saving vary depending on the software used to access the router, but in all cases you must use the XMODEM protocol to perform the download.

Restore Configuration

Selecting option 6 from menu 24, Maintenance, will restore a backup configuration from disk to the DI-106 or DI-106M. You need to upload a backup file to the router. The procedure for uploading varies depending on the software used to access the

router, but you must use the XMODEM protocol to restore the configuration.

Keep in mind that configuration is stored in flash ROM, so even if a power failure occurs, your configuration is safe.

Software Update

Software updates are possible only through an RS-232 cable connection. You cannot use `telnet` to update the DI-106 or DI-106M's software. Note that this function will delete the old software before installing the new software. Do not attempt to utilize this menu unless you have the new software version. There are two different software updates: RAS code and ISDN code.

- **RAS and ISDN code update**—Type **atur** and wait until the DI-106 or DI-106M responds with an OK to begin uploading the new software (upload procedure varies depending on the type of software used to access the router). You must use the XMODEM protocol to perform the upload. After the upload ends, type **atgo** to start the router. Below is an example of downloading RAS and ISDN.

```
To update software, system needs to be rebooted.
After system is rebooted, 'Enter Debug Mode' will be displayed.
Please enter 'atur' to upload RAS and ISDN code.
Do you want to continue (y/n):
Enter Debug Mode
atur
Now erase flash ROM for uploading ...

Starting XMODEM upload.......
■■
Programming successful...
OK
atgo
```

Command Interpreter Mode

This option allows the user to enter the command interpreter mode. This mode allows you to diagnose, test, and configure your DI-106 or DI-106M using a specified set of commands. A list of valid commands can be found by typing help at the command prompt. For more detailed information, contact D-Link technical support.

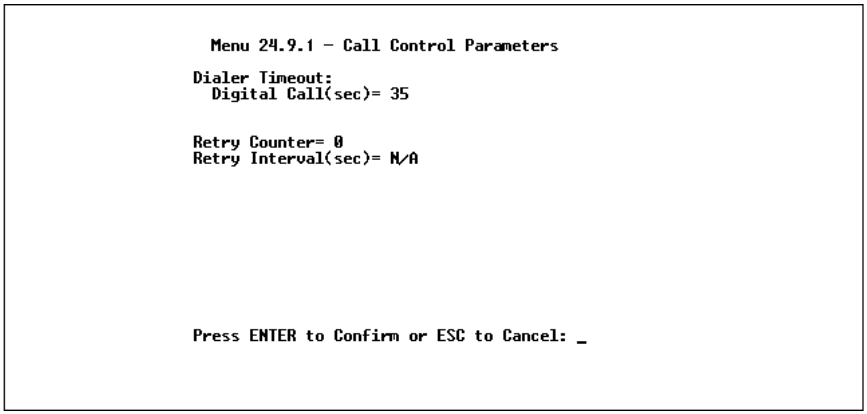
Call Control

The DI-106 or DI-106M provides two Call Control Management functions for the Remote Node and Remote Dial-in User. They are Budget Management and Blacklist.

The Budget Management function provides budget control for outgoing calls and a way for users to set a limit on their ISDN utilization to prevent any accidental usage. It limits the total outgoing call duration over a period of time for each Remote Node or Remote Dial-in User (callback only). If the total outgoing call duration exceeds the set limit, future outgoing calls will not be made and the current call will be dropped.

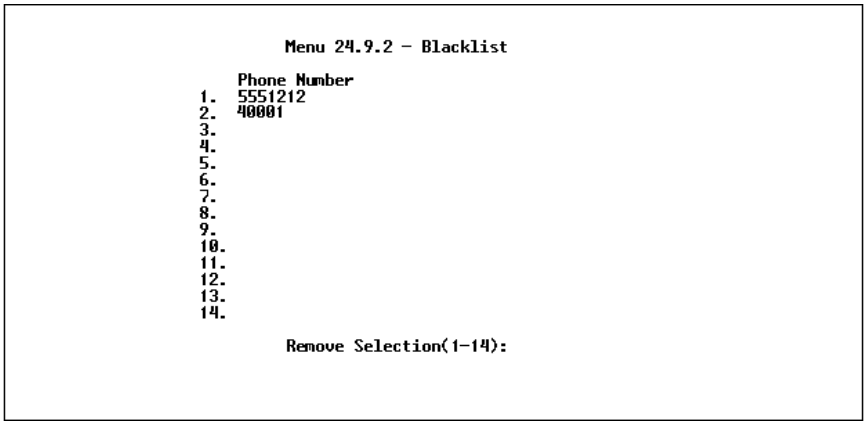
The Blacklist function prevents the DI-106 or DI-106M from re-dialing an unreachable phone number. It is a list of phone numbers, up to a maximum of 14, to which the router will not make an outgoing call. If the router tries to dial a phone number and fails a certain number of times (configurable through menu 24.9.1), the phone number will be put on the blacklist. The user will have to enable the number manually again for it to be dialed.

Call Control Parameters



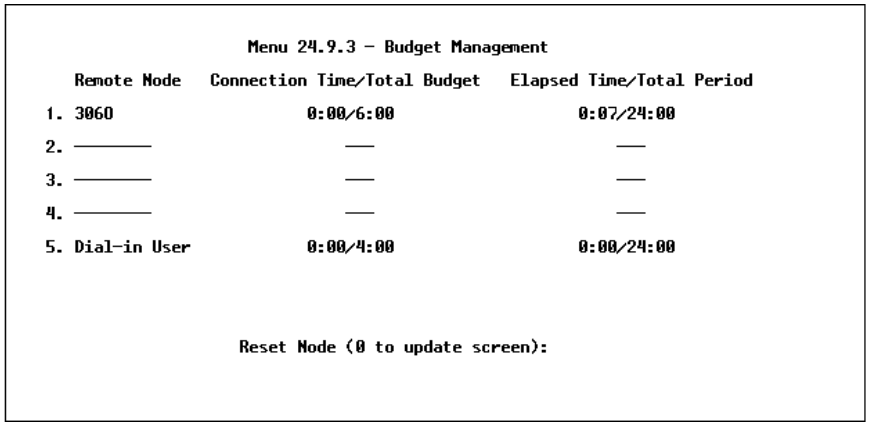
- **Dialer Timeout: Digital Call (sec)**—The DI-106 or DI-106 will "time out" (give up) if it can not set up an outgoing digital call within the timeout value. The default is 30.
- **Retry Counter—**How many times a busy or no-answer phone number is retried before it is put on the blacklist. The default is 0 and the blacklist control is not enabled.
- **Retry Interval (sec)—**Elapsed time after a call fails before another call may be retried. Applies before a phone number is blacklisted.

Blacklist



The phone numbers on this list cannot be entered directly; instead, they are numbers which have had problems connecting in the past. The user can take a phone number off the list by entering its index number.

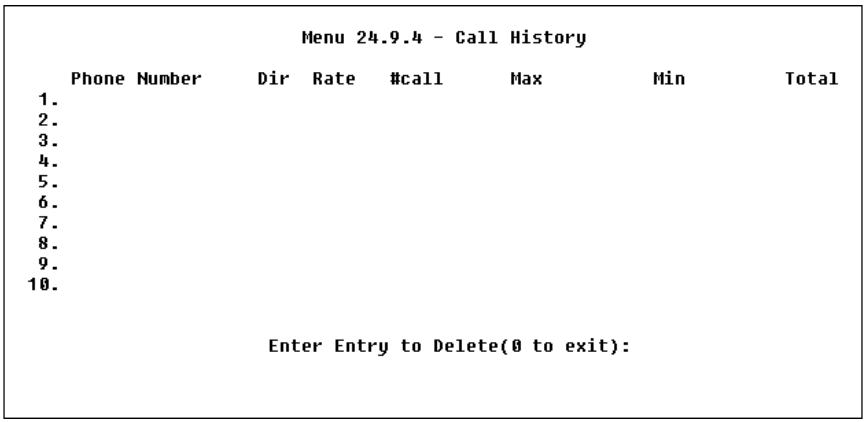
Budget Management



The total budget is the time limit for an outgoing call to a Remote Node or Dial-in User. When this limit is reached, the call will be dropped and further outgoing calls to that Remote Node or Remote Dial-in User (callback) will fail. After each period, the total budget is reset. The defaults for the total budget is 0 minutes and the period is 0 hours. This means no budget control. The user can reset the total outgoing call time through this menu. The total outgoing call timer can be program need to reset itself periodically through menus 11 and 13.

Call History

The call history is erased when you reset the DI-106 or DI-106M. The router keeps track of the first ten calls only; additional calls are not recorded.



The columns in the Call History screen are described briefly below.

1. **Phone Number**—The telephone number of the caller (incoming) or the called party (outgoing). Can contain up to fifteen digits.
2. **Dir**—IN for incoming calls, OUT for outgoing calls.
3. **Rate**—One of the following: 64K, 56K, X75, or V120. (X75 and V120 are available for DSS-1 and 1TR6 firmware only.)
4. **#call**—Number of calls to (OUT) or from (IN) this number.
5. **Max**—Duration of the longest call to or from this number.
6. **Min**—Duration of the shortest call to or from this number.
7. **Total**—Total duration of calls to or from this number.

Troubleshooting

This chapter contains some problems you may run into when using your router. After each problem description, we have provided some instructions to help you diagnose and solve the problem.

Problems Starting Up the DI-106 or DI-106M

None of the LEDs are on when you power up the router

- Check the power cord and the power supply and make sure it is properly connected to your DI-106 or DI-106M. If the error persists you may have a hardware problem. In this case you should contact technical support.

Connecting the RS-232 cable, cannot access the SMT

- Check to see if the DI-106 or DI-106M is connected to your computer's serial port.
- Check to see if the communications program is configured correctly. The communications software should be configured as follows:
  - VT100 terminal emulation.
  - 9600 Baud rate.
  - No parity, 8 Data bits, 1 Stop bit.

Problems With the ISDN Line

The ISDN initialization failed

This problem occurs when you attempt to save the parameters entered in menu 2, but receive the message 'Save successful, but Failed to initialize ISDN; Press ESC to exit'.

1. Check the error log (in menu 24.3.1), you should see a log entry for the ISDN initialization failure in the format, 'ISDN init failed. code<n>...'. Note the code number, n.
2. If the code is 1, the ISDN link is not up. The problem could be either that the ISDN line is not properly connected to the DI-106 or DI-106M, or that the ISDN line is not activated. Verify that the ISDN line is connected to the DI-106 or DI-106M and to the wall outlet (to the telephone company).
3. If the code is 2, this indicates an SPID error. Verify the SPID(s) that you have entered in menu 2. If these are correct, try to initialize again from menu 24.4.3.
4. If the code is 3, this indicates a general failure. Verify the SPID(s) in menu 2. If these are correct, you may also need to verify the provisioning information for your switch by contacting your telephone company.

The ISDN loopback test failed

If the ISDN initialization has passed, then the loopback test should also pass. Verify the phone numbers that have been entered in menu 2. The loopback test will dial the number entered in the 2nd Phone # field (except for switch types with only one phone number). If you need to dial a prefix (e.g., 9) to get an outside line, then you have

to enter the phone number as 95551212 or 914085551212. If it is an internal line, you may only need to enter the last four or five digits (according to your internal dialing plan), e.g., 51212.

Problems with the LAN Interface

Can't PING any station on the LAN

1. Check the LAN LED on the front panel of your router. If it is on, then the link is up. If it is off, then check the cables connecting the router to your LAN.
2. Verify with your network administrator that the IP address and the IP subnet mask configured in menu 3.2 are valid for that LAN.
3. Check the physical Ethernet cable, and make sure the connections on the router and the hub are secure.

Problems Connecting to a Remote Node or ISP

1. Check menu 24.1 to verify the ISDN status. If it indicates down then refer to the section on the ISDN line problems.
2. In menu 24.4.5, do a manual call to that Remote Node. You will see some messages printed onto the screen. The messages will show you whether the call has been connected or not. If the call is not connected, verify the following parameters in menu 11: Pri(mary) Phone #, Sec(ondary) Phone #, and Transfer Rate.
3. If the call is terminated immediately after a connection is established, there may be some kind of negotiation problem. Verify the following parameters in menu 11: My Login, My

Password, Route, IP LAN Addr. Also verify your IP address in menu 3.2.

4. If you check the error log in menu 24.3.1, this will usually give you some logs regarding why the call was dropped. If there is nothing in the log, the call may have been dropped by the remote device that you dialed in to. Make sure that the configuration parameters between these two devices are consistent.

Problems Connecting to a Remote User

1. First verify that you have configured the authentication parameters in menu 13. These would be CLID Authen, Recv. Authen, and Mutual Authen.
2. If the Remote Dial-in User is negotiating IP, verify that the IP address is supplied correctly in menu 13. Check that either the Remote Dial-in User is supplying a valid IP address, or that the router is assigning a valid address from the IP pool.
3. If the Remote Dial-in User is negotiating IPX, verify that the IPX network number is valid from the IPX pool (if it is being used).
4. In menu 14, verify the user name and password for the Remote Dial-in User.

ISDN Switch Types

The following table summarizes the different types of switches supported by the DI-106 and DI-106M, as well as some related information on the switch types (number of phone numbers and SPID numbers). It should be noted that the information in this table is for the common case and is recommended for those cases. Exceptions still exist to these figures. You can locate the provisioning information for the appropriate North American switch type in the next sections.

Switch Type	Geography	No. of Phone #s	No. of SPIDs
AT&T 5ESS NI-1	North American	2	2
AT&T 5ESS Point to Point	North American	1	0
AT&T 5ESS Multipoint	North American	2	2
Northern Telecom NI-1	North American	2	2
Northern Telecom Custom	North American	2	2
DSS1	Europe, Asia	2	N/A
1TR6	Germany	2	N/A

Provisioning For U.S. Switches

For the U.S., the DI-106 and DI-106M (both the U and S/T interface) have been approved by Bellcore and have the IOC (ISDN Ordering Code) “S” Capability, EZ-ISDN 1. Provide this information to your telephone company when you order your ISDN line. If your telephone company is not familiar with this IOC, then ask them what kind of switch you will be connected to and use the information under each switch type to order your ISDN line.

Provisioning For the AT&T 5ESS Switches

The AT&T 5ESS switch type supports three types of ISDN service. These are: National ISDN-1 (NI-1), Multipoint, and Point-to-Point.

For AT&T 5ESS National ISDN-1

Provisioning Feature	Setting
Term Type	A
Circuit Switched Voice (CSV)	1
CSV Additional Call Offering (ACO)	Unrestricted
CSV limit	2
CSV Notification Busy (NB) limit	1
Circuit Switched Data (CSD)	1
CSD Additional Call Offering (ACO)	Unrestricted
CSD limit	2
CSD Notification Busy (NB) limit	1
MTERM	2

For AT&T 5ESS Multipoint

Provisioning Feature	Setting
Term Type	D
Call Appearances (CA)	1
CA Quantity	1
Circuit Switched Voice (CSV)	1
CSV Flexible Call Offering (FCO)	Unrestricted
CSV limit	2
CSV Notification Busy (NB) limit	1
Circuit Switched Data (CSD)	1
CSD Flexible Call Offering (FCO)	Unrestricted
CSD limit	2
CSD Notification Busy (NB) limit	1
MTERM	2

For AT&T 5ESS Point-to-Point

Provisioning Feature	Setting
Term Type	A
Call Appearances (CA)	1
CA Quantity	1
Circuit Switched Voice (CSV)	1
CSV Flexible Call Offering (FCO)	Unrestricted
CSV limit	2
CSV Notification Busy (NB) limit	1
Circuit Switched Data (CSD)	1
CSD Flexible Call Offering (FCO)	Unrestricted
CSD limit	2
CSD Notification Busy (NB) limit	1
MTERM	2

Provisioning For the Northern Telecom Switch

The Northern Telecom switch type supports two types of ISDN service. These are: National ISDN-1 and Custom.

For Northern Telecom National ISDN-1

Provisioning Feature	Setting
Signaling	Functional
Protocol Version Control (PVC)	2 (National ISDN-1)
TEI assignment	Dynamic
Maximum number of keys (maxkeys)	3 (1 to 64 OK)
Release key	No
Ringing indicator	No
Electronic Key Telephone System (EKTS)	Yes or No (set to opposite of ACO)
Additional Call Offering (ACO)	Yes or No (set to opposite of EKTS)
Number of call appearances	2
Notification Busy Limit	3

For Northern Telecom Custom

Provisioning Feature	Setting
Signaling	Functional
Protocol Version Control (PVC)	1 (Custom)
TEI assignment	Dynamic
Maximum number of keys (maxkeys)	3 (1 to 64 OK)
Release key	No
Ringing indicator	No
Electronic Key Telephone System (EKTS)	Yes or No (set to opposite of ACO)
Additional Call Offering (ACO)	Yes or No (set to opposite of EKTS)

Glossary

100BASE-T/TX	100Mbps Ethernet LAN communications standard set by the IEEE (in standard 802.3u); also called “Fast Ethernet.”
100Mbps	100 million bits per second; an expression of transmission speed in a network.
10BASE-T	The original Ethernet LAN communications standard set by the IEEE (in standard 802.3); a 10Mbps standard.
10Mbps	10 million bits per second; an expression of transmission speed in a network.
Address	A number, set of numbers, or name which identifies a computer, network device, or network resource.
Agent	The subsystem in a managed network device that is responsible for responding to SNMP requests and commands, and for sending SNMP traps.
AppleTalk	A network protocol often used with computers running the MacOS operating system.
AUI	Attachment Unit Interface; a 10Mbps external

transceiver interface.

Bandwidth The range of frequencies available across a communications channel; in one sense, the "size" of the communications channel.

Bindery A database containing information about a Novell NetWare file server's configuration and users. See also **NDS**.

BOOTP The BOOTstrap Protocol, a method network devices can use to obtain TCP/IP configuration information from a central location on startup.

Bridge A LAN device used to connect two different LANs so that packets can be transmitted from one to the other. A bridge works on a low level, and does not take higher-level protocols into consideration. A switching hub is a type of bridge.

Broadcast A network transmission intended for all of the stations on a network.

Cascading The practice of connecting identical or similar LAN devices such as hubs together directly so that they function as one device. A collection of cascaded devices is often called a stack.

Category 3, 4, 5	Communication cabling standards referring to the quality of the transmission medium and whether or not the cable includes transmission leakage shielding.
Collision	Simultaneous data transmission on a network medium, resulting in a garbled (and unreadable) transmission. See **CSMA/CD**.
Collision Domain	A section of a network isolated from other sections by a switch, bridge, or hub that detects and resolves collisions locally so that there is less impact on the entire network.
Community Name	A part of an SNMP request, used as a rudimentary form of password. An SNMP agent may grant different levels of access to requests with different community names.
Crossover Cable	A type of twisted-pair cable in which the wires at one end have been reversed in order to match pinouts on a hub or switch.
CSMA/CD	Carrier Sense Multiple Access with Collision Detection; a network communications protocol in which each transmission source (i.e., station, server, switch, etc.) monitors the main data channel for traffic before and during transmission, postponing transmission when the data channel is in use.
Cut-through	Bridge forwarding method where each packet with a valid address is passed on to the next

	node without waiting for the entire message to be received.
DHCP	Dynamic Host Configuration Protocol; a superset of BOOTP that allows TCP/IP address information to be determined automatically and dynamically.
Duplex (full/ half)	A method of transmitting data over a network in both directions. Full-Duplex (FDX) is simultaneous transmission of data over a network channel in both directions. Half-Duplex (HDX) is transmission in both directions but one at a time, not simultaneous.
Ethernet	A particular type of LAN described in a standard (802.3) established by the IEEE, with 10Mbps data transmission.
Fast Ethernet	An extension of Ethernet LAN (defined in standard 802.3u) to allow 100Mbps transmissions.
File Server	A computer specialized for providing file storage to client stations on a network.
Frame	A single packet of information transmitted on the network.
Frame Type	An arrangement for the information transmitted in a network frame.

Gateway	A router on a network which is serves as a gateway to outside non-local networks such as the Internet.
Hub	The central device in a star-topology LAN used to connect each station to the network.
ICMP	Internet Control Message Protocol; part of the TCP/IP suite of protocols, used "behind the scenes" by the TCP/IP network subsystem for controlling and monitoring transmissions.
IEEE	Institute of Electrical and Electronics Engineers, an accredited professional group of scientists and engineers who help set standards for LAN communications technology.
In-band	Communications with a network device using the network medium itself. Contrast with out-of-band.
IP Address	A network address used on TCP/IP networks such as the Internet to uniquely identify the host or device. IP addresses are usually written in the form *xxx.xxx.xxx.xxx*, where each *xxx* is a number between 0 and 255 (for a total of 32 bits).
Jabber	A malfunction on a network where random data is continuously transmitted.
LAN	Local Area Network, an interconnected set of computers and other devices.

LED	Light Emitting Diode – an electronic device that lights up when electricity is passed through it. LEDs are commonly used for status indicators on electronic devices.
MAC Address	Media Access Control (layer) address; a low-level network address which uniquely identifies the network interface. Ethernet addresses are normally written in hexadecimal in the form xx:xx:xx:xx:xx:xx. The first three groups identify the manufacturer of the Ethernet interface, and the last three identify the interface itself.
Mbps	Megabits per second; millions of bits per second.
MIB	Management Information Base; a well-defined collection of statistics and control variables accessible using SNMP.
MIB-II	A standard Management Information Base that provides access to a collection of management statistics common to most network devices.
MII	Media Independent Interface; a type of 100Mbps Fast Ethernet external transceiver connector similar in purpose to the AUI connectors used with 10Mbps Ethernet.

Multicast	A single network transmission intended for a collection of network stations, but not to all (compare Broadcast).
NDS	NetWare Directory Services; an expanded database of configuration and user information shared between a collection of NetWare file servers.
NetBEUI	NetBIOS Extended User Interface, the network protocol normally used with Microsoft Networking services.
NMS	Network Management System, a collection of software used for remotely monitoring and managing network devices.
Out-of-Band	Communications with a network device using some medium other than the network itself.
Packet	An addressed segment of data transmitted on a network.
Peer-to-Peer	A form of networking where all stations on the network can provide file service or other network services, without having to go through a central file server.
PING	Packet Internet Network Groper, a method of testing whether a particular Internet address is reachable.
PPP	Point to Point Protocol; a network protocol used for carrying higher-level protocols such

	as IPX or TCP/IP over point-to-point links such as serial lines or ISDN connections.
Preamble	Data bits at the beginning of each block of data, used for synchronization.
Punch-down Block	Physical connection in a network wiring closet.
Repeater	LAN signal regenerator. An Ethernet hub is a type of repeater.
Router	A device for forwarding packets between networks which uses higher-level network protocols (such as TCP/IP or IPX) to determine where packets should be sent. Most routers are capable of forwarding traffic to Wide Area Network (WAN) connections as well as between LANs.
Segment	Part of an Ethernet or other network on which all traffic is common to all nodes.
SLIP	Serial Line Internet Protocol; a method of encoding TCP/IP for transmission over serial lines or modems.
SNMP	The Simple Network Management Protocol; an industry-standard protocol for remotely monitoring and controlling network devices from a Network Management System (NMS). SNMP requests are usually transmitted using TCP/IP, though other means are possible.

Store-and-Forward	Message passing system where the entire message is received before being passed on to the next node.
STP	Spanning Tree Protocol; a network protocol defined in IEEE standard 802.1d, ensuring that a collection of bridges can forward packets throughout the entire interconnected network, while preventing endless network loops.
STP	Shielded Twisted Pair; twisted-pair wire with interference shielding.
TCP/IP	Transmission Control Protocol/Internet Protocol; a suite of transport and network layer communications protocols.
Telnet	Part of the TCP/IP suite of protocols, used for interacting with remote computers and devices using the keyboard and a text display.
TFTP	Trivial File Transfer Protocol; a low-overhead protocol for file transmission over TCP/IP networks. Often used for obtaining device configuration files or bootstrap image files.
Trap	An SNMP request that managed network devices send to network management stations, to inform them that some problem has been detected.
Twisted-pair	Wire such as is commonly used with telephones consisting of pairs of copper wire

	usually terminating in an RJ-45 connector.
UDP	User Datagram Protocol; part of the TCP/IP suite of protocols.
UTP	Unshielded Twisted Pair; twisted pair wire without shielding.
WAN	Wide Area Network (compare “LAN”).

Index