D-Link®

DI-1162/DI-1162M

Remote Access Router

User's Guide

First Edition (August 2000)
6DI1162M..01
Printed In Taiwan

RECYCLABLE

Limited Warranty

Hardware:

D-Link warrants each of its hardware products to be free from defects in workmanship and materials under normal use and service for a period commencing on the date of purchase from D-Link or its Authorized Reseller and extending for the length of time stipulated by the Authorized Reseller or D-Link Branch Office nearest to the place of purchase.

This Warranty applies on the condition that the product Registration Card is filled out and returned to a D-Link office within ninety (90) days of purchase. A list of D-Link offices is provided at the back of this manual, together with a copy of the Registration Card.

If the product proves defective within the applicable warranty period, D-Link will provide repair or replacement of the product. D-Link shall have the sole discretion whether to repair or replace, and replacement product may be new or reconditioned. Replacement product shall be of equivalent or better specifications, relative to the defective product, but need not be identical. Any product or part repaired by D-Link pursuant to this warranty shall have a warranty period of not less than 90 days, from date of such repair, irrespective of any earlier expiration of original warranty period. When D-Link provides replacement, then the defective product becomes the property of D-Link.

Warranty service may be obtained by contacting a D-Link office within the applicable warranty period, and requesting a Return Material Authorization (RMA) number. If a Registration Card for the product in question has not been returned to D-Link, then a proof of purchase (such as a copy of the dated purchase invoice) must be provided. If Purchaser's circumstances require special handling of warranty correction, then at the time of requesting RMA number, Purchaser may also propose special procedure as may be suitable to the case.

After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. The package must be mailed or otherwise shipped to D-Link with all costs of mailing/shipping/insurance prepaid. D-Link shall never be responsible for any software, firmware, information, or memory data of Purchaser contained in, stored on, or integrated with any product returned to D-Link pursuant to this warranty.

Any package returned to D-Link without an RMA number will be rejected and shipped back to Purchaser at Purchaser's expense, and D-Link reserves the right in such a case to levy a reasonable handling charge in addition mailing or shipping costs.

Software:

Warranty service for software products may be obtained by contacting a D-Link office within the applicable warranty period. A list of D-Link offices is provided at the back of this manual, together with a copy of the Registration Card. If a Registration Card for the product in question has not been returned to a D-Link office, then a proof of purchase (such as a copy of the dated purchase invoice) must be provided when requesting warranty service. The term "purchase" in this software warranty refers to the purchase transaction and resulting license to use such software.

D-Link warrants that its software products will perform in substantial conformance with the applicable product documentation provided by D-Link with such software product, for a period of ninety (90) days from the date of purchase from D-Link or its Authorized Reseller. D-Link warrants the magnetic media, on which D-Link provides its software product, against failure during the same warranty period. This warranty applies to purchased software, and to replacement software provided by D-Link pursuant to this warranty, but shall not apply to any update or replacement which may be provided for download via the Internet, or to any update which may otherwise be provided free of charge.

D-Link's sole obligation under this software warranty shall be to replace any defective software product with product which substantially conforms to D-Link's applicable product documentation. Purchaser assumes responsibility for the selection of appropriate application and system/platform software and associated reference materials. D-Link makes no warranty that its software products will work in combination with any hardware, or any application or system/platform software product provided by any third party, excepting only such products as are expressly represented, in D-Link's applicable product documentation as being compatible. D-Link's obligation under this warranty shall be a reasonable effort to provide compatibility, but D-Link shall have no obligation to provide compatibility when there is fault in the third-party hardware or software. D-Link makes no warranty that operation of its software products will be uninterrupted or absolutely error-free, and no warranty that all defects in the software product, within or without the scope of D-Link's applicable product documentation, will be corrected.

D-Link Offices for Registration and Warranty Service

The product's Registration Card, provided at the back of this manual, must be sent to a D-Link office. To obtain an RMA number for warranty service as to a hardware product, or to obtain warranty service as to a software product, contact the D-Link office nearest you. An address/ telephone/fax/e-mail/Web site list of D-Link offices is provided in the back of this manual.

Trademarks

Copyright Statement

FCC Warning

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this user's guide, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

CE Mark Warning

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

Warnung!

Dies ist in Produkt der Klasse A. Im Wohnbereich kann dieses Produkt Funkstoerungen verursachen. In diesem Fall kann vom Benutzer verlangt werden, angemessene Massnahmen zu ergreifen.

Precaución!

Este es un producto de Clase A. En un entorno doméstico, puede causar interferencias de radio, en cuyo case, puede requerirse al usuario para que adopte las medidas adecuadas.

Attention!

Ceci est un produit de classe A. Dans un environnement domestique, ce produit pourrait causer des interférences radio, auquel cas l`utilisateur devrait prendre les mesures adéquates.

Attenzione!

Il presente prodotto appartiene alla classe A. Se utilizzato in ambiente domestico il prodotto può causare interferenze radio, nel cui caso è possibile che l`utente debba assumere provvedimenti adeguati.

BSMI Warning

警告使用者

這是甲類的資訊產品,在居住的環境中使用時,可能會造成射頻干擾,在這種情況下使用者會被要求採取某些適當的對策.

Table of Contents

Introduction

Congratulations on your purchase of a D-Link DI-1162/DI-1162M Remote Access Router. Your new router offers inexpensive yet complete telecommunications and internetworking solutions for your corporate office, school or business. It is ideal for everything from Internet browsing to receiving calls from Remote Dial-in Users. It incorporates the most recent technologies to make fast, secure and stable connections to remote stations via LAN to WAN and vice versa.

Distinguishing features of the DI-1162/DI-1162M include support for a full range of networking protocols such as TCP/IP (Transmission Control Protocol/Internet Protocol), Ethernet, Fast Ethernet as well as various other networking protocols.

Each DI-1162 /DI-1162M router is packed with features that give it the flexibility to provide a complete networking solution for almost any site. The router fulfills the need for Internet access, IP-based intranetworks and LAN to multiple WAN communications.

Ease of Installation

The DI-1162/DI-1162M is a self-contained unit that is quick and easy to install. It is designed to be a standalone unit or it may be mounted on a standard 19-inch networking equipment rack. It uses standard Ethernet wiring to connect (route) a local area network (LAN) to up to 4 separate wide area networks (WANs) through dial-up or dedicated, leased lines.

Also included with the router is the DI-1162/DI-1162M Router Configuration Utility, a Windows-based application that makes configuring the router a snap.

Networking Compatibility

The DI-1162/DI-1162M is compatible with remote access products from other companies such as Ascend, Cisco, and 3Com. Furthermore, it supports Microsoft Windows 95, Windows 98, and Windows NT remote access capability.

Product Features

LAN Port

The DI-1162/DI-1162M is equipped with an auto-negotiated 10/100 (Ethernet and Fast Ethernet) RJ-45 jack for connecting the router to the LAN.

Multiple WAN Ports

The DI-1162/DI-1162M has two EIA-530 WAN ports, each of which can be connected to a dial-up (dial in or out) line or a dedicated leased line by multiplexing with a modem or CSU/DSU (Channel Service Unit/ Data Service Unit) respectively. We recommend connecting only one WAN port to the Internet.

Expansion Slot/Modules

The DI-1162/DI-1162M contains an expansion slot able to house any one of the following slide-in expansion modules:

- An RJ-45 10/100 Fast Ethernet port, giving the router another LAN connection.

- Two high-speed serial (async/sync) ports for two additional WAN connections.
- A BRI ISDN module (S/T interface only).

These modules allow you to expand the functionality of the DI-1162/DI-1162M to fulfill all your internetworking needs.

Dial on Demand

The Dial-On-Demand feature allows the DI-1162/DI-1162M to automatically place a call to a remote node, via a WAN, whenever there is traffic coming from any workstation on the LAN to that remote site.

Full Network Management

The DI-1162/DI-1162M incorporates SNMP (Simple Network Management Protocol) agents and a menu-driven Network Management System accessible via an RS-232 (console) or Telnet connection.

Security

The DI-1162/DI-1162M supports PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), Layer 2 and IP Filtering, and the creation of firewalls.

RIP-1/ RIP-2 Routing Protocols

The DI-1162/DI-1162M supports both RIP-1 and RIP-2 (Routing Information Protocol versions 1 and 2) exchanges with adjacent routers. These exchanges allow the DI-1162/DI-1162M to send and/or receive routing tables to adjacent routers in order to streamline WAN communications.

DHCP Support

DHCP (Dynamic Host Configuration Protocol) allows the DI-1162/DI-1162M router to automatically assign IP addresses to computers as they enter the network. This feature frees the network administrator from assigning and managing IP addresses for each individual machine on the LAN.

Data Compression

The DI-1162/DI-1162M incorporates the hardware-based Stac LZS Data Compression for CCP (Compression Control Protocol).

Network Address Translation (NAT/NAPT)

This feature allows multiple users on the LAN to access the Internet (through an Internet Service Provider) concurrently through a single IP address. This is especially useful for corporate office environments, where a large number of users need access to the internet, but only a few internet addresses are available.

Applications for the DI-1162/DI-1162M

Some applications for the DI-1162/DI-1162M include:

Internet Access

The DI-1162/DI-1162M supports the TCP/IP (a.k.a. IP) protocol, which is the protocol language used for the Internet. This router allows everyone connected to the LAN to access the Internet.

Internet Security

The DI-1162/DI-1162M can act as a firewall between your office network and the Internet, and can hide the size of your office network and the host addresses of your office computers from prying Internet users. It can also filter traffic to and from the Internet allowing only certain types of communications to or from certain locations to pass through.

Link Branch Offices

The DI-1162/DI-1162M routes communications through its two (upgradeable to four) WAN ports allowing direct communications to a branch office via phone lines, the internet or both.

Local Routing

The DI-1162/DI-1162M can route traffic between up to eight local IP networks.

Telecommuting

The DI-1162/DI-1162M allows remote users to dial in and obtain remote access to the LAN. This feature enables users that have workstations with remote access capability, e.g. Windows 95, to dial in using a modem and access the network resources without physically being in the office.

What This Manual Doesn't Cover

This manual assumes that you are familiar with network management and networking devices, especially routing protocols.

Additional Installation Requirements

In addition to the contents of your package, there are other hardware and software requirements needed before the installation and use of your router. These requirements include:

- Ethernet connection(s) to your computer(s) to form a LAN.
- A computer equipped with an RS-232 serial port (standard on most PC's) and serial line communications software (i.e. Microsoft HyperTerminal included with Windows).
- At least one modem or CSU/DSU for connecting the WAN port(s) to a telephone line.
- At least one Internet IP Address per port on the router.
- An Internet Service Provider (ISP).

Installation

This chapter details installation procedures for the DI-1162/DI-1162M router.

Overview

The DI-1162/DI-1162M can be configured in two ways; through a direct serial connection (a console), or remotely, through the included Router Configuration Utility, Telnet, etc. Please note that if you wish to remotely configure the router, you must still use a console to initially configure the LAN or WAN port for a remote connection.

In general, the installation procedures are as follows:

1. Physically install the router into an equipment rack or onto a desktop.
2. Configure the router through a console.
3. Power off the router and console.
4. Plug in all cables and connectors (LAN, WAN, etc.).
5. Power on all devices.

Each of the above items is discussed in detail below.

Note: Your LAN does not need to be powered down when making a LAN connection to the router via the RJ-45 port. However, when connecting devices to the WAN or Diagnostic (console) ports please make sure the router and the other devices are **turned off** before making the connection.

Other Resources

For more information about your DI-1162/DI-1162M please check the following sources:

- Quick Installation Guide.
- Support disk containing *RouteView*, a Windows-based configuration program used to set up and configure the router.
- Frequently Asked Questions (FAQ) and application notes for this router can be found on the D-Link Web site at **http://tsd.dlink.com.tw/**.

Packing List

Before you proceed further, please check all items you received with your DI-1162/DI-1162M Router with this list to make sure the package is complete. The complete package should include:

- One DI-1162 or DI-1162M Router.
- One 100~240V AC power cord (the plug type depends on the region the router is shipped in).
- One RS-232 (DB-9 to DB-9) cable for console connection.
- One 6 ft. (1.83m) Category 5 UTP cable for LAN connection.
- One EIA-530 (DB-25 to DB-25) cable for WAN connection.
- Four rubber feet with adhesive backing.

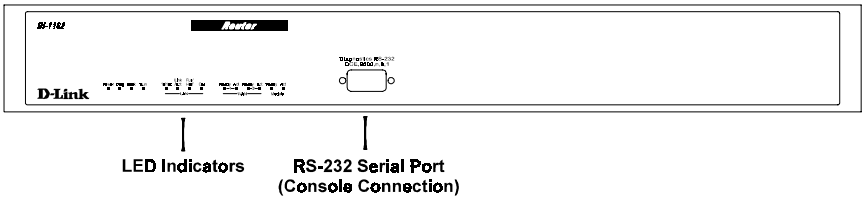
- Rack mount kit including six screws and two mounting brackets.
- One CD-ROM disc or floppy diskette containing the Windows-based Router Configuration Utility.
- This *User's Guide*.

If any item is found missing or damaged, please contact your local D-Link Reseller for replacement.

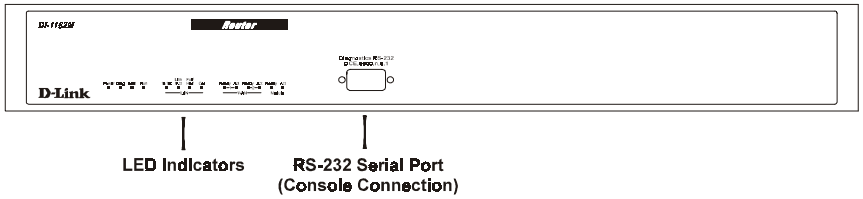
Identifying External Components

The following section illustrates the different components on the router's front and rear panels. Before using the router it is highly recommended to familiarize yourself with these components to ensure effective use of the device.

Front View of DI-1162 Router



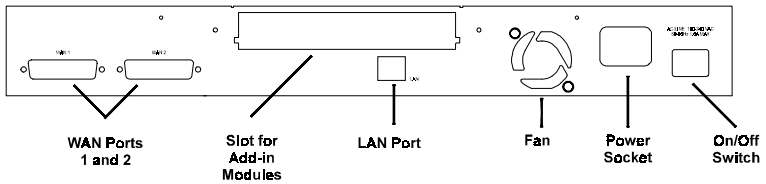
Front View of DI-1162M Router



- **LED Indicators** The front panel consists of the LED indicators of the router. The LED indicators are used to facilitate monitoring and troubleshooting. Please refer to the following chart for detailed descriptions of these indicators.

LED		STATUS/ FUNCTION
Power		Lights whenever the router is plugged in, turned on, and thus receiving power.
Diag		Lights during the startup Power-On Self-Test (POST) test.
Boot		Lights briefly during startup after the PROM program has executed. Indicates a successful boot up.
Run		Should be slowly blinking if the router is functioning properly.
LAN	10/100	This LED is ON for a 100Mbps link, and OFF for a 10Mbps link.
	Link/Act	This LED is ON to show a good link to the LAN, and quickly flashes to show communication activity on the line.
	Full/Half	This LED is ON for a full-duplex connection, and OFF for half-duplex.
	Col	The LED flashes to show transmission collisions on the line.
WANs 1 & 2	Ready	This LED is ON to show a good modem or CSU/DSU link to the WAN port.
	Act	This LED flashes to show communication activity on the line.
Module	Ready	This LED is ON to show a good modem or CSU/DSU link to the WAN module, or a good link to the LAN port module.
	Act	This LED flashes to show communication activity on the line.

- **Diagnostics RS-232 Serial Port** A DB-9 female connector used to connect a console to the router for initial setup and out-of-band management.



- **Wan Ports (1 and 2)** Two DB-25 male connectors each of which can be connected to a dial-up (dial in or out) line or a dedicated leased line by multiplexing with a modem or CSU/DSU (Channel Service Unit/ Data Service Unit), respectively.

- **Slot for Add-in Module** This slot is able to house any one of the following slide-in expansion modules:

  ◊ A single RJ-45 10/100 Ethernet port

  ◊ Two high-speed serial (async/sync) ports

  ◊ A BRI ISDN module (S/T interface only).

- **LAN Port** This jack is a full featured RJ-45 10/100 Ethernet/Fast Ethernet port. This feature allows this port to automatically configure itself to match the settings used by the port it is being connected to. If it is connected

to another 10/100M auto-negotiation capable port, the two ports will configure themselves to attain the best connection possible.

- **Fan** Provides ventilation inside the router. Please ensure to leave adequate space at the rear and sides of the unit for proper ventilation.
- **Power Socket** A standard 100~240V socket for the power cord.
- **Power Switch** A rocker switch that turns the router off and on.

Site Installation

The site where you install the DI-1162/DI-1162M Router may greatly affect its performance. Please follow these guidelines for setting up the router.

- Install the router on a sturdy, level surface that can support at least 2 kg of weight. Do not place heavy objects on the router.
- The power outlet should be within 1.82 meters (6 feet) of the router.
- Visually inspect the power adapter cord and see that it is fully secured to the power socket.
- Make sure that there is proper heat dissipation from and adequate ventilation around the router. Leave at least 10 cm of space at the side and rear of the router for ventilation.
- Install the router in a fairly cool and dry place. See Appendix B for the acceptable temperature and humidity operating ranges.
- Install the router in a site free from strong electromagnetic field generators (such as motors), vibration, dust, and direct exposure to sunlight.
- When installing the router on a level surface, attach the rubber feet to the bottom of the device. The rubber feet cushion the router, protect the casing from scratches and prevent it from scratching other surfaces.

Rack Mounting

The DI-1162/DI-1162M may stand alone or be mounted on a standard 19-inch equipment rack. Rack mounting produces an orderly installation when you have a number of related network devices. Use the six supplied screws to fasten the supplied mounting brackets to either end of the router, then fasten the router into the rack.

Installation and Initial Configuration of the Router

This section discusses the different connections that can be made to the router when setting it up.

Initially, you will only wish to connect the console to the router in order to configure the other ports. Once that is complete, you will need to turn off the power to the router and plug in the connection cables to the other devices. Next, power on the other devices. When they have finished powering up, power on the router. Each of these steps is described in detail in the sections below. Please skip any setting adjustments that do not apply to your configuration needs.

A Warning about Connecting Cables

It is important that correct cables are used for each connection; otherwise, the router could be damaged.

Before connecting or disconnecting an RS-232 cable between the DI-1162/DI-1162M and the console and modems, please make sure all devices are off to avoid any chance of damage.

Step 1 - Setting up the Console

The initial setup of the DI-1162/DI-1162M requires connecting a console to the 9-pin RS-232 Diagnostic port on the router's front panel. A serial cable is supplied with the router in order to make this connection. A console can be a terminal, such as a VT-100, or a normal PC running terminal emulation software (such as Microsoft HyperTerminal, included with Windows). The terminal emulation software needs to be configured to the following parameters:

- ◊ VT100 terminal emulation
- ◊ 9600 baud
- ◊ No parity, 8 data bits, 1 start bit, 1 stop bit
- ◊ No flow control

Step 2 - Connecting the Console to the Router

A serial cable is included in the DI-1162/DI-1162M package. To connect this cable, plug its nine-pin connector into the 9-pin RS-232 Diagnostic port on the router's front panel, then connect the other end to the serial port on the rear of your computer or data terminal.

Please make sure both machines are turned off before making this connection.

After the connection is made, first power on the console. If you are using a PC, run the terminal emulation software at this time. After the PC and the terminal emulation software are up and running, power on the router.

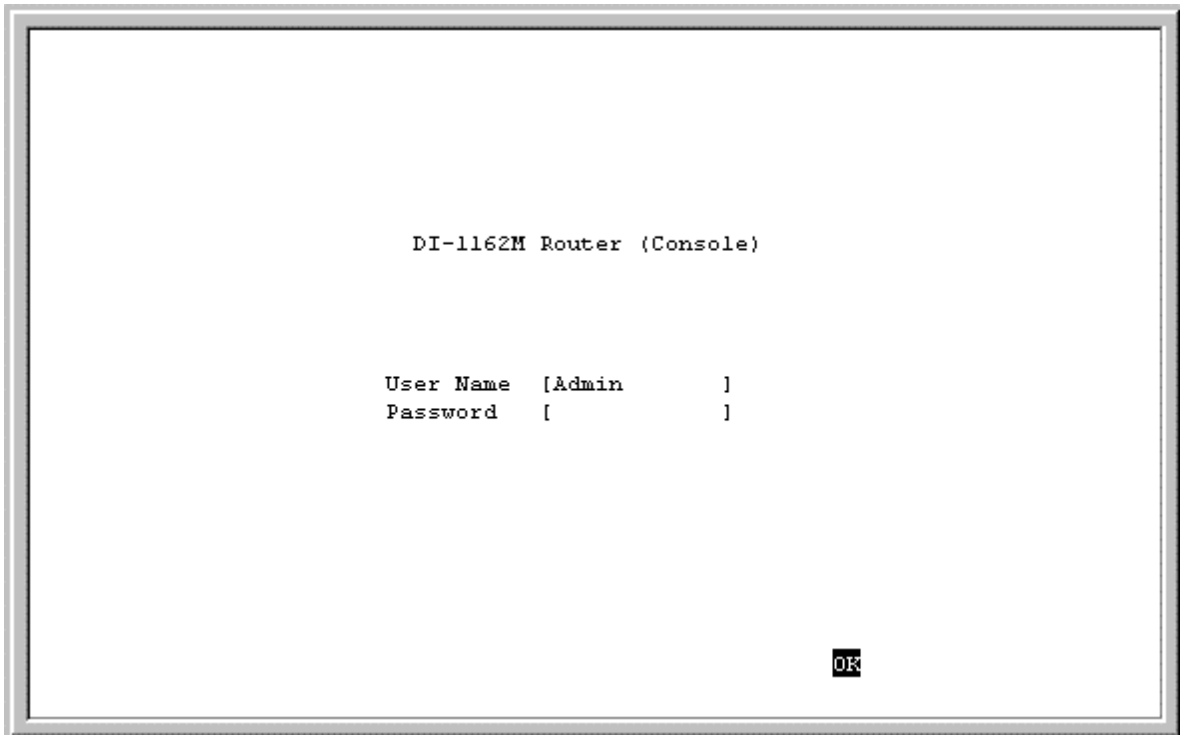
Using the Console

The Console Program is the interface that you will be using to configure your DI-1162/DI-1162M. 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 submenu below the current one, use Tab or arrow keys to position the cursor on the submenu item and press Enter to view the selected submenu.
- ♦ **Moving the Cursor** Within a menu, use Tab and arrow keys to navigate through different information fields.
- ♦ **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. Upon configuring all fields the submenu, position the cursor on SAVE and press Enter to save, or position the cursor on EXIT to cancel.
- ♦ **Refreshing the Screen** Console screens are notorious for becoming garbled. When this happens, simply press <Ctrl> + <R> to refresh the contents of the screen.

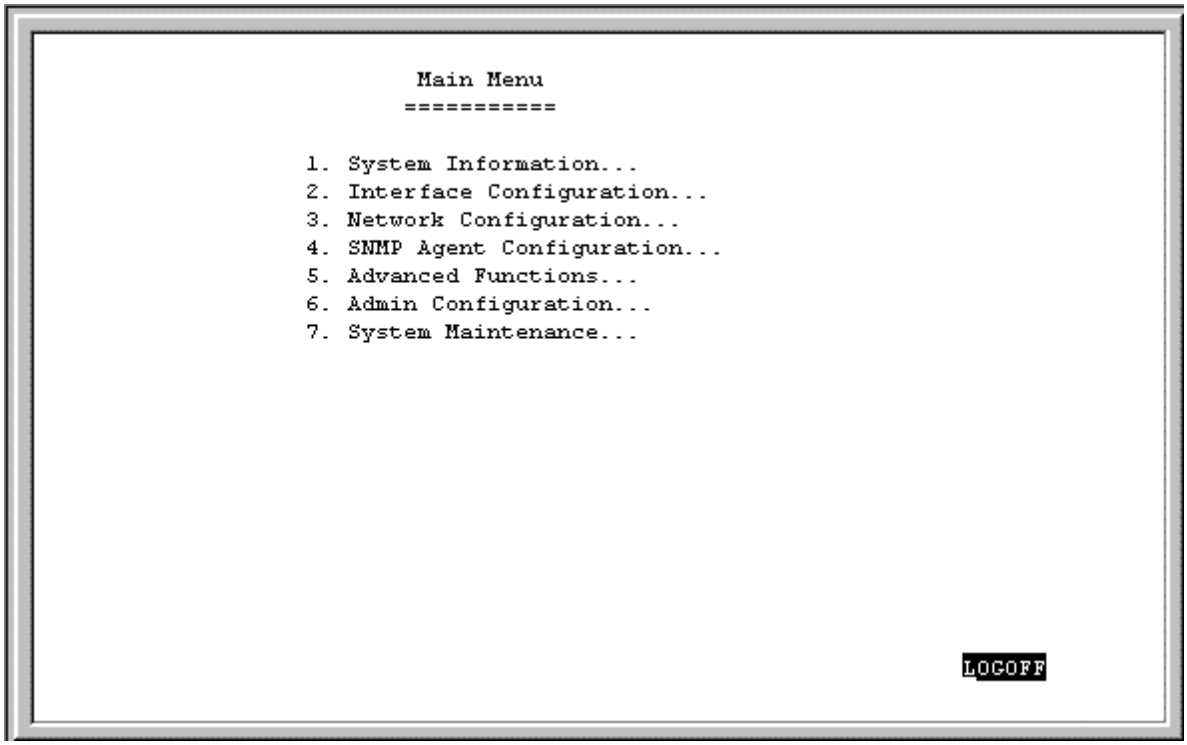
Step 3 - Initial Configuration of the Router

After the console is properly connected and both devices are powered on as described in the preceding sections, you should see the router run through the power on self test (POST). Finally, it will arrive at the logon screen shown below:



To log on to the router, use the factory set username and password 'Admin' (without the quotes). Please note that the user name and password are case-sensitive.

Upon entering the username and password (using the <Tab> key to jump to the next field), position the cursor on OK and press <Enter>. You will then see the following **Main Menu**:



Step 3a - Configuring the LAN Port

Preparing the router for connection to a LAN only requires enabling the LAN port, enabling IP networking ,and assigning the LAN port an IP address. After the LAN port is configured, all other features on the router can be configured remotely through the LAN by using the included Windows-based Router Configuration Utility or Telnet.

To configure the LAN:

1. The LAN port must be enabled in the **Interface Configuration** submenu.
   - Choose **Interface Configuration→LAN 1.**
   - Position the cursor over the State item and press <space bar>. The State will change from *Disable* to *Enable*.
   - Position the cursor on the Save option at the bottom of the screen and press <Enter> to save the new setting.
   - Choose Exit in the submenus to return to the **Main Menu**.
2. Enable IP Networking
   - Choose **Network Configuration→IP Configuration**.
   - Position the cursor on the IP Networking line and press <space bar> to *Enable* it .
   - Position the cursor on the Save option at the bottom of the screen and press <Enter> to save the new setting.
3. Assign an IP address to the LAN port in the **Network Configuration** submenu of the **Main Menu**.
   - Still in **Network Configuration→IP Configuration** submenu from Step 2 above, choose **IP Stack Configuration→LAN 1**.
   - Enter a valid IP address for the LAN in the first item. You may also enter a Netmask if you wish. For more information about IP Addresses and Subnet masks, please refer to "*Appendix C – IP Concepts.*"
   - Position the cursor on the Save option at the bottom of the screen and press <Enter> to save the new setting.
   - Choose Exit in the submenus to return to the **Main Menu**.

The router can now be accessed via the LAN by Telnet, the Windows-based DI-1162/DI-1162M Router Configuration Utility (included with the router) and other SNMP management applications.

If you have any questions regarding the settings you made or other settings in the submenus, please refer to the next chapter, "*Configuration and Management.*"

At this point, please proceed to the next initial configuration step.

Step 3b - Configuring the WAN Ports for Dial-in, Dial-out and Leased Lines

Please configure LAN port as described above to familiarize yourself with the configuration program (the LAN port must be configured in any case). Some settings that were made configuring the LAN will be repeated below. Please disregard the instructions below if the setting has already been changed.

Each WAN port can be configured to either receive dial-in calls (act as a Remote Access Server), dial out to other routers (at branch offices or the Internet, for instance), or both (but not at the same time). The WAN ports can also be configured for a leased line (synchronous) connection. Please note however that we recommend only one single WAN connection to the Internet since a second connection will not significantly enhance the performance of the connection.

Enabling a WAN Port

In this section, we will use WAN1 as an example. Other WAN ports however, will follow the same procedures.

1. The WAN port must be enabled in the **Interface Configuration** submenu.

   - Choose **Interface Configuration→WAN 1**.

   - Configure the Protocol setting. This is a very important setting as it determines what type of device can be connected to the WAN port.

     - *SLIP* Asynchronous mode used for modems.
     - *PPP_ASYN* Asynchronous mode used for modems.
     - *CISCO_HDLC* Synchronous mode used for CSU/DSU's or synchronous modems using a leased line.
     - *PPP_SYN* Synchronous mode used for CSU/DSU's or synchronous modems using a leased line.
     - *FRAME_RELAY* A high-speed protocol available from many ISPs for switched lines. The current version of this router only supports IP over frame relay and PVC. OSPF, IPX, and bridge are not supported.

   - Position the cursor over the State item and press <space bar>. The State will change from *Disable* to *Enable*.

   - Other items in this screen also need to be configured such as the Phone Number, Baud Rate, and additional Frame Delay Config settings, which appear on a series of screens accessed from the bottom of this window if *FRAME_RELAY* is selected. Please refer to the manual for the device being connected to the WAN port for the proper settings. For more information regarding these settings, please refer to the appropriate section in the "*Configuration and Management"* chapter of this manual.

   - Position the cursor on the Save option at the bottom of the screen and press <Enter> to save the new setting.

   - Choose Exit in the submenus to return to the **Main Menu**.

2. Enable IP Networking.

   - Choose **Network Configuration→IP Configuration**.

   - Position the cursor on the IP Networking line and press <space bar> to *Enable* it.

   - Position the cursor on the Save option at the bottom of the screen and press <Enter> to save the new setting.

3. Assign an IP address to the WAN port in the **Network Configuration** submenu of the **Main Menu**.

   - Still in **Network Configuration→IP Configuration** submenu from Step 2 above, choose **IP Stack Configuration→WAN 1**.

   - Enter a valid IP address for the WAN in the first item. You may also enter a Netmask if you wish. For more information about IP Addresses and Subnet masks, please refer to "*Appendix C – IP Concepts*."

- Other items in this screen may also need to be configured such as the State, Routing and Multicast settings. Please refer to the appropriate section in the "*Configuration and Management"* chapter of this manual for detailed explanations concerning the nature and use of these items.

- Position the cursor on the Save option at the bottom of the screen and press <Enter> to save the new setting.

- Choose Exit in the submenus to return to the **Main Menu**.

Configuring for Dial-in, Dial-out or Leased Line

At this point, you need to decide if the WAN port will be used for dialing in, dialing out, both or a leased line connection. The settings you make in next few steps depend on how you wish to use the WAN port. Remember, only one WAN port should be setup to connect to the Internet.

4. Configure the Dial settings in the **Advanced Functions** submenu.

   - Choose **Advanced Functions→Dial Configuration**.

   - Choose **WAN1**.

   - Please refer to the "*Configuration and Management"* chapter of this manual for more detailed information regarding the items in this screen.

   - Position the cursor on the Save option at the bottom of the screen and press <Enter> to save the new setting.

5. Define and configure dial-in users who may access the router and the LAN it is connected to (if applicable).

   - From the **Main Menu** choose **Advanced Functions→Remote Access Configuration→Dial-In User Profile** and press <Enter> in the first empty field.

   - Enter the dial-in user's Username (this might not be their real name) and Password.

   - Change the State to *Enable*.

   - Please refer to the "*Configuration and Management"* chapter of this manual for more detailed information regarding the items in this screen.

   - Position the cursor on the Save option at the bottom of the screen and press <Enter> to save the new setting.

   The WAN port is now setup to receive calls from that user. At this point, you may wish to define other users who will dial-in to the router. Please note that User Profiles for dial-in users are valid for any WAN port configured to receive calls.

6. Define a WAN port for dialing out.

   - From the **Main Menu** choose **Advanced Functions→Remote Access Configuration →Remote Network Profile** and press <Enter> in the first empty field.

   - Set the Direction to *In*, *Out*, or *Both*.

   - Enter a Name and Password used to establish Incoming and/or Outgoing connections (if the remote site uses PAP or CHAP).

   - Configure the other settings shown in this window.

- Change the State to *Enable*.
- Please refer to the "*Configuration and Management"* chapter of this manual for more detailed information regarding the items in this screen.
- Position the cursor on the Save option at the bottom of the screen and press <Enter> to save the new setting.
- Choose Exit in the submenus to return to the **Main Menu**.

7. Define a WAN port for a leased line connection.

   - There are only three steps that need to be done to configure a WAN port for using a leased line and they have already been done. They are numbers 1, 2 and 3; enabling the WAN port in the **Interface Configuration** submenu, configuring the Protocol setting to a synchronous mode, and assigning an IP Address to the WAN port in the **Network Configuration** submenu. Remember to save any submenu screens in which you have made changes.

Choose LOGOFF from the **Main Menu**.

Your WAN ports are now configured and should operate normally. Please note that many of the settings configured here depend on the type and capabilities of the device being connected.

At this point in the installation process, you need to turn off the router. Don't worry. As long as you saved each screen in the configuration process, your settings will have been saved in the EEPROM and will not be lost.

Step 4 - Connecting the Router to a LAN

Your DI-1162/DI-1162M has a single LAN port for connecting to an Ethernet or Fast Ethernet switch or hub.

The jack for the router's Ethernet port is of the type known as EIA RJ-45. The cabling used should be Category 3, 4 or 5 UTP or STP depending on the connection speed, fitted with an RJ-45 connector.

The 10/100M auto-negotiation feature allows this port to automatically configure itself to match the settings used by the port it is being connected to. If it is connected to another 10/100 Fast Ethernet capable port, the two ports will configure themselves to attain the best connection possible.

Full duplex mode will only be enabled if this port is connected to a full-duplex capable switched port.

At this point, please connect the router to the LAN.

Step 5 - Connecting the Router to WAN Devices

The DI-1162/DI-1162M has two DB-25 ports corresponding to WANs 1 & 2. These two WAN ports are both synchronous/asynchronous ports, and can connect to a modem or CSU/DSU using a standard serial cable with a DB-25 connector at one end.

Make sure both the WAN device(s) and the router are turned OFF when making these connections.

Step 6 – Plugging in All Devices

Plug the 100 ~ 240V AC/DC power cord into the power jack on the router's rear panel and into a power strip or grounded wall outlet.

At this point in the installation, you may plug in and power on all other devices. Do not power on the router yet.

Step 7 - Powering Up the DI-1162/DI-1162M

After all the devices are powered up, the DI-1162/DI-1162M can be turned ON. The router will perform a POST (Power-On Self-Test). It is during this POST procedure that the PROM Configuration Menu can be accessed.

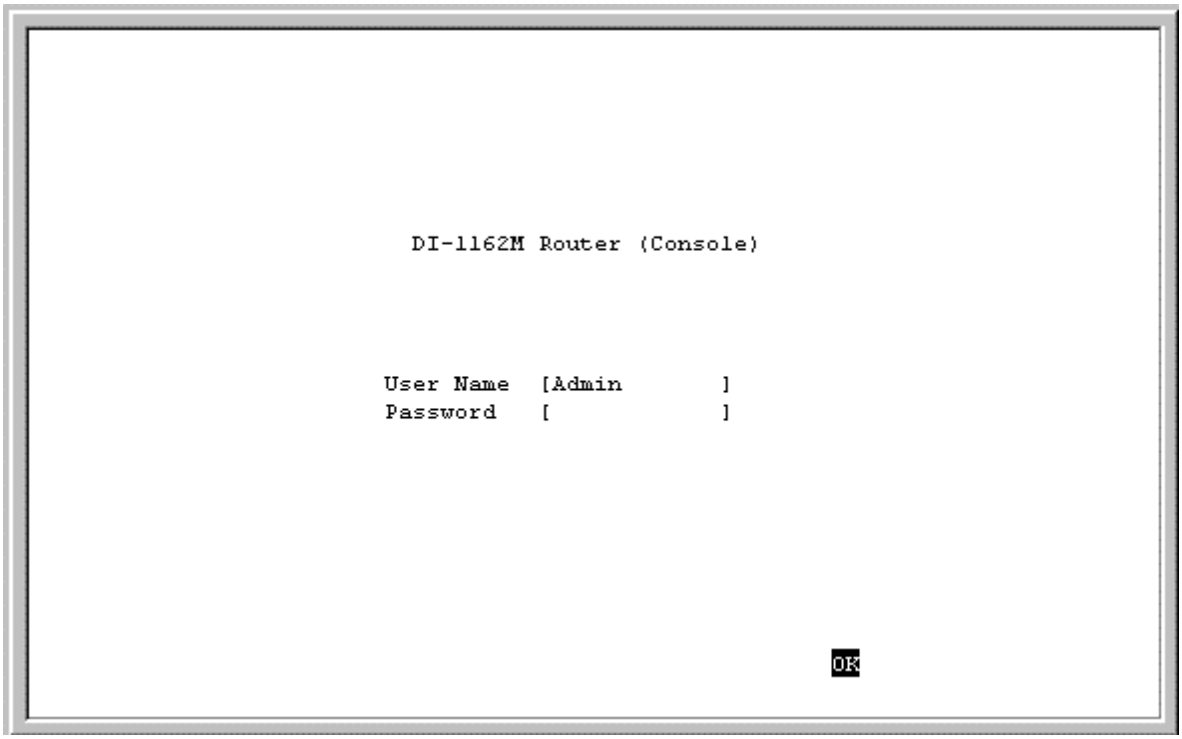
The router is now able to use the LAN and WAN ports.

The router must be further configured for managing your network. This can now be done by using the console, the included Windows-based Configuration Utility, or Telnet.

For more information about configuring or managing the router, please refer to the next chapter, "*Configuration and Management*."

Configuration and Management

After the initial startup (POST) test, the router will prompt you for login and password. This is the opening page of the router's configuration program, called the Console program. The Console program is stored in the Flash memory chips in the router and the settings are written in EEPROM chips in the router. It is the most basic level for configuring and managing the router and the network to which it is connected.



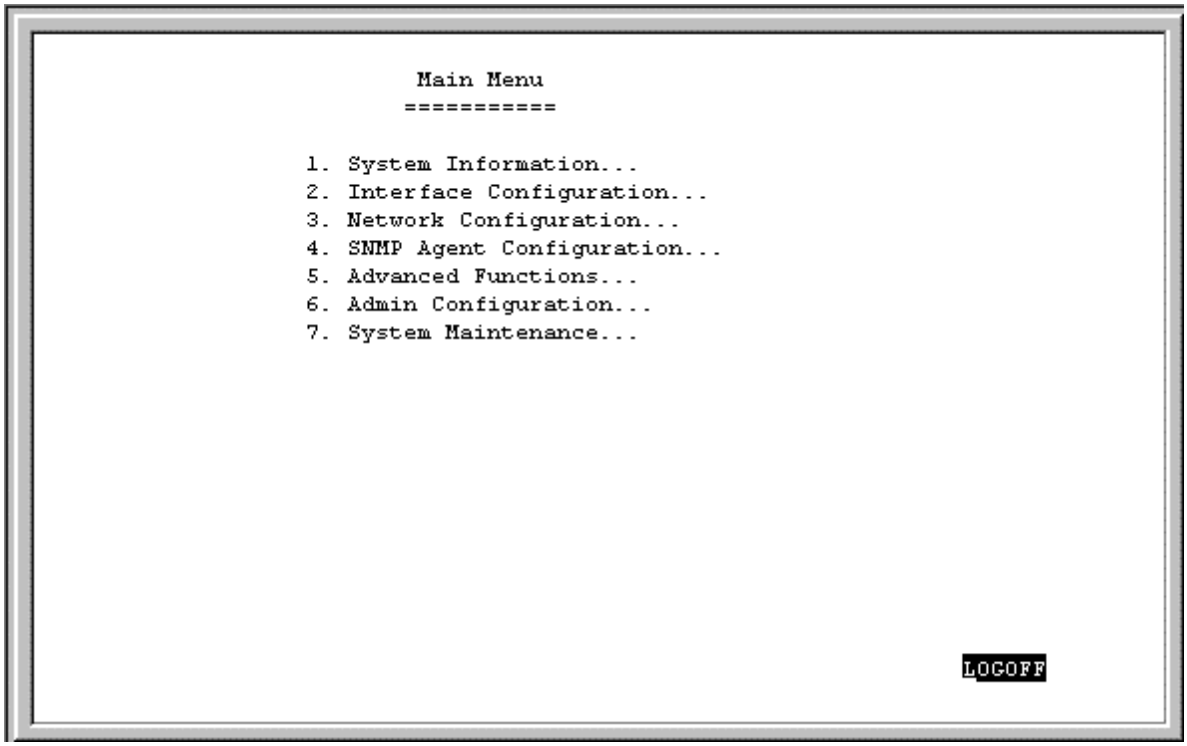
If you're starting the router for the first time, the default login and password is "Admin" – the login and password are case-sensitive, alphanumeric characters.

Note that once you are in the **Main Menu**, if there is no activity for more than 5 minutes, the router will automatically log you out. Your first endeavor should be to increase the 'timeout' time by adjusting the appropriate value in the **System Information** submenu.

The router can also be configured remotely through a LAN or WAN connection by using the included Router Configuration Utility or Telnet. However, if you wish to do this, the console program must first be used to initially configure the relevant port on the router. Please see *Step 3 - Initial Configuration of the Router* on page 8 of this manual for more detailed information.

Console Program Main Menu

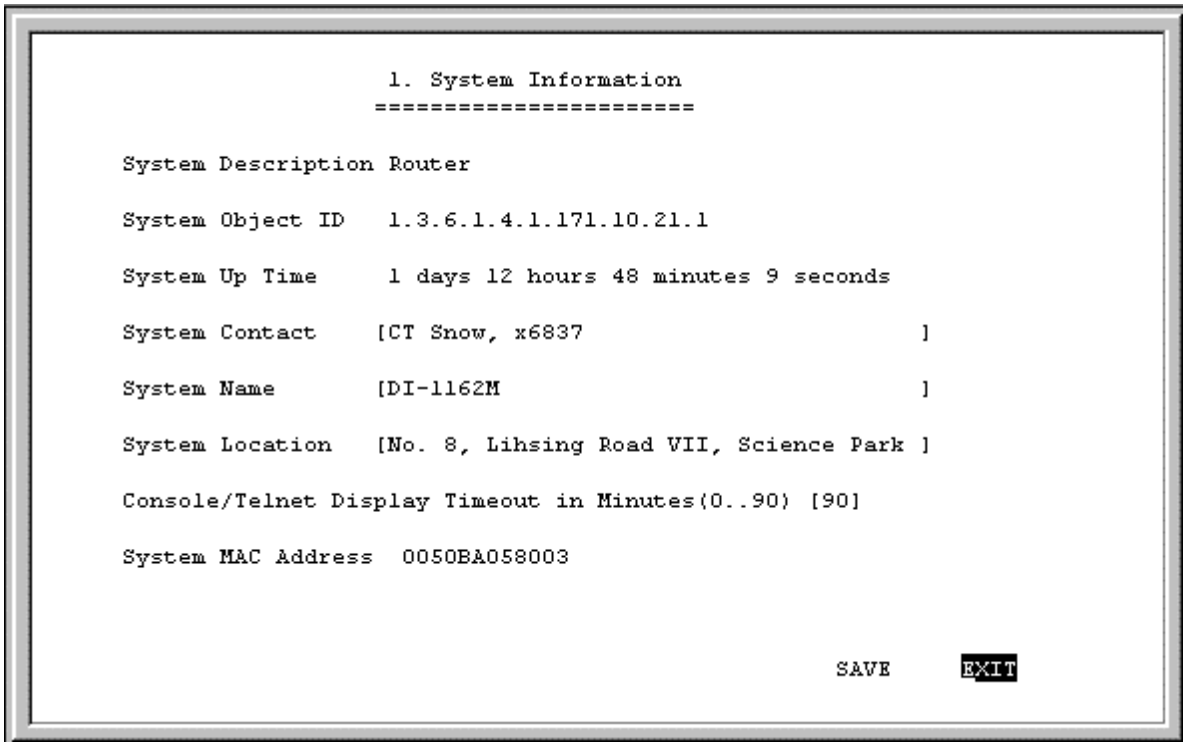
The **Main Menu** is shown below.



As mentioned earlier, your first endeavor should be to increase the automatic timeout. Enter the **System Information** to do this. You will see this screen:

System Information

This menu contains administrative and system-related information:

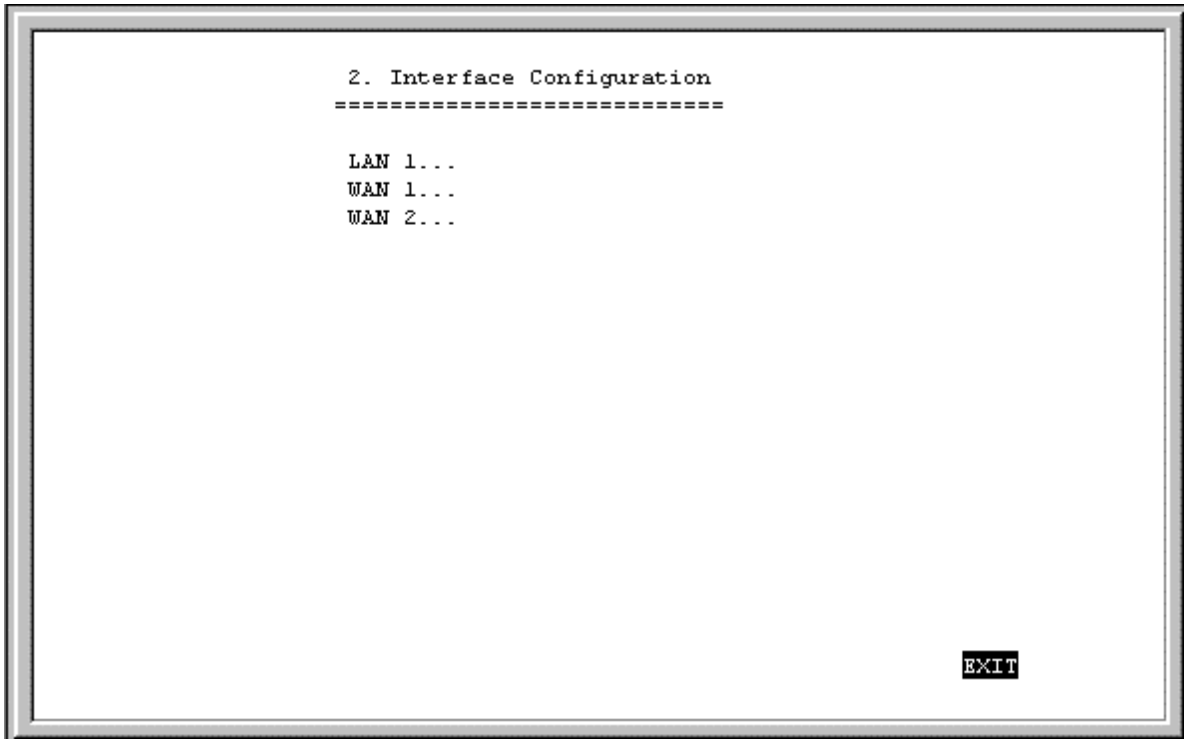


The above parameters are described as follows:

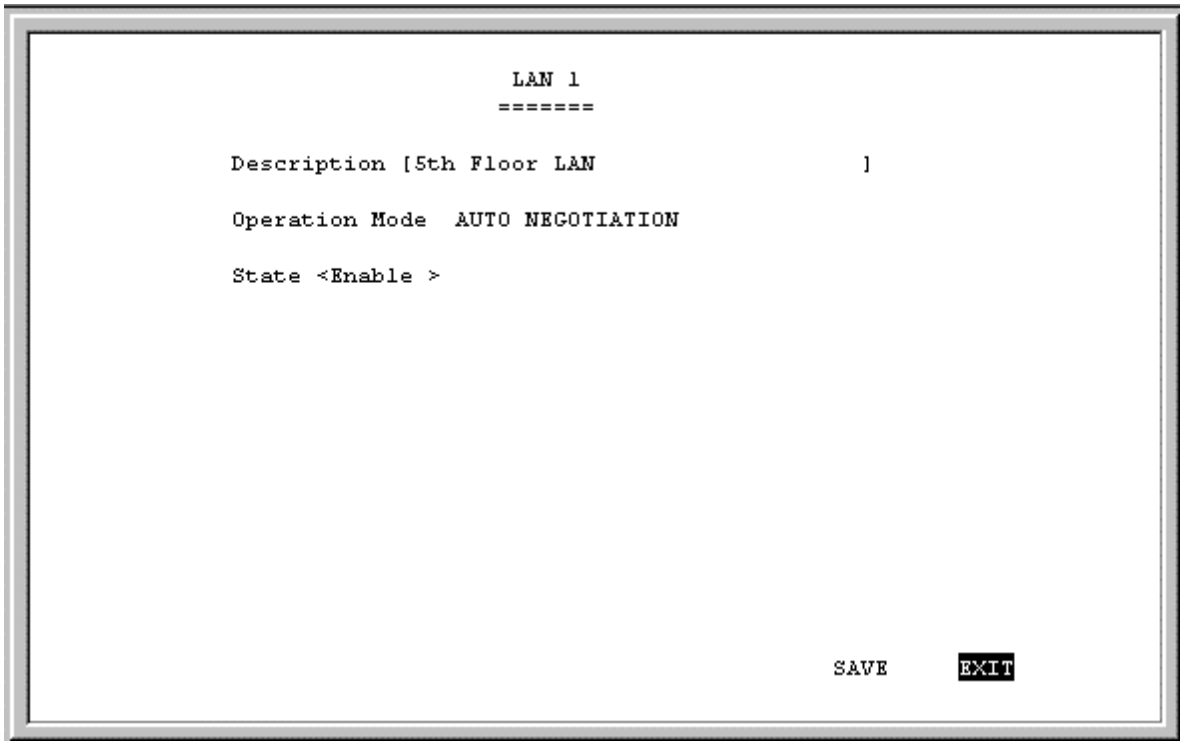
- **System Description –** This is a non-changeable, short description of the product.
- **System Object ID –** This is the enterprise-specific MIB Object ID indicating this type of router.
- **System Up Time –** Shows how long the router has been running since the last power off or reset.
- **System Contact –** Enter the name of the department or individual responsible for maintaining the router.
- **System Name –** Give the router a descriptive name for identification purposes.
- **System Location –** Enter the physical location of the router.
- **Console/Telnet Display Timeout in Minutes –** This is a security measure to automatically logoff from the console menu after a given idle time. Enter a timeout time between 0 and 90 minutes. Zero specifies no timeout.
- **System MAC Address –**The physical address of this router.
- **External MAC Address –** The physical address of the external LAN add-in module, if present.

Interface Configuration

Under Interface Configuration in the main menu is the following **Interface Configuration** screen, used to configure the interfaces for the LAN(s) and two WANs:



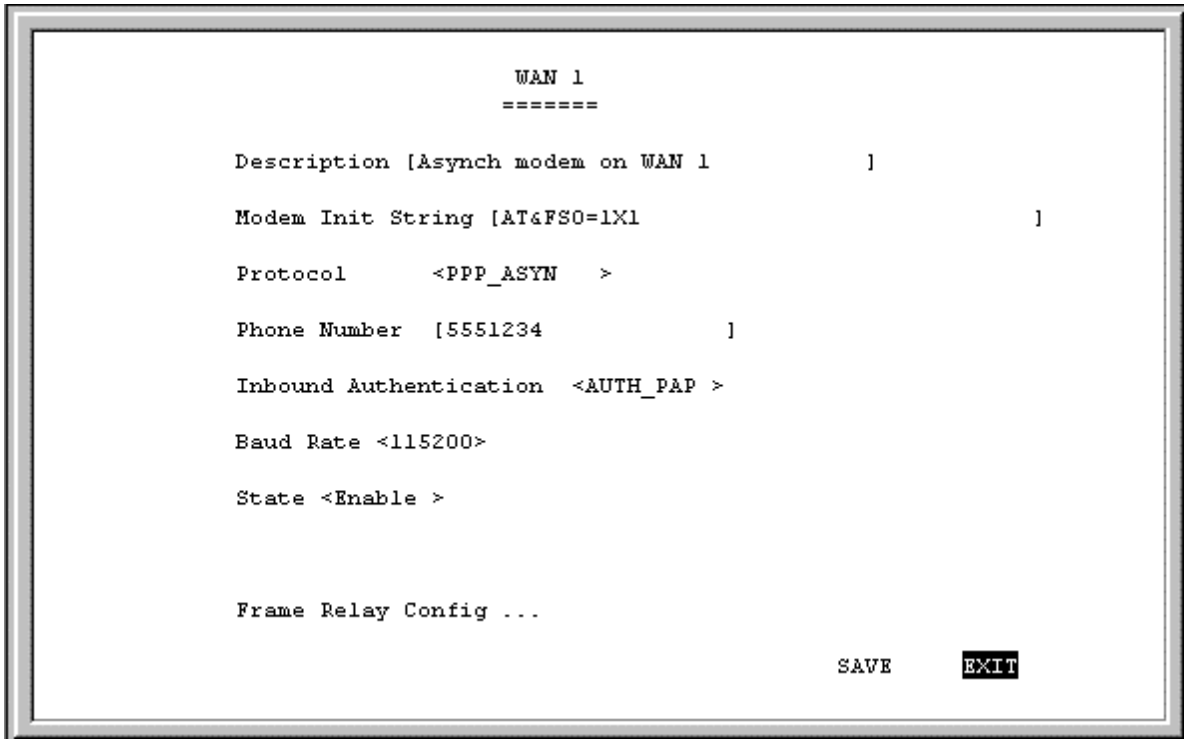
LAN



The parameters are described below:

- **Description –** This is a user-defined, 32-character identifier used to name the LAN.
- **Operation Mode –** The LAN port is automatically set to auto-negotiation. When connected to another LAN port, 10/100 Fast Ethernet will configure this port to match the settings of the other LAN port. If the other port also implements 10/100 Fast Ethernet, the two ports will auto-negotiate the best possible settings achievable by both ports.
- **State –** This is a toggle, to *Disable* or *Enable* the LAN interface.

WAN



The parameters are described below:

- **Description –** This is a user-defined, 32-character identifier used to name the WAN.
- **Modem Init String –** This parameter is valid only for asynchronous connections. It is a user input AT command string to initialize a modem or ISDN TA attached to the WAN interface. Please refer to your WAN device's handbook for more information about using initialization command strings.

  The default setting is for Hayes-compatible asynchronous modems and is `AT&FS0=1X1`, where:

  AT– The mandatory first two characters of an AT command string.

  &F– Initializes the modem to its default settings.

  S0=1– Sets the modem to auto-answer.

  X1 – Displays the established connection speed to the dial-in user (e.g. Connection established at 56.6 kps).

- **Protocol –** This is a protocol used to encapsulate IP messages over synchronous and asynchronous serial links. The device being connected to must be using the same protocol for a connection to succeed. The five protocols are described:

  1. *CISCO_HDLC* – This is a serial line encapsulation method for transmitting datagrams over synchronous serial point-to-point links.
  2. *SLIP* – Serial Line Internet Protocol. A serial line encapsulation method for transmitting datagrams over asynchronous serial point-to-point links. If linking the router to a computer, each end must know the other's IP address.
  3. *PPP_SYN* – This serial line encapsulation provides a method for transmitting datagrams over synchronous serial point-to-point links. Unlike the SLIP protocol, PPP can determine the IP address configuration automatically.

4. *PPP_ASYN* – This serial line encapsulation provides a method for transmitting datagrams over asynchronous serial point-to-point links. Unlike the SLIP protocol, PPP can determine the IP address configuration automatically.

5. *FRAME_RELAY* – This serial line encapsulation provides a method for high speed transmission of datagrams over dedicated lines. We currently only support PVC.

- **Phone Number –** This is only a reference field, used to contain your line's phone number when using an asynchronous dial-in modem.

- **Inbound Authentication** – This defines the authorization protocol that will be used when accepting a dial-in connection. The choices are Password Authentication Protocol [*AUTH_PAP*], Challenge Handshake Authentication Protocol [*AUTH_CHAP*] or *None*. *AUTH_PAP* and *AUTH_CHAP* do not provide a screen for users to manually enter their Username and Password – instead, this data must be entered into the dialing software before placing the call. Make sure the device dialing in is using the same protocol as defined here. The *None* setting may be used when you do not wish dial-in users or networks to identify themselves or be subject to security.

- **Baud Rate –** This parameter must be set to configure the communication speed for asynchronous communication devices (modems). Please refer to the communication device's handbook to get the proper setting.

  Available synchronous communication device speeds are: *9600*, *19200*, *38400*, *64K*, *128K*, *256K*, *512K*, *1M*, *1.544M*, and *2M* baud. Available asynchronous communication device speeds are: *9600*, *19200*, *38400*, *57600*, and *115200.*

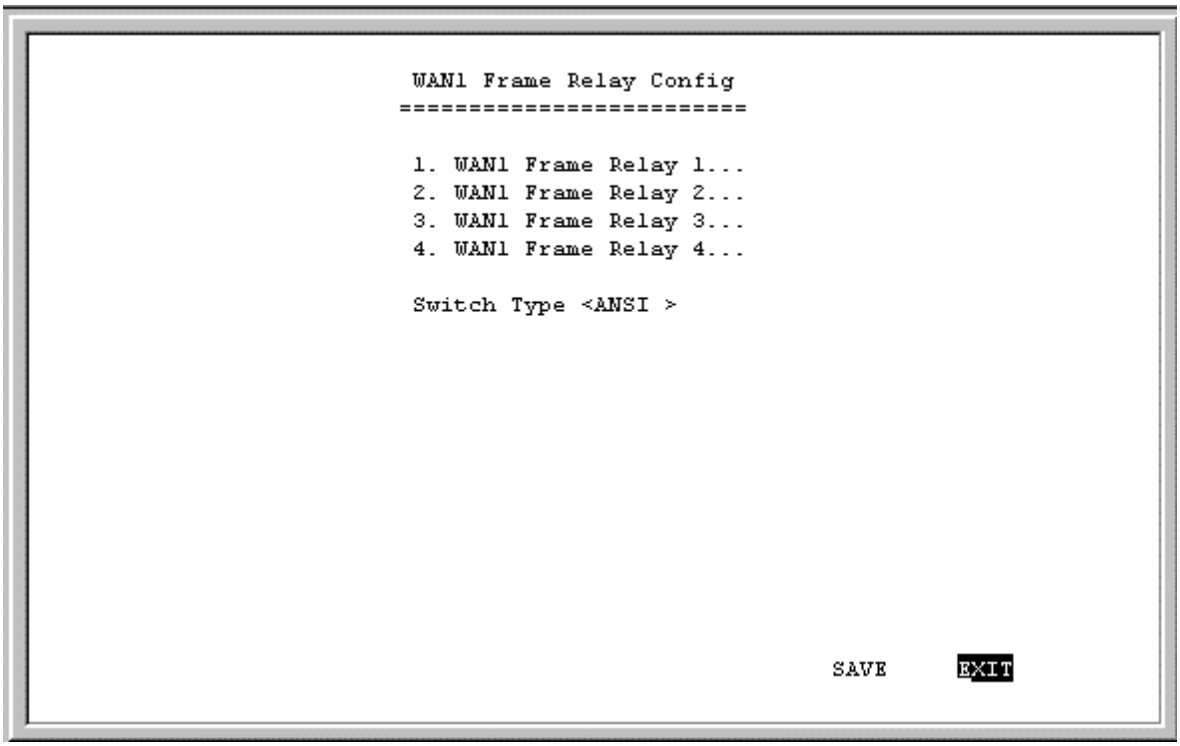
  For synchronous connections, the router will automatically match the clock speed of the device being connected.

- **State –** This is used to *Disable* or *Enable* this interface.

- **Frame Relay Config . . . –** Highlight this item and hit <Enter> if *FRAME_RELAY* is selected as the Protocol above and then complete the WAN Frame Relay configuration settings on the screens described below.

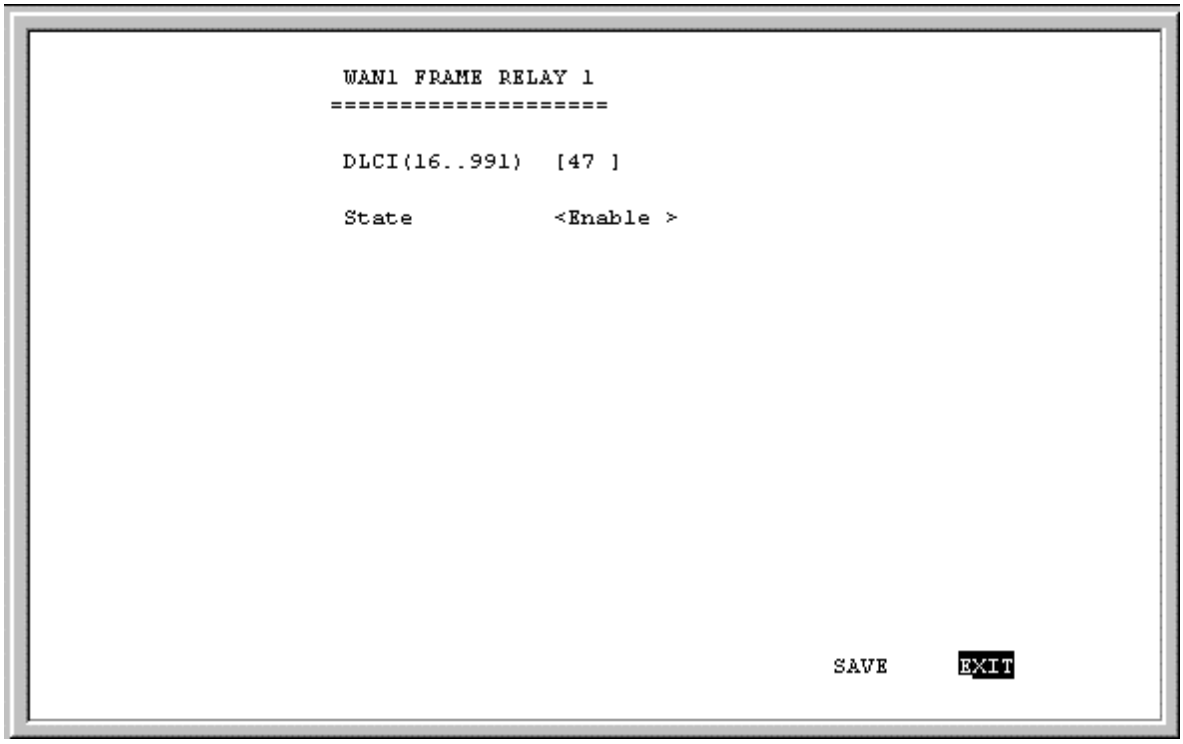
WAN Frame Relay Config

This screen allows you to specify which WAN 1 or WAN 2 Frame Relay is to be configured by highlighting the desired entry below and then hitting <Enter>. Next, enter a Data Link Connection Identifier (DLCI) between 16 and 991 and *Enable* it in the State field on the following screen. Additionally, you must choose the appropriate Switch Type on the **WAN Frame Relay Config** screen below to complete the WAN Frame Relay configuration.



The parameter is described below:

- **Switch Type –** This allows you to choose Local Management Interface (LMI) specification. Currently, we support ANSI T1.617 Annex D and ITU Q.933 Annex A specifications. This switch type must be configured to match your Frame Relay subscription. Once a change has been made, the router must be rebooted.

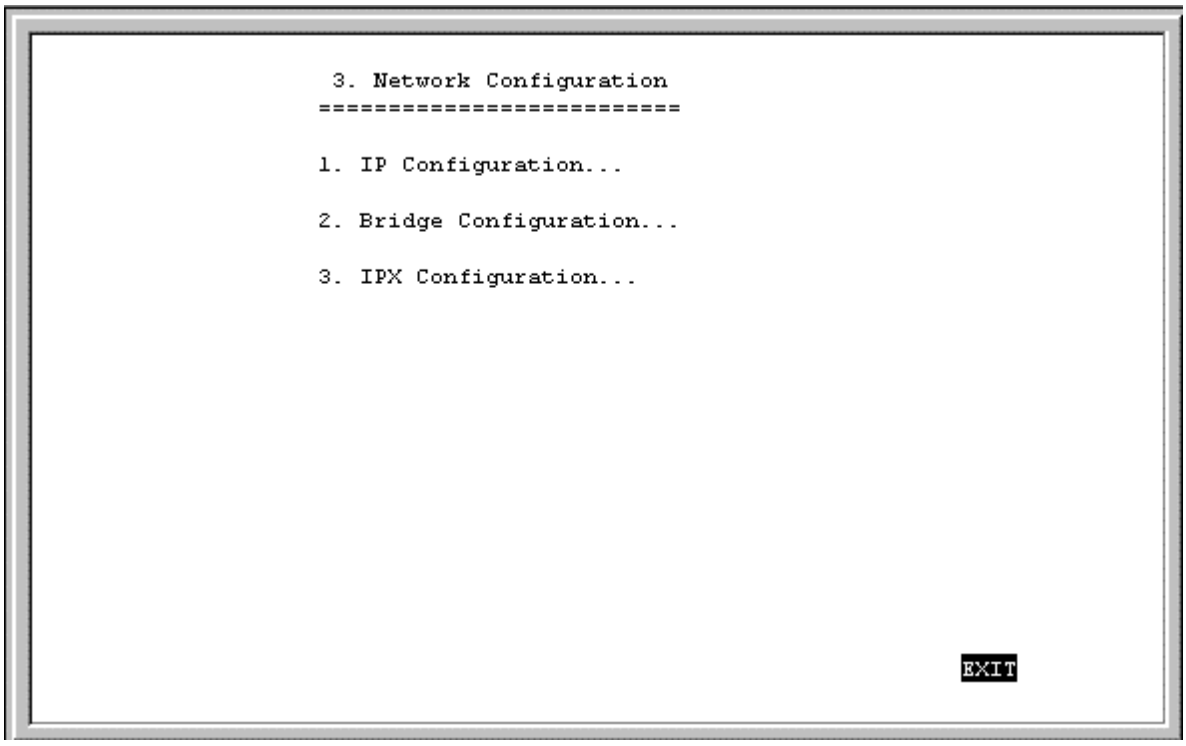


The parameters are described below:

- **DLCI(16. .991) –** This Data Link Connection Identifier is used to match your Frame Relay subscription..
- **State –** This is a toggle, to *Disable* or *Enable* the WAN interface.

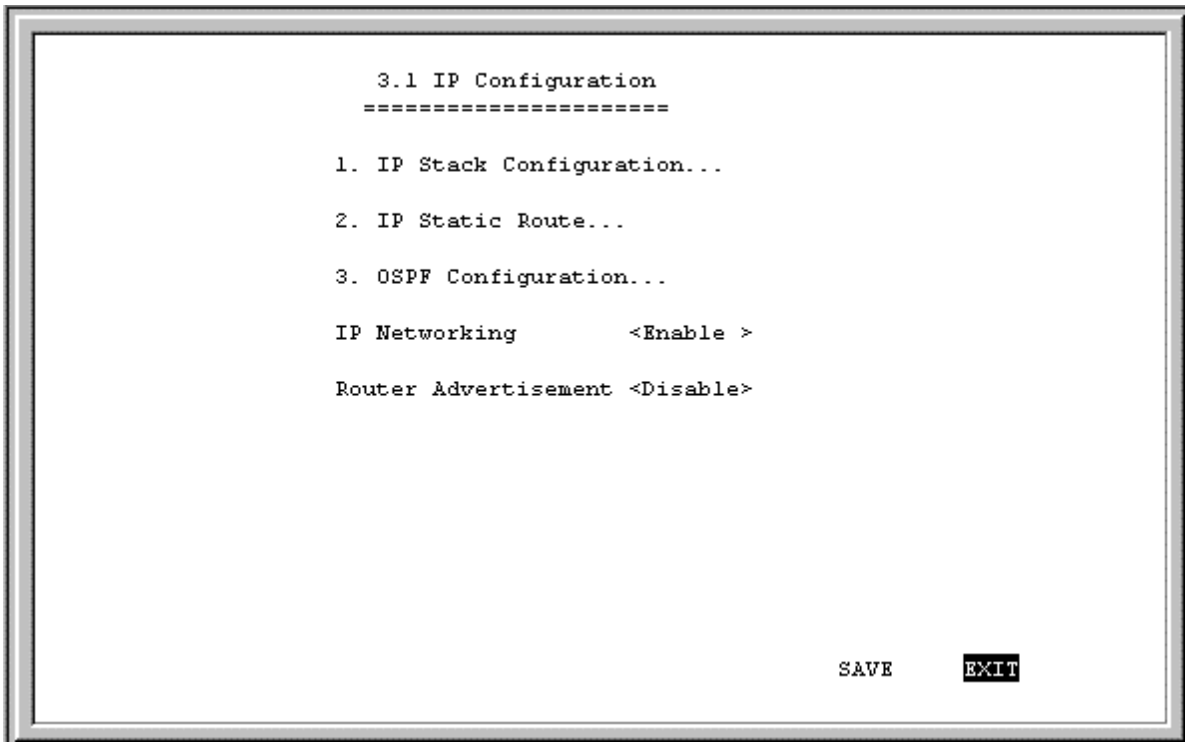
Network Configuration

There are three items on the **Network Configuration** menu: (Bridge Configuration and IPX Configuration appear on DI-1162M only):



IP Configuration

IP networking and router advertisement are enabled on the **IP Configuration** screen:

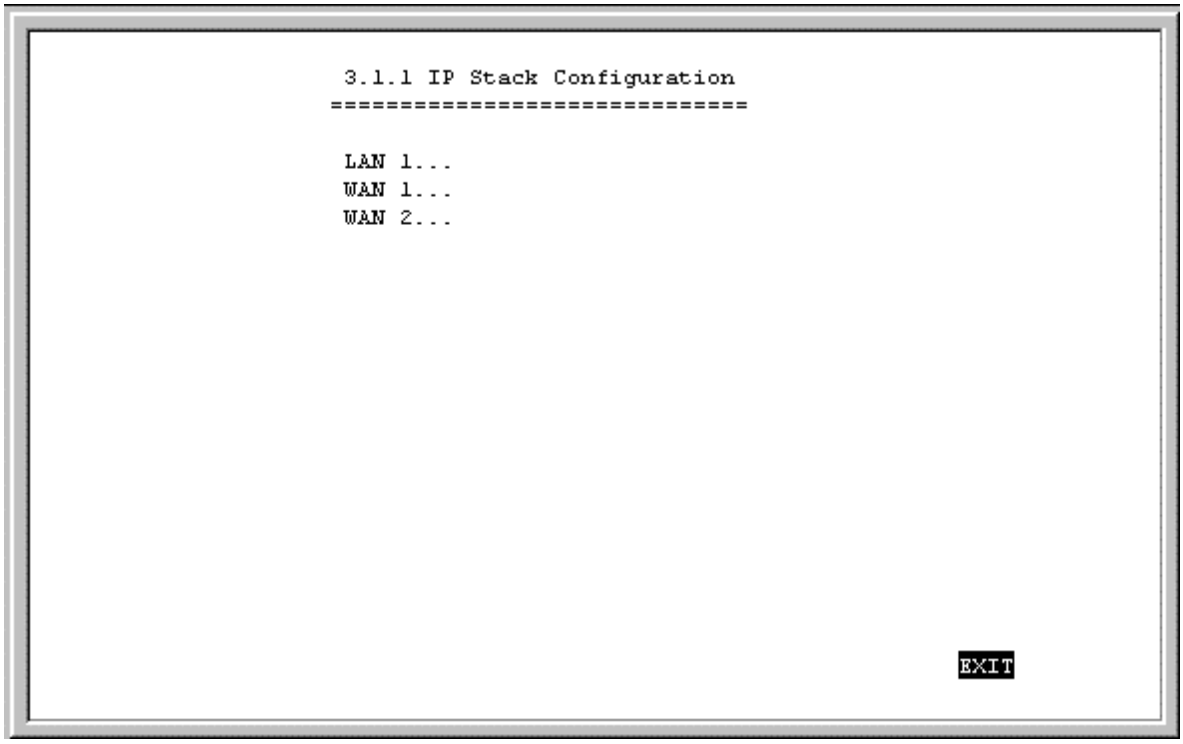


The parameters are described below:

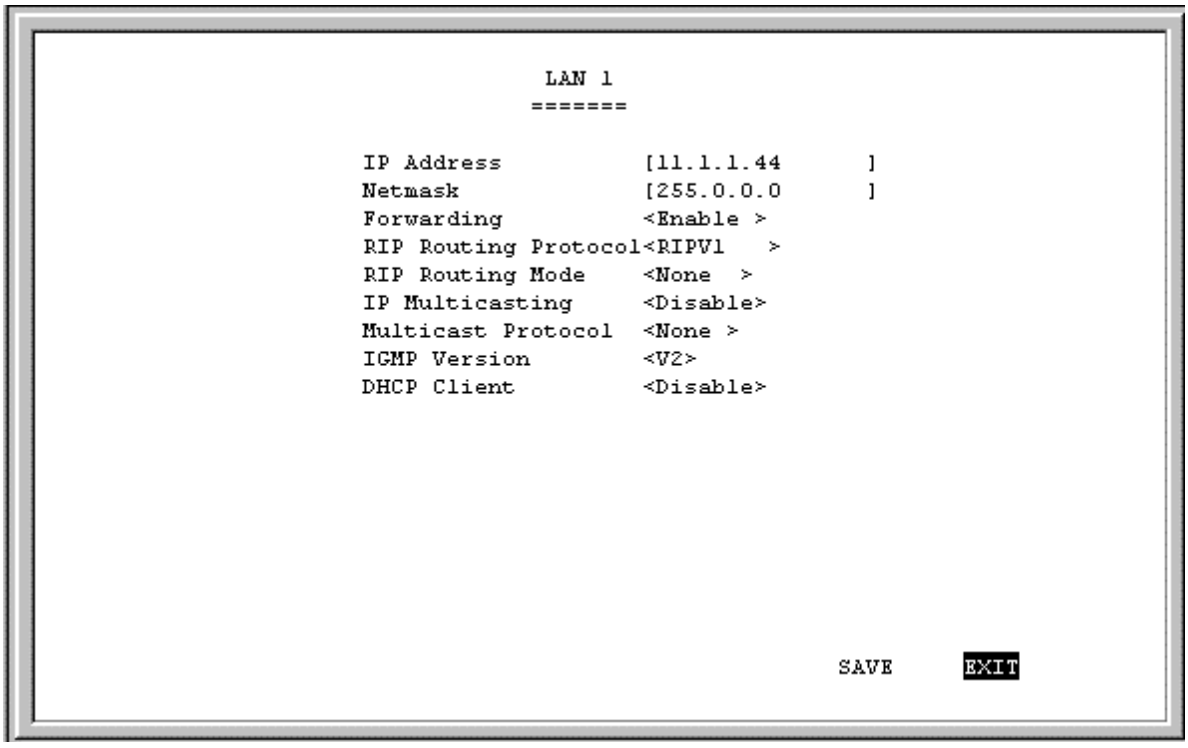
- **IP Networking –** The IP Networking function can toggle to connect/disconnect this router from the entire IP network. When IP Networking is disabled, all routing functions are stopped. The only IP Address the router will act on is it's own, via Telnet for example.
- **Router Advertisement –** When this option is enabled, the router will periodically send out ICMP packets that announce itself on the network. These ICMP packets are utilized by the Windows 98 or later operating system, which will automatically update the default gateway setting on the computer in which it is installed.

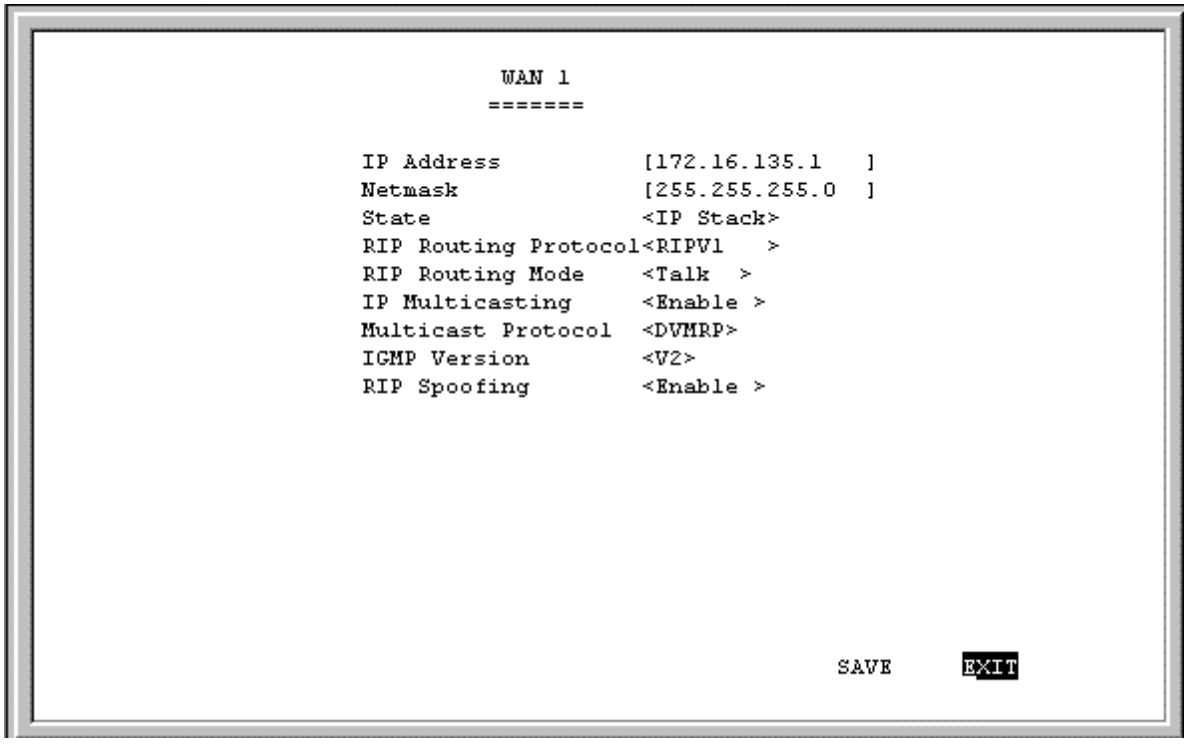
IP Stack Configuration

The network interface IP address, mask and protocols are specified in the IP Stack Configuration submenus. Choose the desired interface from the **IP Stack Configuration** menu below:



Below, the submenus for both the LAN and WAN interfaces are shown.





The parameters are described below:

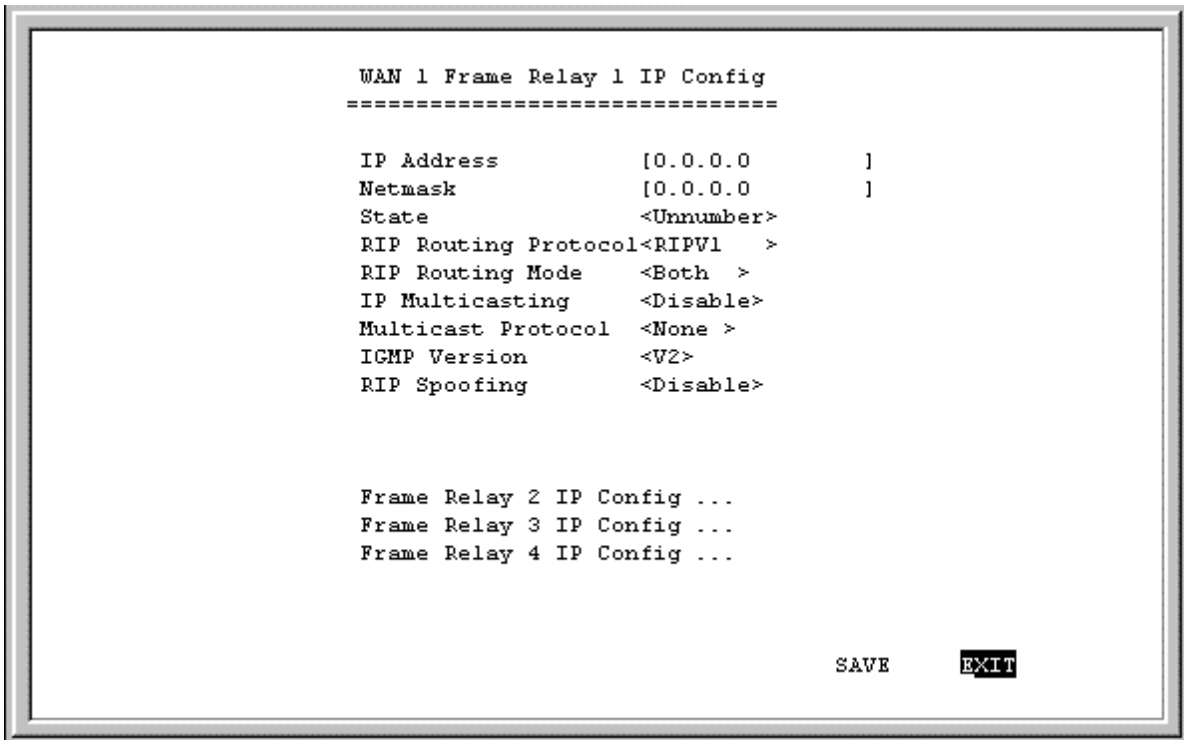
- **IP Address –** This is the IP address for the router on the network to which this interface is connected.
- **Netmask –** This is a 32-bit bit mask that shows how the IP address is to be divided into network, subnet and host parts. The netmask has ones in the bit positions in the 32-bit address which are to be used for the network and subnet parts, and zeros for the host part. The mask should contain at least the standard network portion (as determined by the address's class), and the subnet field should be contiguous with the network portion.
- **Forwarding (LAN) –** This enables or disables communications between this interface and other router(s) on the LAN.
- **State (WAN) –** This is a link method between this interface and adjacent router(s). The methods are described as follows:
  1. *Auto* – This obtains and utilizes the IP address assignment from your ISP (Internet Service Provider).
  2. *Disable* – This disables this interface.
  3. *IP Stack* – This enables this interface, and the IP address used will be the value of the parameter, IP Address.
  4. *Unnumber* – This utilizes a method of connecting this router with adjacent routers, without having to define an IP network prefix between them. The adjacent routers must have *Unnumber* capability, too.
- **RIP Routing Protocol –** This is a distance vector routing protocol. RIP is an Internet standard Interior Gateway Protocol defined in RFC 1058 and RFC 1723. Routing information is sent periodically (each 30 seconds, or triggered by topology change) to an adjacent router. The adjacent router must be using the same protocol. Setting this to *RIPV1&V2* will give the router the ability to make routing information exchanges with any adjacent router.
- **RIP Routing Mode** – This parameter allows the router to specify the extent to which it partakes in the RIP on this port. The options are described below:
  1. *None* – The router will not participate in any RIP exchange with adjacent routers.
  2. *Listen* – The router will incorporate routing information from adjacent routers, but will not send it’s own routing table.

3. *Talk* – The router will send adjacent routers it's own routing table, but will not incorporate routing information from them.
4. *Both* – The router will incorporate routing information from adjacent routers, and will send adjacent routers it's own routing table.

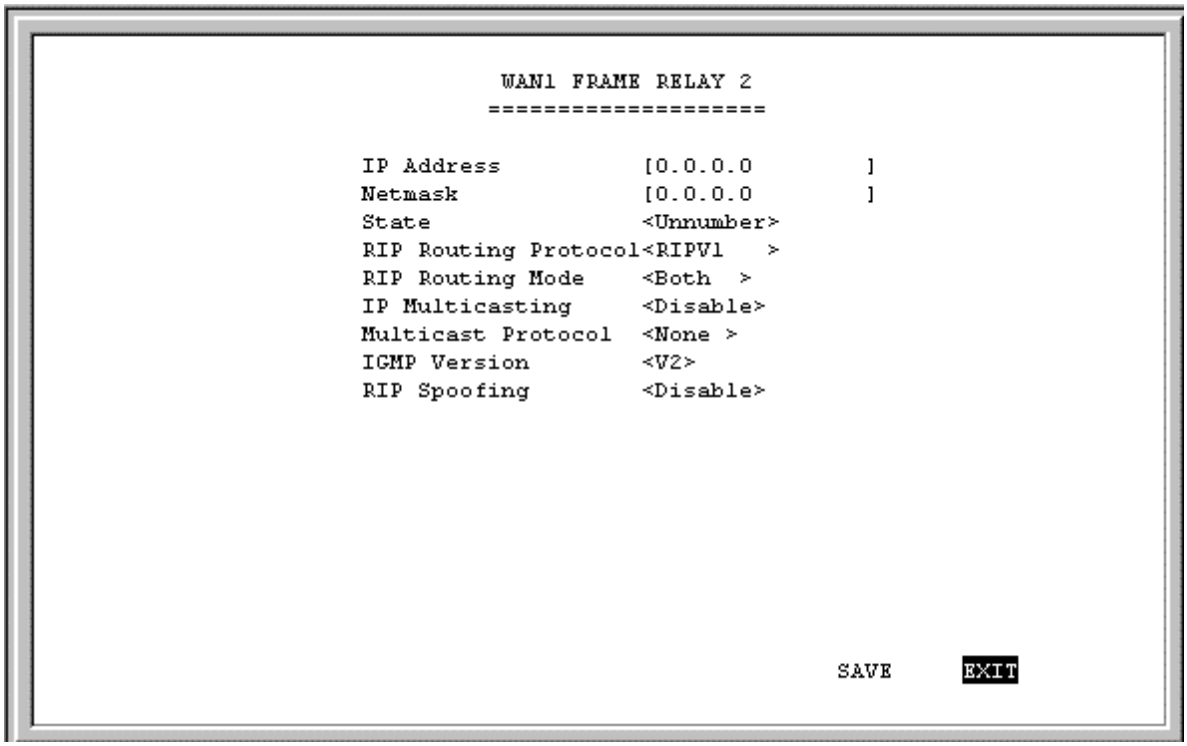
- **IP Multicasting –** This feature enables or disables the router's ability to perform IP multicasting. When enabled, the router will perform IGMP. It can also perform DVMRP if this feature is enabled below.
- **Multicast Protocol –** If this parameter is set to *None*, the router will only use the Internet Group Management Protocol (IGMP). If it is set to *DVMRP*, the router will also use the Distance Vector Multicast Routing Protocol (DVMRP).
- **IGMP Version –** Configures the router to use either IGMP version 1 or 2.
- **DHCP Client (LAN)** – This feature allows the LAN port to be assigned an IP address from a DHCP server other than the one in the router. This feature should be enabled only for special configurations (such as the presence of a cable modem on the LAN) where you wish the router to work with a device on the network that must act as a DHCP server. Otherwise, this feature should be kept disabled.
- **RIP Spoofing (WAN)** – This feature should only be enabled if you have more than one router on your network and this router is providing your WAN connection. In this case, if the WAN connection is dropped due to inactivity and this feature is enabled, RIP packets will be sent to the other routers on the network telling them that data can still be sent to the WAN via this router. Otherwise, the other routers will learn that the WAN link has been disconnected and will no longer forward packets destined for the WAN to this router, causing the packets to be dropped before Bandwidth on Demand has a chance to reestablish the WAN connection.

WAN Frame Relay IP Config

If *FRAME_RELAY* is selected for the Protocol on **WAN 1** or **WAN 2** under **Interface Configuration**, the following screen will appear:



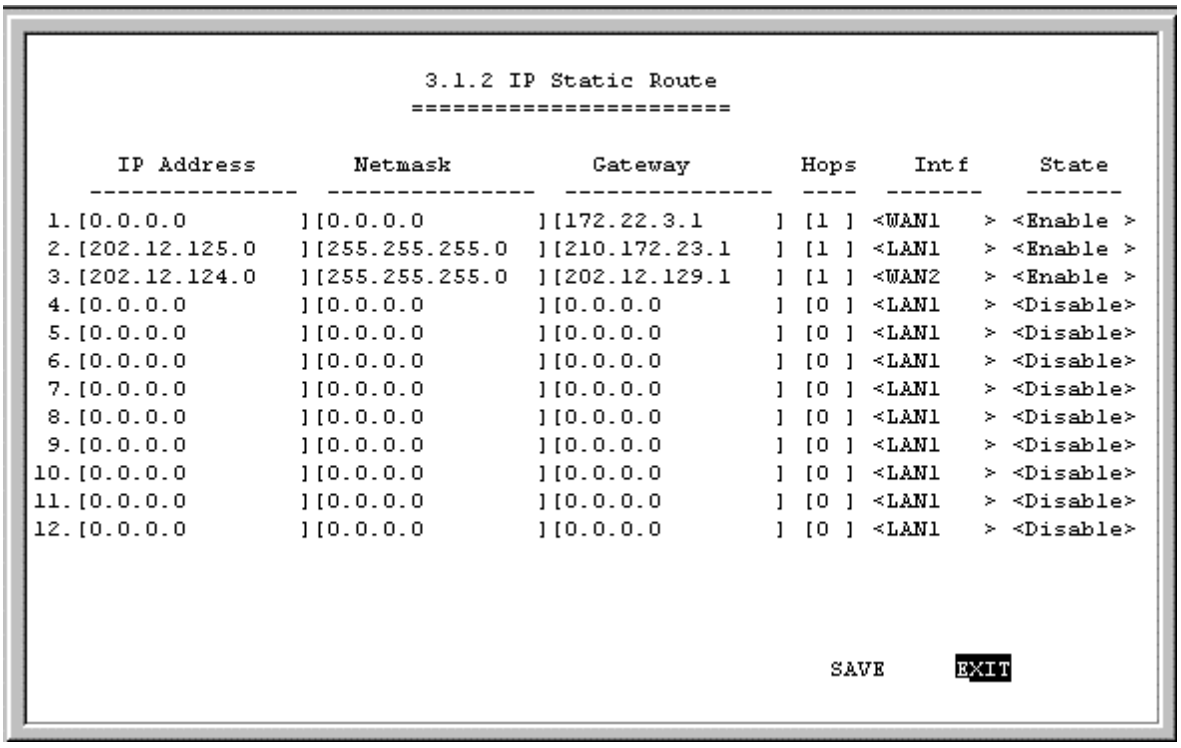
The descriptions for all the fields are the same as in the previous section. Select one of the Frame Relay IP Config items at the bottom of the screen to access the following screen:



The descriptions for all the fields are the same as in the previous section.

IP Static Route

A static route is a permanent entry in the routing table. Static routing provides a means of explicitly defining the next hop router for a particular destination network IP address. Each static route entry also allows for a metric (a.k.a. hop count) to be specified.



The parameters are described below:

- **IP Address** – This specifies the destination network IP address (or a host, depending on the netmask) and pairs it with a gateway.
- **Netmask** – This mask shows how the destination IP address is to be divided into network, subnet and host parts. The netmask has ones in the bit positions in the 32-bit address which are to be used for the network and subnet parts, and zeros for the host part.
- **Gateway** – This is the adjacent next hop router, for which the packets, arriving to this router with this destination IP address, will be forwarded.
- **Hops** – This is an associated RIP metric that may have its value set between 1 and 15, inclusive. A metric value higher than 15 (such as 16) means that the network is unreachable.
- **Intf** – This is the network interface containing the gateway that the packets will be forwarded through.
- **State** – This enables or disables a particular entry.

IP Static Route Examples

The IP Static Route Table shown in the example IP Static Route screen above has the first three entries configured for common implementations of static routing.

The first entry assumes that WAN1 has a connection to the Internet and defines the default next hop router. If you use this router to connect to the Internet it is very important that you create an entry here that defines the default next hop router as your ISP. This configuration is also commonly used when RIP exchanges with other Internet routers (on WAN1) are disabled.

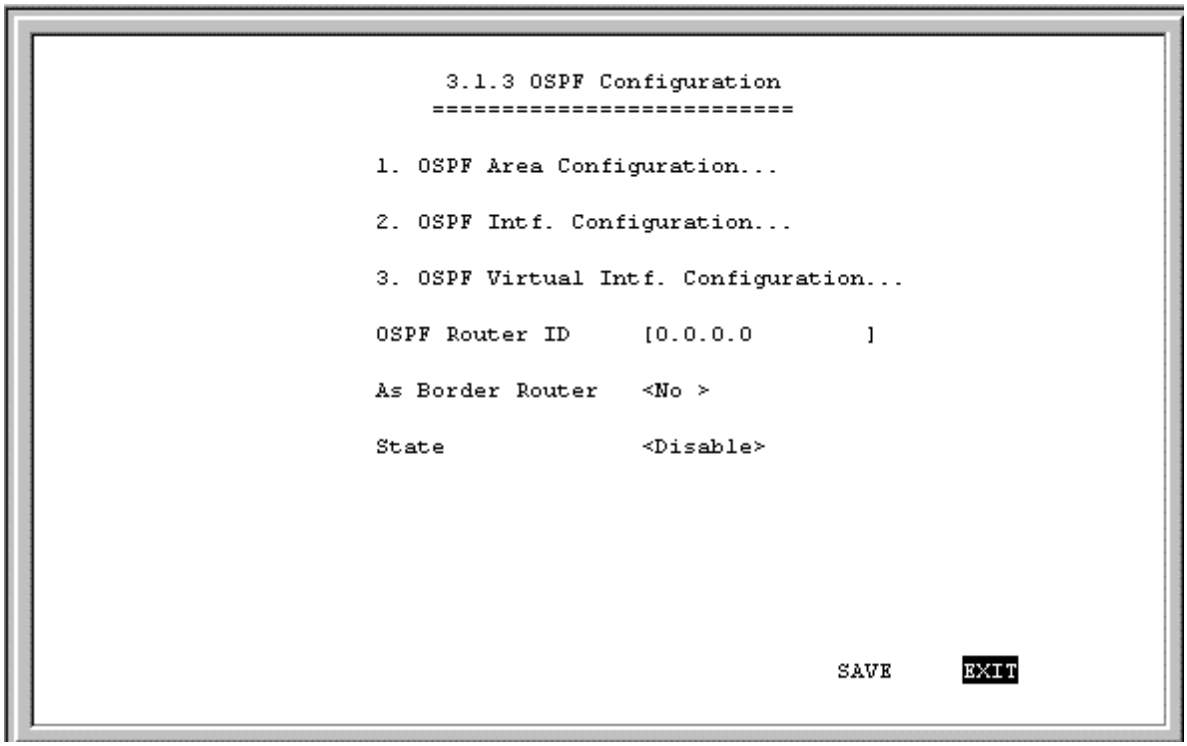
The second entry shows how to configure static routes when there is another router on the LAN. The IP Address shown (202.12.125.0) is the network address for a branch office, for example. The Gateway Address (210.172.23.1) is the IP address to the LAN port on another router on LAN1 that maintains a WAN connection to the branch office.

The third entry is an example of an enterprise WAN connection (through telephone lines) to another router, at a branch office for example. The IP Address is the network address of the branch office. The Gateway Address is the IP Address of the WAN port on the branch office router. This configuration assumes there is a modem on WAN2 maintaining a dial-up connection to the branch office.

OSPF Configuration

Open Shortest Path First (OSPF) is a link-state routing algorithm that provides more control over the routing process and responds faster to changes as compared to distance-vector routing. OSPF routing table updates only take place when necessary rather than at regular intervals, thereby reducing traffic and saving network bandwidth.

The **OSPF Configuration** screen below allows you to specify an OSPF Router ID, determine As Border Router status, and *Enable* OSPF under State. Currently, OSPF over frame relay is not supported.



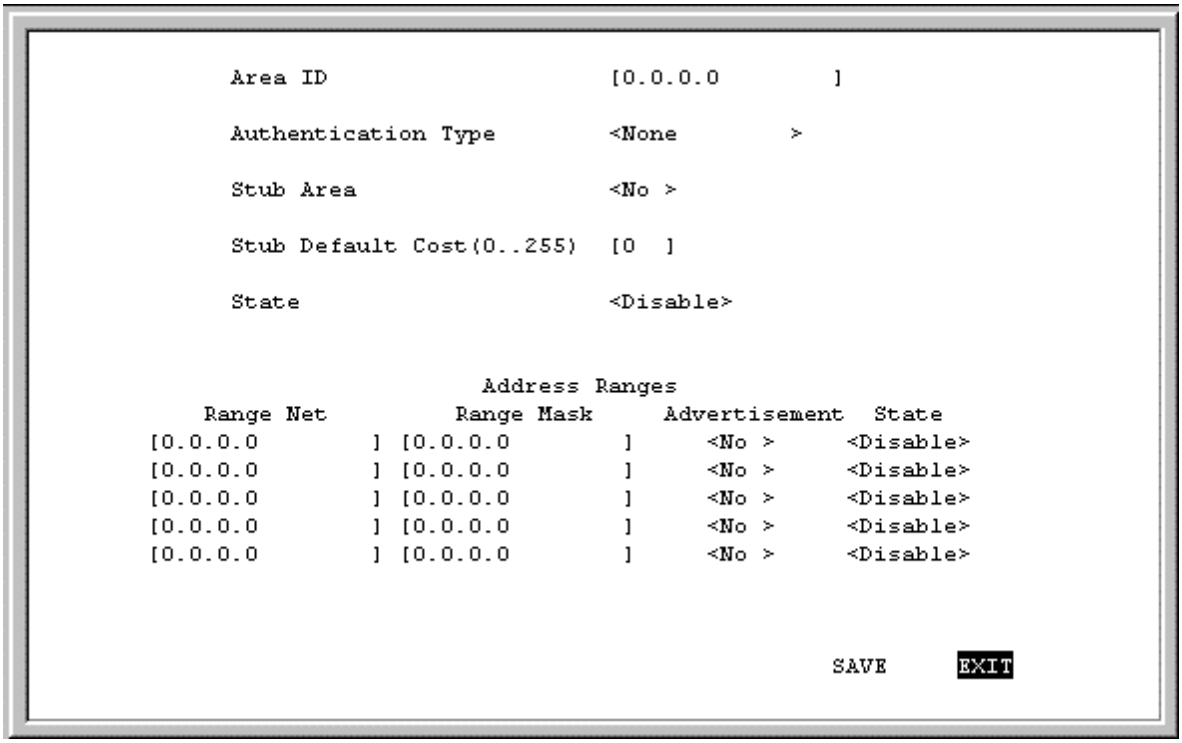
The parameters are described below:

- **OSPF Router ID** – This is a 32-bit number that uniquely identifies the router in the Autonomous System. If the OSPF Router ID is not configured, the router will automatically choose LAN 1's IP as the OSPF Router ID.
- **AS Border Router** – Setting to allow DI-1162/DI-1162M to act as Autonomous System Border Router. As an AS Border Router, the router can import and export routing information of other Autonomous Systems, such as RIP.
- **State** – Toggle between *Enable* and *Disable*.

OSPF Area Configuration

Select the desired OSPF Router ID to either make changes to or configure for the first time on the **OSPF Area Configuration** screen (in which case, the five entries will be blank and all you need to do is press <Enter>.

Complete the OSPF configuration information on the screen below:



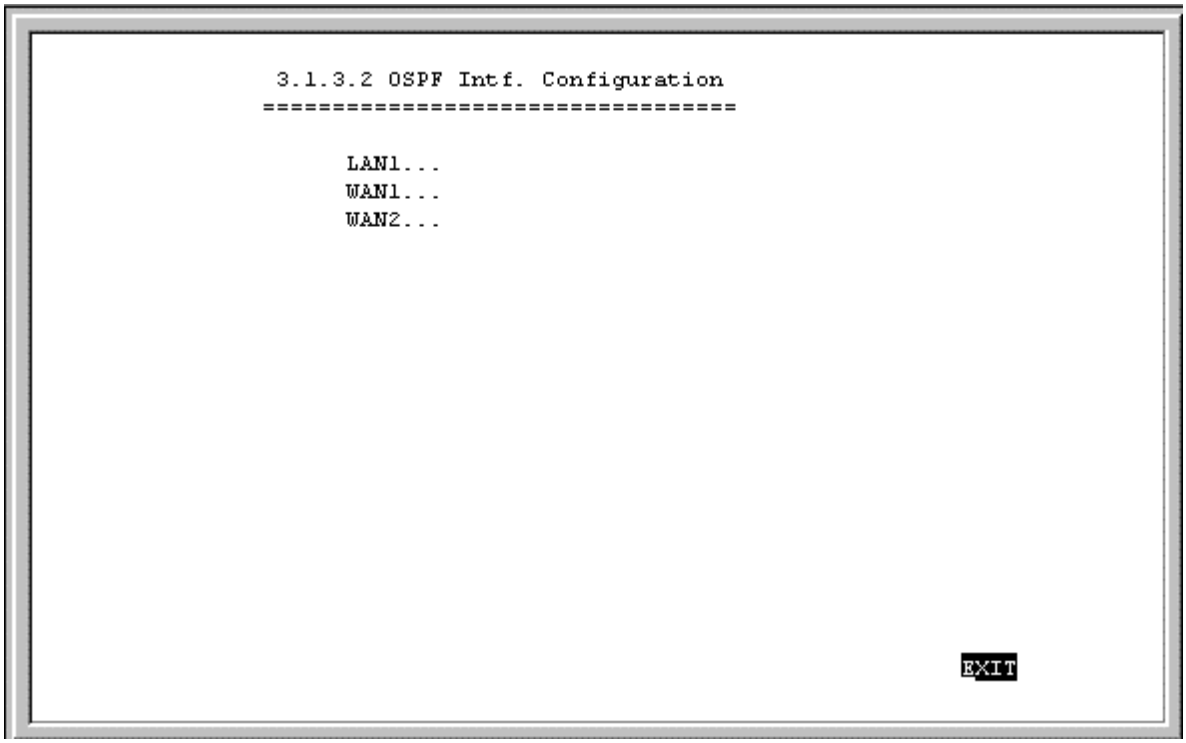
The parameters are described below:

- **Area ID** – Enter the OSPF Area ID number in this field.
- **Authentication Type** – Toggle between *None* and *SimplePasswd*.

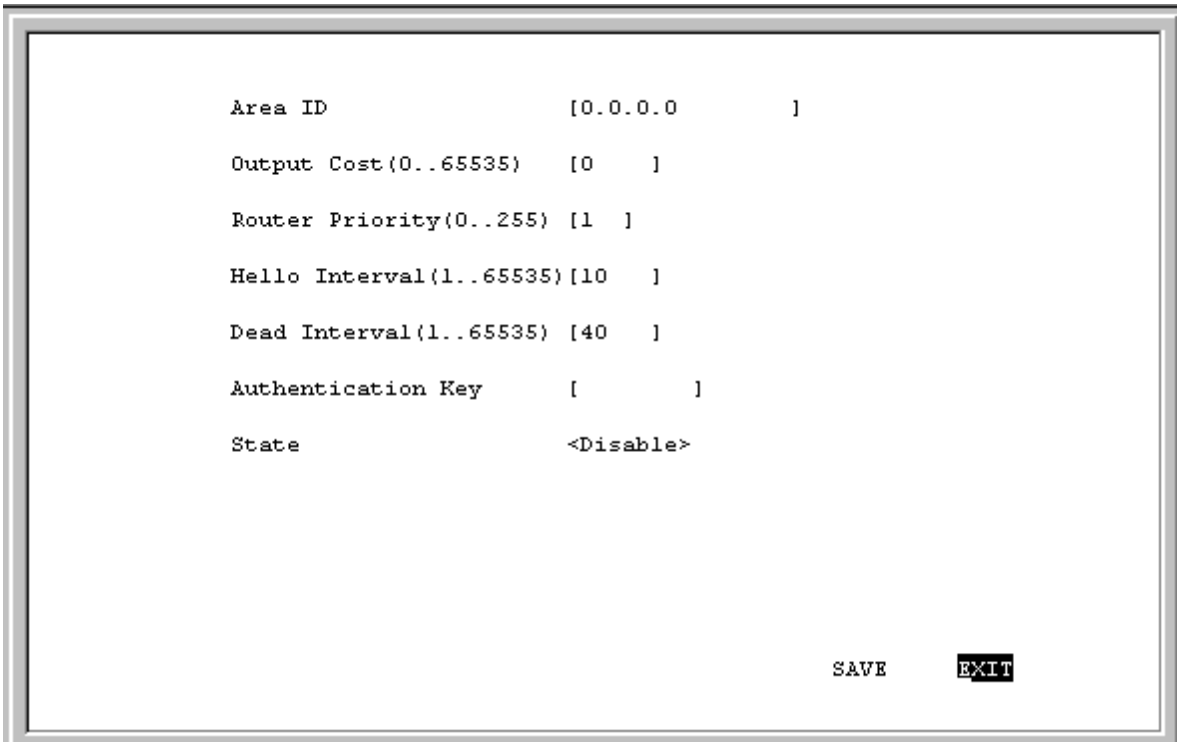
- **Stub Area** – Toggle between *Yes* and *No*. AS external advertisements are not flooded into/throughout stub areas. Routing to AS external destinations in these areas is based on (per area) default only.
- **Stub Default Cost (0. . 255)** – Enter a Stub Default Cost between 0 and 255 in this field.
- **State** – This enables or disables a particular entry.
- **Address Ranges** – Enter the Range Net, Range Mask, Advertisement status, and *Enable* the State of up to five OSPF entries in these fields. This allows users to manually enter OSPF subnet information. Range Net and Range Mask describe the collection of IP addresses contained in the range. Networks and hosts are assigned to an area depending on whether their addresses fall into one of the area's defining address ranges. Advertisement is set to either *Yes* or *No*. Routing information of these address ranges is advertised external to the area if and only if such status is set to *Yes*.

OSPF Intf. Configuration

Select the desired interface on the **OSPF Intf. Configuration** screen:



Complete the OSPF interface configuration information on the screen below:

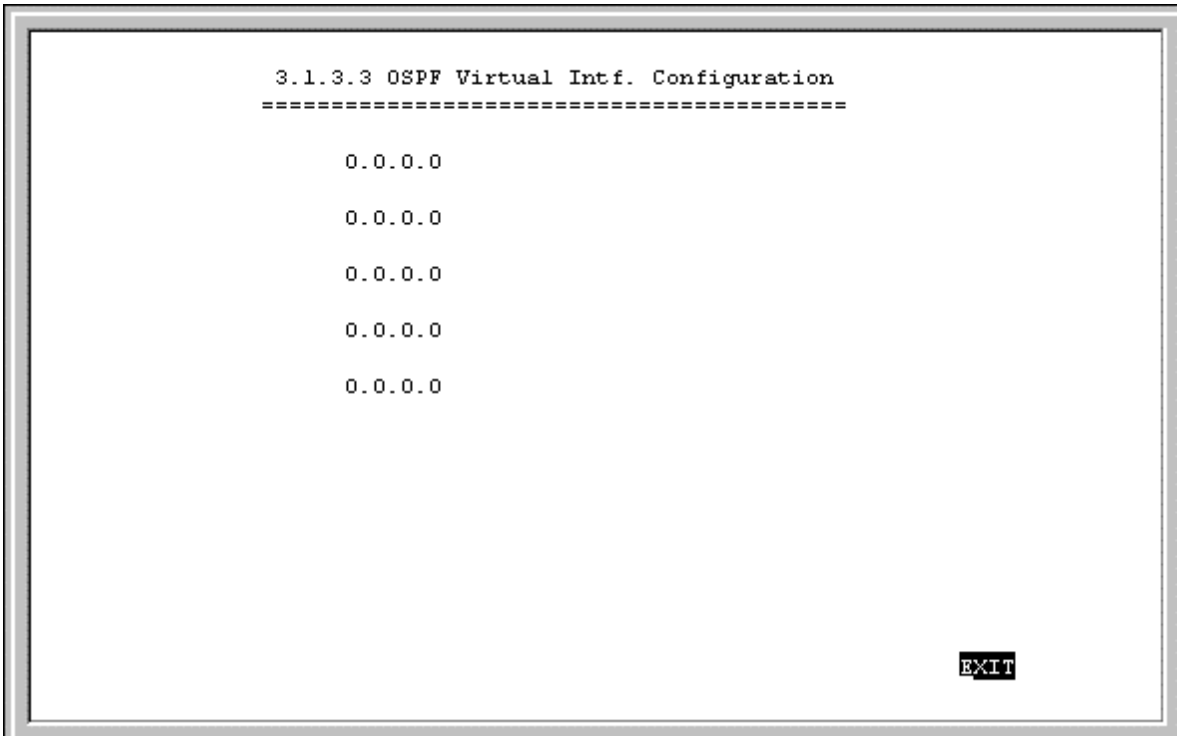


The parameters are described below:

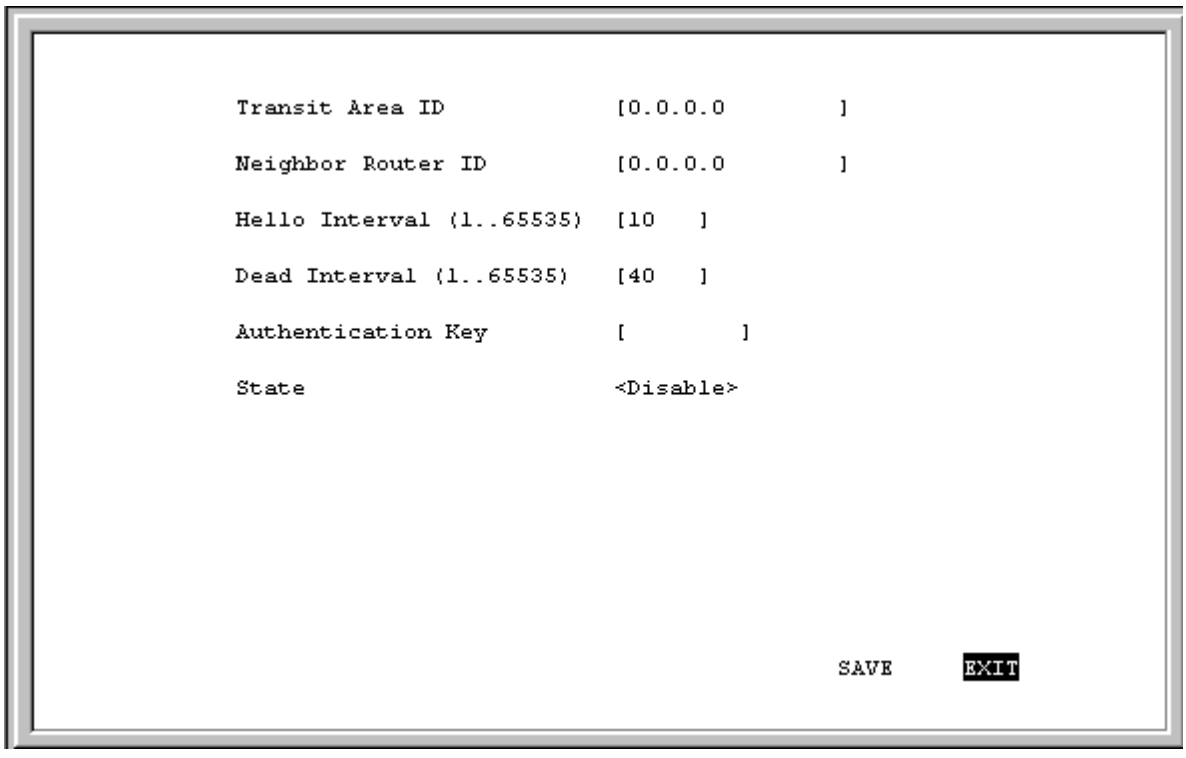
- **Area ID** – Enter the OSPF Area ID number in this field.
- **Output Cost (0 . . 65535)** – The cost of sending a packet on the interface, expressed in the link static metric. This is advertised as the link cost for this interface in the router's router links.advertisement. The interface Output Cost(s) must always be greater than 0.
- **Router Priority (0. . 255)** – This number determines priority when two routers attached to a network both attempt to become the Designated Router. The router with the highest priority takes precedence.
- **Hello Interval (1. . 65535)** – The length of time (in seconds) between the Hello Packets that the router sends on the interface. This value is advertised in the router's Hello Packets. It must be the same for all routers attached to a common network. The smaller the Hello Interval, the faster topological changes will be detected, but more OSPF routing protocol traffic will ensue.
- **Dead Interval (1. . 65535)** – After ceasing to hear a router's Hello Packets, the number of seconds before its neighbors declare the router down. This should be some multiple of the Hello Interval. The value must be the same for all the routers attached to a common network.
- **Authentication Key** – This configured data allows the authentication procedure to generate and/or verify the authentication field in the OSPF header. This value must be the same for all routers attached to a common network.
- **State** – This enables or disables a particular entry.

OSPF Virtual Intf. Configuration

Select the desired virtual interface to either make changes to or configure for the first time on the **OSPF Virtual Intf. Configuration** screen (in which case, the five entries will be blank and all you need to do is press <Enter>.



Complete the OSPF virtual interface configuration information on the screen below:



The parameters are described below:

- **Transit Area ID** – Enter the Transit Area ID number in this field.
- **Neighbor Router ID** – Enter the Neighbor Router ID number in this field.

- **Hello Interval (1. . 65535)** – The length of time (in seconds) between the Hello Packets that the router sends on the interface. This value is advertised in the router's Hello Packets. It must be the same for all routers attached to a common network. The smaller the Hello Interval, the faster topological changes will be detected, but more OSPF routing protocol traffic will ensue.

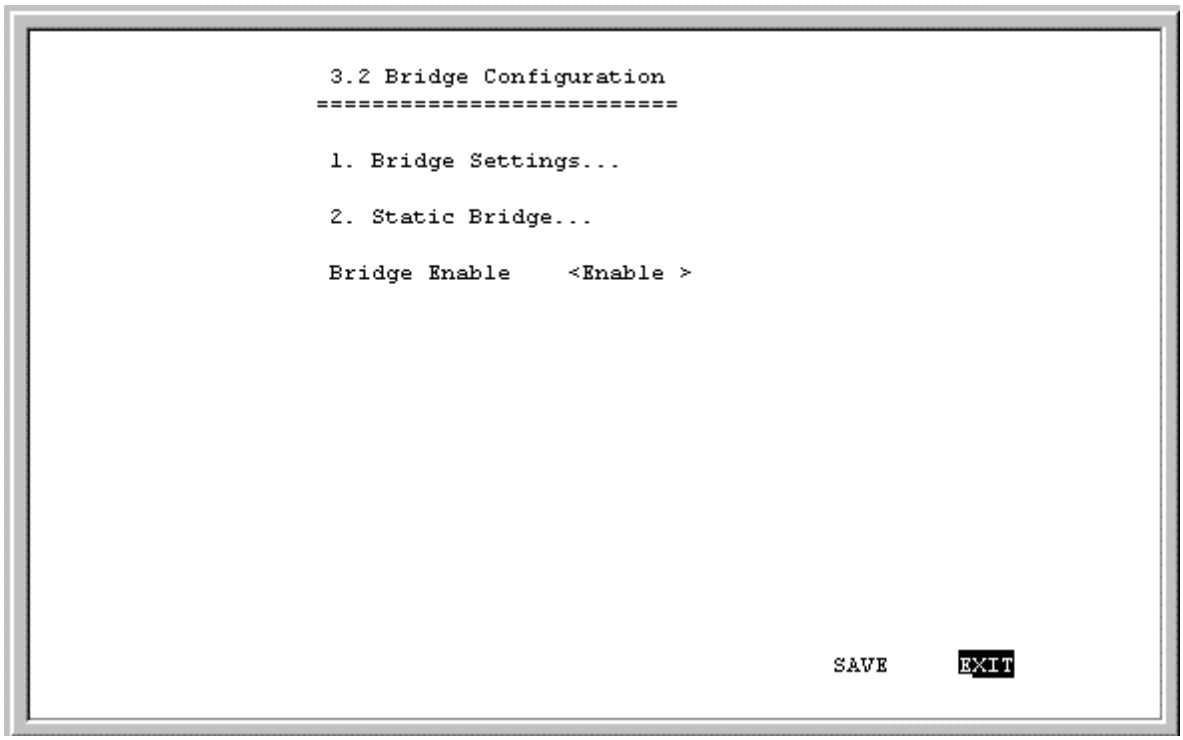
- **Dead Interval (1. . 65535)** – After ceasing to hear a router's Hello Packets, the number of seconds before its neighbors declare the router down. This should be some multiple of the Hello Interval. The value must be the same for all the routers attached to a common network.

- **Authentication Key** – This configured data allows the authentication procedure to generate and/or verify the authentication field in the OSPF header. This value must be the same for all routers attached to a common network.

- **State** – This enables or disables a particular entry.

Bridge Configuration

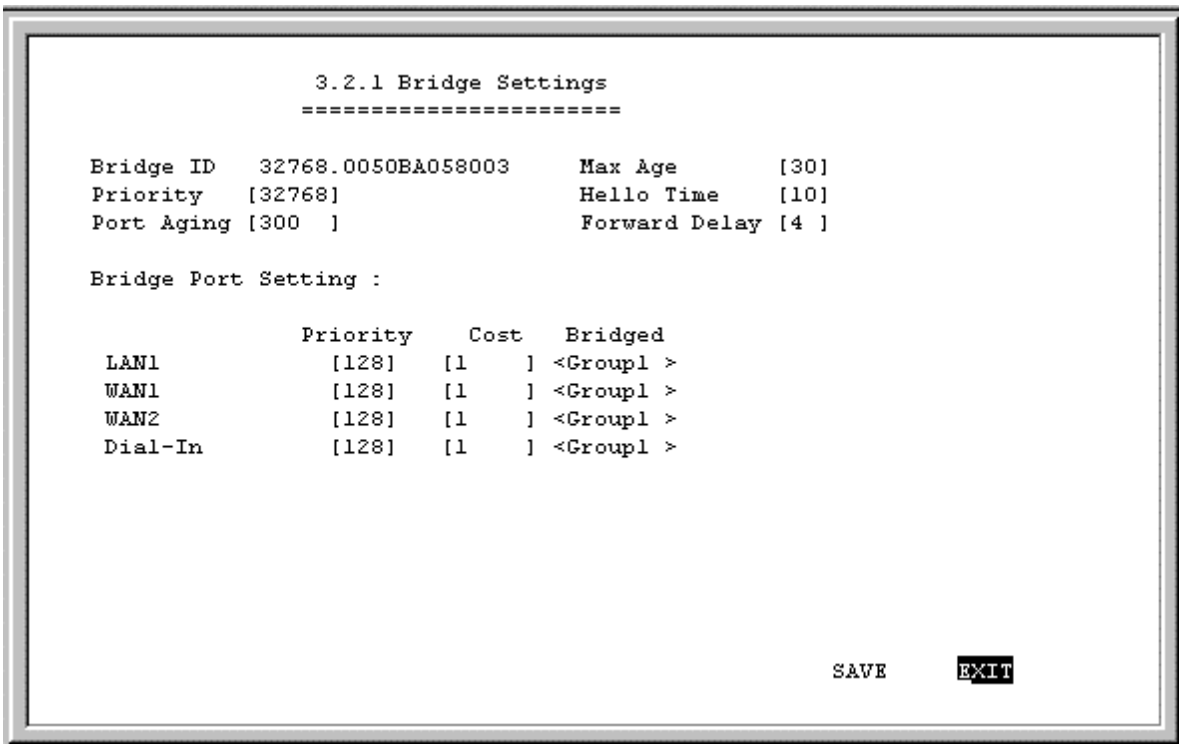
Bridges are enabled on the **Bridge Configuration** screen:



The parameter you can set is described below:

- **Bridge Enable –** The third option on the **Bridge Configuration** menu allows you to enable or disable bridging. Press SAVE once you are finished

Bridge Settings



The parameters are described below:

- **Bridge ID** – The Bridge ID is a read-only object composed of the bridge priority and the MAC address. So in the screen above, the Priority is 32768 and the MAC address is zero since it was yet to be entered.

- **Priority** – A Bridge Priority is a read-write object that can be set from 0 to 65535. This is the priority number of the bridge. The value is used in conjunction with the bridge MAC address to set the bridge ID, which in turn is used when determining the root bridge of a multi-bridged network. The root bridge is responsible for processing data packets when network loops occur. The smaller the number set, the higher the bridge priority is. The higher the bridge priority, the more chance the bridge has of becoming the root bridge. Zero is the highest priority.

- **Port Aging** – This is a read-write object that allows you to set the aging time for MAC addresses in a port's address table. When the time-out figure is reached, the bridge will remove the MAC address.

- **Max Age** – Maximum Age is a read-write object that can be set from 6 to 40 seconds. At the end of the Maximum Age, if a BPDU has still not been received from the Root Bridge, your Switch will start sending its own BPDU to all other switches for permission to become the Root Bridge. If it turns out that your Switch has the lowest Bridge Identifier, it will become the Root Bridge.

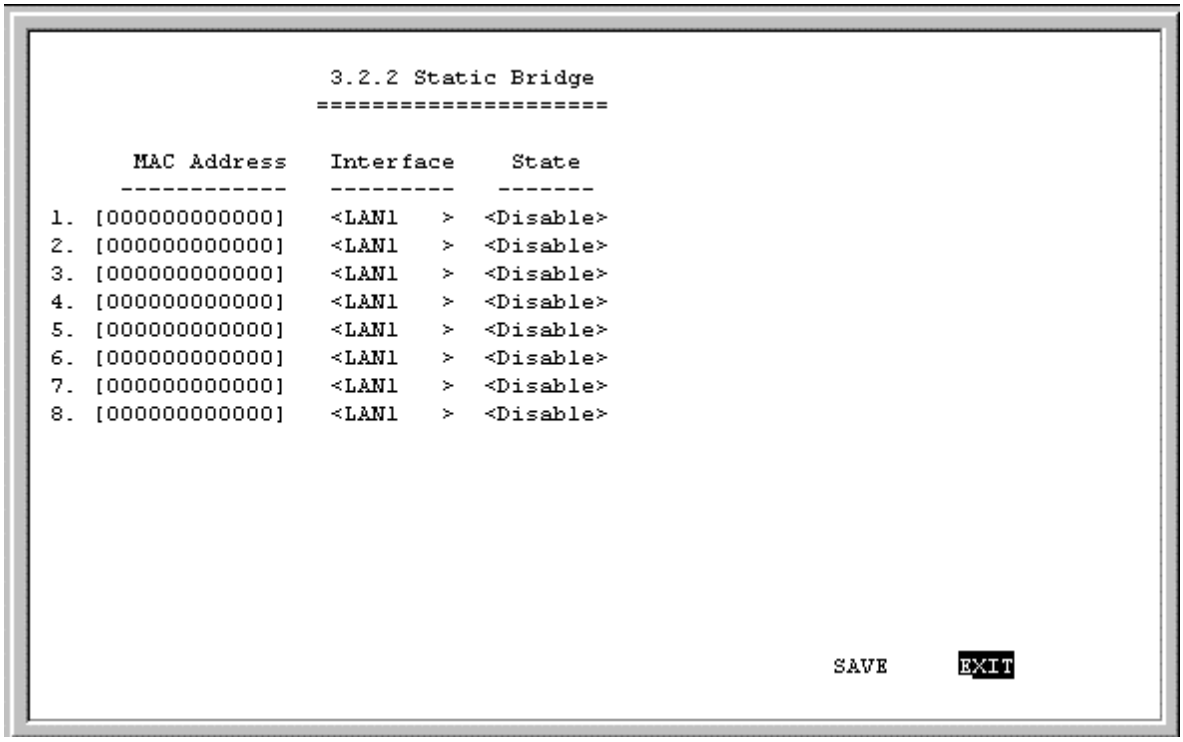
- **Hello Time** – Hello Time is a read-write object that can be set from 1 to 10 seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other switches that it is indeed the Root Bridge. If you set a Hello Time for your Switch, and it is not the Root Bridge, the set Hello Time will be used if and when your Switch becomes the Root Bridge.

- **Forward Delay** – The Forward Delay is a read-write object that can be set from 4 to 30 seconds. This is the time any port on the Switch spends in the listening state while moving from the blocking state to the forwarding state.

Bridge Port Setting:

- **Priority** – Port Priority is a read-write object that can be set from 0 to 255. The priority is used to determine the designated port if the Path costs of redundant switch to switch connections are the same. The higher the port priority, the more chance the port has of becoming the designated port. Zero is the highest priority.
- **Cost** – Path Cost is a read-write object which is the first consideration when deciding on a designated port for switch to switch connections.
- **Bridged** – Select the desired group.

Static Bridge

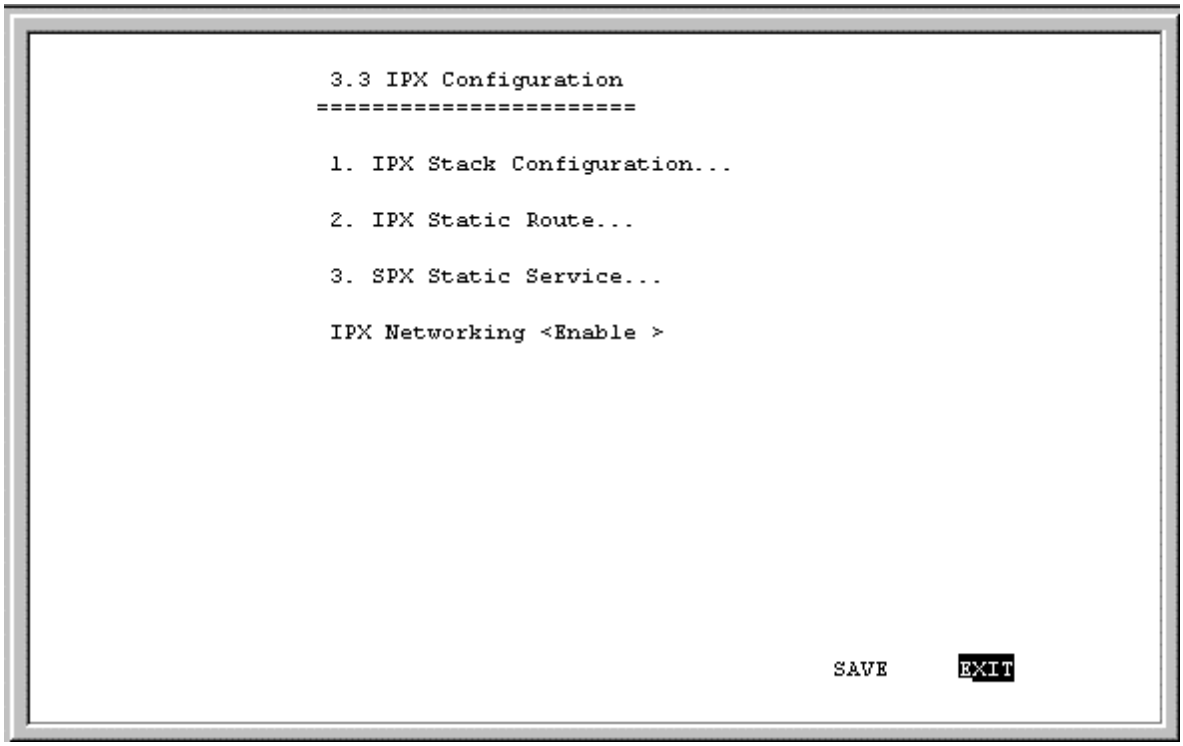


The parameters are described below:

- **MAC Address** – This is the MAC address of the network host, or node, that you wish to statically bridge.
- **Interface** – This designates the specific interface, either *LAN*, one of the *ISDN* interfaces, or *Dial-In.*
- **State** – This enables or disables a particular entry.

IPX Configuration

If you are working on a Novell network, you may want to set up IPX routing. IPX (Internetwork Packet eXchange) is the routing protocol used in Novell networking environments.

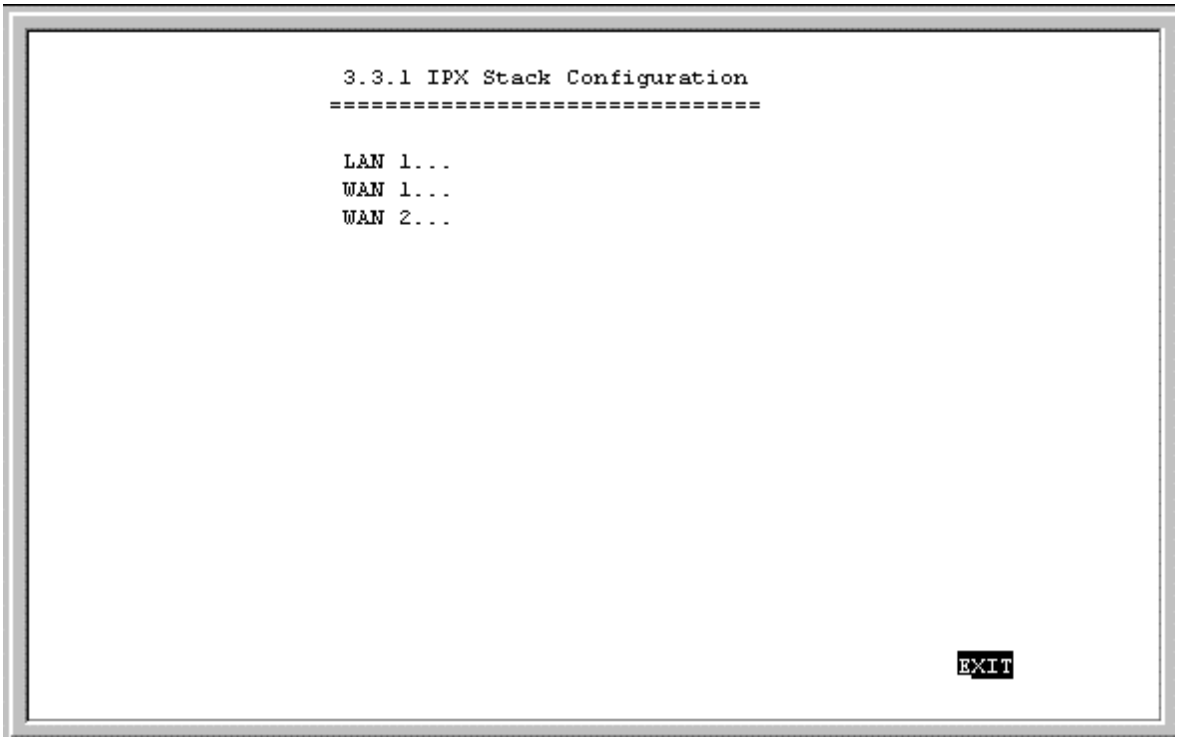


The parameters you can set is described below:

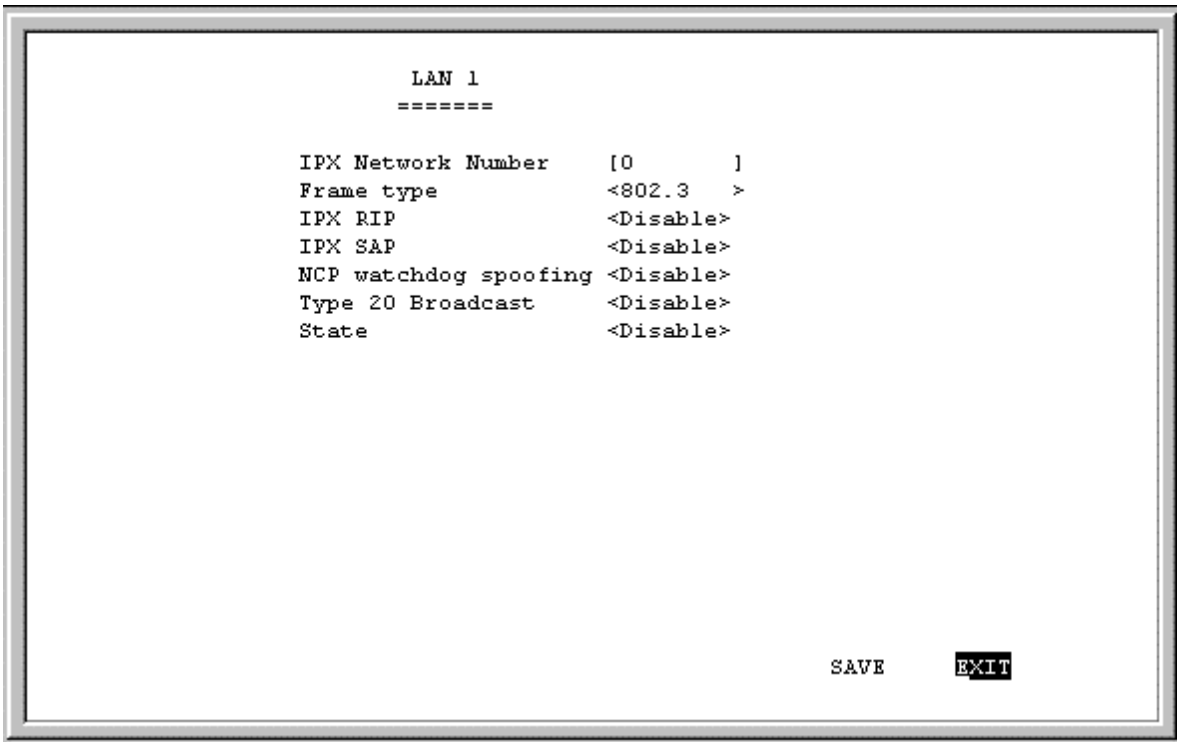
- **IPX Networking –** The IPX Networking function is enabled or disabled in this field. *Enable* it to set up IPX (Internetwork Packet eXchange), a routing protocol for Novell networking environments.

IPX Stack Configuration

This menu is used to configure the LAN and WAN interfaces.



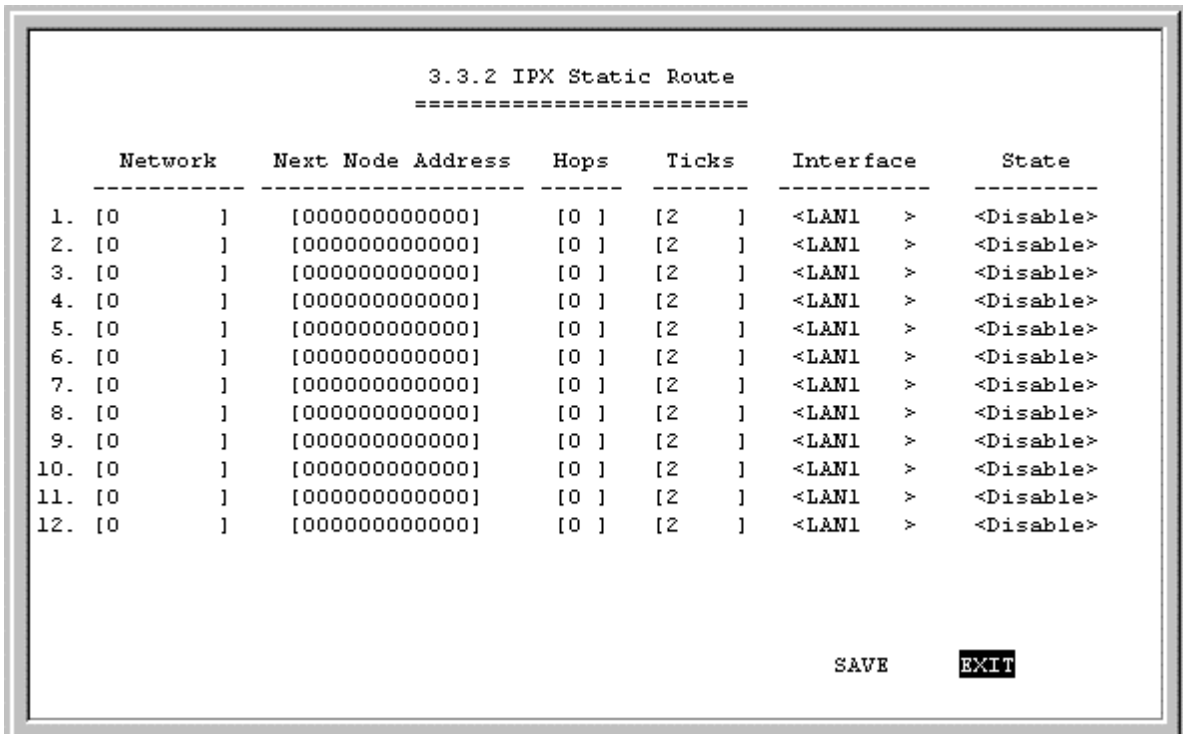
Complete the IPX stack configuration information for the desired interface on the screen below:



The parameters described below also apply to WAN interfaces.:

- **IPX Network Number** – This determines which IPX network you belong to.
- **Frame type** – Select from the following: *Ether II, SNAP*, *802.2*, or *802.3*
- **IPX RIP** – Enable IPX Routing Information Protocols (RIP) to provide a measure of distance, or hops, from a transmitting system to a receiving system.
- **IPX SAP** – Enable IPX Service Access Protocol (SAP) to disseminate information about network services and their addresses to all nodes in an IPX network.
- **NCP watchdog spoofing** – Enable this for Dial On Demand. Novell defines special packets to send and check to see if each side of the connection is fine. This minimizes the number of unnecessary packets sent through the Internet.
- **Type 20 Broadcast** – Enable this if NetBIOS requires forwarding by the router. Type 20 Broadcast must be enabled on both ends for this function to work.
- **State** – This enables or disables a particular entry.

IPX Static Route



3.3.2 IPX Static Route

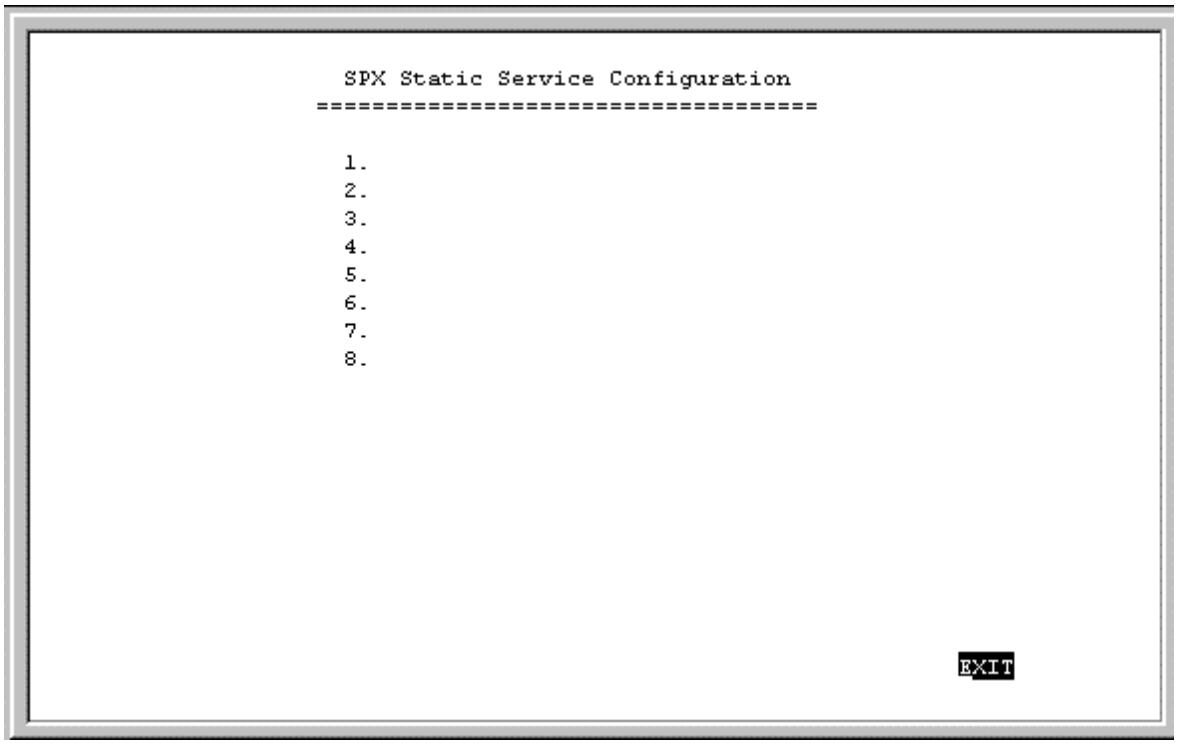
	Network	Next Node Address	Hops	Ticks	Interface	State
1.	[0]	[0000000000000]	[0]	[2]	<LAN1 >	<Disable>
2.	[0]	[0000000000000]	[0]	[2]	<LAN1 >	<Disable>
3.	[0]	[0000000000000]	[0]	[2]	<LAN1 >	<Disable>
4.	[0]	[0000000000000]	[0]	[2]	<LAN1 >	<Disable>
5.	[0]	[0000000000000]	[0]	[2]	<LAN1 >	<Disable>
6.	[0]	[0000000000000]	[0]	[2]	<LAN1 >	<Disable>
7.	[0]	[0000000000000]	[0]	[2]	<LAN1 >	<Disable>
8.	[0]	[0000000000000]	[0]	[2]	<LAN1 >	<Disable>
9.	[0]	[0000000000000]	[0]	[2]	<LAN1 >	<Disable>
10.	[0]	[0000000000000]	[0]	[2]	<LAN1 >	<Disable>
11.	[0]	[0000000000000]	[0]	[2]	<LAN1 >	<Disable>
12.	[0]	[0000000000000]	[0]	[2]	<LAN1 >	<Disable>

SAVE EXIT

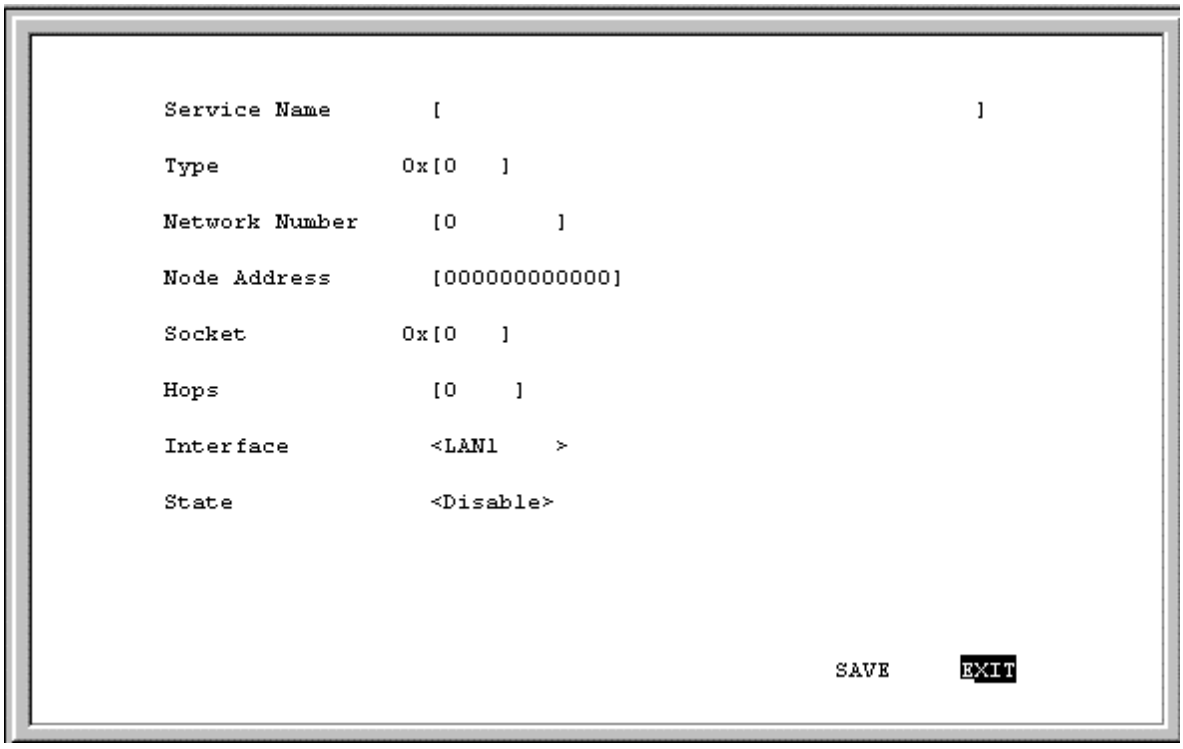
The parameters are described below:

- **Network** – This is the IPX network number.
- **Next Node Address** – This is the next node address of the device that the router will attempt to reach.
- **Hops** – This counts how many routers were passed through before the packet's final destination on a network was reached. The number of hops is part of each network entry in a RIP packet.
- **Ticks** – This is the time delay to reach a network. The number of ticks is part of each network entry in a RIP packet. There are about 18 ticks in a second.
- **Interface** – Select the desired interface containing the gateway that the packets will be forwarded through.
- **State** – This enables or disables a particular entry.

SPX Static Service



Select an entry and then press <Enter>.



The parameters are described below:

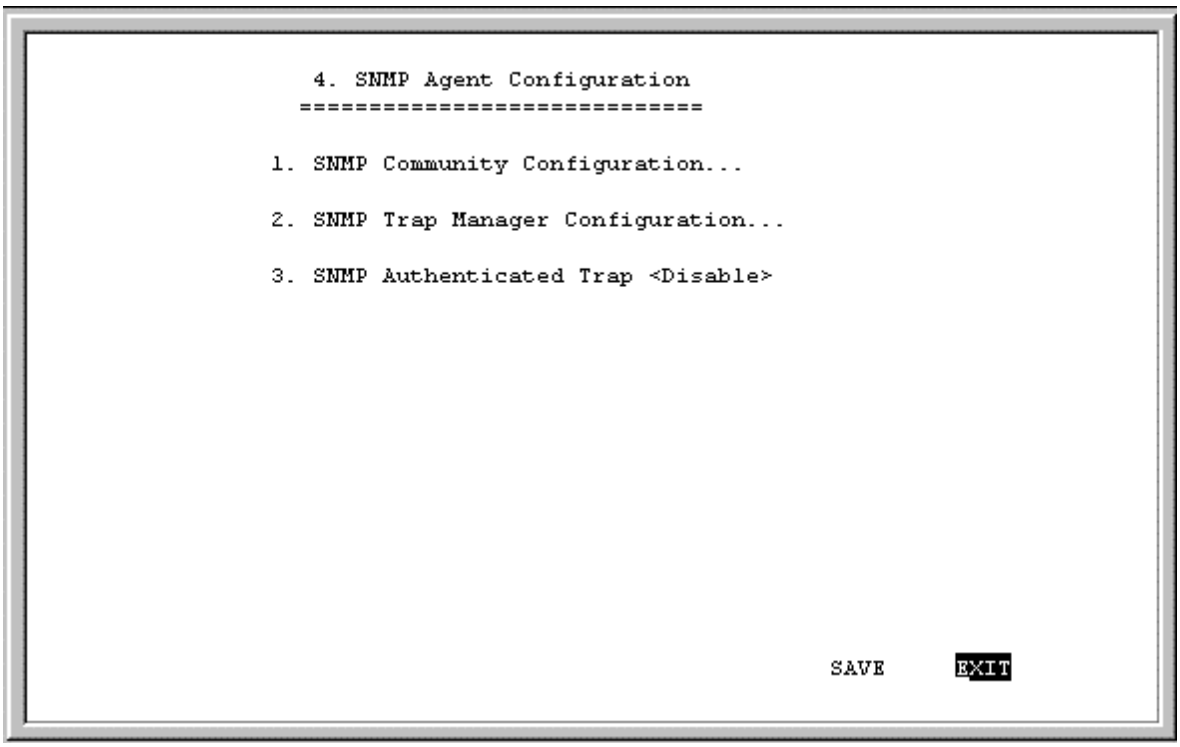
- **Service Name** – This is the name that has been configured for the server. This name must be the *exact* name configured in the NetWare server.

- **Type** – This field identifies the type of service the server provides.
- **Network Number** – This is the SPX network number.
- **Node Address** – This field contains the address of the node on which the server resides.
- **Socket** – This field contains the socket number on which the server will receive service requests.
- **Hops** – This counts how many routers were passed through before the packet's final destination on a network was reached. The number of hops is part of each network entry in a RIP packet.
- **Interface** – Select the desired interface.
- **State** – This enables or disables a particular entry.

SNMP Agent Configuration

The Simple Network Management Protocol (SNMP), defined in STD 15, RFC 1157, is a protocol governing the management and the monitoring of IP network devices and their functions. The DI-1162/DI-1162M supports the use of SNMP to acknowledge communication between management stations and itself. Basically, the DI-1162/DI-1162M, when connected to the network, acts as an SNMP agent, a software process that responds to queries using SNMP to provide status and statistics about the router.

Following is a description of how to configure the DI-1162/DI-1162M for SNMP management.

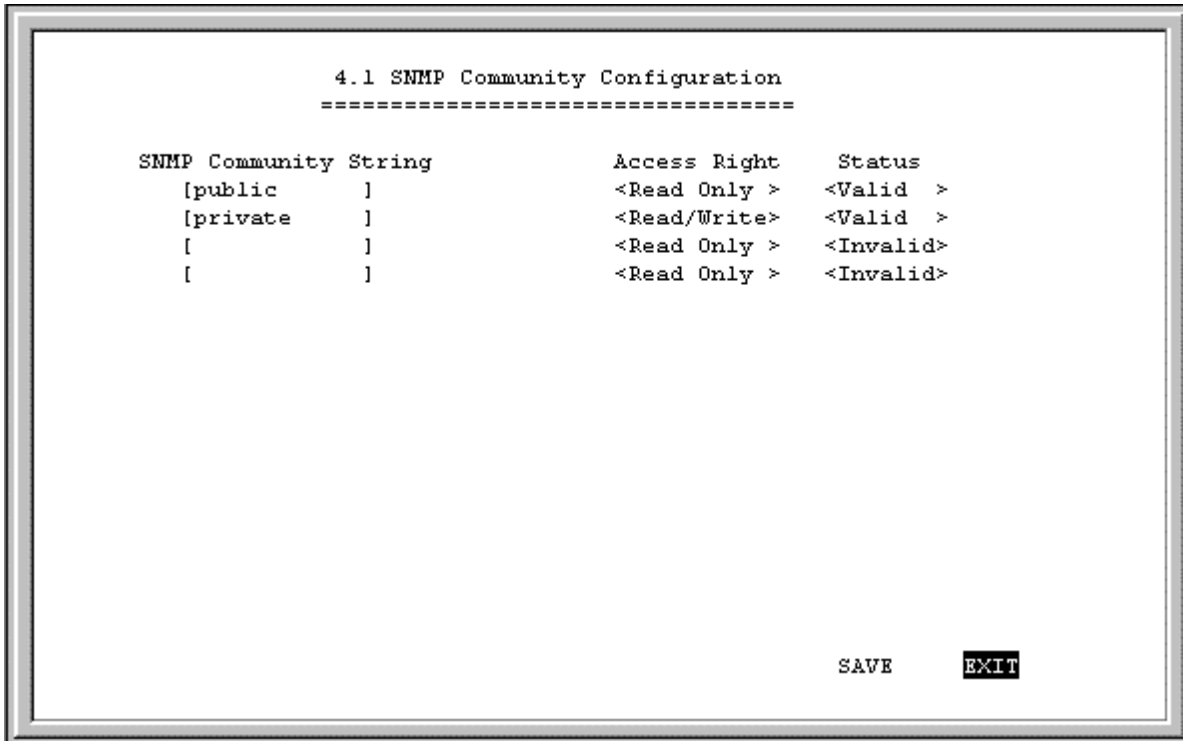


The parameters you can set is described below:

- **SNMP Authenticated Trap –** You can *Enable* or *Disable* an authentication failure trap message being sent to the Management Station by the router. When an SNMP packet with an invalid community name is received, it will be dropped. If this parameter is enabled, a trap will be sent to the network manager; if this parameter is disabled, no trap will be sent.

SNMP Community Configuration

Select and enter the **SNMP Community Configuration** submenu. You will see the following configuration screen:

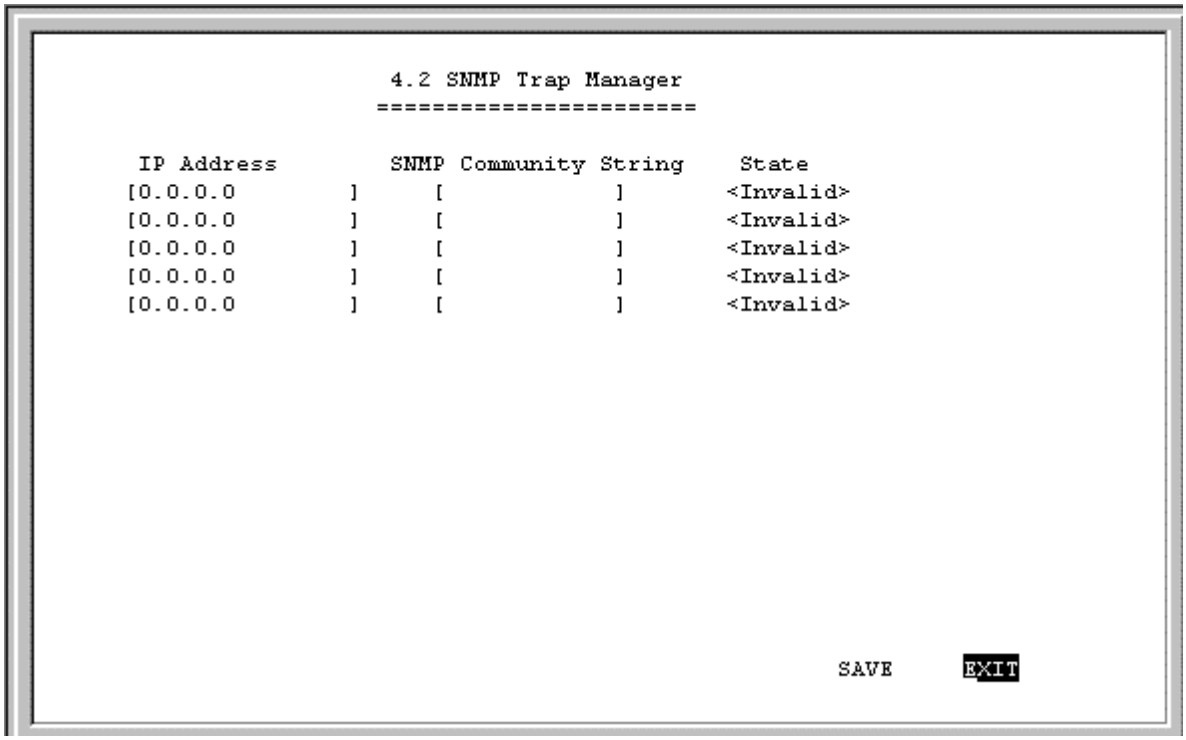


The parameters are described below:

- **SNMP Community String** – This community string is a user-defined identifying name used to group together some arbitrary set of SNMP application entities managed by the network manager.
- **Access Right** – This element of the set (*Read Only, Read/Write*) is called the SNMP access mode. If the SNMP Community String has an Access Right of *Read/Write*, then that Community String is available as an operand for the *get*, *set*, and *get next* operations. Otherwise, if the Community String's corresponding Access Right is *Read Only*, then it is available as an operand for the *get* and *get next* operations only.
- **Status** – This validates or invalidates the use SNMP Community String, by setting the string to *Valid* or *Invalid*. Note that setting the use of the string to *Invalid* is the same as removing the string, however, the string remains so as to be validated at an appropriate time.

SNMP Trap Manager

From the **SNMP Agent Configuration** menu, select and enter the **SNMP Trap Manager** submenu. You will see the following configuration screen:

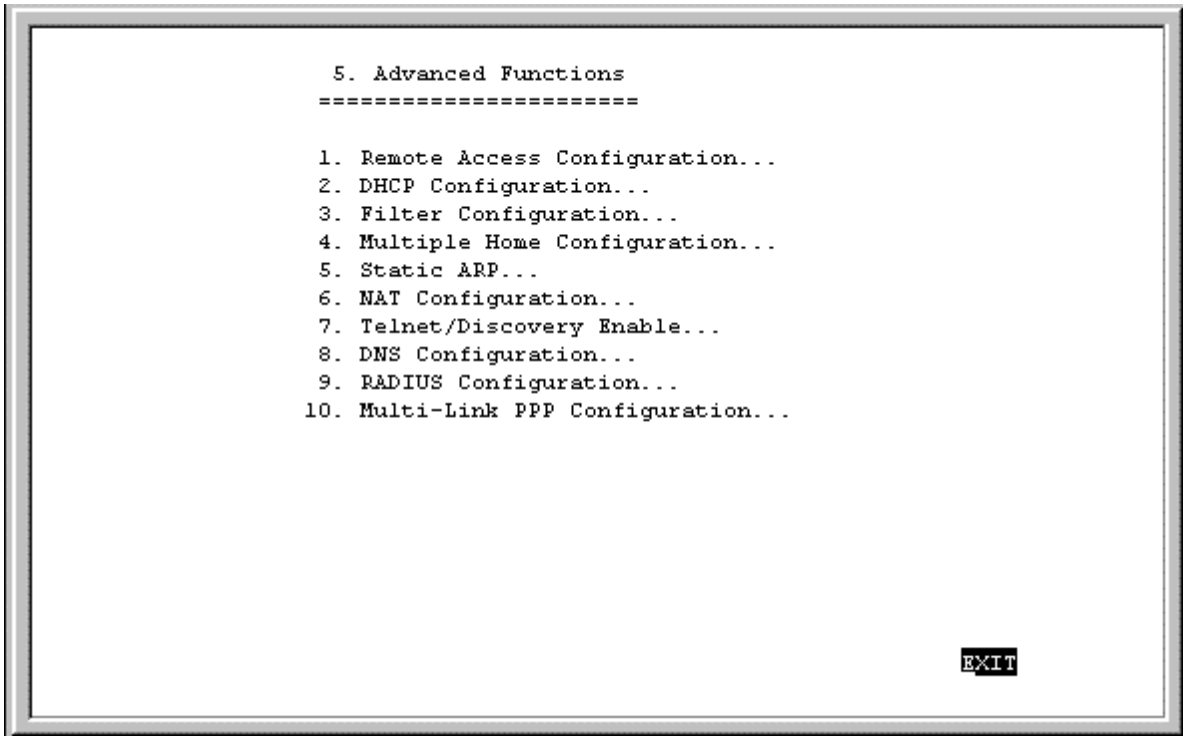


The parameters are described below:

- **IP Address –** Enter the IP address of the host who will act as an SNMP Management Station. The DI-1162/DI-1162M router will send SNMP traps to these addresses.
- **SNMP Community String –** The community string is a user-defined identifying name used to group together some arbitrary set of SNMP application entities managed by the network manager. Traps will be sent to the IP Address (previous parameter) as long as the corresponding Community String, in the Management Station's trap manager software, is the same.
- **Status –** This validates or invalidates the use of the SNMP Community String, by setting the use of the string to *Valid* or *Invalid*. Note that setting the string to *Invalid* is the same as removing the string, however, the string remains so as to be validated again at an appropriate time.

Advanced Functions

The **Advanced Functions** menu holds most of the more complex configuration settings and is shown below:



Remote Access Configuration

The Remote Access Configuration menu is used to set up the router for dial-in and dial-out connections through modems and/or ISDN devices attached to the WAN ports. The two B channels on the ISDN line or two modems, one connected to each WAN port, can support two independent remote connections or be banded together using Multi-link PPP to implement Bandwidth on Demand (configured separately in the **PPP Configuration** menu, the last item in the **Advanced Functions** window).

Remote Operation Overview

The DI-1162/DI-1162M is very flexible and can be configured for a variety of remote connections. Since configuring the router can be quite complex - depending on the number and type of remote connection(s) you wish to implement – we have described some of the basic functions and procedures below.

Dial-In User Connections

Dial-in users are defined as a single user on a computer, such as a person working at home, who dials into the office to use network resources. In almost all cases, a Dial-In User Profile needs to be set up for each user who will dial in to the router so the router can tailor the connection for each user. Once this is done, the remote user will be able to use network resources as if he were connected locally. When the user dials into the DI-1162/DI-1162M, the call comes into the WAN port and after answering the phone, the DI-1162/DI-1162M:

1. Identifies the Username and Password using the authentication protocol defined in the **Interface Configuration→WAN** submenu. The dial-in user is not prompted for this information, but must enter it into his dialing software before dialing.
2. Checks the Username and Password against those defined in the Dial-In User Profiles and Remote Network Profiles.
3. Assuming a matching Dial-In User Profile is found, the router may configure the IP address of the remote station (as defined in the Dial-In User Profile).
4. Configures a dial-in Interface (a virtual circuit) to handle the connection.
5. Establishes the connection.

6. In the case where the Dial-In User does not need to supply a Username and Password (Auth Type is set to *None* in the **Interface Configuration** submenu) the remote computer must have its own IP address.

Remote Network Connections

Remote networks are defined as other networks (LANs) that have WAN connections using a router, Internet server, network modem or similar device (in this document however, we will assume the remote device is a router). In almost all cases, a Remote Network Profile needs to be set up for each network that will connect to the DI-1162/DI-1162M via a WAN connection. The Remote Network Profiles are necessary for the router to identify and tailor the connection to the remote network's router. Once this is done, a connection between the two routers can be made and computers on each network can communicate with each other.

Dial-In Network Connections

A dial-in network connection is very similar to a dial-in user connection. When the remote router dials into the DI-1162/DI-1162M, the call comes into the WAN port and after answering the phone, the DI-1162:

1. Identifies the Username and Password using the authentication protocol defined in the **Interface Configuration→WAN** submenu.
2. Checks the Username and Password against those defined in the Dial-In User Profiles and Remote Network Profiles.
3. Assuming a matching Remote Network Profile is found, the router may configure the IP address of the remote station (as defined in the Remote Network Profile).
4. Configures the specified WAN Interface (a virtual circuit) using the configuration parameters defined in the **Interface Configuration** menu and the Remote Network Profile to handle the connection.
5. Establishes the connection.

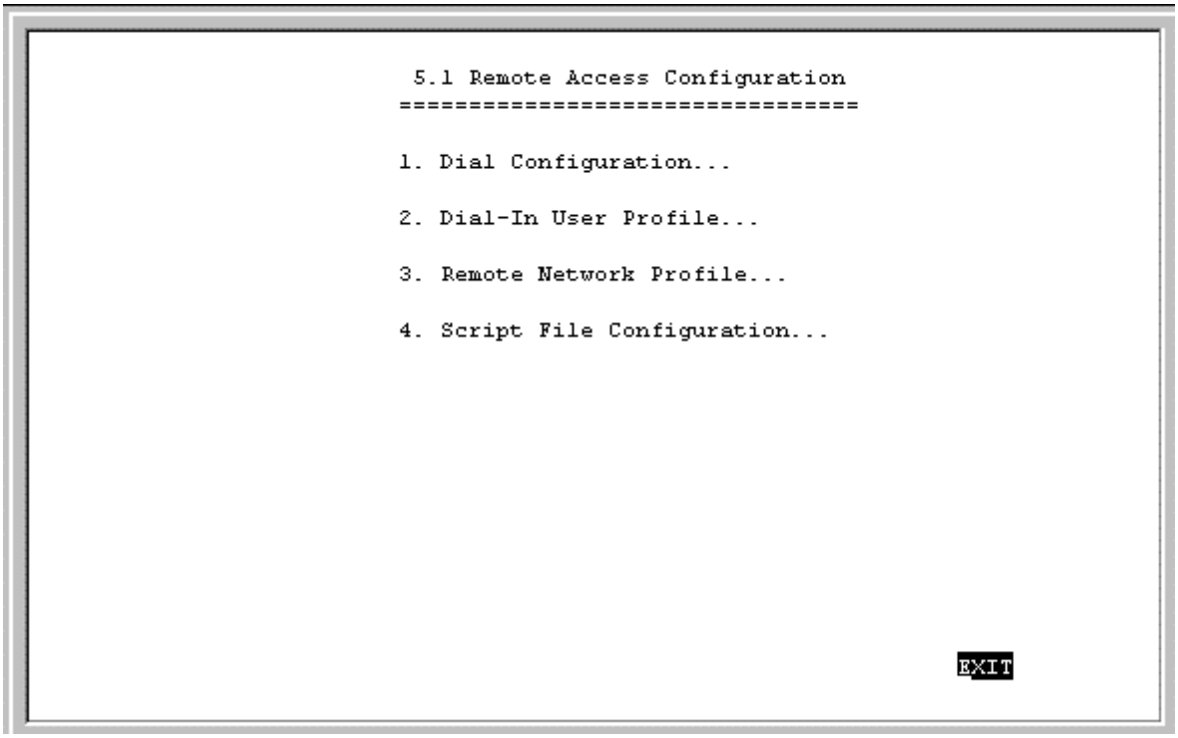
Dial-Out Network Connections

Dial-out network connections are much different than dial-in connections.

When a packet on the LAN reaches the router, the DI-1162/DI-1162M will:

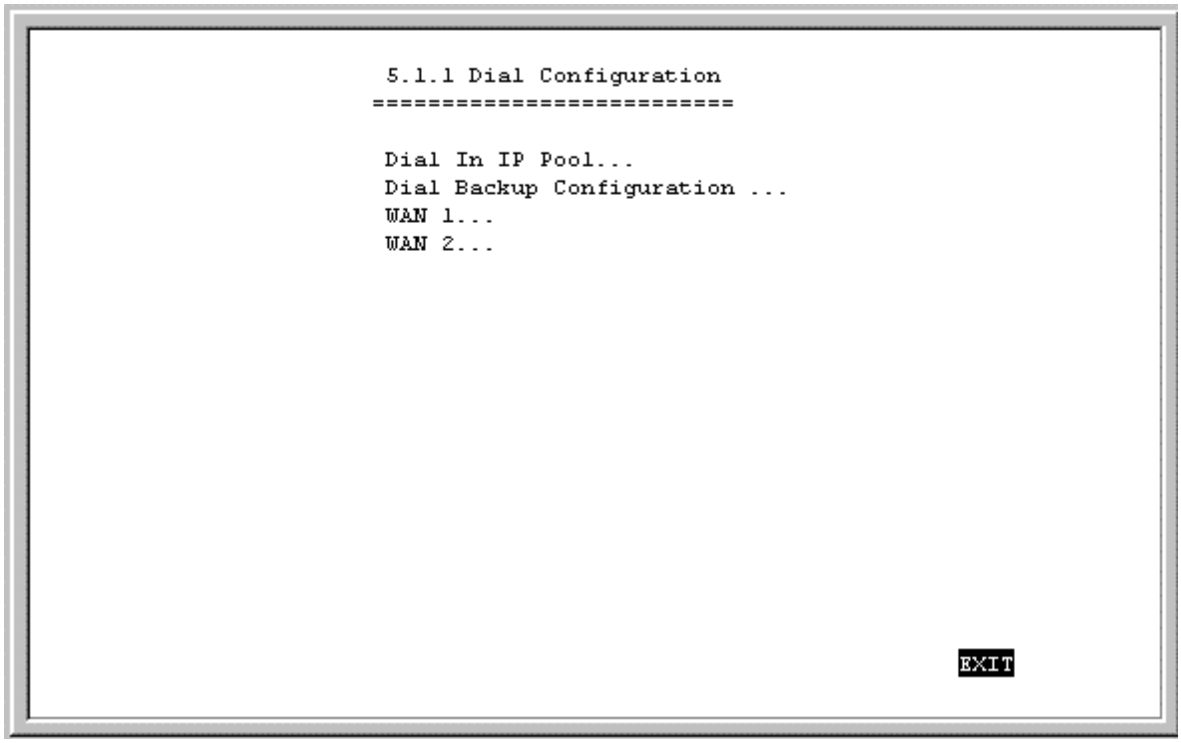
1. Check it's routing table to try to identify where this packet should go. It looks for two variables in the routing table, Gateway address and Interface. There are four possible results:
   I. In the case where the destination resides on the LAN, the router will send out an ARP request to obtain the MAC address of the destination computer and deliver the packet. Note that defining Static ARPs can speed up delivery since the router won't need to send out an ARP request.
   II. In the case where the router finds a match in the routing table, it uses the Gateway address and Interface numbers to identify the correct Remote Network Profile to use to dial out. From the Remote Network Profile, the router gets the telephone number and other information and dials out, establishes a connection and delivers the packet
   III. In the case where no match is found in the routing table, the router will search for IP Static Routes. If a match is found in the static routing table, the router will use the information there to find the correct Remote Network Profile to use to dial out. If you have a connection to the Internet, it is very important that you define the default next hop router in the **IP Static Routes** submenu of the console program as your ISP (see the *IP Static Routes* section of this manual for more detailed configuration information). This is because if a user on your LAN makes a request to download a web page for the first time, for instance, since it is the first time, the DI-1162/DI-1162M will not have any record of the web page's IP address. If no default next hop router is defined, the request will be dropped and the user will get a 'Destination Unreachable' error message. However, if a default next hop router is defined in the IP Static Routes, the DI-1162/DI-1162M will pass this request on to the ISP (the request will go through) and the user will receive the web page.
   IV. In the case where there is no match for the destination IP address in the routing table or the static routing table, and no default next hop router is defined, the packet will be dropped and no action will be taken.

The **Remote Access Configuration** submenu is shown below. All items in the submenu are described as follows.



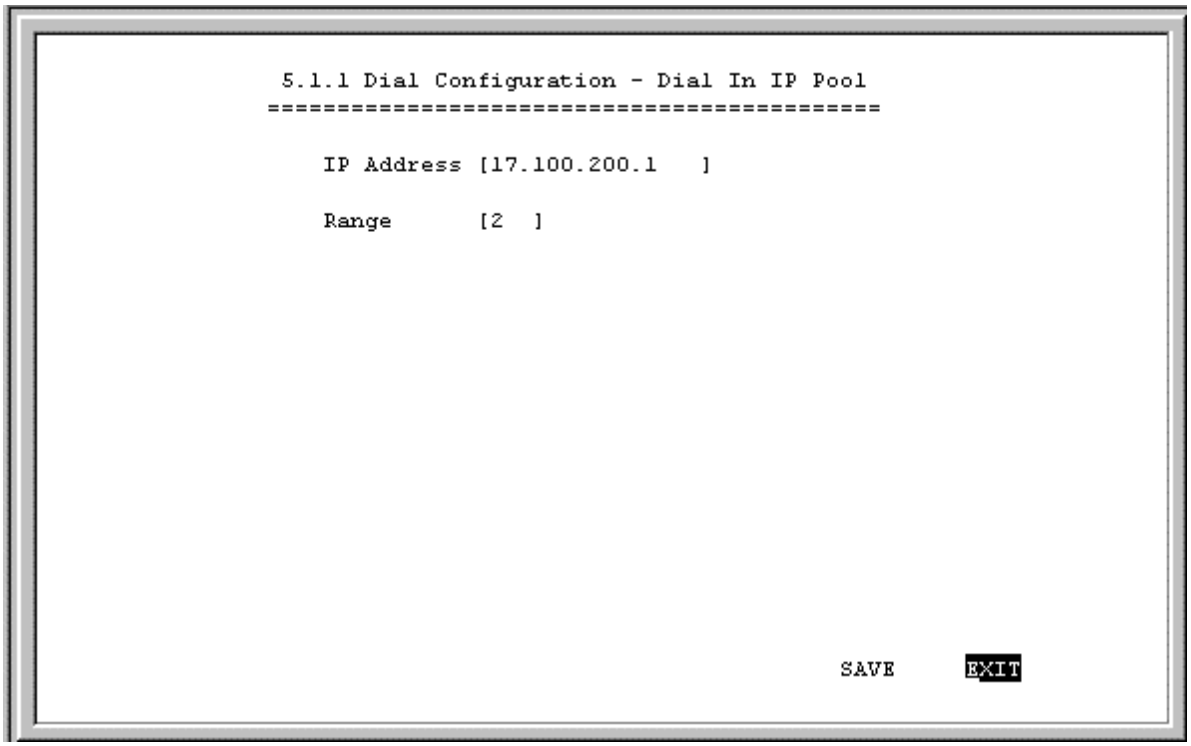
Dial Configuration

You can configure the two WAN interfaces on your DI-1162/DI-1162M to dial-out only when a packet is forwarded to that interface, and hang up after all data has been transferred and the link is idle. This can be used to lower the cost of an unpopular link or used as a backup link to your ISP. This feature is commonly called “Dial on Demand”. WAN interfaces can also be configured here to receive calls from dial in users and other networks, called “Remote Access”. Please note however, that in all cases, after configuring the WAN interfaces in the **Dial Configuration** submenu, they must be further configured in the **Dial-In User Profile** submenu or **Remote Network Profile** submenu.



Dial In IP Pool

The dial in IP pool allows you to define a range of IP addresses that will be reserved for and assigned to dial-in users.

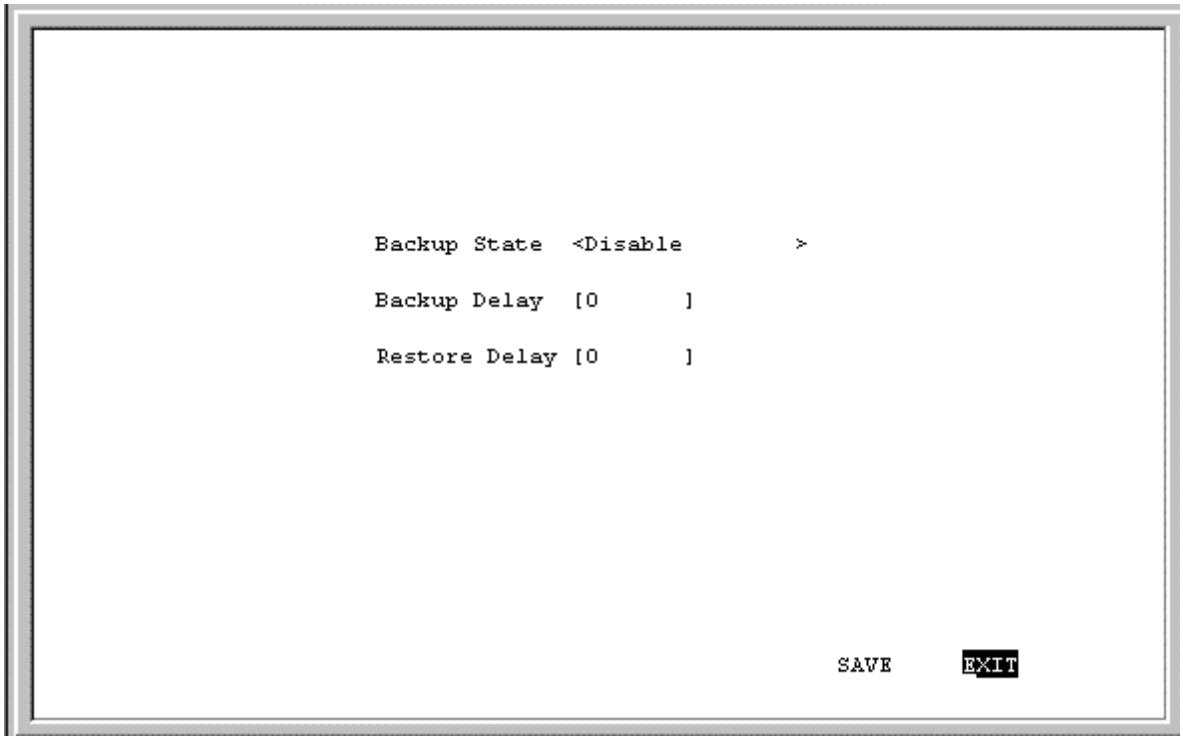


The items are described as follows:

- **IP Address** – This is the first IP Address that will be assigned to a dial-in user.
- **Range** – This is the number of IP Addresses that can be assigned. In the window shown above, dial-in users will be assigned the IP Addresses 170.100.200.1 or 170.100.200.2 (only two are necessary since the router used in the examples has only two WAN ports).

Dial Backup Configuration

The dial backup configuration function allows you to configure information about a backup interface. An example of a backup interface on the **Remote Network Profile** menu would be making WAN 2 a backup interface for WAN 1. Enter configuration information below to complete the dial backup configuration.

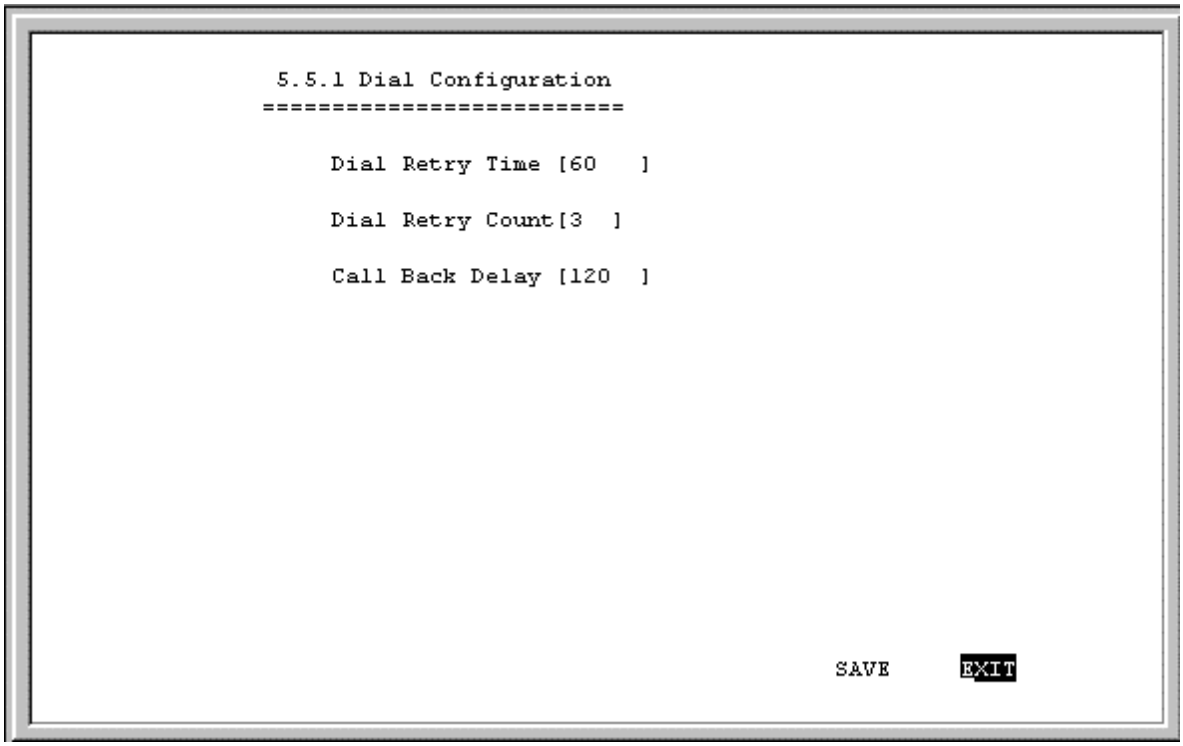


The items are described as follows:

- **Backup State** – Choose among *Answer*, *Dial on Demand*, *Always Connect*, or *Disable.*
  - ◊ *Answer* Select this to accept phone calls.
  - ◊ *Dial on Demand* This initiates phone calls to make a connection.
  - ◊ *Always Connect* When this is selected, the primary line will never have a chance to be activated again.
  - ◊ *Disable* Select this if you don't want the backup function to be used.
- **Backup Delay** – This value (in seconds) is used when the primary interface fails. Once the Backup Delay value is reached, the backup interface will be activated for use.
- **Restore Delay** – This value is used if and when the master interface is operational again. Once the Restore Delay value is reached, the backup interface will be disconnected

WAN 1

This submenu contains a number of settings (shown below) which allow you to configure the router to dial out.



The parameters are described below:

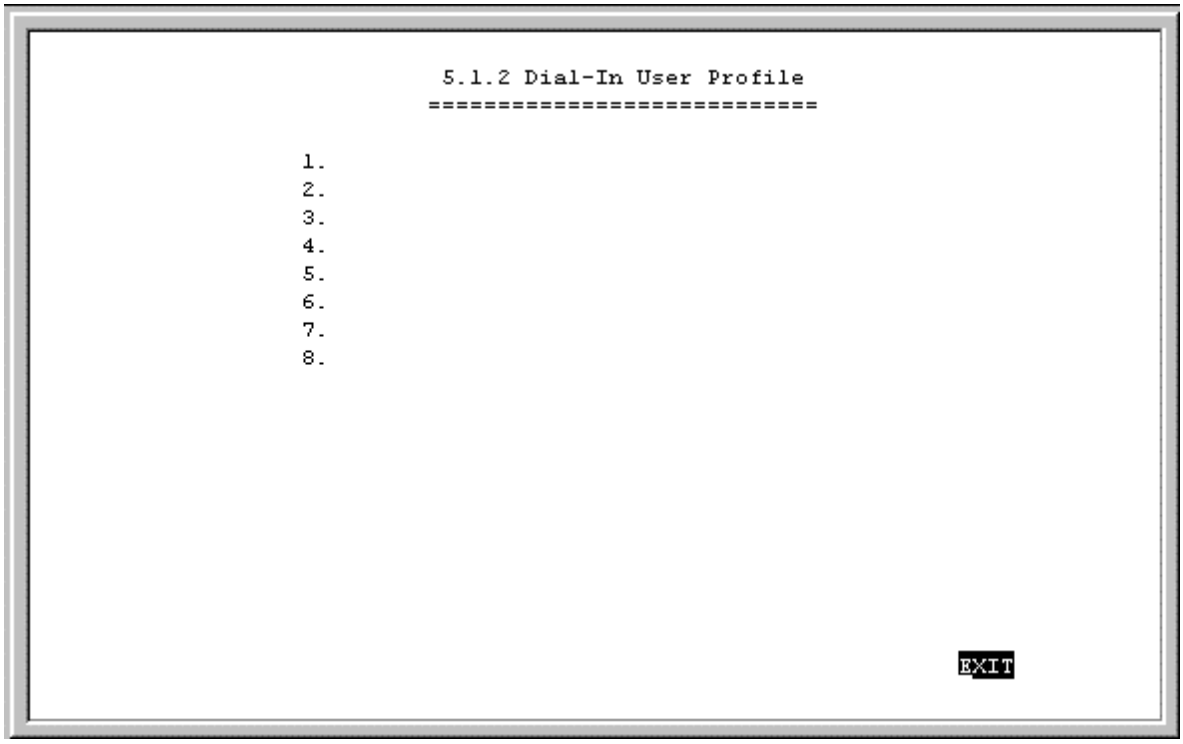
- **Dial Retry Time –** This is the time (in seconds) the router will wait before the next dial attempt.
- **Dial Retry Count –** This is the specified maximum number of dial attempts the router will make when trying to establish a connection on this interface.
- **Call Back Delay –** This is the time (in seconds) the router will wait before calling the number designated for a specified dial-in user.

Dial-In User Profile

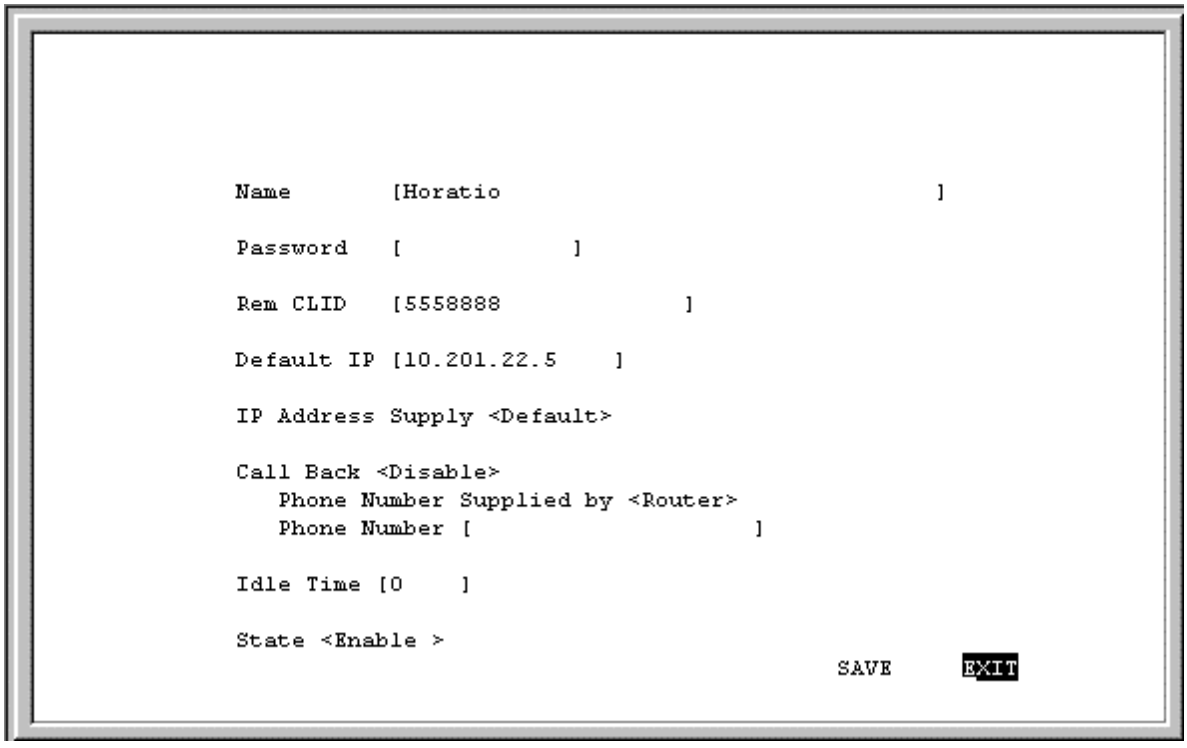
The Dial-In User Profile is used to configure the DI-1162/DI-1162M for single users (for example a person working at home) to dial in to the router and gain access to the network. At least one User Profile must be configured for each user who will dial in (in conjunction with Dial Configuration settings). Please note that WAN connections to computers on other networks must be defined in the **Remote Network Profile** submenu.

Up to eight users can be set up to dial in to the router. However, more dial-in users can be accommodated by using a RADIUS server as described in the *RADIUS Configuration* section of this manual.

The **Dial-In User Profile** submenu appears below:



Select an entry from above and hit <Enter>. This screen will be blank if a dial-in user profile has not been configured yet.



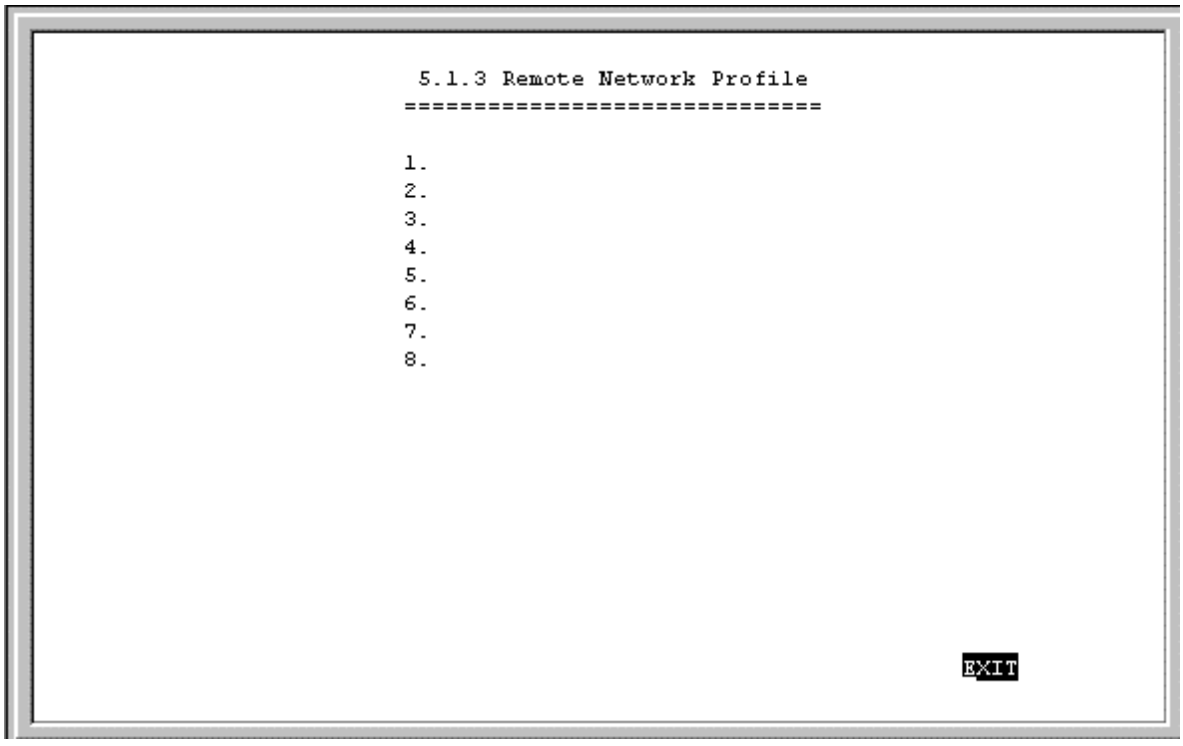
The parameters in the above window are described as follows:

- **Name –** The maximum length is 64 characters. This username is for password challenges (authentication). The user dialing in must supply this username in order to be allowed access to the router.
- **Password –** This is the password associated with the above Name field.

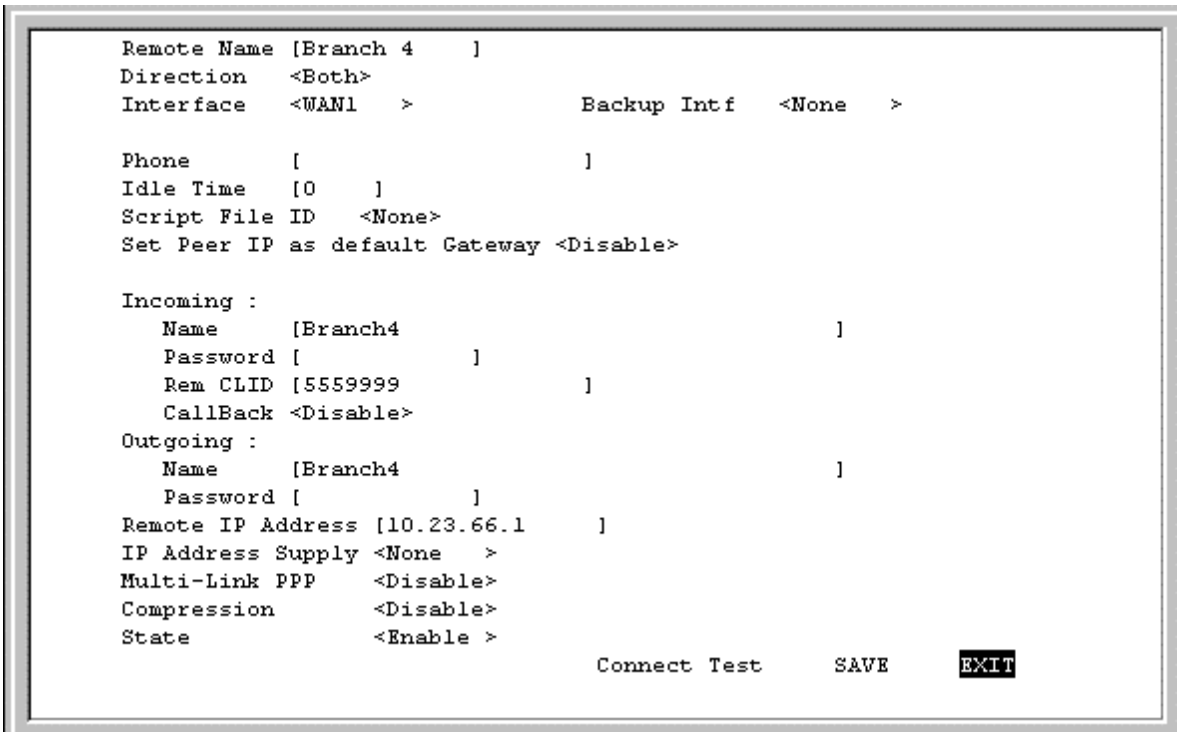
- **Rem CLID** – Remote Caller ID. This is the telephone number of the Remote User and is used for security. When a phone number is entered in this field, the router will make sure that the incoming call is coming from the same phone number as the one defined here. In other words, the remote user can only be calling from the telephone number defined here, otherwise the call will not be accepted. This function is disabled if the field is left blank.
- **Default IP –** This is the IP address that will be assigned to the dial-in user when the IP Address Supply setting below is set to Default. Assigning an IP address to the remote computer ensures that the IP address does not clash with other IP addresses on your network.
- **IP Address Supply** – This field defines how the remote user will obtain an IP address. The choices include:
  - ◊ *Default* – Uses the Default IP address defined above.
  - ◊ *Dynamic* - Taken from the Dial-In IP pool.
  - ◊ *None* - The remote user supplies their own IP Address.
- **Call Back** – This field determines if the router will allow call back to the Remote Dial-In User upon dial-in. If this option is enabled, the router will be able to call back to the Remote Dial-In User if they request it. In such a case, the router will disconnect the initial call from this user and dial back to the specified call back number. The default is no call back.
- **Phone Number Supplied by** – Toggle between *Router* and *Caller*.
- **Phone Number** – If *Caller* is selected above, then this phone number is usually provided by the person who initially set up the router. If *Router* is selected, you must enter the phone number that will be called back yourself.
- **Idle Time –** This is the elapsed time (in seconds), of inactivity, that will trigger the router to disconnect this interface.
- **State –** Enables/disables this User Profile.

Remote Network Profile

The Remote Network Profile is used to configure the router for WAN connections to other networks. In practice, the DI-1162/DI-1162M will either dial-out to or receive incoming calls from another router, the 'gateway' to the other network.



Select an entry from above and hit <Enter>. This screen will be blank if a remote network profile has not been configured yet.



The parameters in the above window are described as follows:

- **Remote Name** – Name for the remote network that the DI-1162/DI-1162M is being set up to connect with.
- **Direction –** Dial-[*In*], dial-[*Out*], or [*Both*]. This field defines whether the router on the other network will dial-[*In*] to the DI-1162/DI-1162M to establish a connection, the router will dial-[*Out*] to the other network, or a connection can be established [*Both*] ways.

  When this is set to *In*, the DI-1162/DI-1162M will only establish a connection with the other network by receiving calls on the WAN port specified in the Interface field below. Also, the incoming calls will be subject to the Name, Password, and Rem CLID fields in the Incoming section below.

  When this is set to *Out*, the router will only make calls on the WAN interface specified in the Interface field below. Also, the outgoing calls will be subject to the Name, Password and Phone Number fields in the Outgoing section below.

  When set to *Both*, the dial in and dial out conditions described above will both be observed.
- **Interface** – *WAN1* or *WAN2*. This field is used to assign a remote network to a logical (virtual) interface called a virtual circuit. More than one remote network can be configured to use the same interface, but they cannot be connected at the same time. Thus, if you wish to have two WAN connections operate simultaneously, make sure they are configured on different interfaces. On the other hand, if you have two dial-out remote network profiles but wish to keep one line always open for dial-in users, make sure the two dial-out profiles use the same interface. In this case, the two profiles will share the same interface; the second one using it after the first one's idle time has expired and it has relinquished it.
- **Backup Intf** – Enter a backup interface in this field is desired.
- **Phone -** This is the telephone number that will be dialed to make the outgoing connection.
- **Idle Time –** This is the elapsed time (in seconds), of inactivity, that will trigger the router to disconnect this interface.
- **Script File ID** – This is the ID in the **Script File Configuration** menu.

- **Set Peer as default Gateway –** When enabled, this feature sets the IP address of the remote device as the default gateway (default next hop router) for all packets not found in the routing table. If the Peer IP is set as the default gateway here, you still need to define a static default route in the **Network Configuration→IP Static Route** submenu, but you don't need to designate a gateway IP address for the static route (the routers will automatically negotiate and adjust the gateway IP setting accordingly). And also make sure that the Remote IP Address in the Remote Networks Profile is set to 0.0.0.0.

Incoming:

- **Name** – The maximum length is 64 characters. This username is for password challenges (authentication). The user dialing in must supply this username in order to be allowed access to the router.
- **Password** – This is the password associated with the above Name field.
- **Rem CLID** – Remote Caller ID. This is the telephone number of the Remote User and is used for security. When a phone number is entered in this field, the router will make sure that the incoming call is coming from the same phone number as the one defined here. In other words, the remote user can only be calling from the telephone number defined here, otherwise the call will not be accepted. This function is disabled if the field is left blank.
- **Call Back** – This field determines whether the router calls back after receiving a call from this Remote Network Profile. If this option is enabled, the router will disconnect the initial call and call back to the phone number that you provide. Note that this field will be valid only if the Direction setting above is *Both*.

Outgoing:

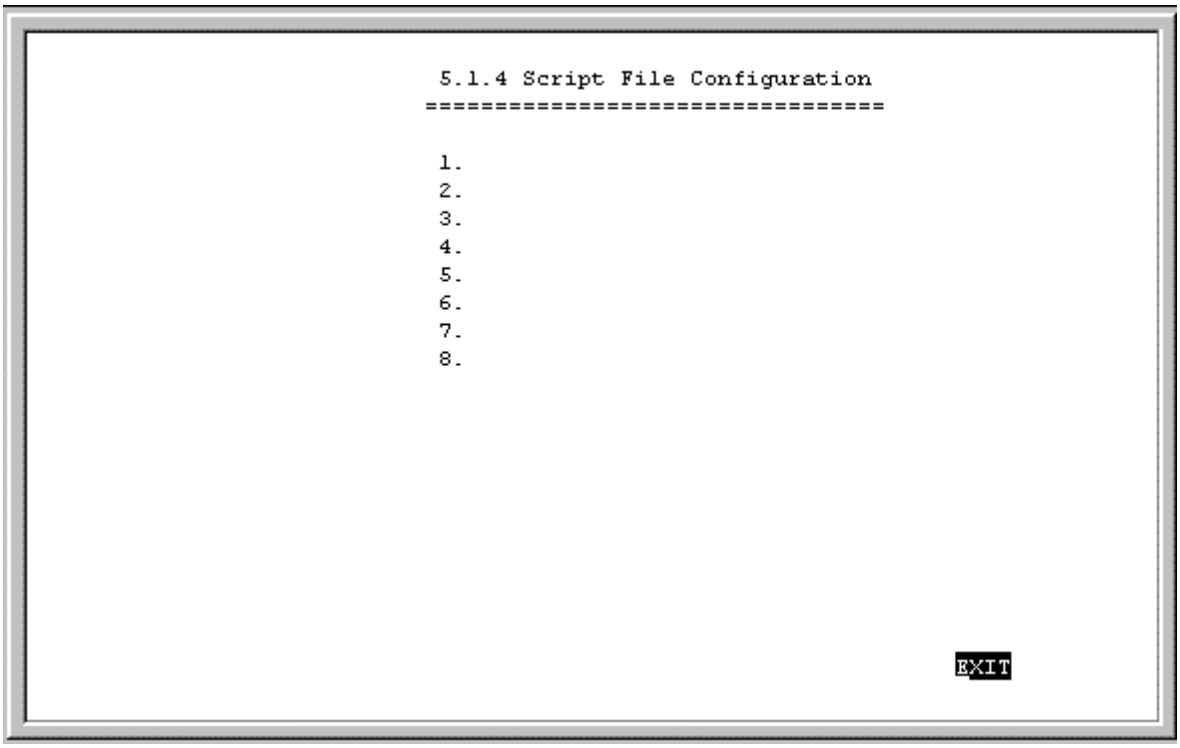
- **Name** – The maximum length is 64 characters. Spaces and punctuation are not usually accepted. This username is for password challenges (authentication) which are automatically handled by the router when dialing out. The DI-1162/DI-1162 will use PAP and CHAP (whichever works) to make the connection.
- **Password** – This is the password associated with the above Name field.
- **Remote IP Address** – This is the IP address that will be assigned to the dial-in network when the IP Address Supply setting below is set to *Default*. Assigning an IP address to the router dialing in ensures that the IP address does not clash with other IP addresses on your network. For dial out connections utilizing dial on demand, the IP address of the remote router needs to be entered here so the router knows which remote network to establish a connection with to deliver the packet.
- **IP Address Supply** – This field defines how the router will assign an IP address to a device dialing in. The choices include:
  - *Default* – Uses the Remote IP address defined above.
  - *Dynamic* – Taken from the Dial In IP pool.
  - *None* – The remote user supplies their own IP Address.
- **Multi-Link PPP** – Enables/disables multi-link PPP on this port. Individual ports can be set to join the MLPPP bundle by enabling Multi-Link on each port. When enabled, the port will join the MLPPP bundle. Please note that this router contains only one MLPPP bundle. All ports taking part in MLPPP, even the first or primary port which initially establishes the connection, must have Multi-Link enabled. The port that first established the connection is the Primary Port and will not disconnect due to a BOD Low Threshold event, but is subject to Dial on Demand (DOD) settings.
- **Compression** – Enables or disables Stac compression. This is an industry standard using a 4:1 compression scheme. When enabled, the router will try to use Stac compression on the designated port whenever possible. If the destination device is not capable of using Stac compression, the two devices will still communicate, albeit without using Stac compression. When disabled, Stac compression will never be used on this port
- **State** – Enables or disables this Remote Network Profile.

Script File Configuration

Script files are used on dial-out connections where the server you are connecting to uses a script for the logon procedure (common with many ISP's). If you would like the router to automatically logon to a remote server, you must define a script file.

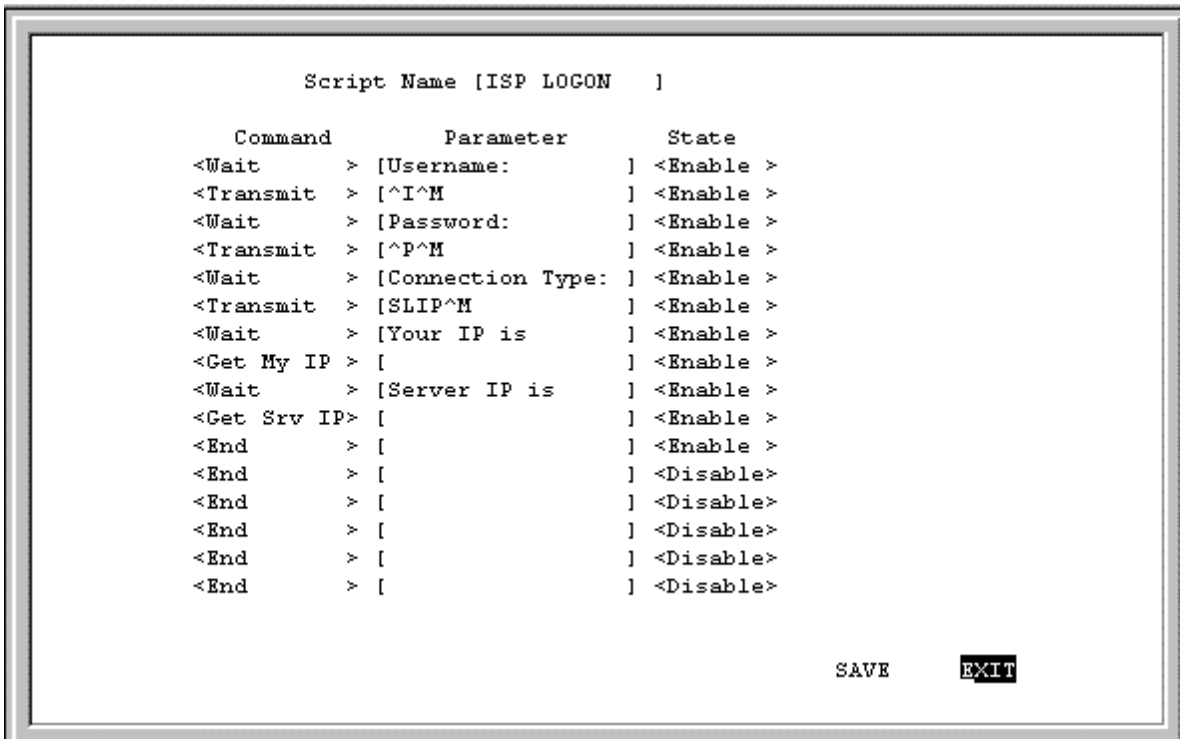
Script files are executed immediately upon successfully establishing a connection. The DI-1162/DI-1162M can hold up to 8 different script files.

Press <Enter> in a script name field to define a script file.



Script File Example

The example script file shown below assumes a connection to an Internet Service Provider.



Commands

Script files can perform six Commands. You can choose the appropriate command by positioning the cursor in the Command field and pressing <space bar> to toggle to the desired command. The script commands are defined as follows:

- `Wait` – This command waits for text defined in the Parameter field to be transmitted by the ISP. In the above example, the router will wait for the ISP to prompt for '`Username:`'. Please note that the parameters are case-sensitive and must be an exact match.

- `Transmit` – Transmits the exact characters written in the Parameter field. There are also three keywords that can be transmitted:

  - ◊ ^I – Username, as defined in the **Remote Network Profile** submenu.
  - ◊ ^P – Password, as defined in the **Remote Network Profile** submenu.
  - ◊ ^M – <Enter> or <Return>.

- `Delay` – Will delay for the number of seconds defined in the Parameter field.
- `Get My IP` – Will get the IP address from the ISP if the ISP sends it. This command is only valid for SLIP connections.
- `Get Srv IP` – Will get the Servers IP address if it is sent. This command is only valid for SLIP connections.
- `End` – Ends the script file.

Parameters

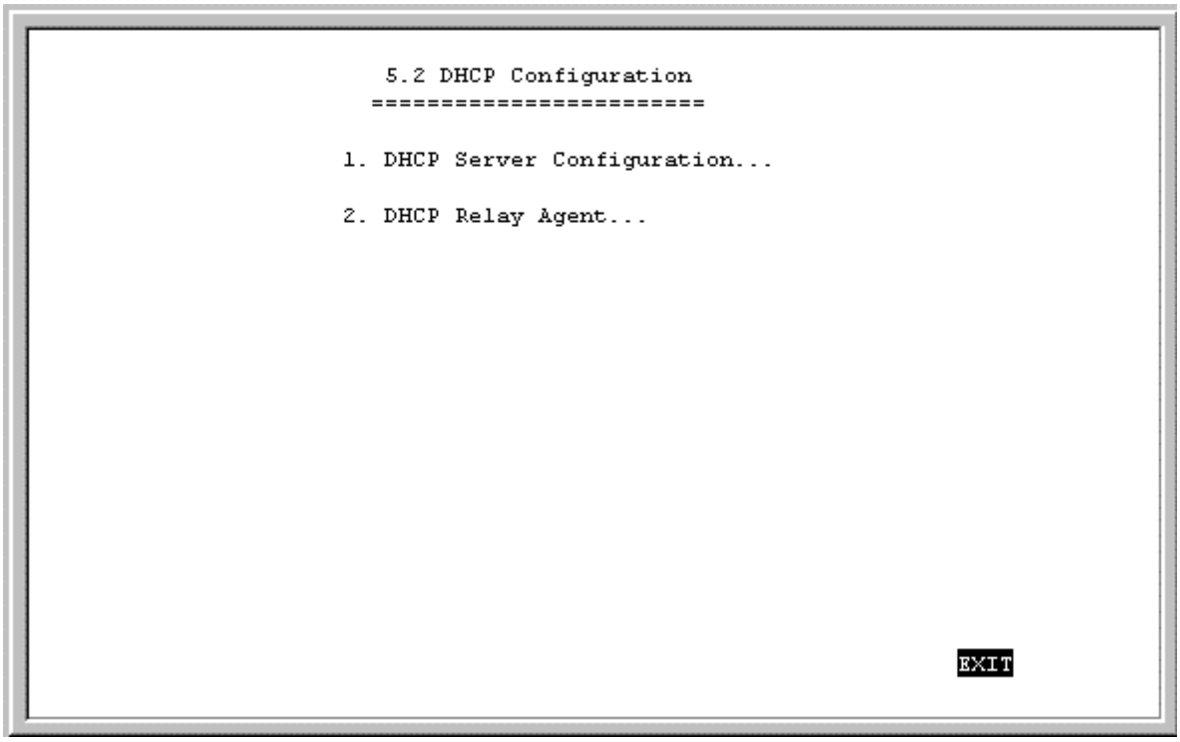
Parameters are data fields which hold text or numbers that are used in the `Wait, Transmit,` and `Delay` commands.

State

Toggles to enable or disable the line item.

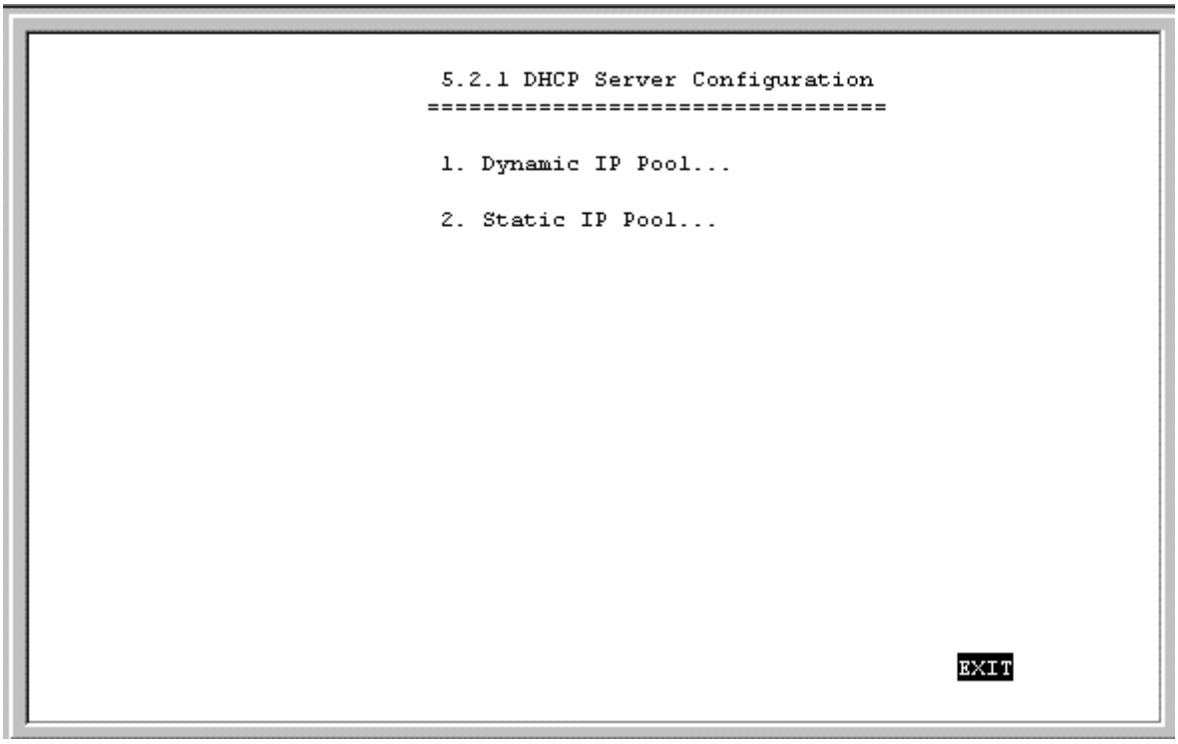
DHCP Configuration

The DI-1162/DI-1162M Router implements the Dynamic Host Configuration Protocol (DHCP), which allows the entire IP network to be centrally managed by the router. It does this by assigning IP addresses and configuration parameters to hosts as they are powered on and come onto the network. This can be a great help for network administration since many administrative tasks such as keeping track of each computer's IP address are handled by the router. The DI-1162/DI-1162M can implement DHCP in one of the two ways shown below:



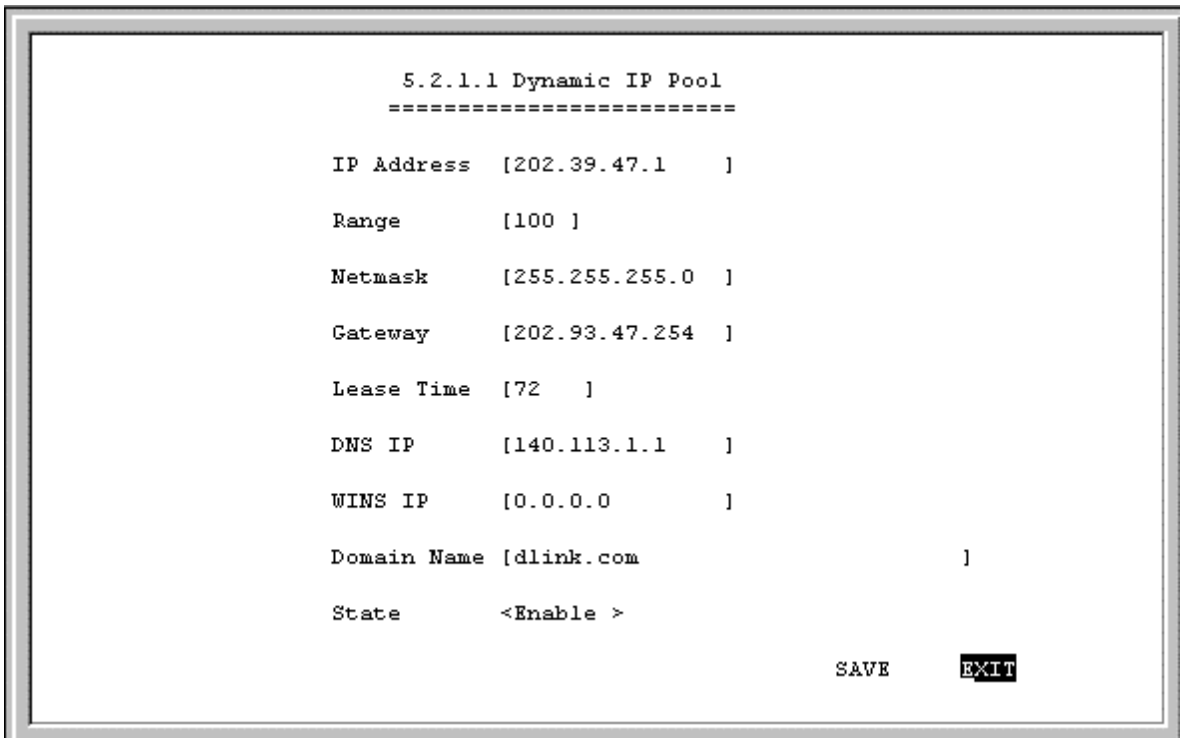
DHCP Server Configuration

When acting as a DHCP server, the DI-1162/DI-1162M will manage many of the IP network parameters. The DI-1162/DI-1162M will never assign a broadcast or network IP addresses to hosts, even if such an address is included in the specified range.



Dynamic IP Pool

The **Dynamic IP Pool** screen shown below contains the parameters that the router can set on the hosts. Please note that the Dynamic IP Pool cannot be enabled when the DHCP Agent feature is enabled.



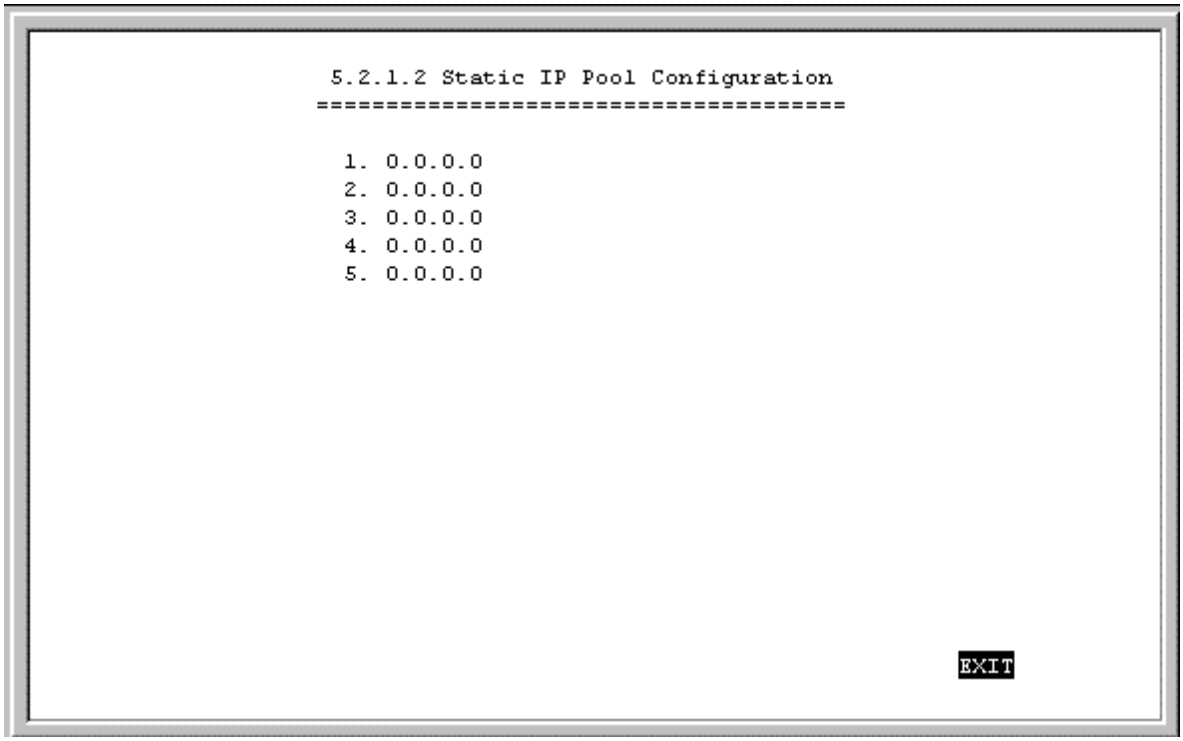
The parameters are described below:

- **IP Address –** This is the base (starting) address for the IP pool of unassigned IP addresses.

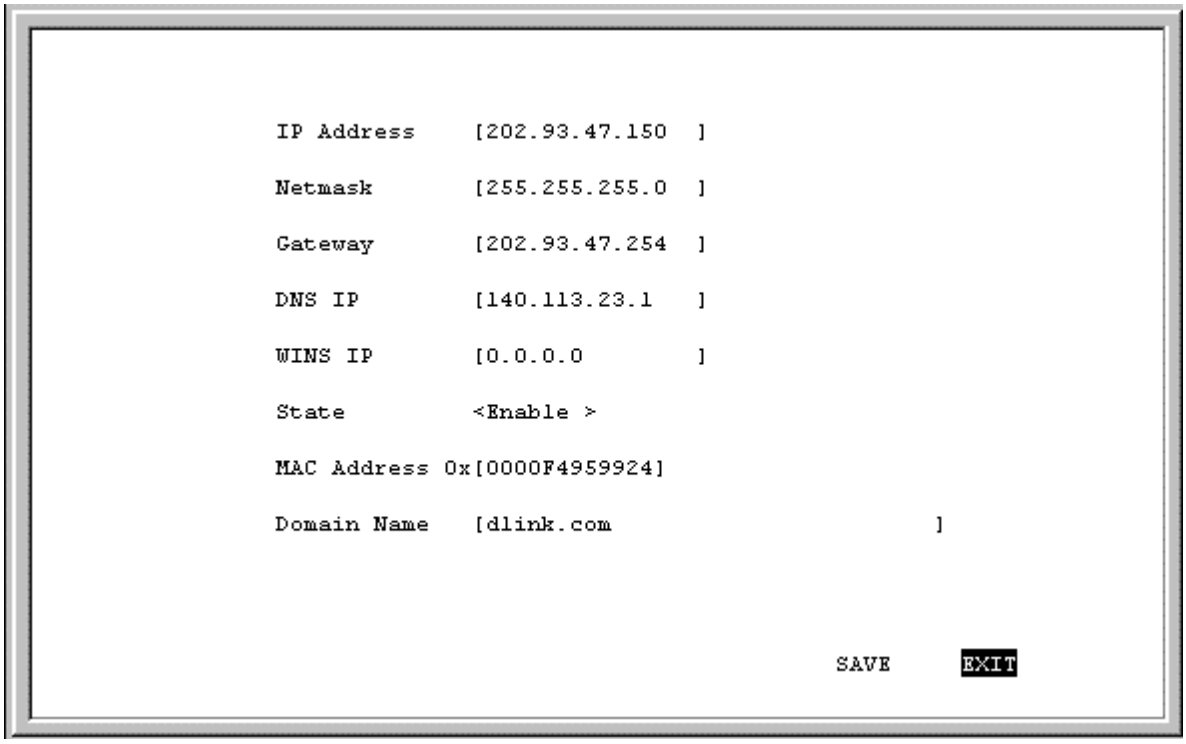
- **Range –** This is the range of contiguous, IP addresses, above the base IP Address above. In the above example, the IP Addresses assigned would be 202.93.47.1, 202.93.47.2, … 202.93.47.100.
- **Netmask –** This mask informs the client, how the destination IP address is to be divided into network, subnet, and host parts. The netmask has ones in the bit positions in the 32-bit address which are to be used for the network and subnet parts, and zeros for the host part.
- **Gateway –** This specifies the Gateway IP Address that will be assigned to and used by the DHCP clients.
- **Lease Time –** This specifies the number of hours a client can lease an IP address, from the dynamically allocated IP pool. A value of 65535 means the lease is permanent.
- **DNS IP –** This specifies the Domain Name System server, used by the DHCP clients using leased IP addresses, to translate hostnames into IP addresses or vice-versa.
- **WINS IP –** This specifies the IP address of the Windows Internet Naming Service server. This server has software that resolves NetBIOS names to IP addresses.
- **Domain Name –** This is the common suffix, shared by networked hosts, used to represent a common network domain.
- **State –** This toggles *Disable* and *Enable* for DHCP function.

Static IP Pool

The Static IP Pool configuration functions in much the same way as the Dynamic IP Pool configuration. The only difference is that a particular IP address can be assigned to a particular host. The host is identified by the MAC Address of its NIC, which must be entered on this screen.



Select an entry from above and hit <Enter>. This screen will be blank if a static IP pool has not been configured yet.



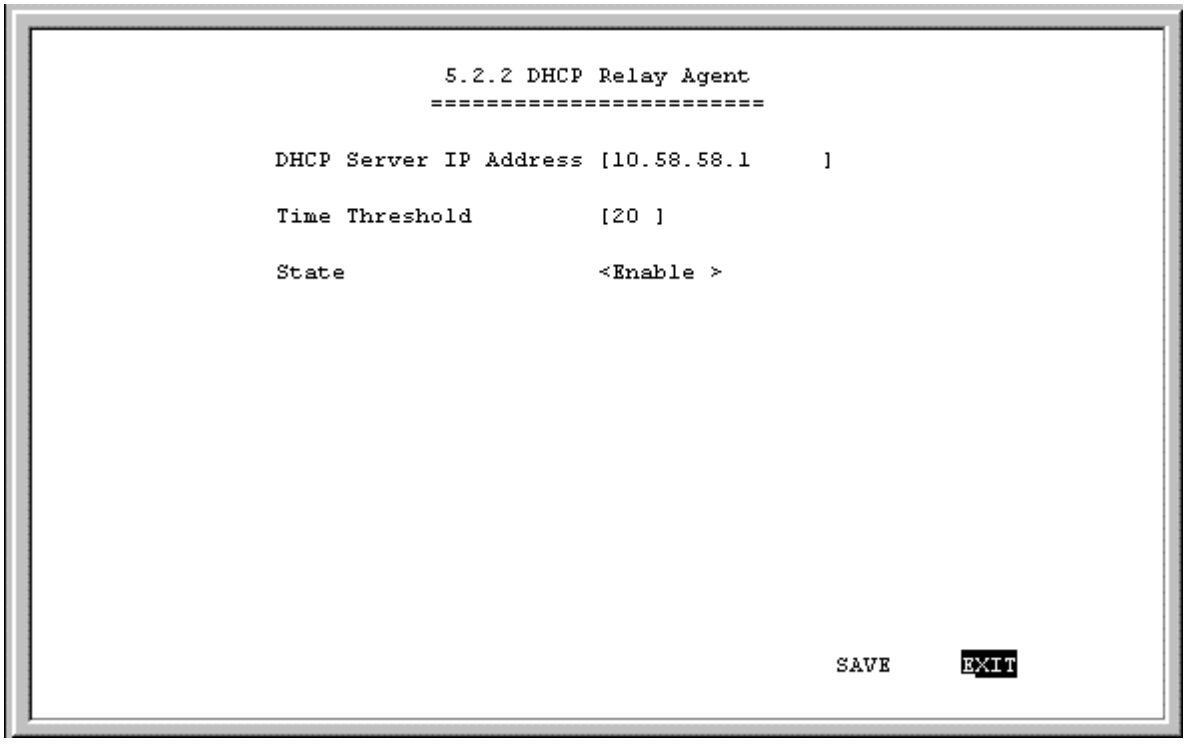
The parameters are described below:

- **IP Address –** This is the static IP address to be assigned.
- **MAC Address –** This specifies the physical address of the particular host that will receive the above IP address.

All other parameters (Netmask, Gateway, DNS IP, WINS IP, State, and Domain Name) are identical to those in the Dynamic IP Pool configuration, in the previous section.

DHCP Relay Agent

The DHCP Relay Agent feature allows the DI-1162 to act as a go-between for a remote DHCP server assigning IP addresses to local clients. This can be useful if you wish to have all IP addresses in your company, including those in branch offices, assigned from a DHCP server centrally located at your headquarters, for example.



Items are described as follows:

- **DHCP Server IP Address –** This is the IP address of the remote DHCP server. When a local computer powers up and sends a DHCP request for an IP address, the DI-1162/DI-1162M will forward the request to the address specified here.
- **Time Threshold –** This specifies the maximum amount of time (in seconds) since the host began requesting an IP address. If the value define here is exceeded, the relay agent will not pass along the request from the host.
- **State** – Enables or disables the DHCP Relay Agent function.

Filter Configuration

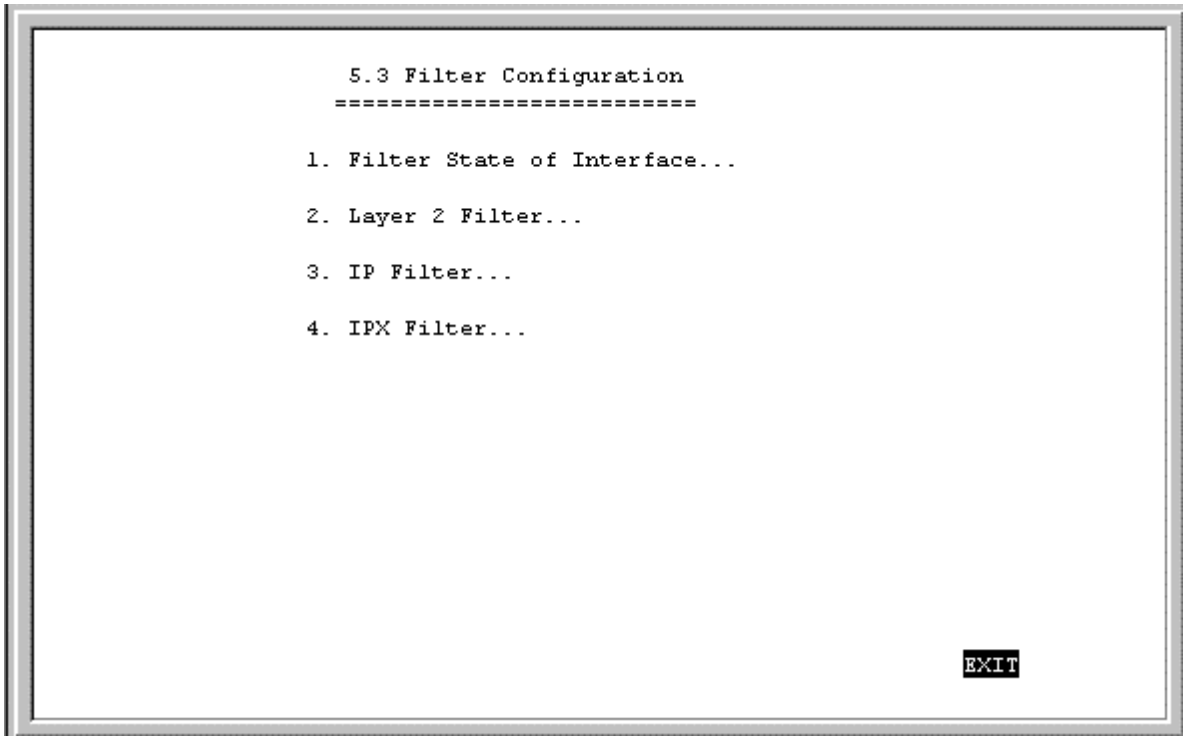
Your DI-1162/DI-1162M uses filters (configurable at two layers) to screen packet data, and apply a routing decision. There are two methods of configuring a filter: you can configure a filter at the network layer (IP filter) to restrict access between networks and reduce unnecessary internetwork traffic; and you can configure a filter at the data-link layer (a general filter) to provide a protocol independent filter.

Good knowledge of network protocols is required to configure a specific filter appropriately. It is important for the router to operate correctly, therefore, necessary packets must be allowed to pass through the filters. In other words, do not attempt to configure filters on a utilized router unless you understand what you are doing.

The following section describes how to configure the router filter parameters.

Configuring a Filter Set

Under the **Advanced Functions** menu, select and enter the **Filter Configuration** screen:

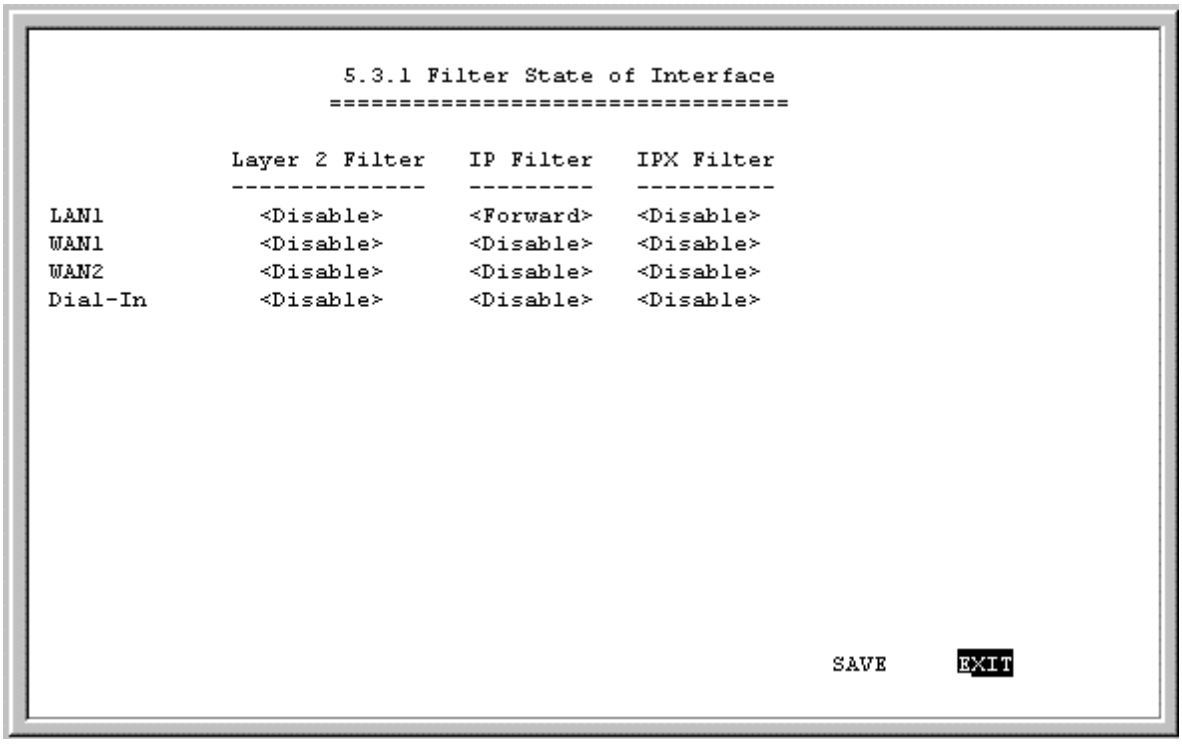


The three submenus are described as follows:

1. **Filter State of Interface** – This is used to choose the default, routing decisions for packets, not meeting the criteria for specific filters.
2. **Layer 2 Filter** – This is a data-link layer (protocol independent) filter. Foreknowledge of the specific protocol, used on the interface (LAN or WANs), is needed to make effective use of this filter.
3. **IP Filter** – This is an IP protocol specific filter, allowing you to, among other things, prohibit specific packets from entering the LAN. Alternatively, you can set up filters that allow certain types of IP packets to enter the LAN.
4. **IPX Filter** – This contains information necessary to set up an IPX filter (DI-1162M only).

Filter State of Interface

The **Filter State of Interface** submenu lets you toggle default, routing decisions, if the packets are not subjected to a filter, routing decision. In other words, a packet, having not met the criteria for a specific filter that was applied to a specific interface, will be subjected to this default, routing decision.

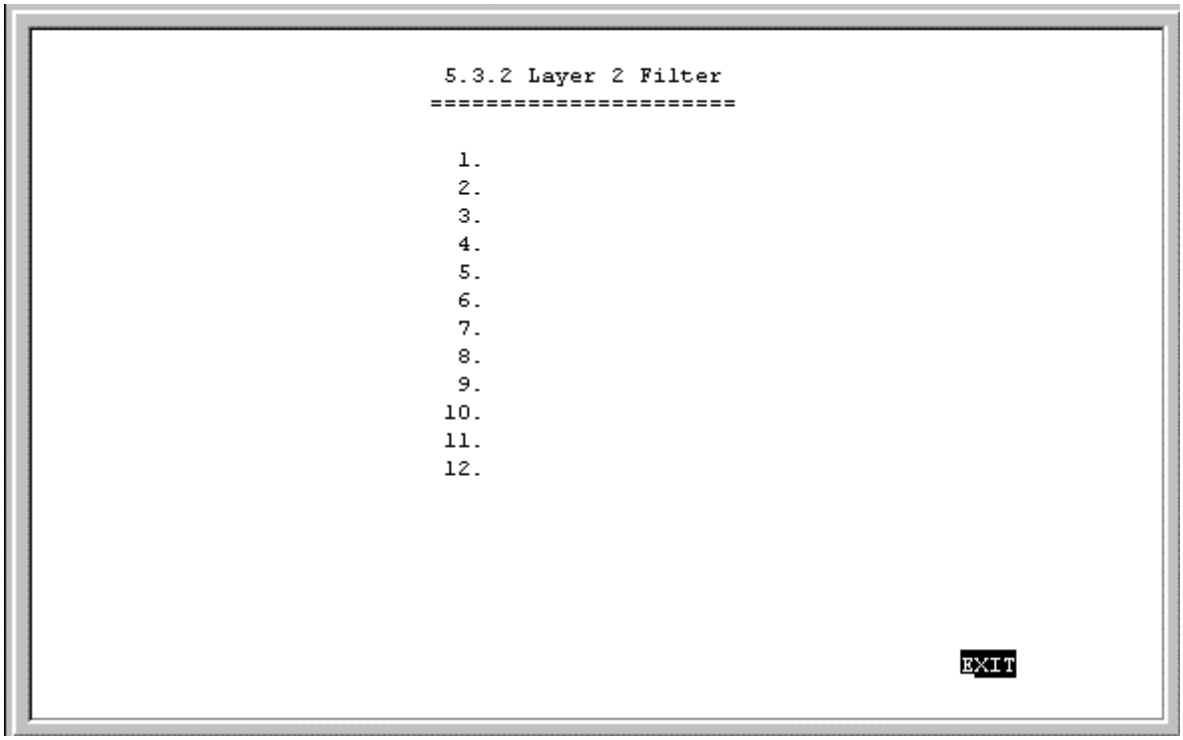


Please note that the IPX Filter column will only appear on DI-1162M models. Each decision on handling packets is described below:

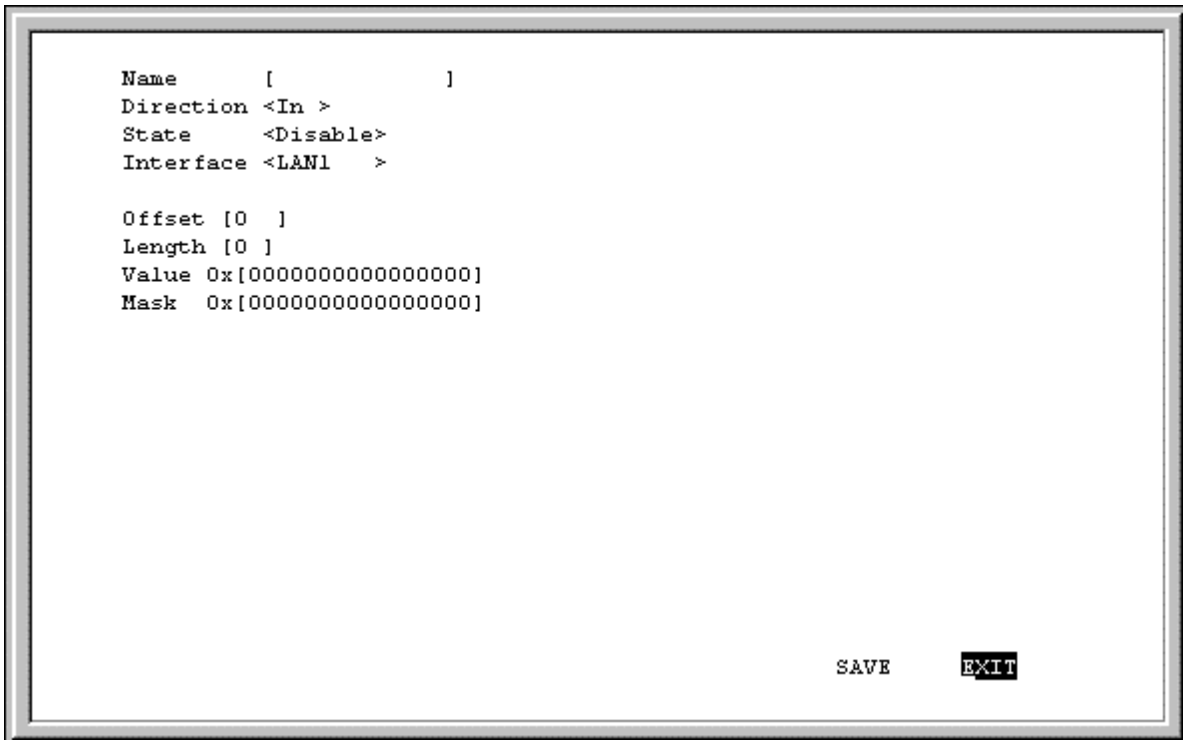
1. **Disable –** This does not apply a default, routing decision.
2. **Forward –** This allows the routing of a packet, even though it has not met the criteria of the corresponding filter.
3. **Drop –** This drops (doesn't allow routing for) a packet that has not met the criteria for the corresponding filter.

Layer 2 Filter

The **Layer 2 Filter** submenu contains a protocol independent (data-link layer) filter. Foreknowledge of the specific protocol used on the interface (LAN or WANs) is needed to make effective use of this filter.



Select an entry from above and hit <Enter>. This screen will be blank if a layer 2 filter has not been configured yet.



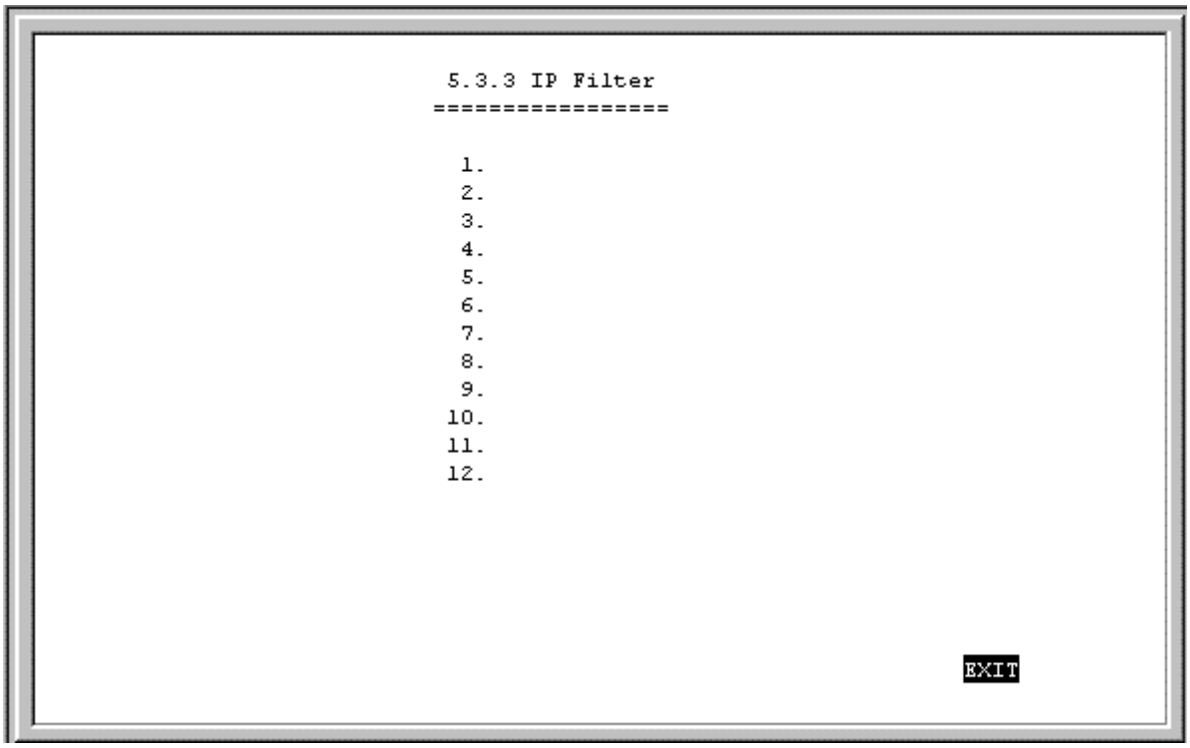
The parameters of a filter are described below:

- **Name –** This is a 12 character (maximum), alphanumeric, user-defined name, used to identify the filter.
- **Direction –** This defines the direction of the frame relative to the Interface parameter. *In* means that packets will be checked when they are received from this interface. *Out* means that packets are checked as they are sent out from this interface.

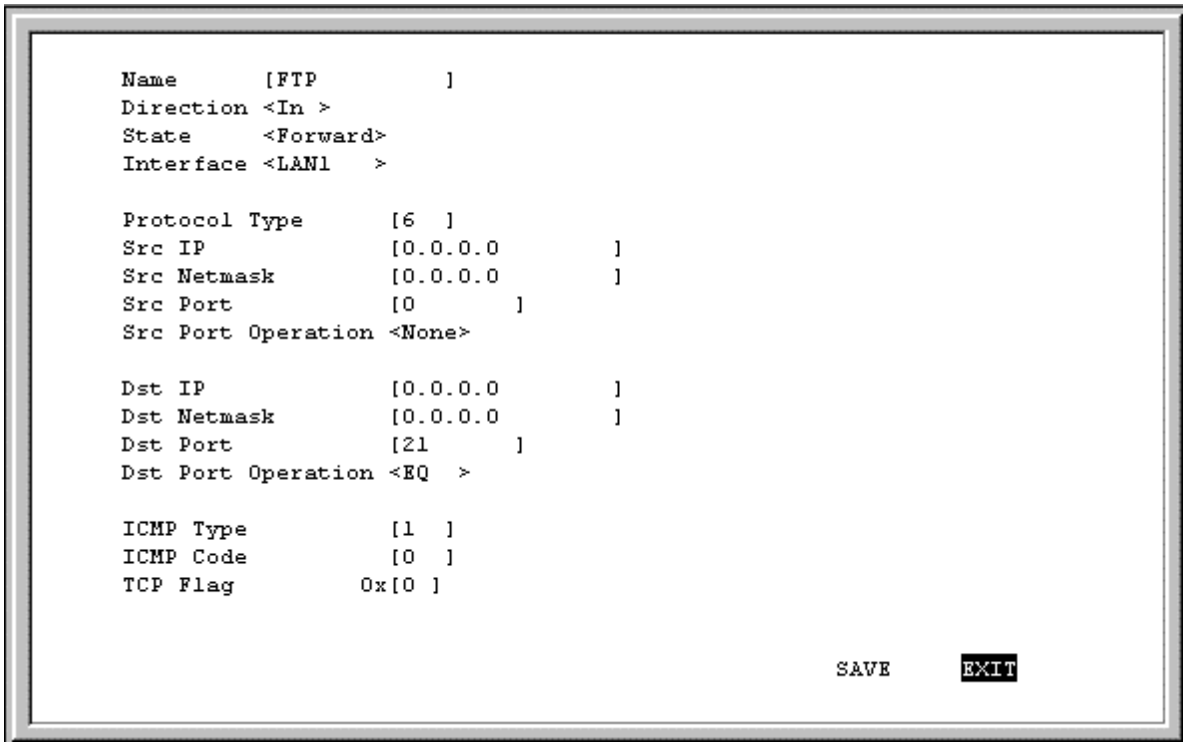
- **State –** This is used to choose the routing decision applied to the frame. The three decisions are described:
  1. *Forward* **–** This allows the routing of the frame, if it has met the criteria of the corresponding filter.
  2. *Drop* – This drops (doesn't allow routing for) a specific frame that has met the criteria of the corresponding filter.
  3. *Disable* – This does not apply the protocol independent filter.
- **Interface –** This applies the filter to a specific interface, either LAN or one of the WANs.
- **Offset –** This defines the reference byte for the Length parameter (described below). The Offset is the number of bytes (octets) from the beginning of the first byte of the frame header, immediately after the preamble. The range of the Offset parameter is from 0 to 255 octets. The first byte in a packet has an offset 0.
- **Length –** This is the number of bytes (octets) from the offset value (the Offset reference byte).
- **Value –** This is a 16 digit, hexadecimal field, defining the actual bit values used to compare with the frame data, at the specified (Offset + Length) position.
- **Mask –** This is a 16 digit, hexadecimal bit mask, used as an operand in the bit-wise AND operation that will be applied to the Value parameter.

IP Filter

The IP Filter is specifically an IP protocols filter, allowing you to, among other things, firewall your LAN, prohibiting specific packets from entering your LAN. It is necessary to have good knowledge of IP protocol before effectively configuring this filter.



Select an entry from above and hit <Enter>. This screen will be blank if an IP filter has not been configured yet.



The IP Filter parameters are described below:

- **Name –** This is a 12 character (maximum), alphanumeric, user-defined name, used to identify the IP filter.
- **Direction –** This defines the direction of the packet relative to the Interface parameter below.
- **State –** This is used to define the routing decision applied to the packet. The three routing decisions are described:

  1. *Forward* **–** This allows the routing of the packet, if it has met the criteria of the corresponding IP filter.
  2. *Drop* – This drops (doesn't allow routing for) a specific packet that has met the criteria of the corresponding IP filter.
  3. *Disable* – This does not apply the IP filter.

- **Interface –** This applies the IP filter to a specific interface, LAN or one of the WANs.
- **Protocol Type –** This is a protocol identifier, as assigned by the Internet Assigned Numbers Authority (IANA). The values of this identifier are described in RFC-1700. This router supports the following:

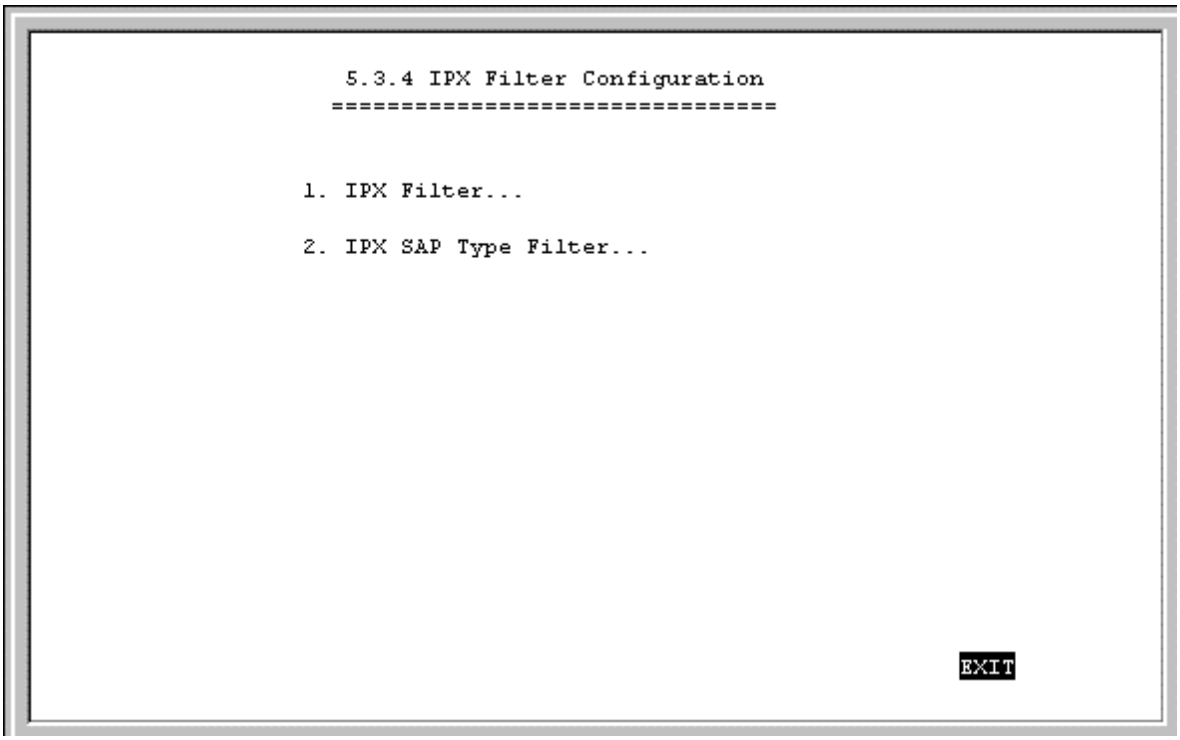
  1. *protocol type* = 1, this is Internet Control Message (ICMP), defined in RFC 792.
  2. *protocol type* = 6, this is Transmission Control (TCP), defined in RFC 793.
  3. *protocol type* = 17, this is User Datagram (UDP), defined in RFC 798.
  4. *protocol type* = 0, this includes ICMP (1), TCP (6), and UDP (17).

- **Src IP –** This is the source address in the IP header of this packet.
- **Src Netmask –** This mask is bit-wise AND'd with the source IP address, and compared to the IP address of the incoming interface, for which the packet arrived.
- **Src Port –** This is the source port in the TCP or UDP header of the packet.
- **Src Port Operation –** Select a source port operation: *None*, *EQ*, *GT*, or *LT*.
- **Dst IP –** This is the destination address in the IP header of the packet.

- **Dst Netmask –** This mask is bit-wise AND'd with the destination IP address, and compared to the IP address of the outgoing interfaces.
- **Dst Port –** This is the destination port, in the TCP or UDP header, of the packet.
- **Dst Port Operation –** This comparison operation is applied to the destination port (the Dst Port parameter) value, of the TCP or UDP header.
- **ICMP Type –** This is the type field, in the ICMP header, used to identify a particular ICMP message.
- **ICMP Code –** This is the code field, in the ICMP header, used to further specify the ICMP type.
- **TCP Flag –** This is a decimal number, representing the six flag bits in the TCP header.

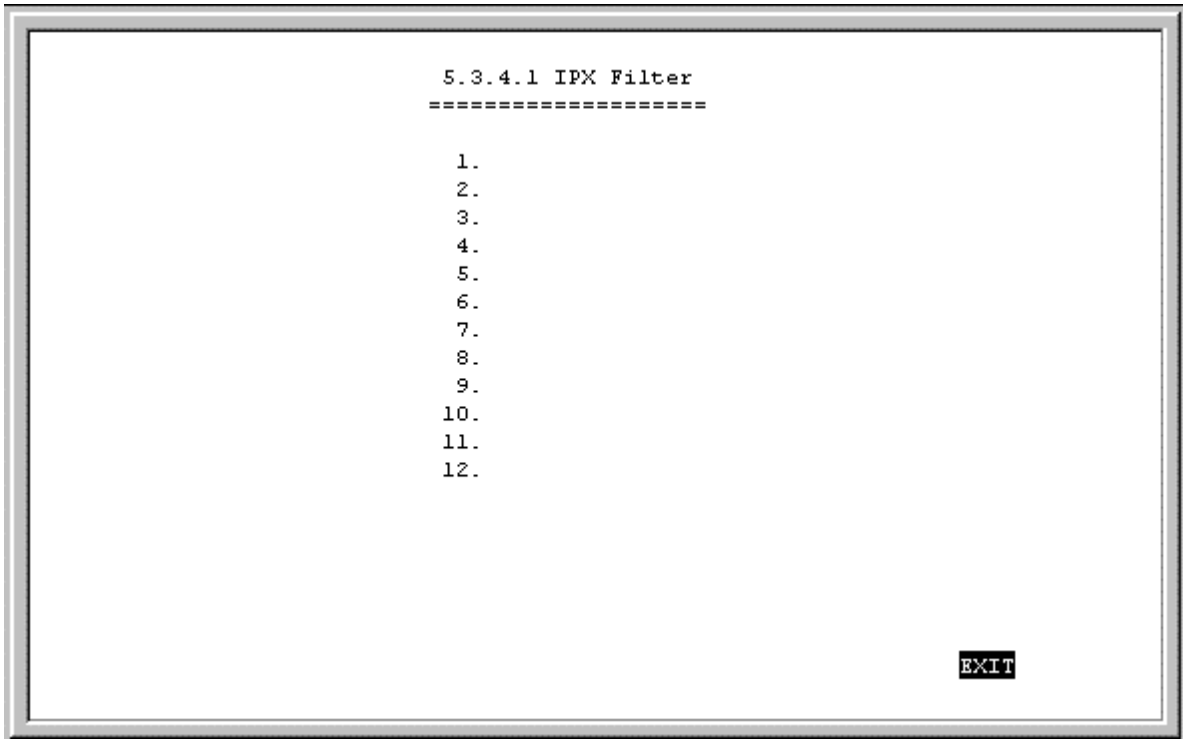
IPX Filter Configuration

Highlight the desired entry on the **IPX Filter Configuration** screen and then press <Enter> to access the following screen

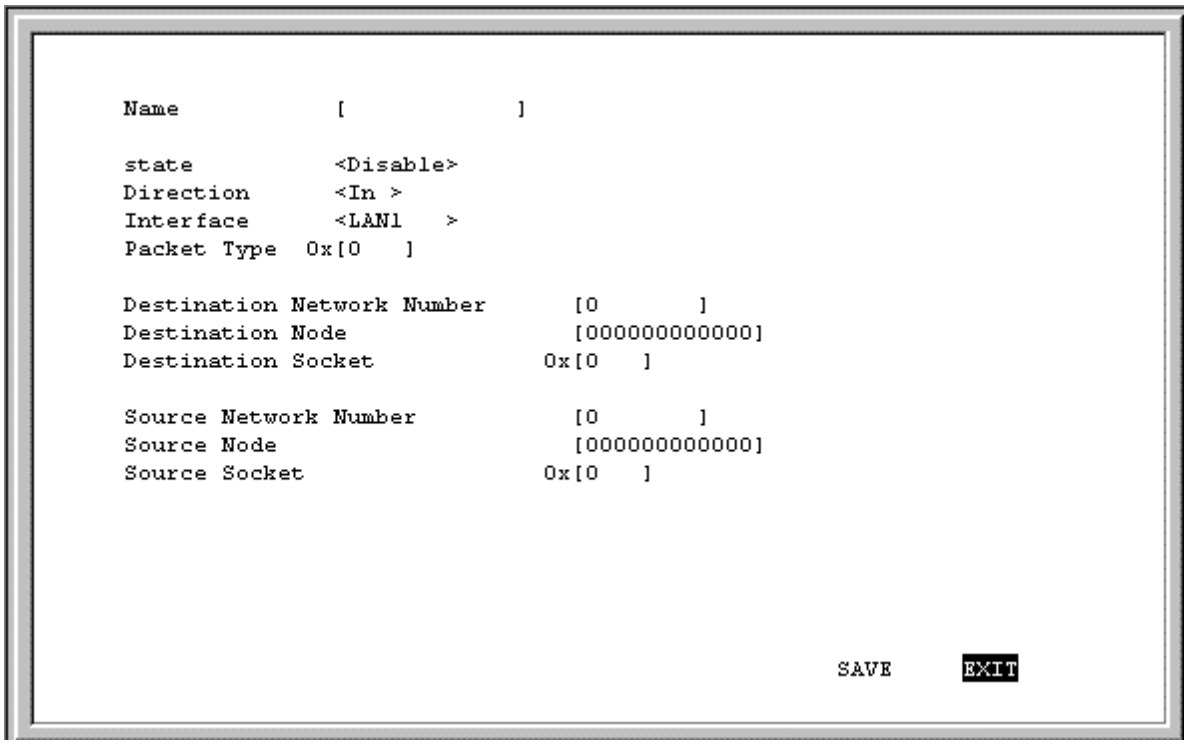


IPX Filter

The IPX Filter is specifically an IPX protocols filter, allowing you to, among other things, firewall your network, prohibiting specific packets from entering or going out from your network. It is necessary to have knowledge of IPX protocol before effectively configuring this filter.



Select an entry from above and hit <Enter>. This screen will be blank if an IPX filter has not been configured yet.



The IPX Filter parameters are described below:

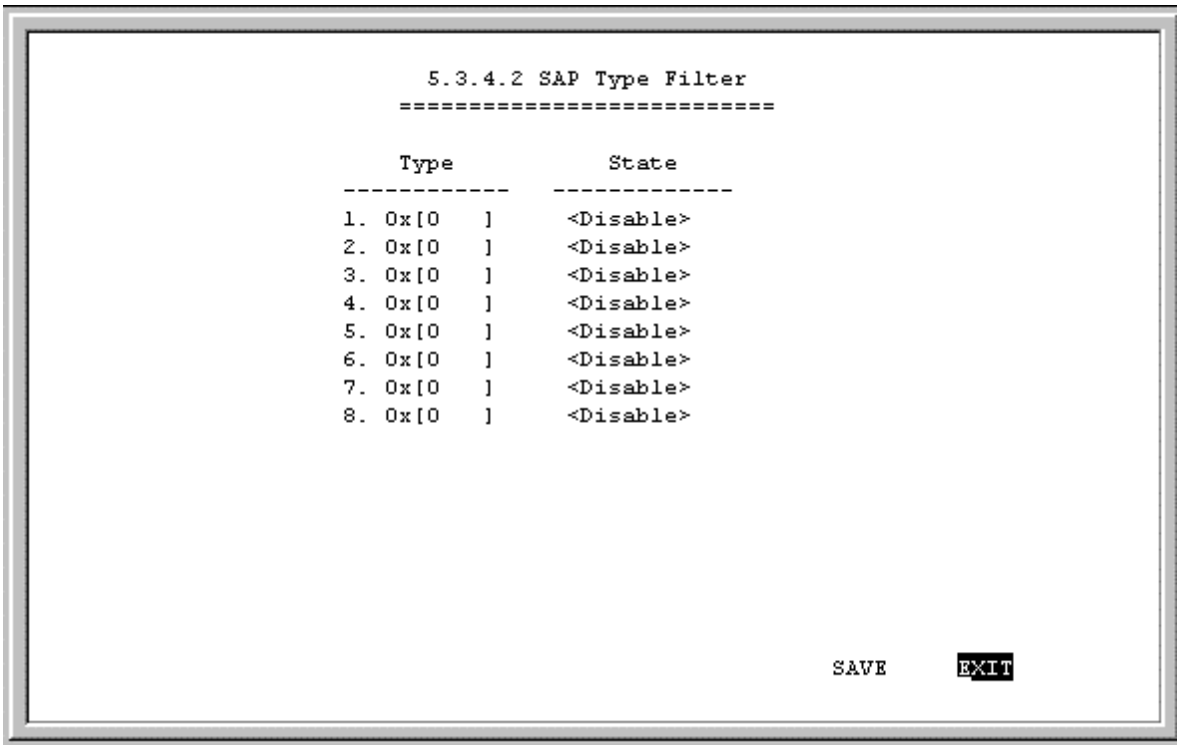
- **Name –** This is a 12 character (maximum), alphanumeric, user-defined name, used to identify the IPX filter.
- **State –** This is used to define the routing decision applied to the packet. The three routing decisions are described:

    1. *Forward* **–** This allows the routing of the packet, if it has met the criteria of the corresponding IPX filter.

2. *Drop* – This drops (doesn't allow routing for) a specific packet that has met the criteria of the corresponding IPX filter.
3. *Disable* – This does not apply the IPX filter.

- **Direction –** This defines the direction of the packet relative to the Interface parameter below.
- **Interface –** This applies the filter to a specific interface, LAN or one of the WANs.
- **Packet Type –** Defined by Novell for special services.
- **Destination Network Number –** This is the IPX network number of each device in a subnet created by a user.
- **Destination Node –** This field contains the address of the node on which the router resides. This is usually the MAC address of this device.
- **Destination Socket –** This field contains the socket number on which the router will receive service requests.
- **Source Network Number –** This is the IPX network number of the network where the packet originated.
- **Source Node –** This field contains the MAC address of the originating machine.
- **Source Socket –** This field contains a specific socket number which IPX packets can be discarded.

IPX SAP Type Filter



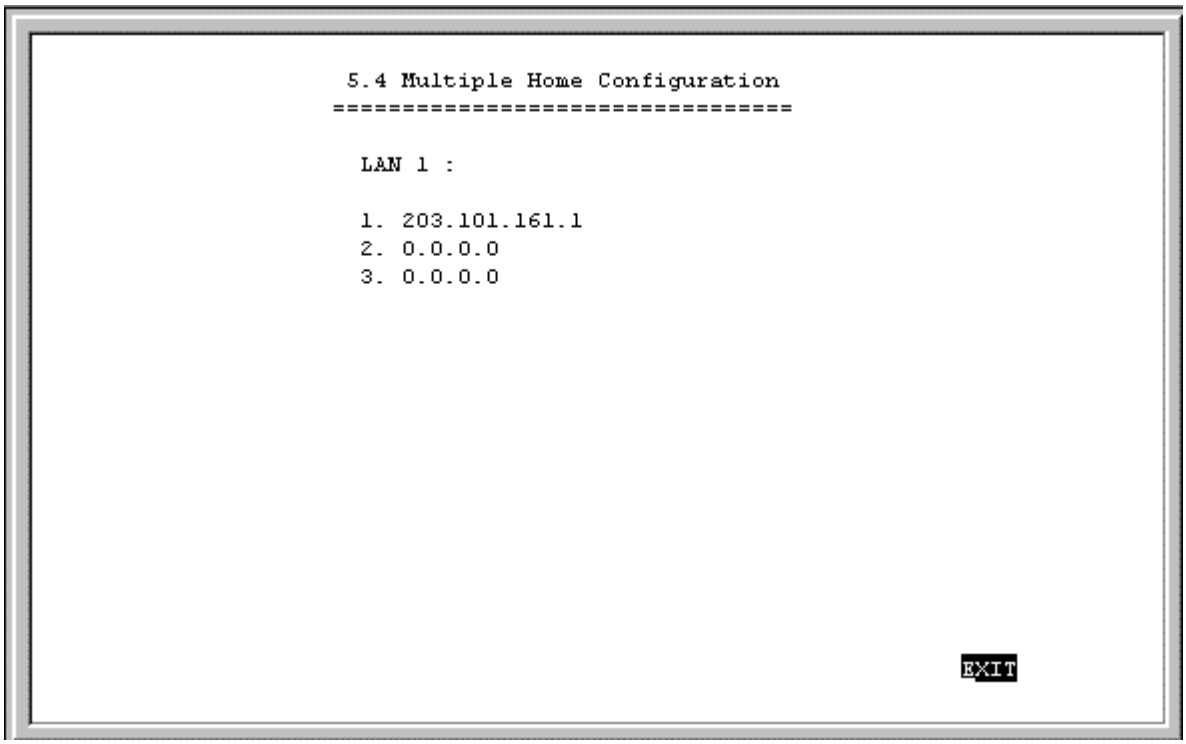
The SAP type filter parameters are described below:

- **Type –** This is used to remove selected incoming service access information before it is entered into the service information table for the router.
- **State –** Toggle to *Enable* or *Disable* this filter.

Multiple Home Configuration

Besides the IP address assigned to the LAN interface in the **Network Configuration** menu, each LAN may have up to 3 additional IP interfaces. These additional IP interfaces are referred to as MIP's and MIP1 to MIP3 are

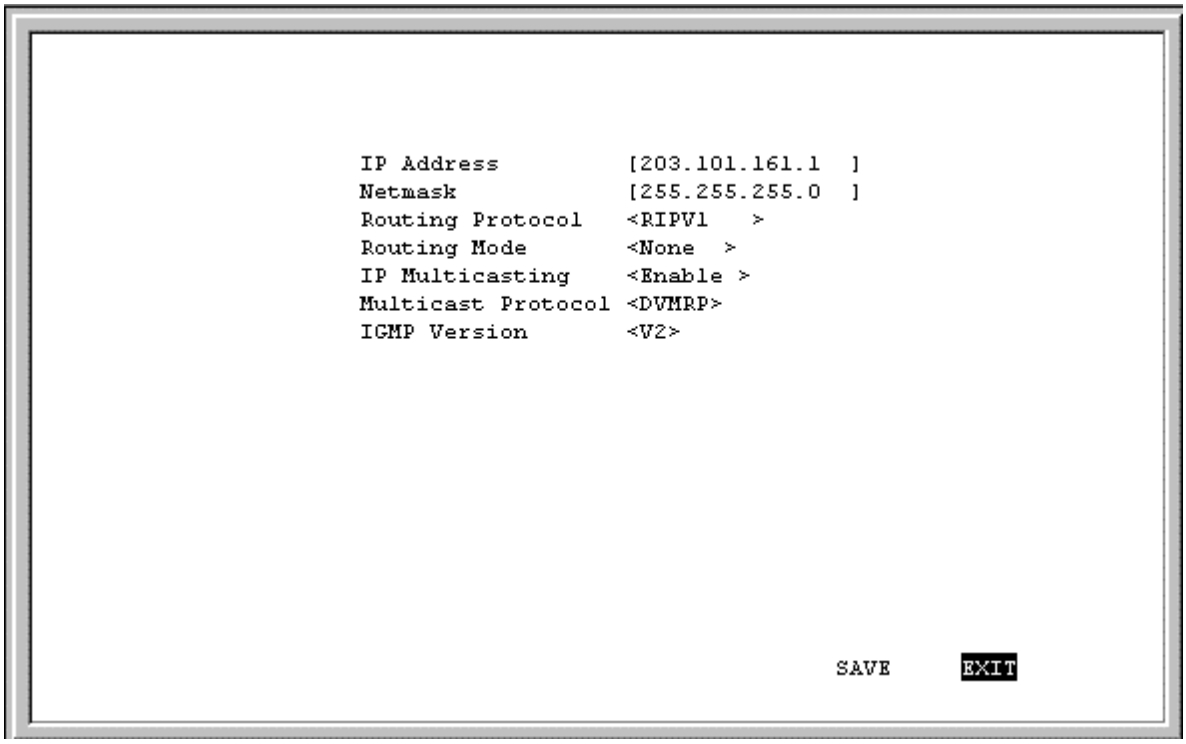
reserved for LAN1 and MIP4 to MIP6 are reserved for LAN2 (if present). This type of configuration is known as a multiple home configuration.



Multiple Home can be demonstrated by this example:

A company has 625 users (computers) all connected to one physical network using Ethernet. However, the company only has one Class C IP network address, 202.100.160.0. This network address will only support 254 users. To solve the shortage of IP address problem and to plan for future growth, the company applies for and receives two more Class C IP network addresses, 203.101.161.0 and 204.102.162.0. This gives the company a total of 254 x 3 = 762 IP Addresses, which it assigns to the computer users, with a few left over for future needs. Due to the nature of IP networks, however, the users in one IP network domain (202.100.160.0, for example) cannot communicate with users on a different IP domain (203.101.161.0). Multiple home solves this problem. When you register the additional IP network addresses in the Multiple Home Configuration menu on the router, the router will route data between the three IP networks using the single LAN.

In this router, multiple home configurations only apply to the LAN interface.



The parameters are described below:

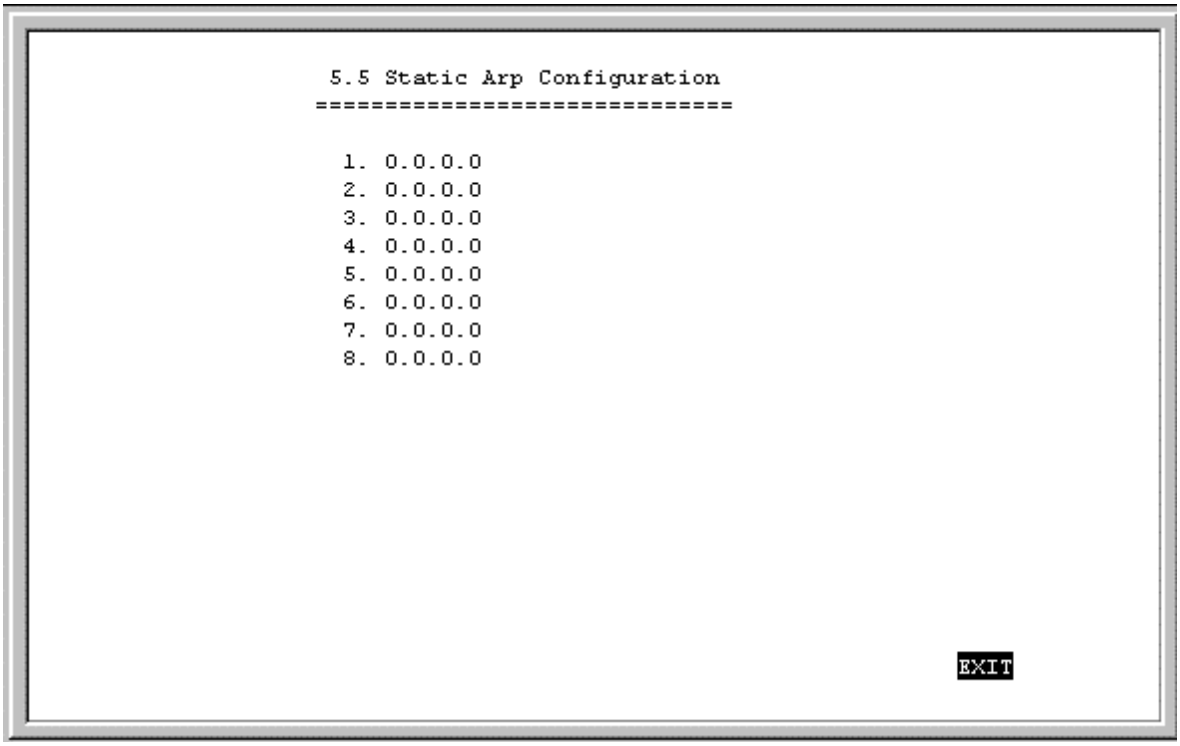
- **IP Address** – This is a network IP address, access point, to a separate, physical network, on the LAN.
- **Routing Protocol** – This is the same as in the *Network Configuration* section. Keep in mind that these exchanges are made with adjacent routers on the LAN, if present.
- **IP Multicasting** – This enables/disables IP multicasting on the IP network you are defining.

All other parameters (Netmask, Routing Mode, Multicast Protocol and IGMP Version) are identical to those in the *Network Configuration* section.

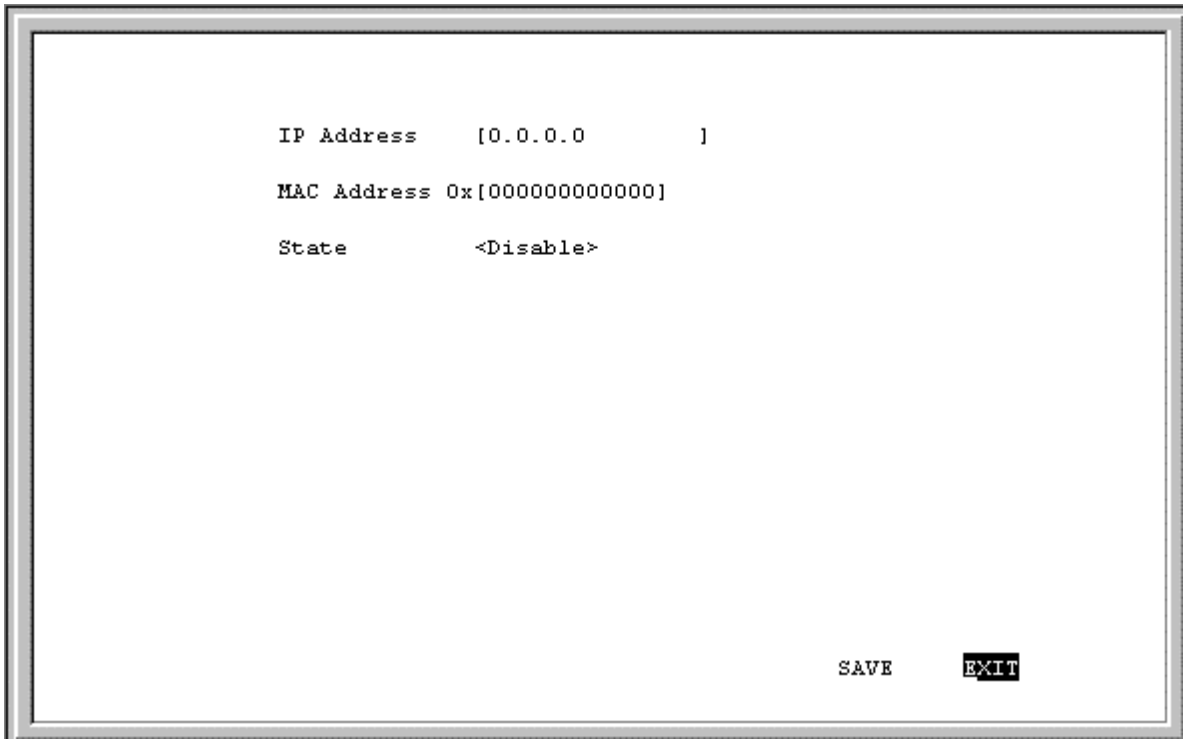
Static ARP

This special function is intended to speed up the process of finding a host's Ethernet (MAC) address from its network address, and provides a special condition – any other host acting as an impostor by using the same IP address as the legitimate host, will be ignored by this router.

Basically, when a packet comes into the router from a WAN port and is destined for a host on the LAN, the router will use information defined here to immediately send the packet to the host rather than send out an ARP request to find the host’s MAC address.



Select an entry from above and hit <Enter>. This screen will be blank if a static ARP entry has not been configured yet.



The parameters are described as follows:

- **IP Address –** This is the IP address that causes the router to reply with the MAC Address upon receiving an ARP request.
- **MAC Address –** This is the physical address, of the host, that is the authorized owner of the IP address.

- **State –** This toggles *Enable* and *Disable*.

NAT Configuration

Network Address Translation (NAT) is a routing protocol that allows your network to become a *private* network that is isolated from, yet connected to the Internet. It does this by changing the IP address of packets from a *global* IP address usable on the Internet to a *local* IP address usable on your private network (but not on the Internet) and vice-versa.

NAT has two major benefits. First, NAT allows many users to access the Internet using a small number or even a single global IP address. This can greatly reduce the costs associated with Internet access and also helps alleviate the current shortage of Internet IP addresses. Secondly, the NAT process creates a firewall which hides your local network from Internet users, providing a degree of security to your Internet connection.

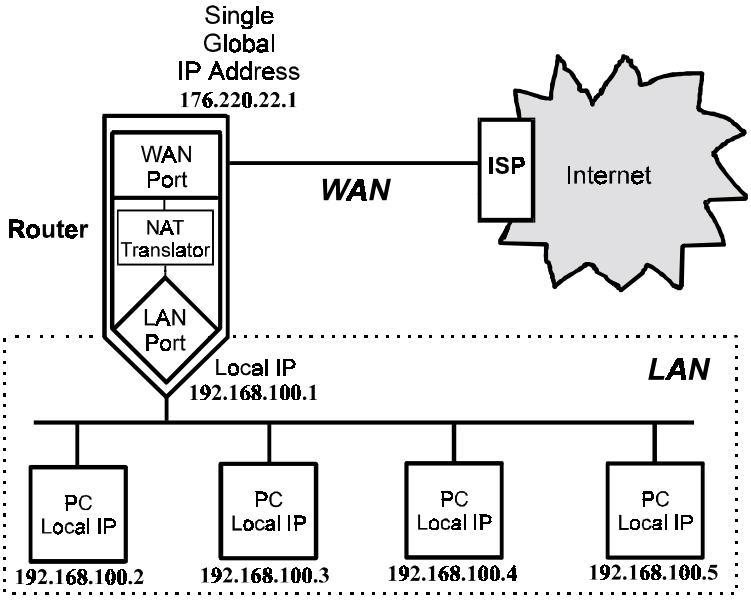
To be successfully implemented, NAT should be used only when the majority of network traffic remains on the local network. In cases where a large percentage of network traffic is destined for the Internet, NAT can adversely affect the speed and performance of your Internet connection. Also, your network servers such as ftp servers, web servers or mail servers will probably need to be assigned *static* NAT IP addresses so their IP addresses remain consistent. This issue will be further discussed later.

Network Address Port Translation (NAPT) is a subset of NAT where many local IP addresses and their TCP/UDP port numbers are translated to a single global IP address and it's TCP/UDP port number. In this document, the term NAT will refer to both NAT and NAPT unless otherwise stated.

NAT can work in conjunction with DHCP. Thus, if both are enabled and properly configured, the DHCP server in the DI-1162/DI-1162M will assign local IP addresses to computers on your network.

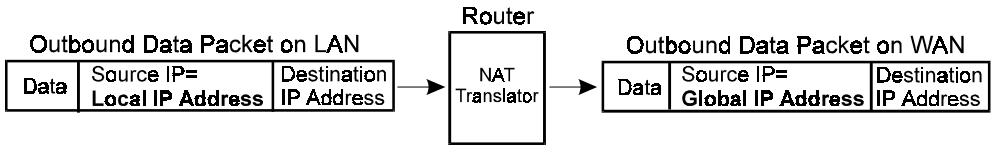
How NAT Works

In the most common NAT configuration, your network uses local IP addresses that are not valid on the Internet. Internet (global) IP addresses are unique, with no two devices have the same IP address. The local IP addresses can be freely assigned to computers on your network by your network administrator (within guidelines defined later in this chapter and in "*Appendix C, IP Concepts"*). This can be done manually or by using DHCP. The WAN port on the router is assigned a globally unique IP Address that IS valid on the Internet, since it will be sending and receiving data directly to the Internet and is therefore part of it. Please study the example diagram below carefully.



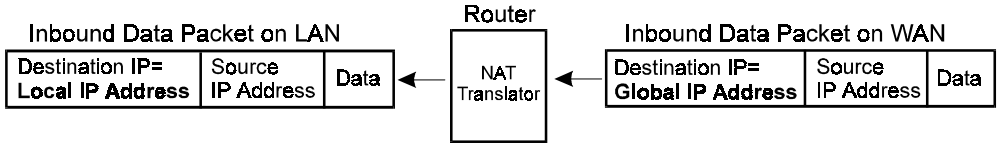
Please note that in the above diagram, the Gateway IP address settings for the local PC's needs to be set to 192.168.100.1, the LAN IP address of the router.

NAT manipulates the IP addresses in packet headers on a one-to-one basis. An outgoing data packet (a packet originating from a computer on the local LAN and destined for a computer outside the private network) will have its IP address translated as shown below.



In the Outgoing Data Packet above, the *Source IP address* is the IP address that is translated by NAT. The *Destination IP Address* is the IP address of a computer outside the private network, on the Internet for example. And the *Data* portion of the packet is the information payload borne by the packet, for instance a request to view a web page.

The router logs the changes made to the IP header in its NAT table. The NAT table enables the router to send replies back to the local computer as shown below.



In the Inbound Data Packet above, the *Destination IP Address* is the IP address that is translated by NAT. The *Source IP Address* is the IP address of a computer outside the private network. And the *Data* portion of the packet is the information payload borne by the packet, in this case, web page contents.

The actual information in the NAT table depends whether the router is implementing NAT or NAPT.

NAT

This section discusses the NAT protocol as opposed to NAPT which is discussed in the next section.

NAT is the initial protocol set forth by RFC 1631 and provides a means in which private networks can communicate with the Internet by using a small number of IP addresses. In our discussion, we will use the example IP addresses listed in the table below and the network diagram shown at the beginning of this section.

Global IP Addresses (for use with NAT)	Local IP Addresses (assigned to computers on the local network)
200.100.50.1	192.168.100.1
200.100.50.2	192.168.100.2
200.100.50.3	192.168.100.3
200.100.50.4	192.168.100.4
200.100.50.5	192.168.100.5
	192.168.100.6
	192.168.100.7
	192.168.100.8
	192.168.100.9
	192.168.100.10

Please note that in the above table there are 9 users on the local network using 5 global IP addresses to access the Internet.

When a packet on the local network arrives at the router and needs to be sent to the Internet, NAT will change the source IP address (for example 192.169.100.2) to a global address (200.100.50.1, for example). If this packet generates a reply (as for example, a request to view a web page will), NAT will change the destination IP address on the reply packet back to the local IP address for delivery to the machine on the local (stub) network.

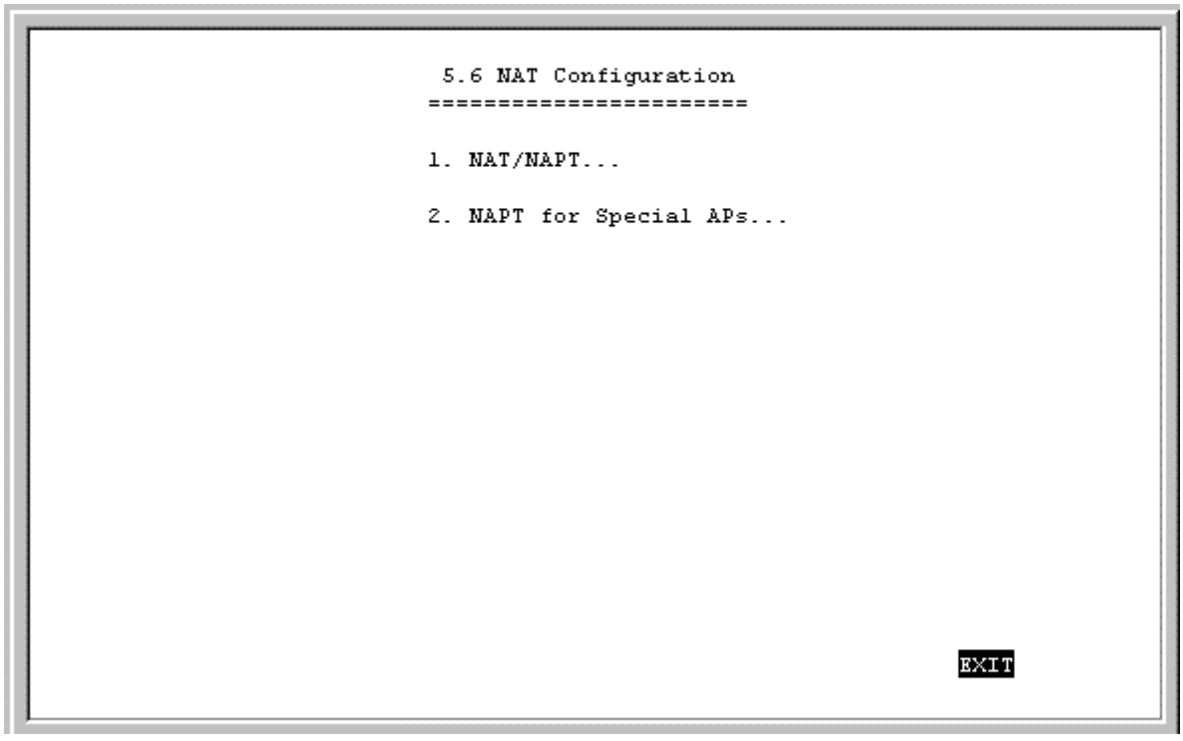
The difference between static and dynamic NAT is that once the five global addresses are assigned when using static NAT, they will never change. The only way to change them is by using the console program to manually reassign them. When using dynamic NAT, the router will map a local IP address to a global IP address whenever a request is made. Since there are only 5 global IP addresses in the example above, there can only be 5 mappings at any one time. In other words, much like static NAT, only 5 local machines can access the Internet at any one time. However, contrary to static NAT, the router will discard the mapping between the global and local IP addresses after a certain length of time (which is quite long so rarely happens), or after the session is finished (an example of a session is when requesting a web page, the entire page has completed downloading). The most common implementation of NAT is to define a range of dynamic addresses to be used by hosts, but assign static addresses to your servers if you wish for them to be accessible from outside your network.

Setting Local IP Addresses

When implementing NAT and thus creating a private network that is isolated from the Internet, you can assign any IP addresses to host computers without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP Addresses specifically for private networks:

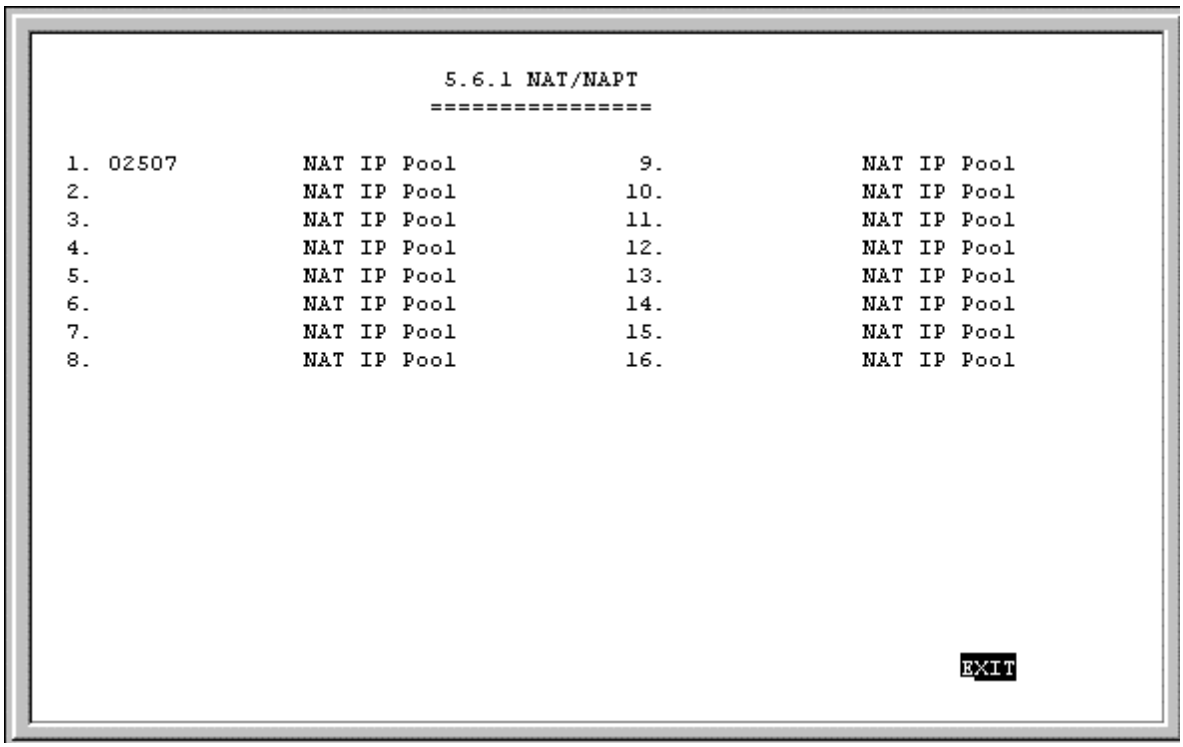
Class	Beginning Address	Ending Address
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

It is recommended that you choose local IP addresses for use with NAT from the private network IP addresses in the above list. 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*.



Configure NAT/NAPT

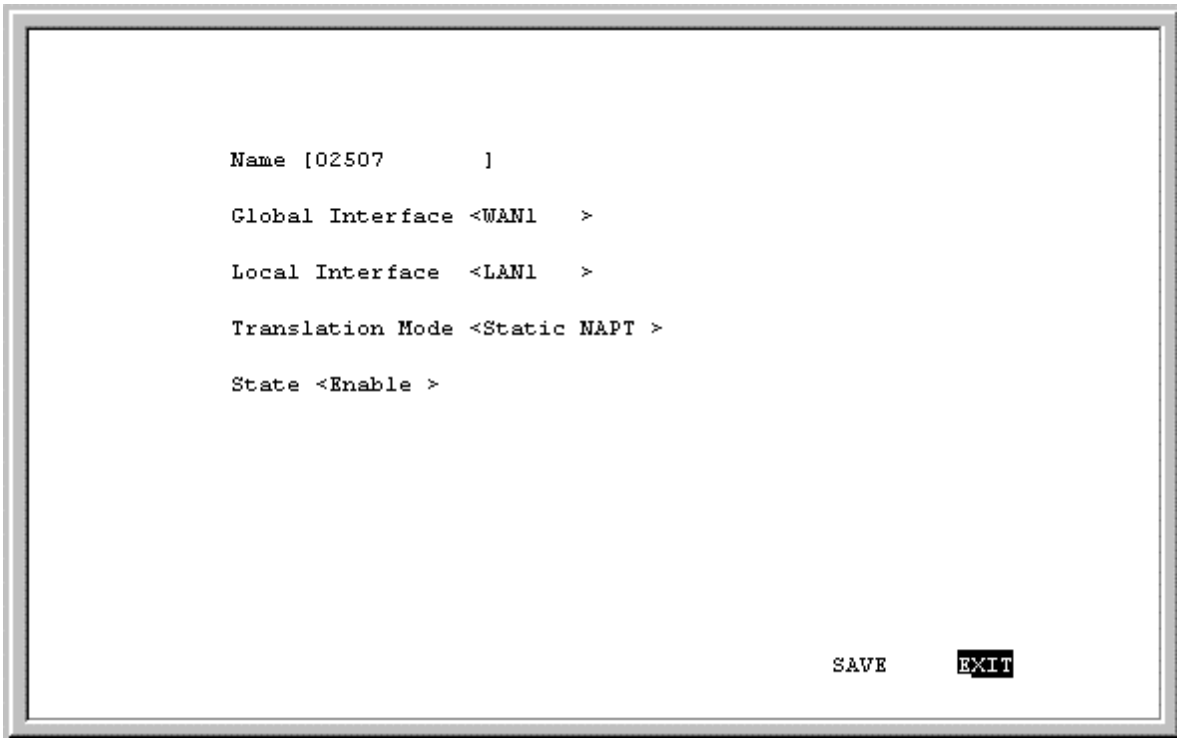
The first screen shows the complete NAT table that is defined by the network manager:



For any NAT entry, you must configure two different screens. The first one is accessible by positioning the cursor over the name field and hitting <Enter> (in the window shown above, this corresponds to the field '02507'). After configuring the NAT options in the Name field, you must save the changes, exit, and position the cursor over the NAT IP Pool to configure variables there.

Name Field Configuration Screen

The configuration screen for the name field appears as follows:



The parameters are described as follows:

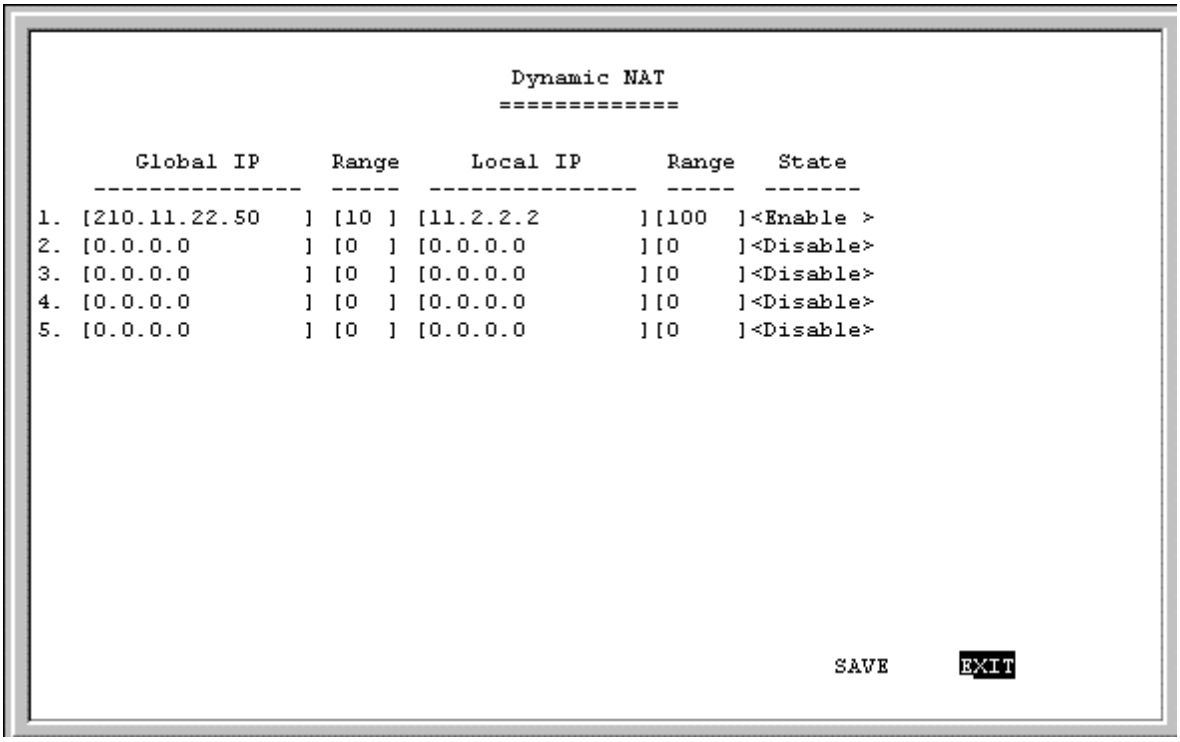
- **Name –** This is a 12 character, alphanumeric, user-defined name, used to identify the network address translation.
- **Global Interface –** This is the interface corresponding to the Global IP and Range parameters, in the NAT table, to form unique IP address[es], known to the outside (regional or Internet) routers, on this interface.
- **Local Interface –** This is the interface corresponding to the Local IP and Range parameters, in the NAT table, to form local IP address[es], known only to this interface and the network within.
- **Translation Mode –** This toggles choices of four types of NATs:
  - *Static NAT* **–** Maps one global IP address to one local IP address. After all global IP addresses are assigned, they will remain static. This option may be necessary for email, web, ftp servers, etc. where static IP addresses are essential for operation.
  - *Dynamic NAT* **–** Maps one global IP address to one local IP address. Global IP addresses will be dynamically reassigned to different local IP addresses if not currently being used. This allows a larger number of users to use a small number of IP addresses.
  - *Static NAPT* **–** One to one mapping of UDP/TCP port numbers to let packets with specific UDP/TCP port numbers enter the local IP domain. The NAPT map table will not age. This option may be necessary for email, web, ftp servers, etc. where static port numbers are essential for operation. Setting the global port number to 0 opens port numbers 1024 to 65535 for the designated local IP address, creating a visible computer. This allows a computer to be freely accessed by other computers on the Internet, which is necessary for some applications to function correctly when using NAPT, including Microsoft NetMeeting, CUSeeMe, etc.
  - *Dynamic NAPT* **-** One to one mapping of UDP/TCP port numbers. The NAPT map table will age. This option allows many hosts to use a single, globally unique IP address, and thus will only be used on outbound packets.
- **State –** Enables/disables this NAT configuration.

NAT IP Pool Configuration Screen

Now you must select, enter, and configure the NAT IP Pool from the **NAT Configuration** submenu, shown below.

Dynamic NAT

This screen (below) is how the NAT IP Pool appears, if *Dynamic NAT* was chosen for the Translation Mode parameter. Each entry, in this configuration, can be used to map multiple, contiguous global addresses and local addresses to each other.

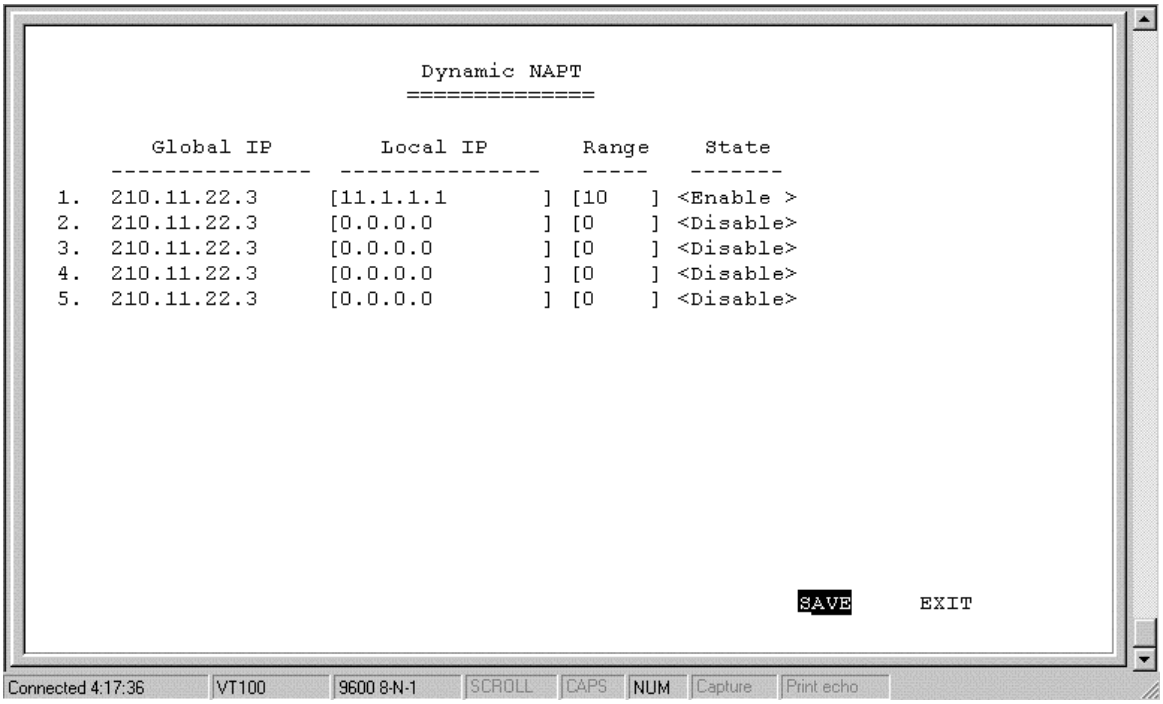


The parameters are described below:

- **Global IP –** An IP Address that is globally unique and valid on the Internet. It is the base, global address for the global addresses that will be recognized by the interface in the Global Interface parameter.
- **Range –** This is the range of contiguous, global addresses above (and including) the base Global IP.
- **Local IP –** An IP Address that is only used in the stub domain since it is not unique. It is the base, local address for the local addresses that will be recognized by the interface in the Local Interface parameter.
- **Range –** This is the range of contiguous local addresses above (and including) the base Local IP.
- **State –** This toggles *Enable* or *Disable* for this NAT entry.

Dynamic NAPT

This screen (below) is how the NAT IP Pool appears, if *Dynamic NAPT* was chosen for the Translation Mode parameter. Each entry, in this configuration, can be used to map a single global address and multiple, contiguous local addresses to each other.

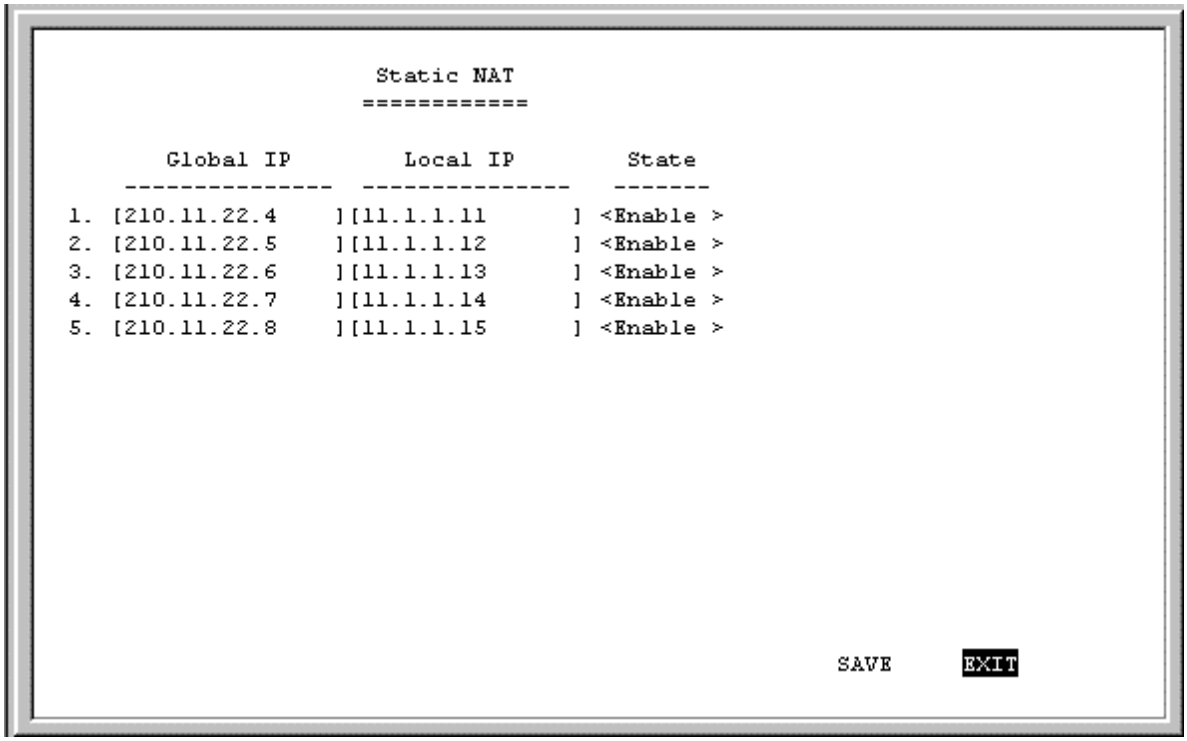


All of the parameters are the same as in Dynamic NAT, except the Global IP is a solitary, global address.

- **Global IP** – this is a single, globally unique IP Address of the global interface (the interface to which it is assigned, in this case, one of the WAN interfaces) that is valid on the Internet.

Static NAT

This screen (below) is how the NAT IP Pool appears, if *Static NAT* was chosen for the Translation Mode parameter. Each entry in this configuration is used to map a single global IP address a single local IP address.



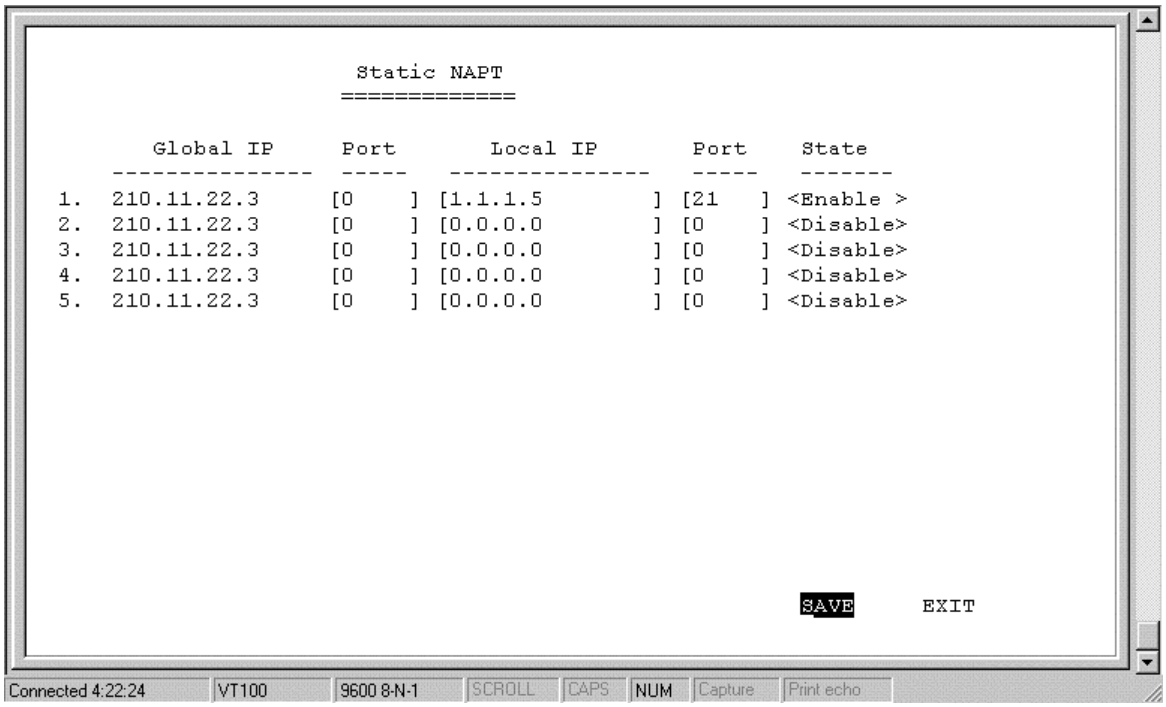
The parameters are described as follows:

- **Global IP** – This is a single, global IP Address that is valid on the Internet, or on the same subnet of the global interface.

- **Local IP** – This is a single, local IP Address that is not valid on the Internet.

Static NAPT

This screen (below) is how the *NAT IP Pool* appears, if Static NAPT was chosen for the *Translation Mode* parameter. Each entry in this configuration can be used to map a global address and port to a local address and port. Notice that the global address will be the external IP address of the global interface.



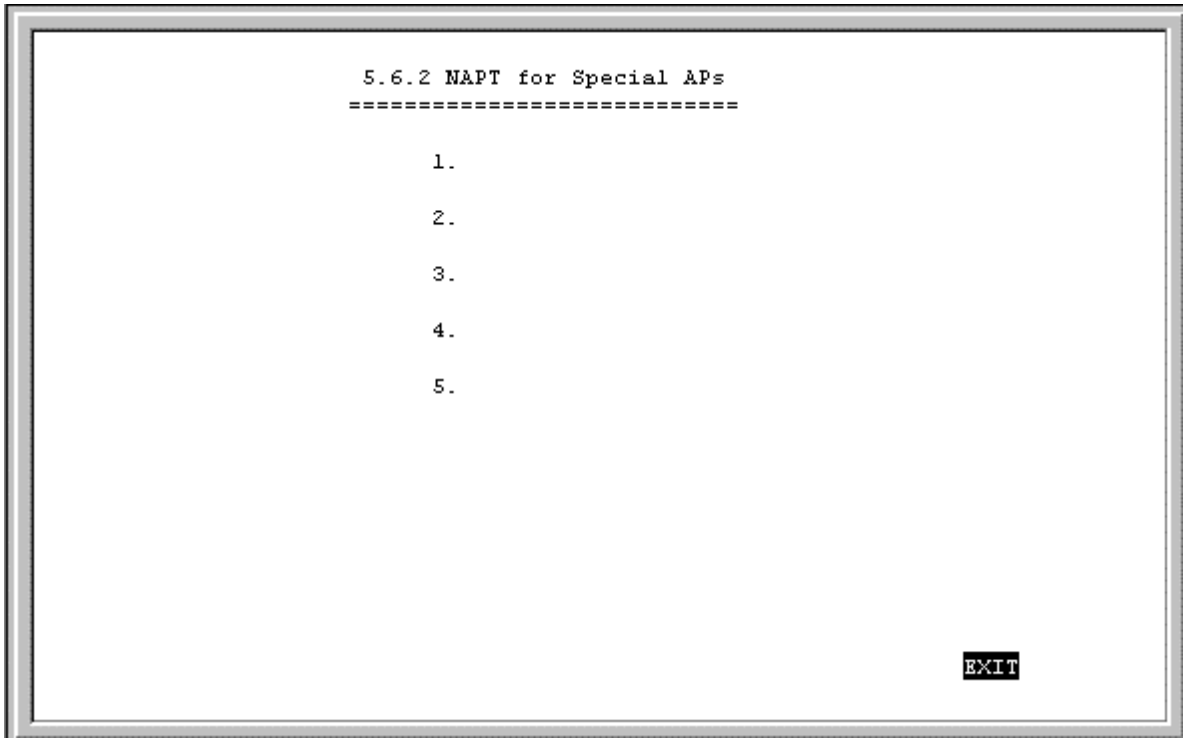
- **Port –** This is a destination port number, used by TCP and UDP, to de-multiplex the incoming IP packet.

In the above example, incoming packets with the global destination IP Address (211.11.22.2) and global destination TCP/UDP port (21) will be translated to a packet with the local destination IP Address (1.1.1.5) and local TCP/UDP port (21).

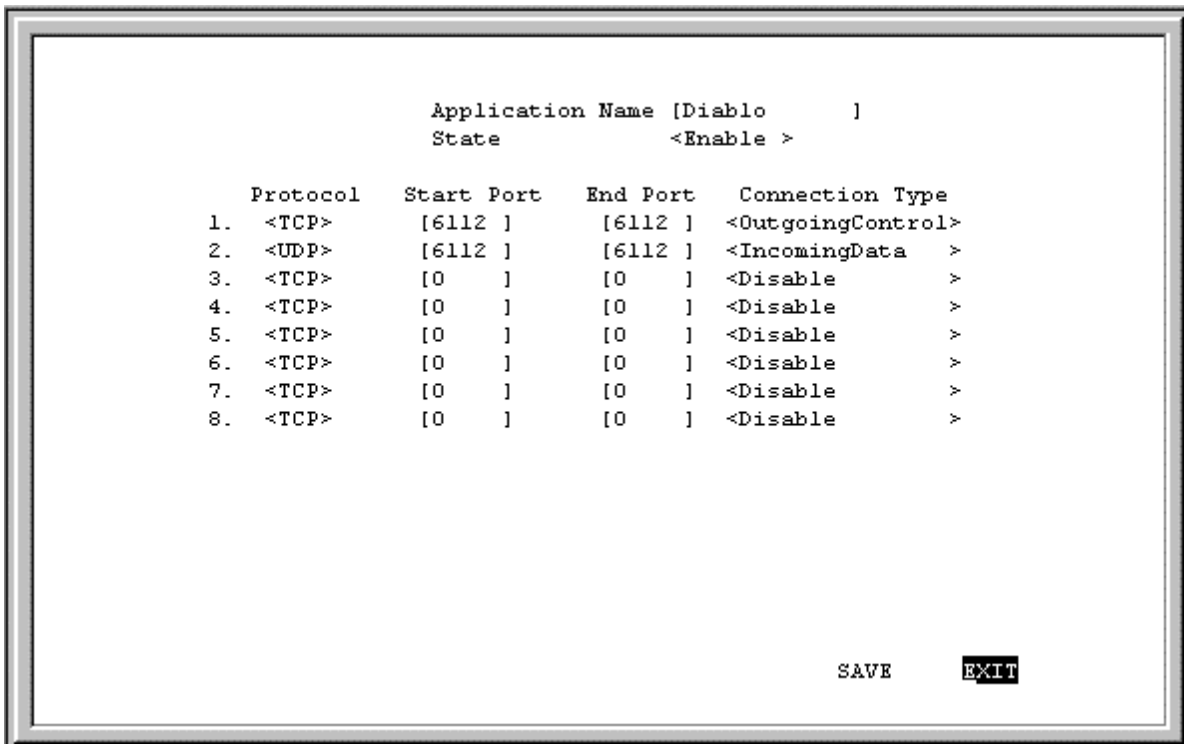
Port 21 is assigned to FTP servers. Please see *"Appendix D"* for more commonly assigned port numbers, or RFC 1700 for a more complete list.

NAPT for Special Aps

Some applications programs that are used over the Internet such as Microsoft NetMeeting, Diablo, and CU See Me send information to a certain port number or within a specified range of port numbers. The exact port number used is specific to the application. However, if you find that you are having trouble using an application over the Internet and you are using NAPT, you may need to exempt certain port numbers from the NAPT port translation process. Please refer to the user guide for the program to find out whether it transmits and receives data only through specified IP port numbers. In order for these programs to work with NAPT, the IP port numbers required by these applications must be entered in the Configure NAPT for Special APs screen shown below.



In the above window, position the cursor on any of the numbered name fields and press <Enter>. This will take you to the NAPT configuration screen for special applications shown below.



The fields in the above window are described as follows:

- **Protocol** – *UDP* or *TCP*. This field designates the type of packets that will be acted on.

- **Start Port** – Some applications can only send data over a certain range of port numbers. Thus, all port numbers in the specified range must be exempt from the NAPT port translation process. This field defines the beginning range of the port numbers to be exempted from the NAPT port translation process.

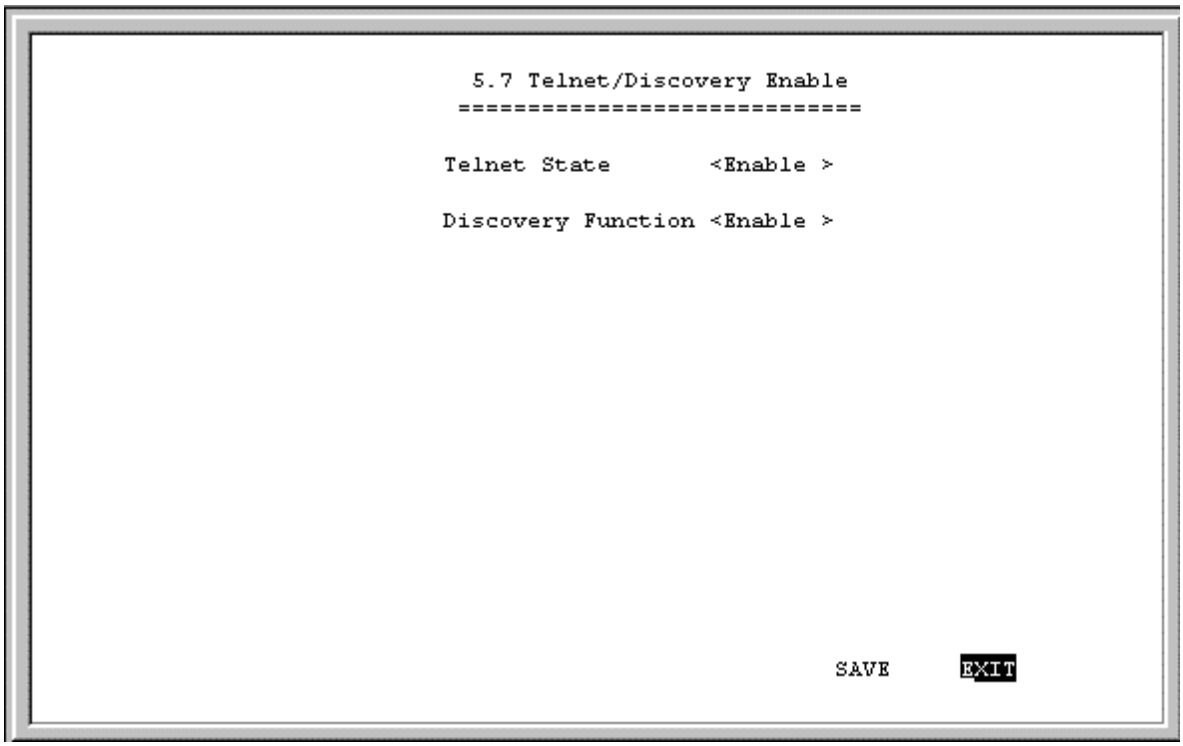
- **End Port** – This field defines the last port number in the range of numbers excluded from the NAPT process (see Start Port above).

- **Connection Type** – *OutgoingControl* or *IncomingData*. The user must initially run the special application and send a request to the application server on the Internet. This outgoing request to join a Netmeeting session, for example, is used to trigger the exemption process for the incoming data.

In the example for the game Diablo shown in the above screen, if a packet is sent out on the TCP port number 6112 (a request by a local user to a Diablo server on the Internet to join a group game), all incoming packets on the UDP port 6112 (game data) will not be translated by NAPT.

Please keep in mind that the user will always initiate use of the special application. Thus, the first entry should always have the Connection Type of Outgoing Control. Also, since the defined port number or range of port numbers will be mapped to the user who triggered the outgoing control, all incoming data will be sent to that user. Consequently, only one user can use the special application at a time.

Telnet/Discovery Enable



The fields in the above window are described as follows:

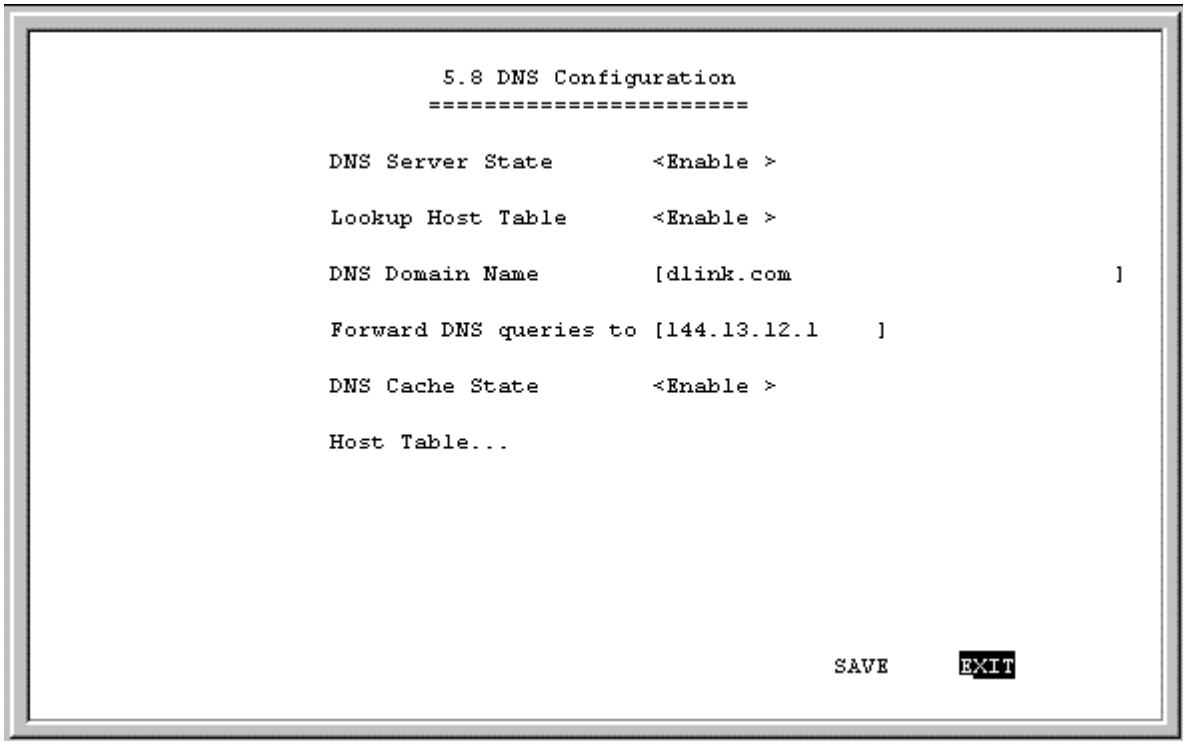
- **Telnet State** - This feature enables or disables the router's ability to be configured over the LAN using telnet.

- **Discovery Function** – Enabling this feature allows the router to be auto-discovered by D-Link SNMP management software and the included Windows-based configuration software called *RouterView*.

DNS Configuration

The DI-1162/DI-1162M router has a built in recursive DNS server. The maximum amount of memory that will be used by the router's Domain Name Server is 64Kb which averages out to be about 800 entries. In other words, up to 800 domain names and their associated IP Addresses can be stored, which can significantly speed up access to those domains. The routers DNS table will age out about every 24 hours, ensuring that the most frequently accessed domains consistently benefit from the improved access times provided by using the routers own DNS.

The IP Addresses for domain names not stored in the router must be acquired from a DNS server on the Internet. Thus, if you are using DNS, make sure you also specify an IP Address to a DNS server in the Forward DNS queries *to* field.



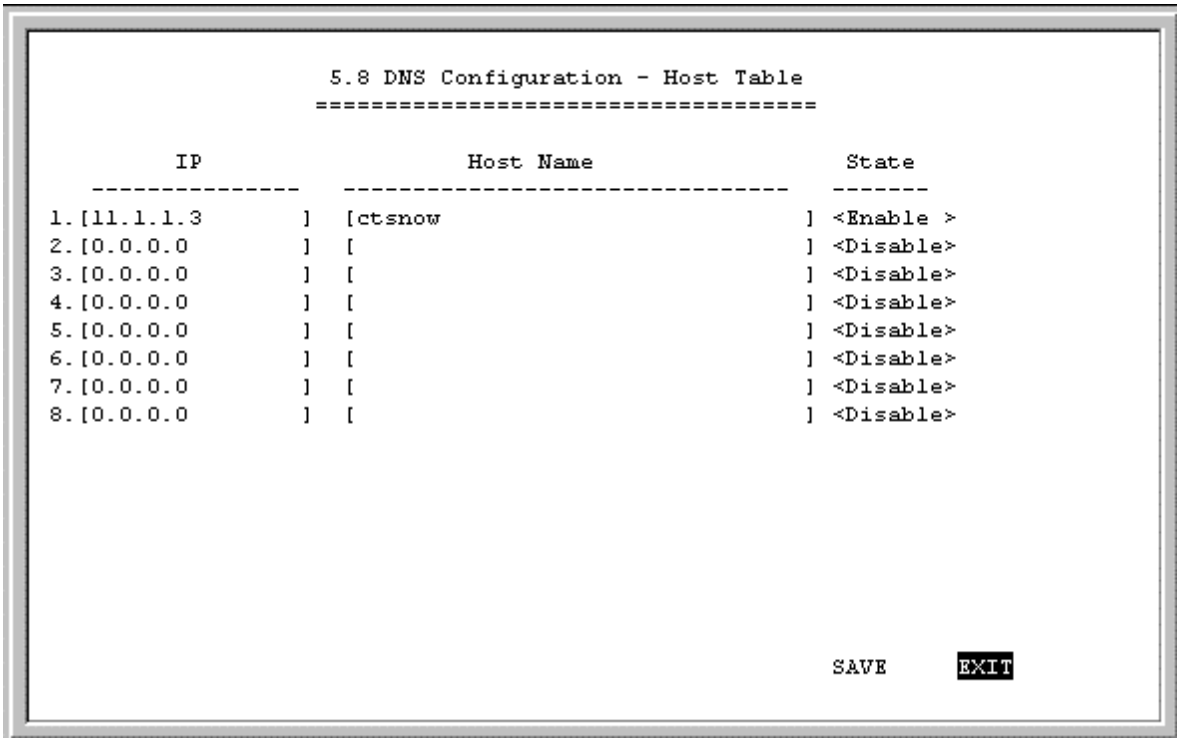
The items in the above submenu are described as follows:

- **DNS Server State** – Enables or disables recursive DNS on this router.
- **Lookup Host Table** – Enables or disables DNS to reference up to eight host names defined in the Host Table shown below.
- **DNS Domain Name** – The domain name suffix in which the router resides, to be appended to the host name defined in the host table.
- **Forward DNS queries to** – A large server dedicated to resolving domain names on the Internet. This field should contain the IP Address for the DNS closest to you.
- **DNS Cache State –** When this item is enabled, the router will add the domain names and IP Addresses it retrieves from DNS queries to it's own recursive DNS table.
- **Host Table –** Select this item to access the screen below.

Host Table

The host table allows the router to recognize host names on the network. Up to eight host names can be entered in the table. Your network servers, especially your mail server should be defined here. Leftover places in the table can be assigned to individual hosts to speed up routing.

In the example below, the host name ctsnow is combined with the domain name defined in the **DNS Configuration** submenu above (in this case, dlink.com) to produce ctsnow.dlink.com. The mapping in the example of ctsnow.dlink.com to the IP Address of 11.1.1.3 is only valid for computers which set the DI-1162/DI-1162M router as their DNS server.

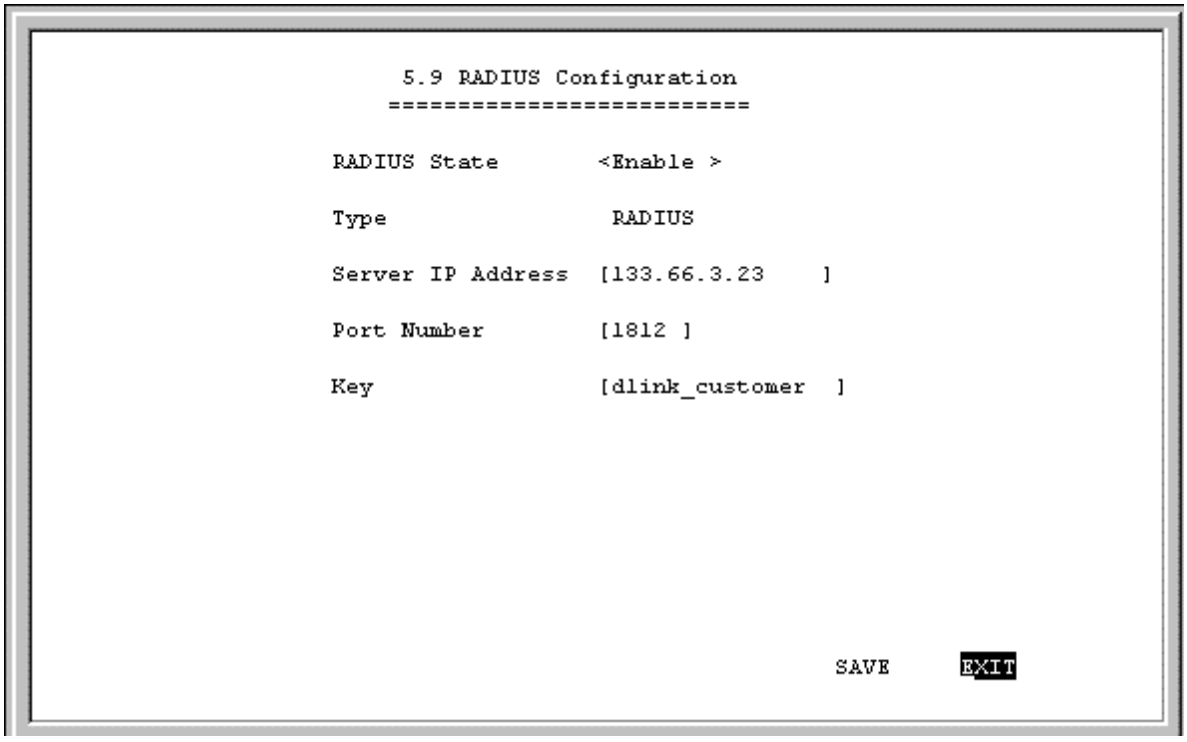


Items are described as follows:

- **IP –** The IP address for the host.
- **Host Name –** The host name used by the host.
- **State –** Enables or disables entry.

RADIUS Configuration

RADIUS is a password protocol where passwords are stored on a RADIUS server. RADIUS allows large numbers of passwords to be stored in a centralized location. Before instituting RADIUS, please setup and install a RADIUS server on the LAN.



Items in the above submenu are described as follows:

- **RADIUS State –** Enables or disables RADIUS.
- **Type –** Refers to the type of external password protocol. Currently, only RADIUS is supported.
- **Server IP Address –** This is the IP Address of your UNIX or NT-based RADIUS server.
- **Port –** The port number for the RADIUS server. The standard port number specified by RFC 1700 is 1812 (shown above).
- **Key –** This is a password used to identify the router as a valid RADIUS client.

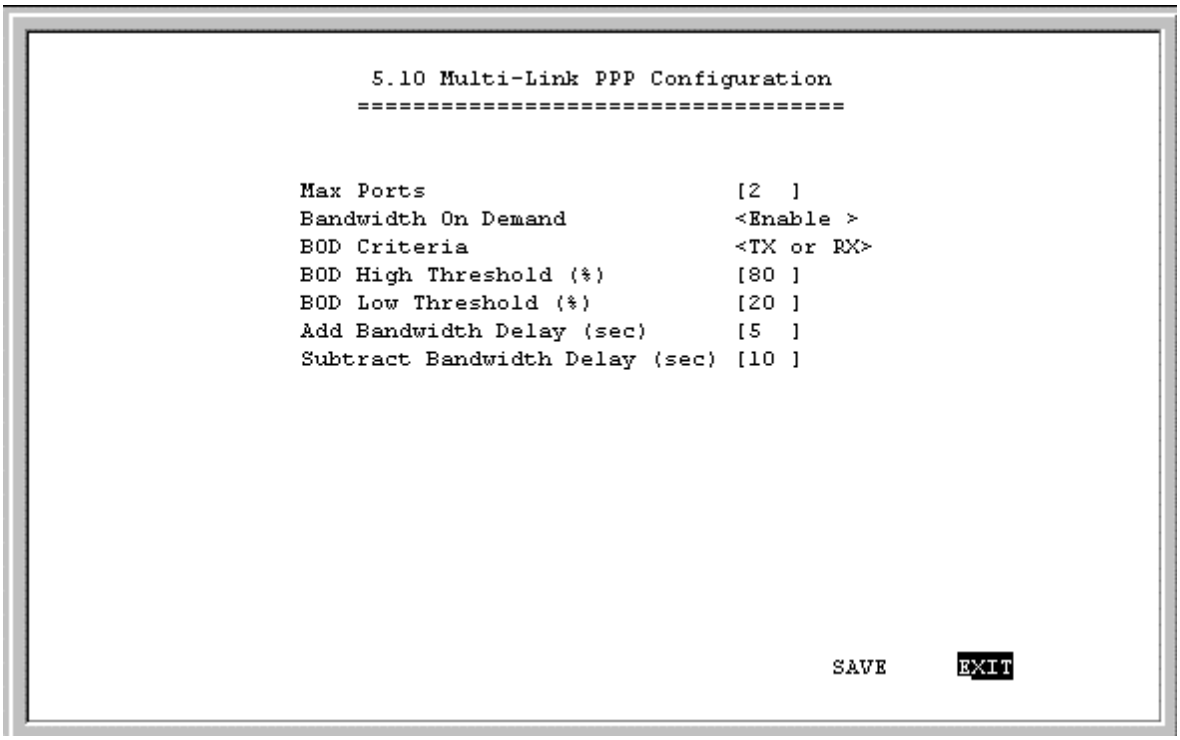
Multi-Link PPP Configuration

Multi-link PPP (MLPPP) is a standard (RFC 1990 and RFC 1717) for inverse multiplexing, a method of combining individually dialed channels into a single, higher speed data stream. MLPPP is an extension of PPP that supports the ordering of data packets across multiple channels. Although MLPPP can be implemented on any WAN device, it was the rapid emergence of ISDN BRI as a cost efficient higher bandwidth alternative to modems which has driven the evolution and acceptance of MLPPP. Typically MLPPP is used to combine the speed of two ISDN BRI B-Channels to get 128Kbps of virtual capacity.

Before implementing MLPPP on the DI-1162/DI-1162M, please ensure that your ISP or the device to which you are connecting supports, and is configured for MLPPP.

MLPPP can be implemented in two ways, dynamically through the use of the Bandwidth on Demand (BOD), and statically. BOD causes the second WAN port to place a call and add bandwidth to the WAN connection when the BOD High Threshold is exceeded for the Add Bandwidth Delay period. Bandwidth can also be subtracted when WAN throughput falls below the BOD Low Threshold and Subtract Bandwidth Delay parameters. Thus, BOD economizes MLPPP by maintaining only the bandwidth needed.

A static implementation of MLPPP is achieved when BOD is disabled but the WAN ports have Multi-Link enabled. In this case, when the two WAN ports have established a connection, the router will check to see if they are connected to the same source and whether the source supports MLPPP. If both conditions are met, the router will automatically bundle the two links together as an MLPPP connection.



Items in the screen are described as follows:

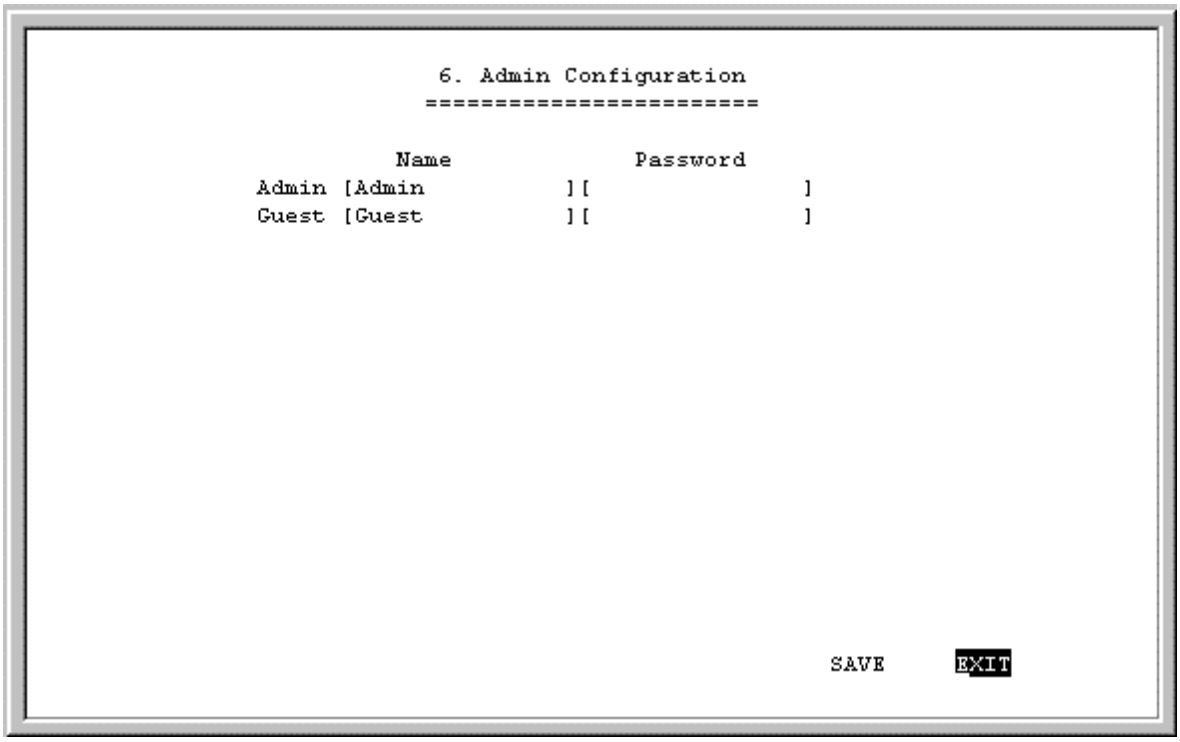
- **Max Ports** – Maximum ports allowed per multi-link bundle.
- **Bandwidth on Demand** – Enables or disables BOD. When enabled, BOD will manage the implementation of MLPPP using the parameters defined in this window.
- **BOD Criteria** – Either *TX*, *RX* or *TX or RX*, where *TX* is Transmit and *RX* is Receive. The parameter defined here is used when monitoring the BOD High Threshold and BOD Low Threshold.
- **BOD High Threshold (%)** – (0 to 100) The throughput value as a percentage of total bandwidth which will cause the next WAN port having Multi-Link PPP enabled to dial up and add bandwidth to the connection. This value, however, must be constantly exceeded for the time designated in the Add Bandwidth Delay field before the next WAN port dials out.
- **BOD Low Threshold (%)** – (0 to 100) The throughput value as a percentage of total bandwidth which will cause the highest numbered WAN port in the MLPPP bundle to hang up, thus subtracting bandwidth from the connection. Before actually hanging up however, the throughput must be below this value for the time designated in the Subtract Bandwidth Delay field.
- **Add Bandwidth Delay (sec)** – (0 to 999) The amount of time in seconds the router will wait and sample the BOD Criteria before adding bandwidth once the throughput exceeds the BOD High Threshold. This prevents costly bandwidth from being unnecessarily added due to temporary bursts in traffic.
- **Subtract Bandwidth Delay (sec)** – (0 to 999) The amount of time in seconds the router will wait and sample the BOD Criteria before subtracting bandwidth once the throughput falls below the BOD Low Threshold. This prevents bandwidth from being unnecessarily subtracted due to temporary lulls in traffic.

The example Multi-link PPP settings shown in the **Multi-Link PPP Configuration** window above assumes that WAN 1 and WAN 2 each have a 64 kps connection configured to dial up to the Internet. When WAN 1 receives a packet destined for the Internet it will dial the ISP and establish a connection. If the total throughput on WAN 1 (*TX or RX*) ever exceeds 80% of the 64 kps (51.2 kps), the router will sample the line for an additional 5 seconds. If the traffic continuously exceeds 80% for the 5-second delay time, WAN 2 will dial up and add bandwidth to the connection. Assuming sustained traffic of 70 kps, MLPPP will balance the traffic on the two WAN ports so they are handling roughly 35 kps each. If the traffic on WAN 1 + WAN 2 falls below 20% of the 128 kps connection (25.6 kps) for more than 10 seconds, WAN 2 will hang up and all traffic will be handled by WAN 1.

For the above configuration to work, both WAN ports need to have been properly setup to establish dial-out PPP connections, and have Multi-Link enabled. Also note that WAN 1, being the lowest numbered WAN port in the MLPPP bundle and thus the primary link, is not subject to the BOD Low Threshold parameter and will never hang up due to BOD considerations.

Admin Configuration

This feature allows you to define two names and passwords, which are used to login to the router for configuration and management:

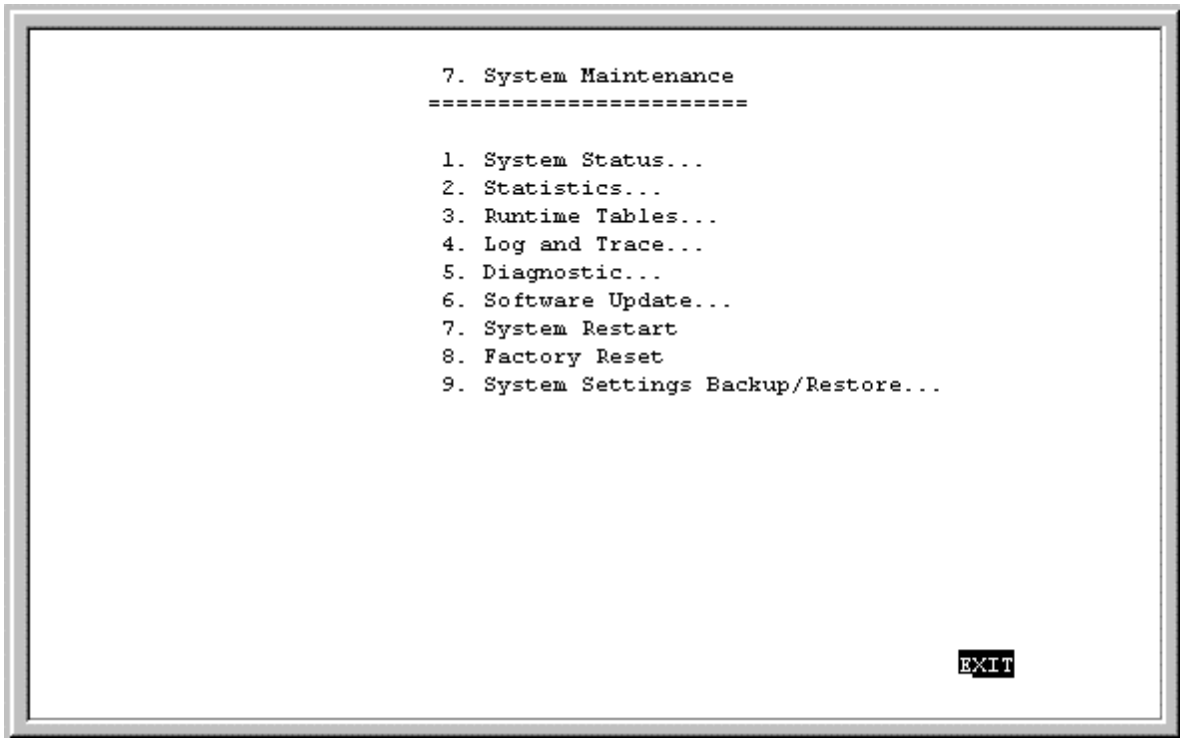


Please note any changes made here as they are necessary for logging into the console program.

System Maintenance

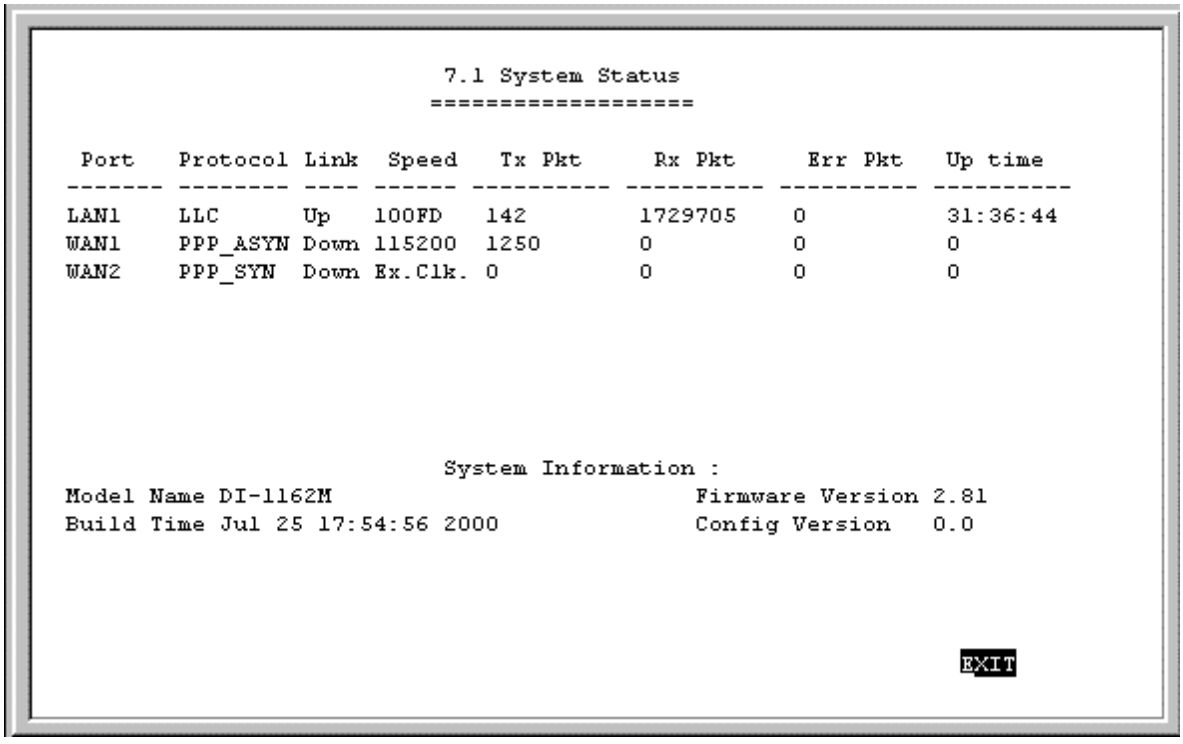
Your DI-1162/DI-1162M provides useful tools for maintaining your device. These tools include updates on system status, upgrades to the system software, analysis, diagnostic tools, and more. This section will describe how to use these tools in greater detail.

The **System Maintenance** submenu appears as follows:



System Status

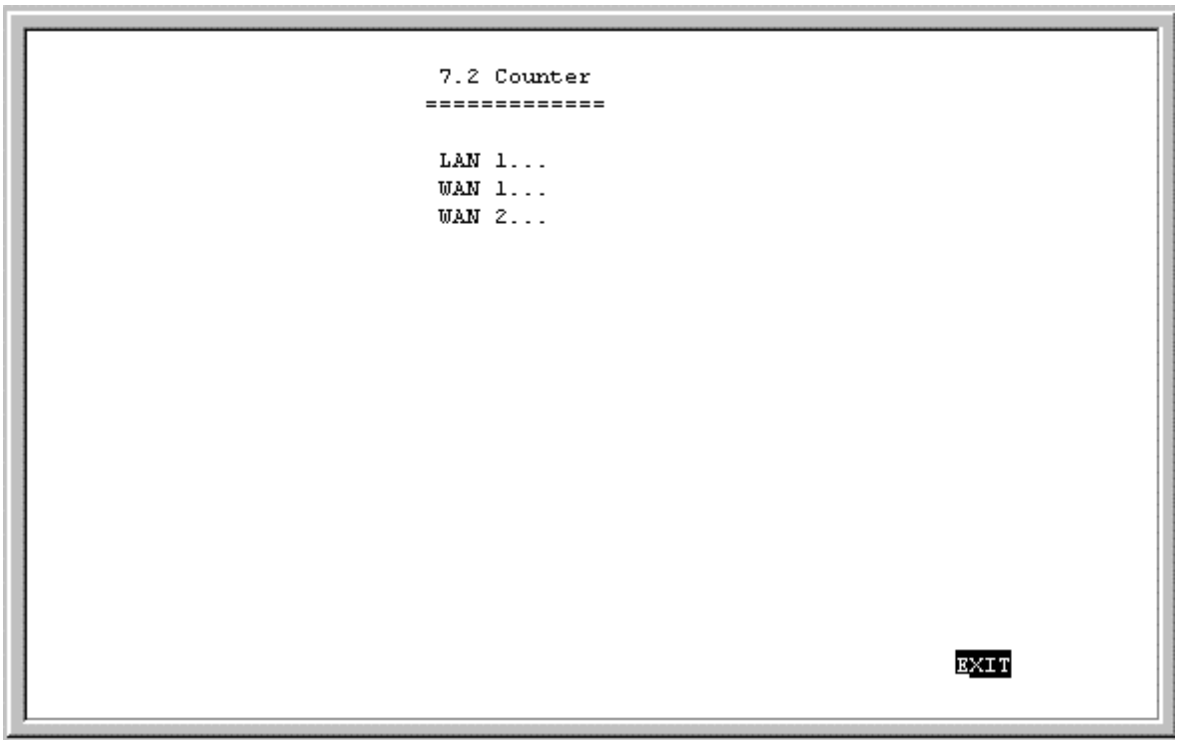
The **System Status** submenu displays key information about the router and appears as follows:



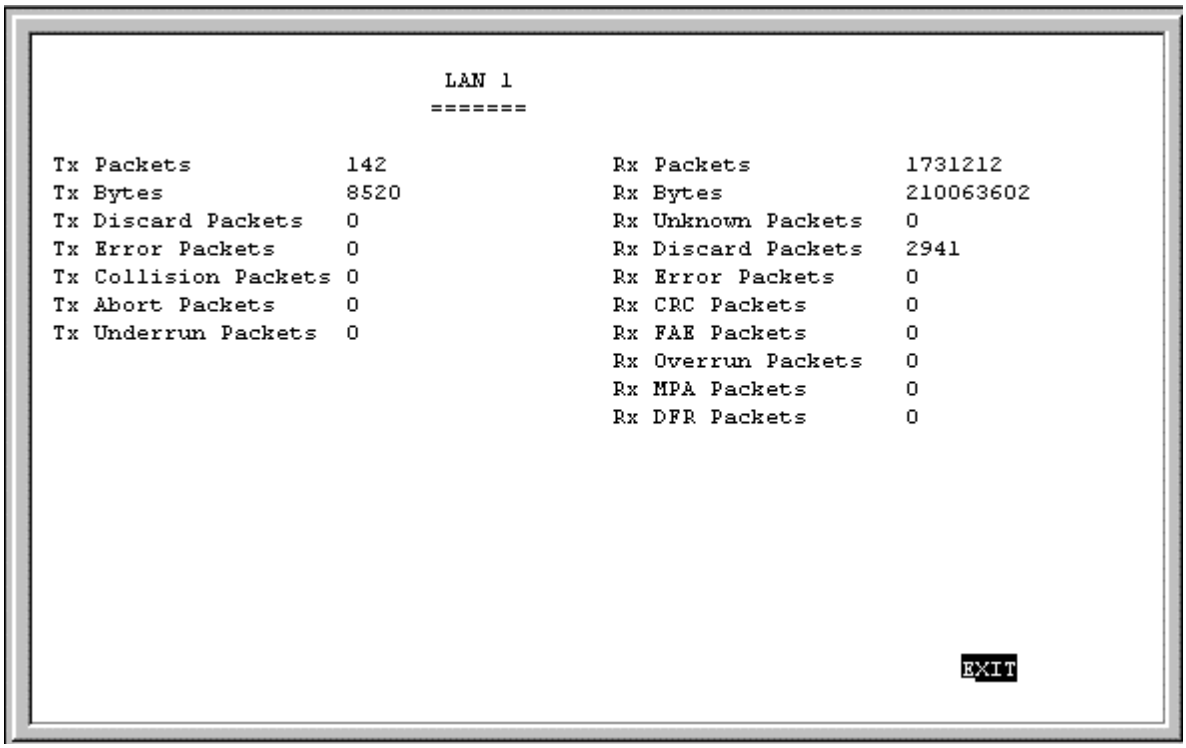
Counter

Under the Statistics item of the **System Maintenance** screen is a **Counter** menu that displays some of the counters contained in MIB-II and the proprietary MIB. The table is updated every 5 seconds and can be reset by performing

a system reset on the router. Note that performing a system reset clears ALL tables in the router, including the routing table. Select the desired entry from the screen below and then press <Enter>.



LAN 1

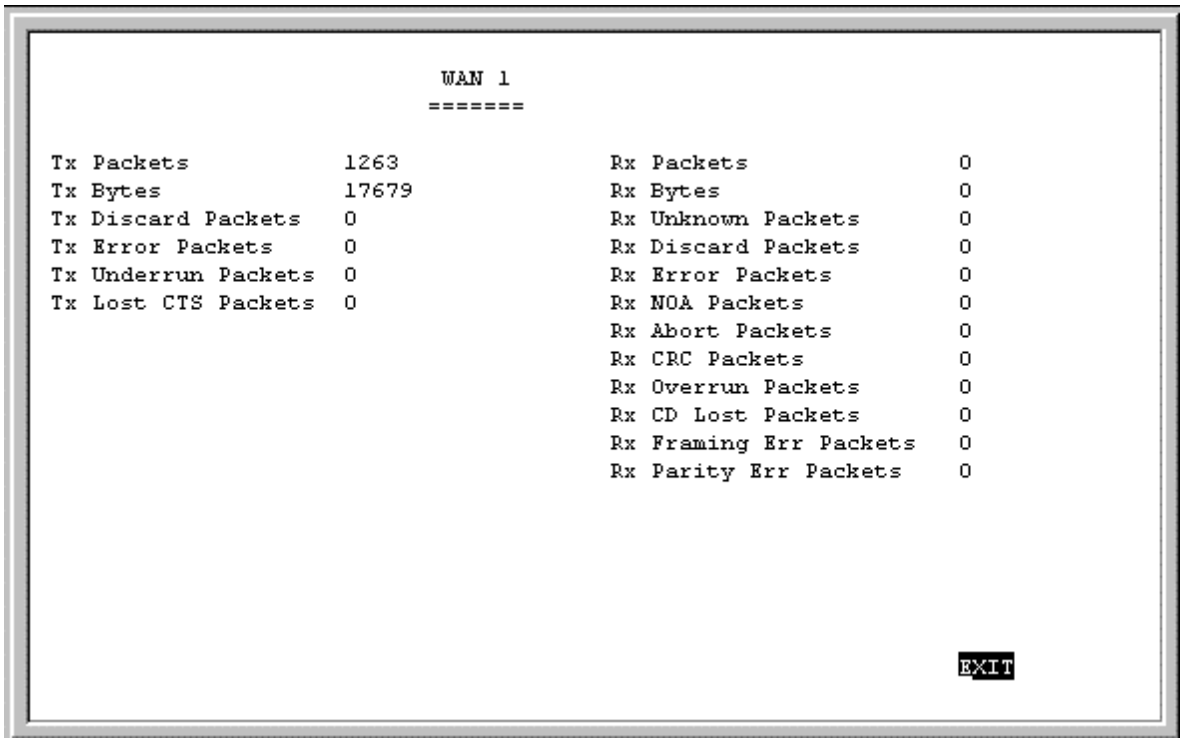


Items in the screen are described as follows:

- **Tx Packets –** The total number of valid packets transmitted by the router since the last reset.

- **Tx Bytes –** The total number of bytes transmitted by the router.
- **Tx Discard Packets –** The number of packets dropped by the router.
- **Tx Error Packets –** The number of invalid packets transmitted by the router. This hardware counter shows the sum of Collisions, Abort, and Underrun packets.
- **Tx Collision Packets –** The number of packets sent out of the router that collided on the line. Some collisions are inevitable due to the shared nature of Ethernet. Excessive collisions show excessive utilization of the network.
- **Tx Abort Packets –** When the router transmits a packet and a collision occurs, the router will wait a random period and try to retransmit the packet. If a collision occurs 16 times in a row, the transmission will be aborted and be logged by this counter. An aborted packet shows extremely heavy utilization of the network.
- **Tx Underrun Packets –** Runt packets. The number of packets transmitted by the router that are less than the allowed 64 octets minimum length. Underrun packets occur due to jam signals generated by collisions, backpressure, etc.
- **Rx Packets –** The number of valid packets received by the router.
- **Rx Bytes –** The total number of bytes contained in the valid packets received by the router.
- **Rx Unknown Packets –** The number of packets received by the router that were of an unsupported protocol.
- **Rx Discard Packets –** The number of packets dropped by the router.
- **Rx Error Packets –** The number of invalid packets received by the router. This hardware counter shows the sum of CRC, FAE, Overrun, MPA and DFR error packets.
- **Rx CRC Packets –** The number of packets received that failed the CRC checksum test.
- **Rx FAE Packets –** Frame Alignment Error. The number of packets received that does not end on a byte boundary and the CRC does not match.
- **Rx Overrun Packets –** The number of packets received that exceed the 1518-octet maximum length imposed on Ethernet packets. Overrun packets are generated by some proprietary software applications.
- **Rx MPA Packets –** Missed Packet. This is a count of packets intended for the router, but at the time, the router could not receive the packet (usually due to the temporary lack of receive buffers).
- **Rx DFR Packets –** Deferred Packets. This is a count of incidents where CRS (carrier signal lost) and COL both occur at the same time. These two events happen simultaneously as a result of jabber (produced by faulty networking equipment, usually NIC's).

WAN 1

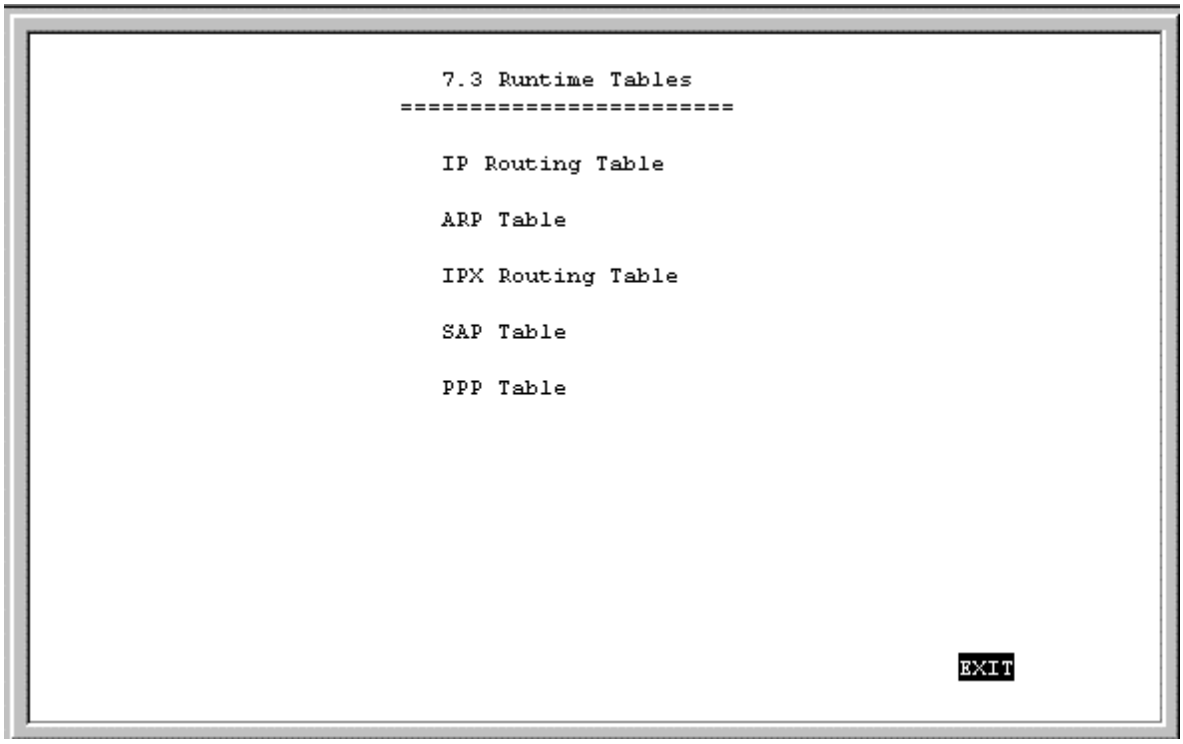


Items in the screen are described as follows:

- **Tx Packets –** The total number of valid packets transmitted by the router since the last reset.
- **Tx Bytes –** The total number of bytes transmitted by the router.
- **Tx Discard Packets –** The number of packets dropped by the router.
- **Tx Error Packets –** the number of invalid packets transmitted by the router. This hardware counter shows the sum of Collisions, Abort, and Underrun packets.
- **Tx Underrun Packets –** Runt packets. This counter shows the number of packets transmitted by the router that are less than the allowed 64-octet minimum length. Underrun packets occur due to jam signals generated by collisions, backpressure, etc.
- **Tx Lost CTS Packets –** The number of Clear To Send packets that were lost by the router.
- **Rx Packets –** The total number of packets received by the router.
- **Rx Bytes –** The total number of bytes contained in packets received by the router.
- **Rx Unknown Packets –** The number of packets received by the router that were of an unsupported protocol.
- **Rx Discard Packets –** The number of packets dropped by the router.
- **Rx Error Packets -** Number of invalid packets received by the router. This hardware counter shows the sum of NOA, Abort, CRC, Overrun, CD Lost, Framing, and Parity error packets.
- **Rx NOA Packets –** Non-Octet Alignment. This counts the number of packets received by the router that did not end on a byte boundary. The receipt of a misaligned packet will generate a single NOA event regardless of the number of misaligned octets in the packet.
- **Rx Abort Packet –** The number of packets that were dropped due to user generated breaks in the transmission that occurred while a packet is being received.
- **Rx CRC Packets –** The number of packets received that failed the CRC checksum test.

- **Rx Overrun Packets –** The number of packets received that exceed the 1518 octet maximum length imposed on Ethernet packets. Overrun packets are generated by some proprietary software applications.
- **Rx CD Lost Packets –** Carrier Detect Lost. This counts the number of Carrier Detect packets that were lost by the router.
- **Rx Framing Err Packets –** Packets with framing errors can occur on the WAN port only when using HDLC in sync mode. This parameter counts the number of lost start/stop flags.
- **Rx Parity Err Packets –** The number of times parity errors occurred on the line.

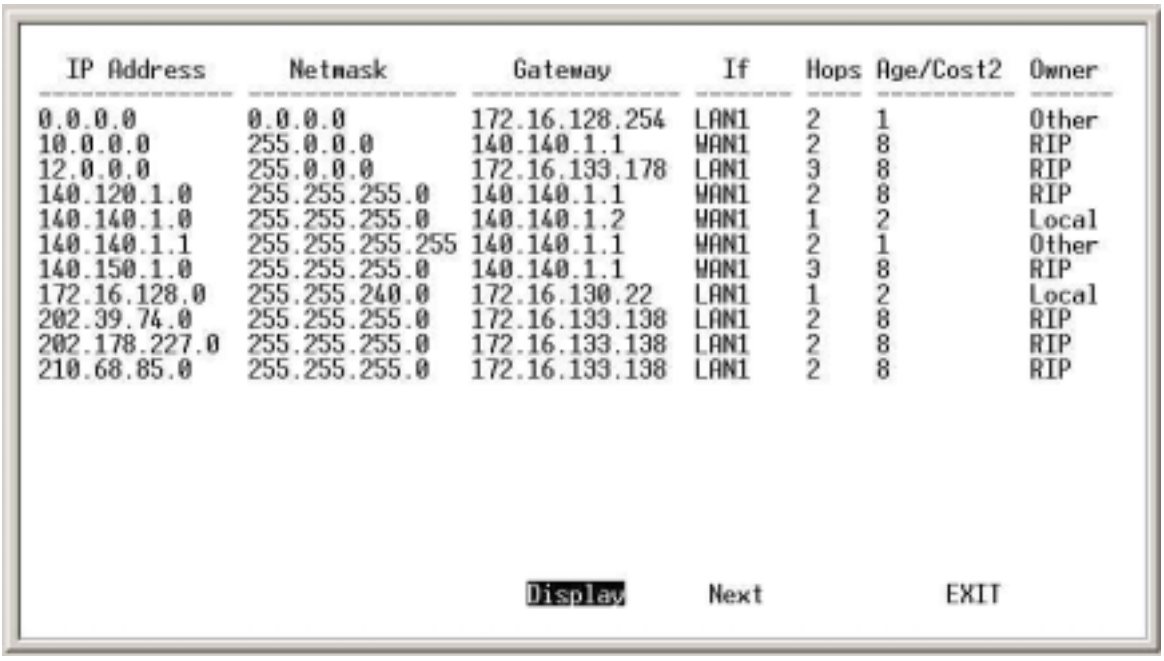
Runtime Tables



Please note that the IPX Routing Table and SAP Table will only appear on DI-1162M models.

IP Routing Table

The IP Routing Table gives you a snapshot of the IP routing table. Table entries will expire after the Age value in the table counts down to zero seconds (except for entries for the router itself which have an age value of zero but will never expire).



IP Address	Netmask	Gateway	If	Hops	Age/Cost2	Owner
0.0.0.0	0.0.0.0	172.16.128.254	LAN1	2	1	Other
10.0.0.0	255.0.0.0	140.140.1.1	WAN1	2	8	RIP
12.0.0.0	255.0.0.0	172.16.133.178	LAN1	3	8	RIP
140.120.1.0	255.255.255.0	140.140.1.1	WAN1	2	8	RIP
140.140.1.0	255.255.255.0	140.140.1.2	WAN1	1	2	Local
140.140.1.1	255.255.255.255	140.140.1.1	WAN1	2	1	Other
140.150.1.0	255.255.255.0	140.140.1.1	WAN1	3	8	RIP
172.16.128.0	255.255.240.0	172.16.130.22	LAN1	1	2	Local
202.39.74.0	255.255.255.0	172.16.133.138	LAN1	2	8	RIP
202.178.227.0	255.255.255.0	172.16.133.138	LAN1	2	8	RIP
210.68.85.0	255.255.255.0	172.16.133.138	LAN1	2	8	RIP

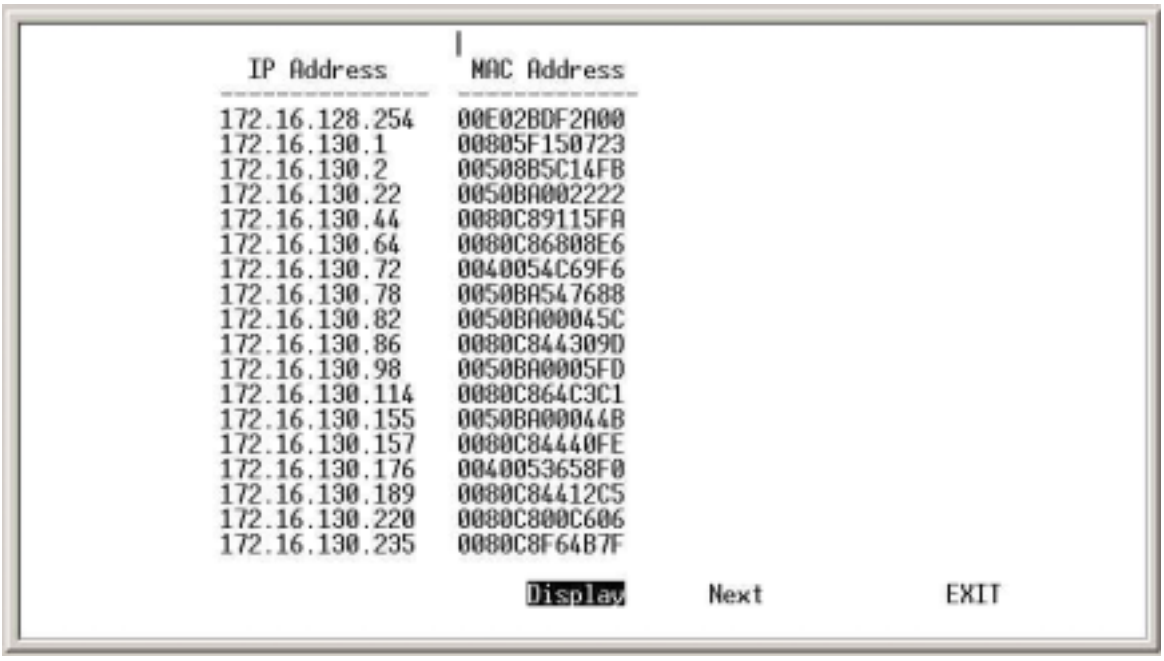
Display Next EXIT

Items in the screen are described as follows:

- **IP Address –** This is the destination, network IP address from an incoming packet.
- **Netmask –** This mask is received from RIP exchanges and internal calculations, as the router learns.
- **Gateway –** This is the next-hop router for which the packet, with destination IP Address and qualifying Netmask, will be forwarded.
- **If –** This is the outgoing interface for which the acceptable, routing packet will be forwarded.
- **Hops –** This is the remaining hop-count.
- **Age/Cost2 –** This is the time-to-live (TTL) value.
- **Owner –** This indicates who the routing table entry is added by. *Other* means added by a static route. *Local* means added by the router interface. *RIP* means added by the entry received by RIP protocol.

ARP Table

This Address Resolution Protocol table displays how the router maps individual IP addresses to specific MAC addresses.



IPX Routing Table

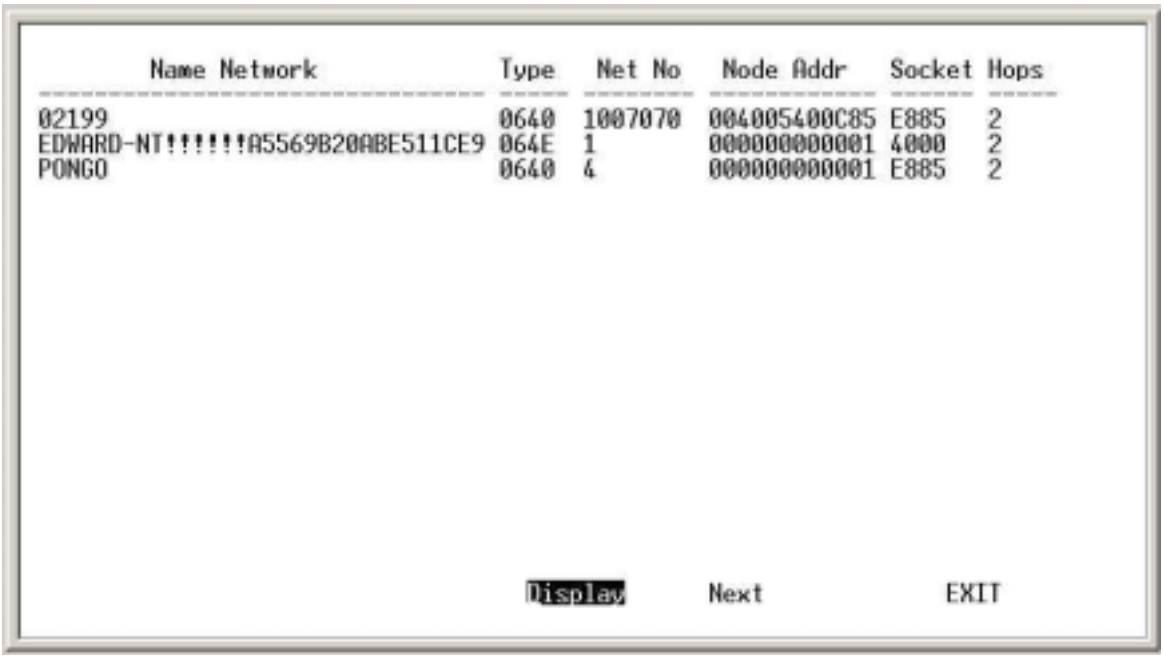
This table displays IPX topology information (DI-1162M only).

Items in the screen are described as follows:

- **Net No** – This displays the selected network number.
- **Next Node Address** – This is the node address that will be used next.
- **Interface –** This is the interface of this item.
- **Hop** – This is the hop count.

SAP Table

This table displays Service Advertising Protocol information (DI-1162M only).



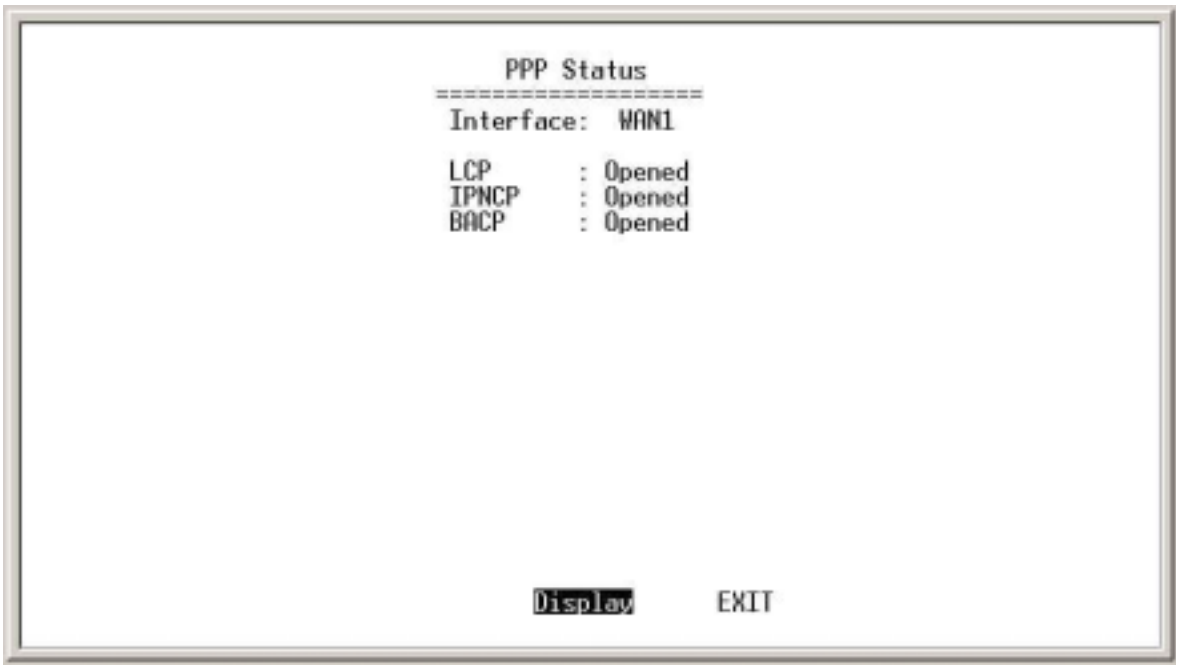
Items in the screen are described as follows:

- **Name Network** – This displays the selected name network.
- **Type** – This displays the type of service based on numbers and services defined by Novell.
- **Net No** –This displays the network number.
- **Node Addr** – This displays the node address.
- **Socket** – This displays the socket number.
- **Hops** –This displays the hop count.

PPP Status

This table displays which PPP protocol is negotiated and its present status.

Select an interface from the screen above and press <Enter> to view the current PPP status:

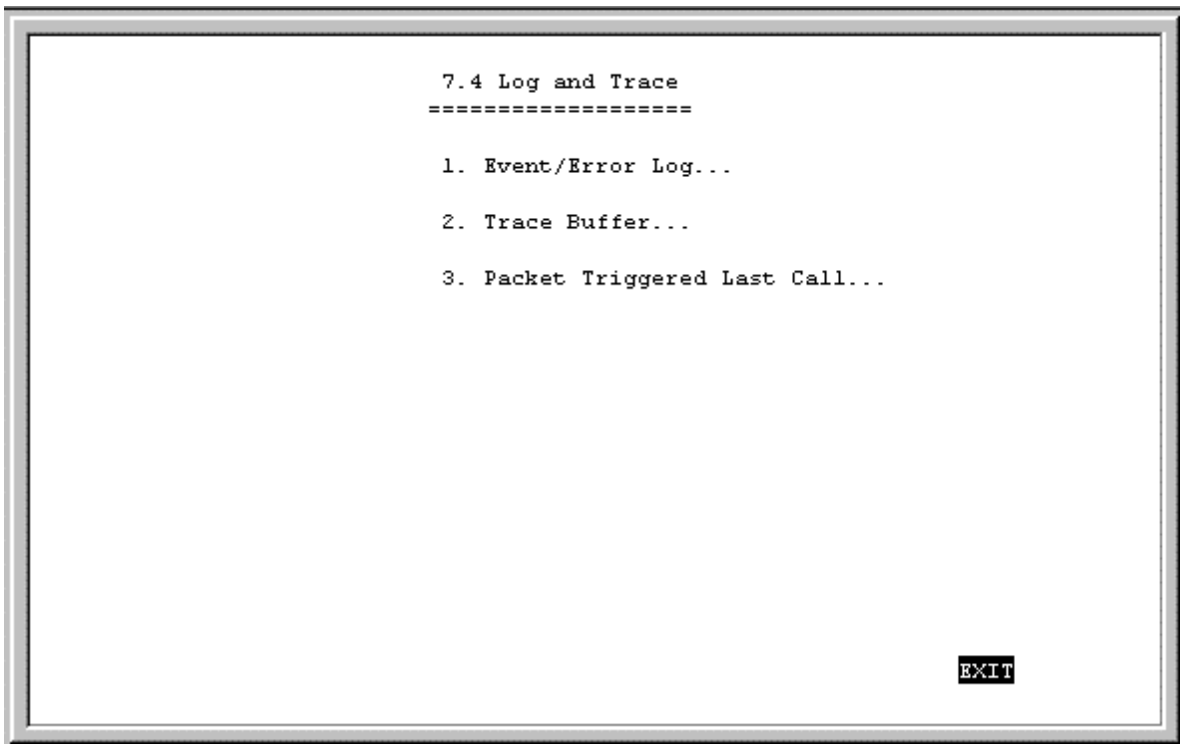


Items in the screen are described as follows:

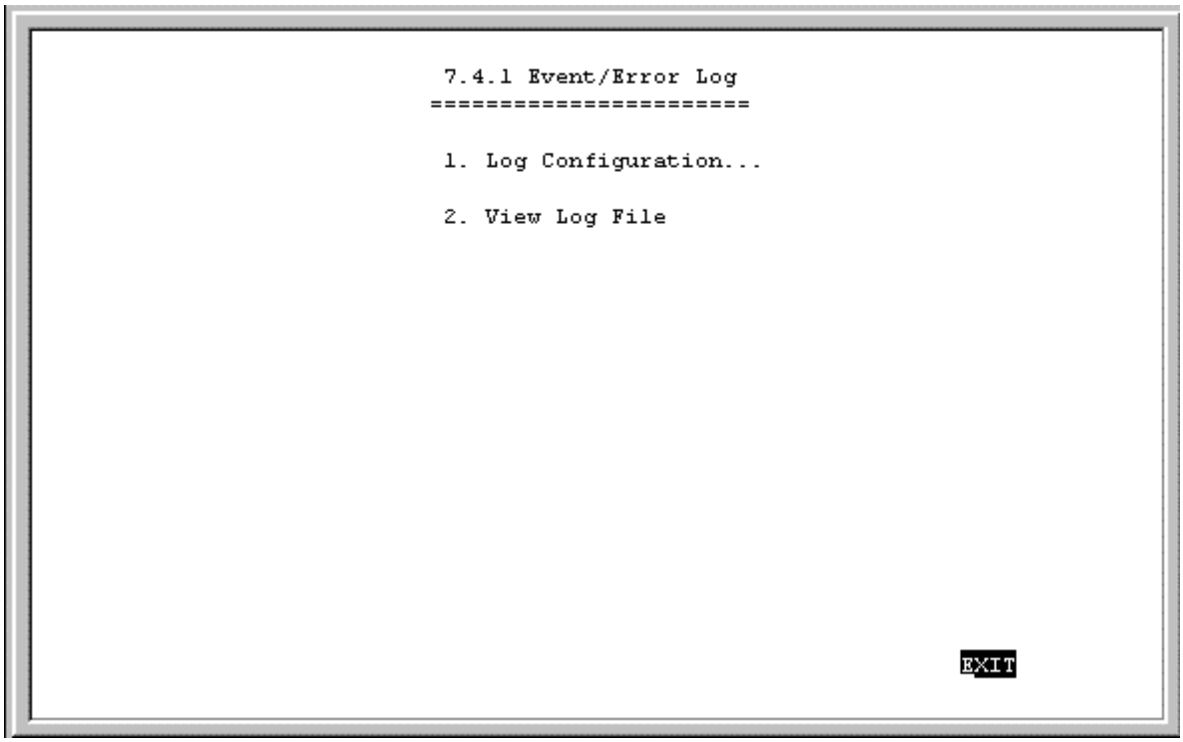
- **Interface** – This displays the selected interface.
- **BACP –** Bandwidth Access Control Protocol is used to control bandwidth between routers.
- **CCP –** Compress Communication Protocol is used to compress data sent between routers.
- **IPNCP –** IP Network Control Protocol is used to keep lines open between IPs.
- **LCP –** Link Control Protocol is used to maintain a link state between routers.

Log and Trace

This feature file events and errors that occurred and allows individual packets to be captured in a buffer. These items are to help D-Link technical support personnel identify problems that may be affecting your router. If problems occur with your router, D-Link technical support personnel will guide you through the use of these features.

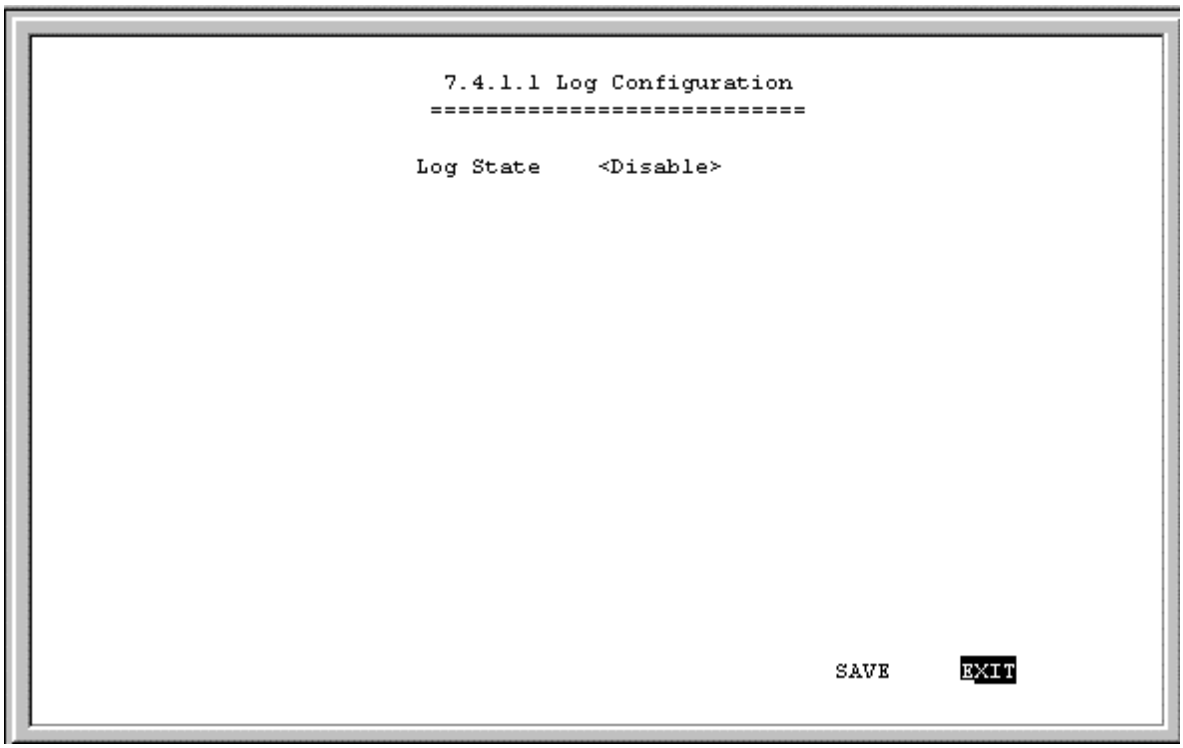


Event/Error Log



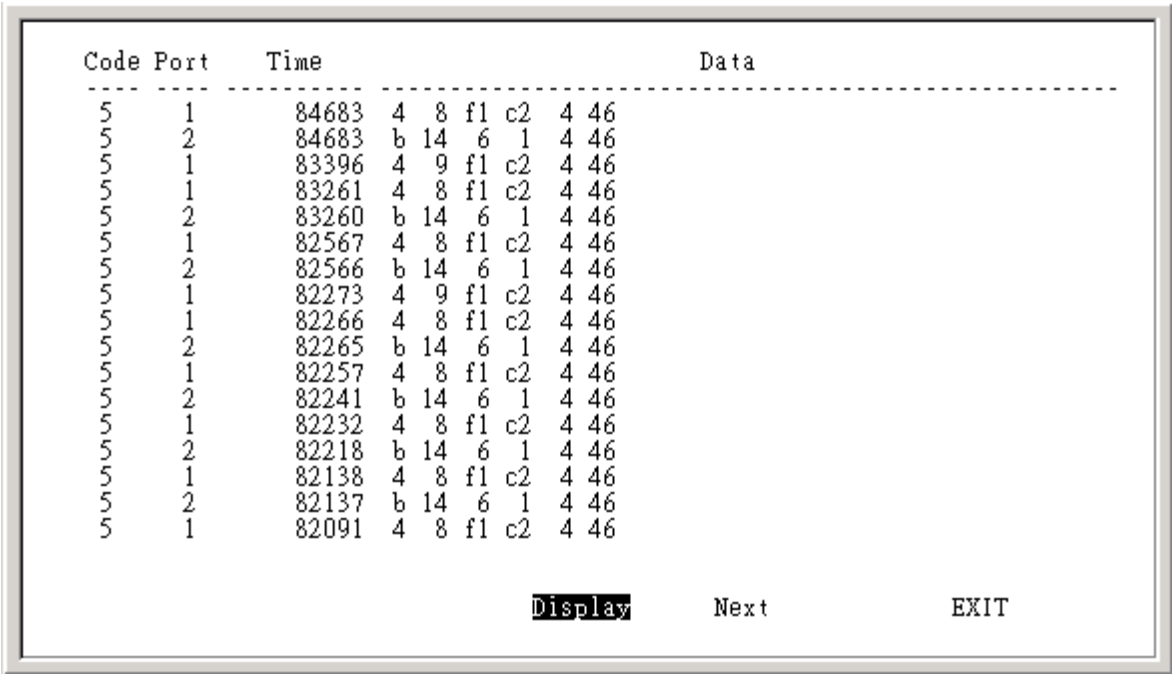
Log Configuration

This option allows you to *Enable* or *Disable* the Event/Error log and begin recording events.



View Log File

This displays the Event/Error Log file shown below:

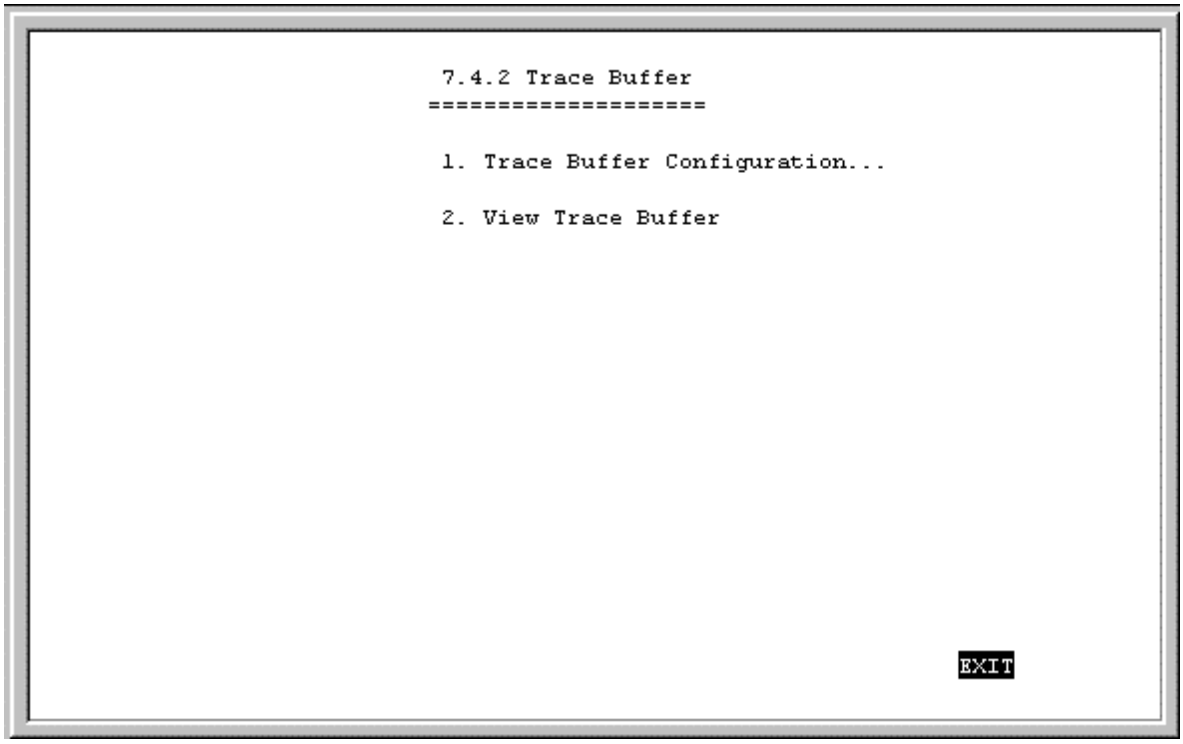


The following parameters help technical support personnel evaluate events:

- **Code –** A special code for categorizing events.
- **Port –** The interface on which an event occurs.
- **Time –** Tick-times denoting when events occurred.
- **Data –** Data petaining to specific events.

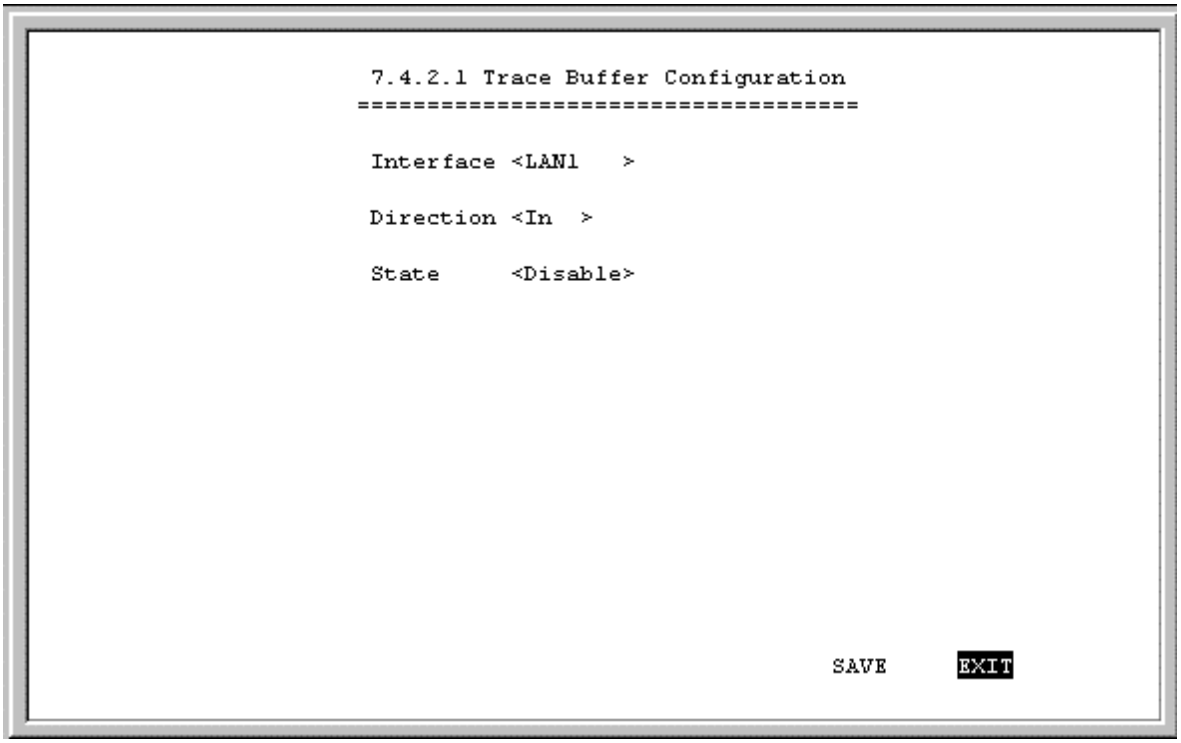
Trace Buffer

This feature captures packets in a buffer to help D-Link technical support personnel identify problems with your router.



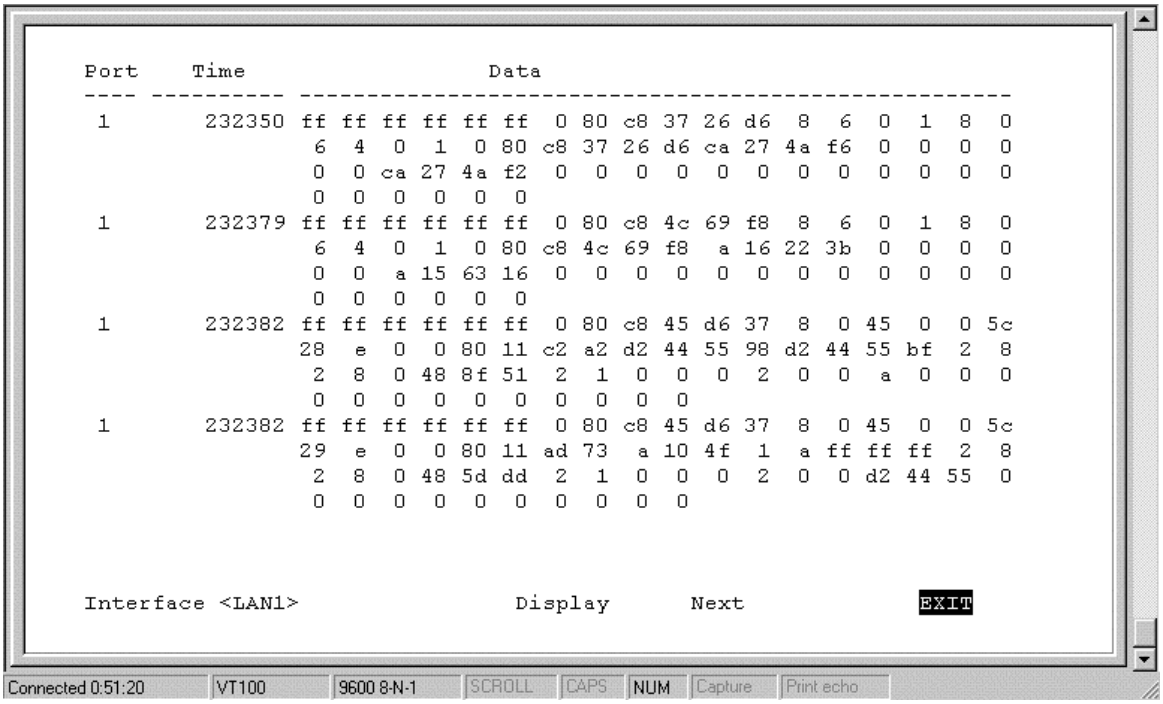
Trace Buffer Configuration

Enables or disables the Trace buffer feature.



View Trace Buffer

Displays the header of packets captured in the buffer.

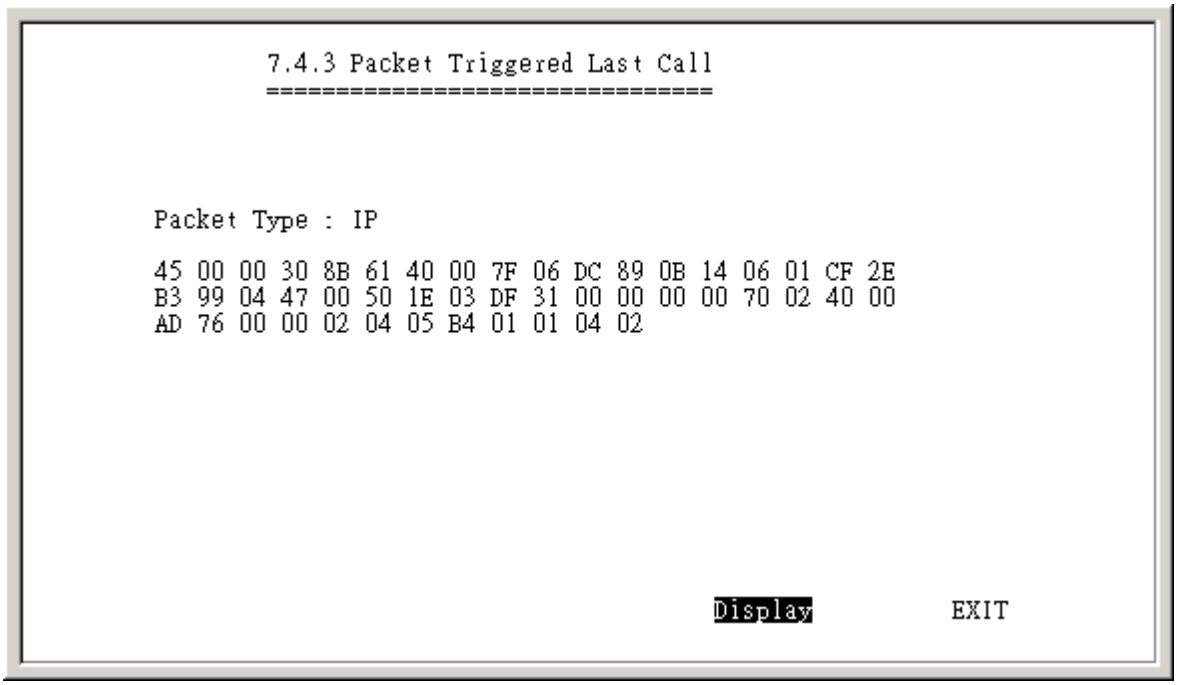


The contents are described as follows:

- **Port** – This is the interface from which the packets were captured.
- **Time** – In clock ticks. The time the packet was captured.
- **Data** – The contents of the header of the packet.

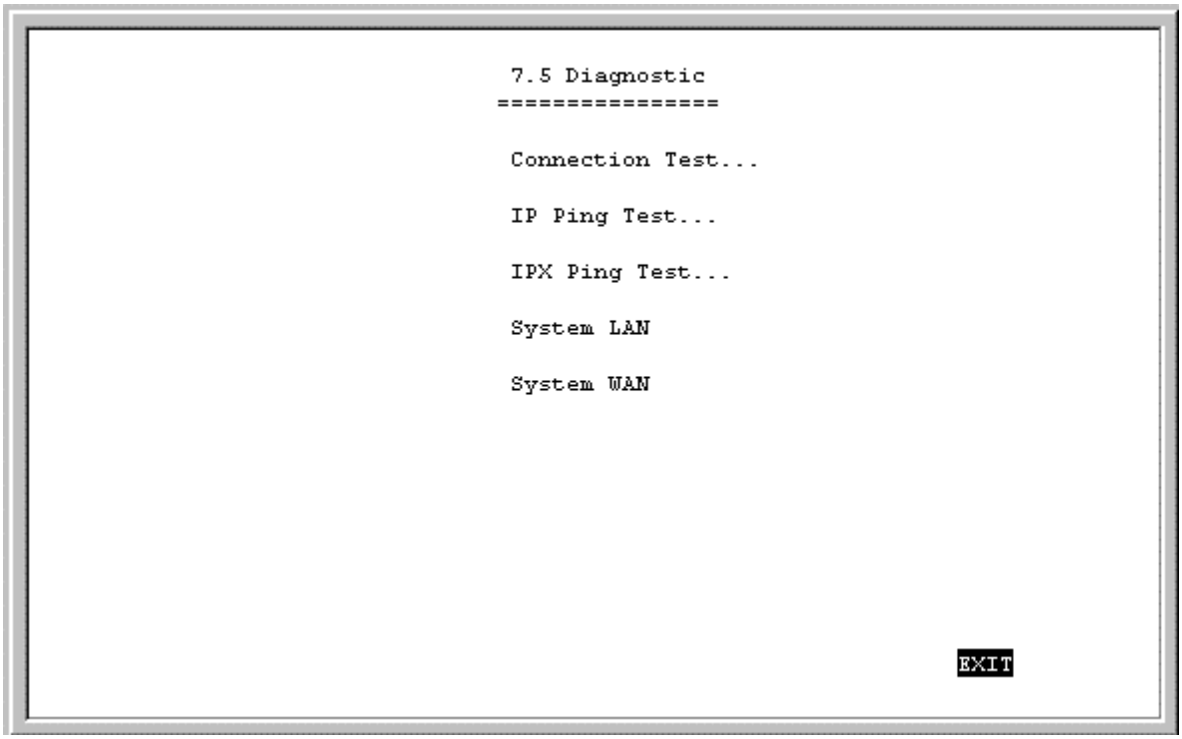
Packet Triggered Last Call

This function enables you to determine what type of packet triggered the last call. This is useful when a network administrator wants to control access and costs. If a packet from an undesired source is found, an IP Filter can be created to insure such a packet is discarded when received.



Diagnostic

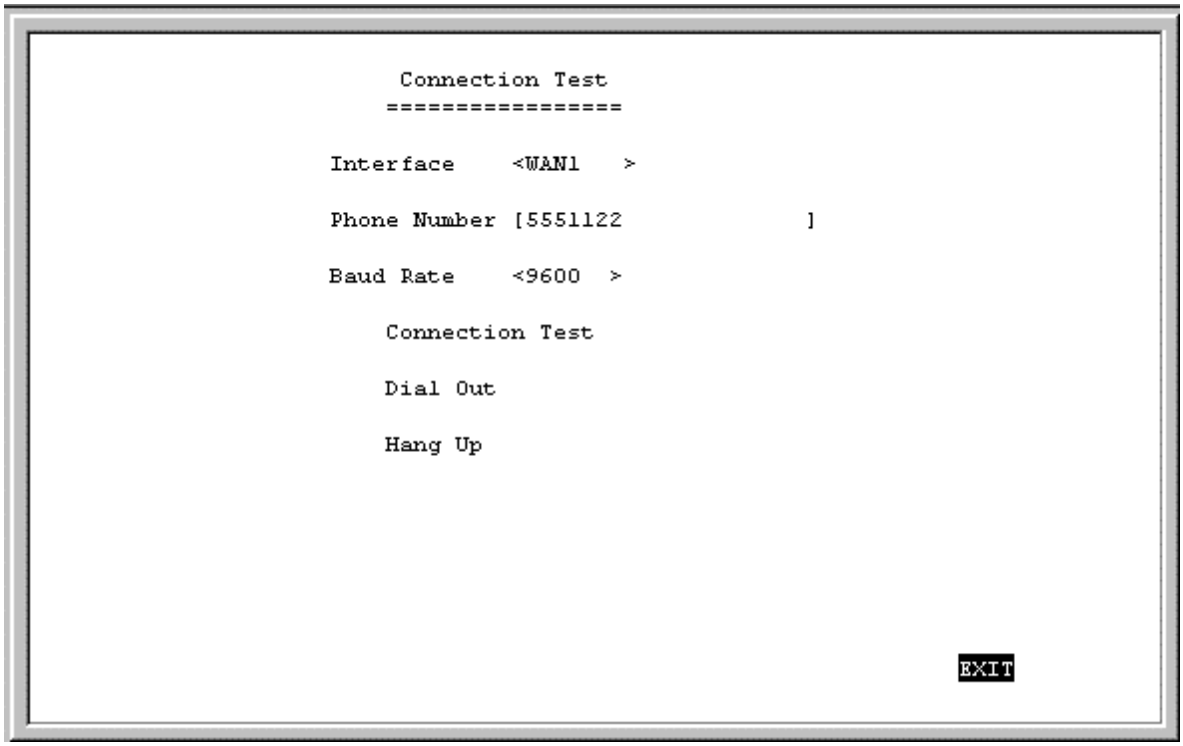
This feature tests the connection between the router and connected peripherals on a given interface.



Please note that the IPX Ping Test is for the DI-1162M only.

Connection Test

This feature tests a dial-out WAN connection.

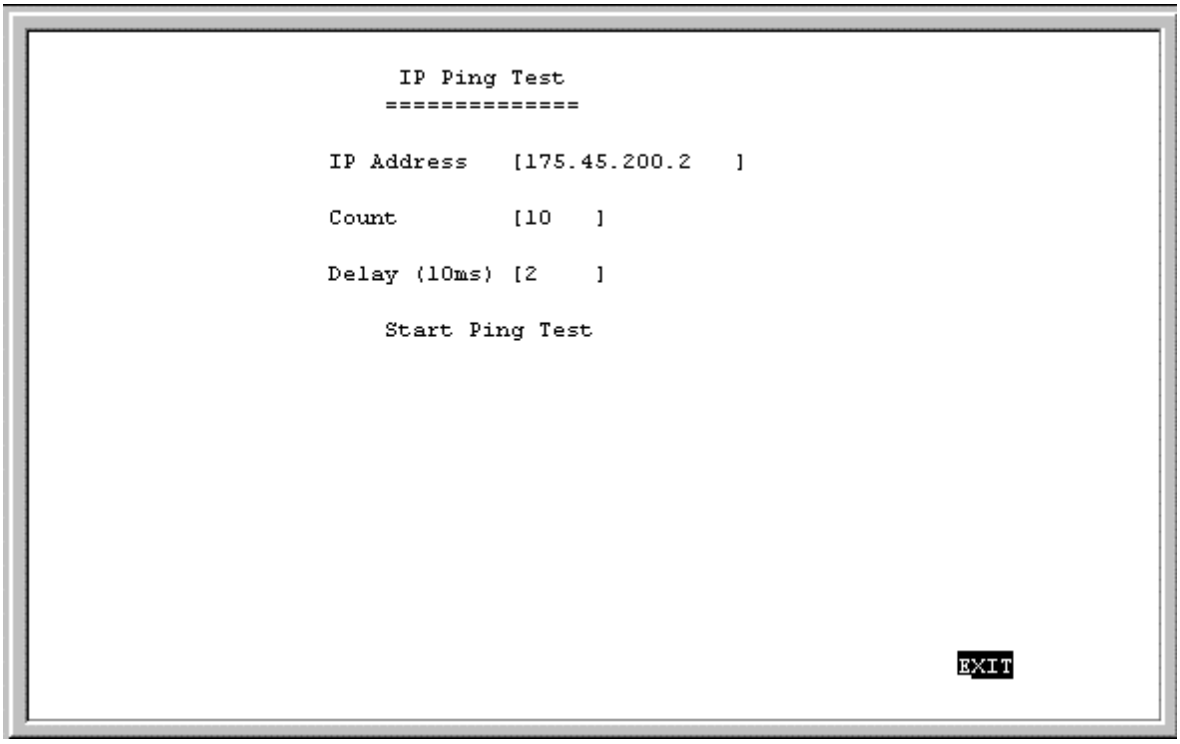


The parameters are described as follows:

- **Interface –** The WAN interface to be tested.
- **Phone Number –** The phone number that will be dialed by the WAN Interface. Please ensure that a modem answers the phone on the other end.
- **Baud Rate –** The rate of data transmission. The answering modem must be capable of operating at the baud rate defined here.
- **Connection Test –** Press <Enter> to begin the test. The router will dial the phone number defined above, try to establish a valid link with the answering WAN device and hang up.
- **Dial Out** – Press <Enter> to begin the test. The router will dial the phone number above and negotiate a connection with the answering device.
- **Hang up** – Press <Enter> to hang up after Dialing Out.

IP Ping Test

This test makes sure there is an IP network connection to a particular IP address.

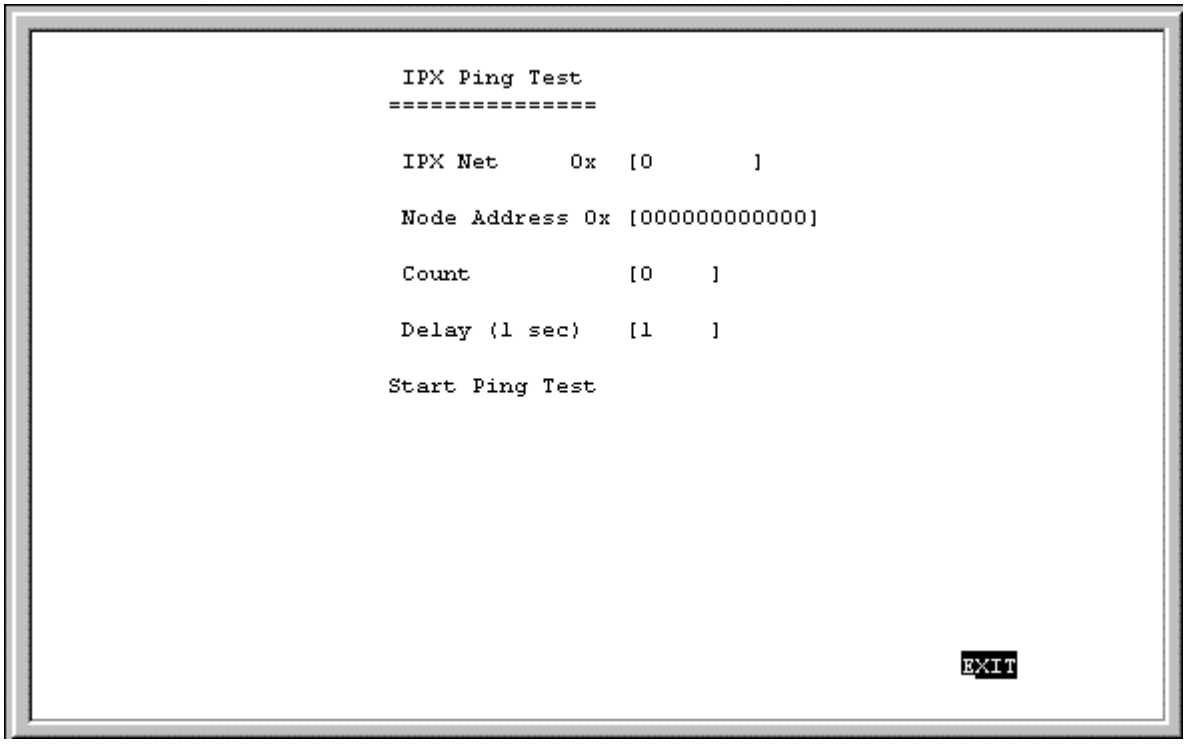


The parameters are described as follows:

- **IP Address –** This is the IP Address of the device that the router will attempt to reach. The router will check it routing table and try to locate the IP Address.
- **Count –** The number of pings (packets) that will be sent.
- **Delay (10ms) –** The amount of time in 10 millisecond intervals between each ping in the Count.
- **Start Ping Test -** Press <Enter> or <Return> to begin the test.

IPX Ping Test

This test makes sure there is an IPX network connection to a particular IP address (DI-1162M only).

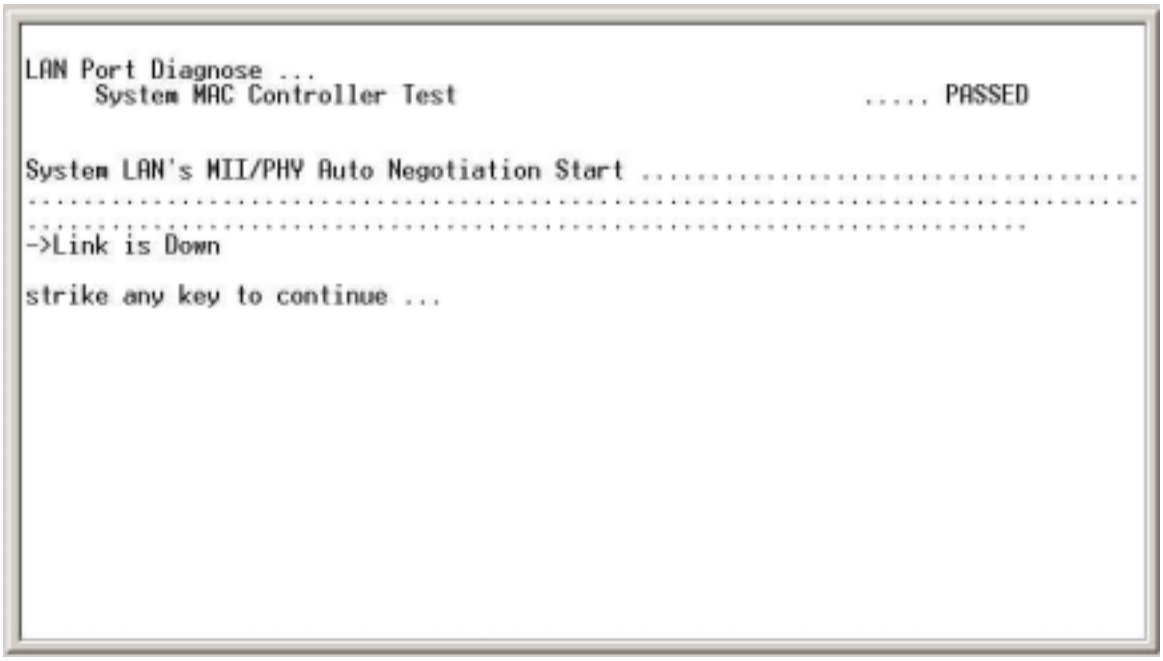


The parameters are described as follows:

- **IPX Net –** This is the IPX network number.
- **Node Address –** This is the node address of the device that the router will attempt to reach. The router will check its routing table and try to locate the IPX Address.
- **Count –** The number of pings (packets) that will be sent.
- **Delay (1 sec) –** The amount of time in 1 second intervals between each ping in the Count.
- **Start Ping Test -** Press <Enter> or <Return> to begin the test.

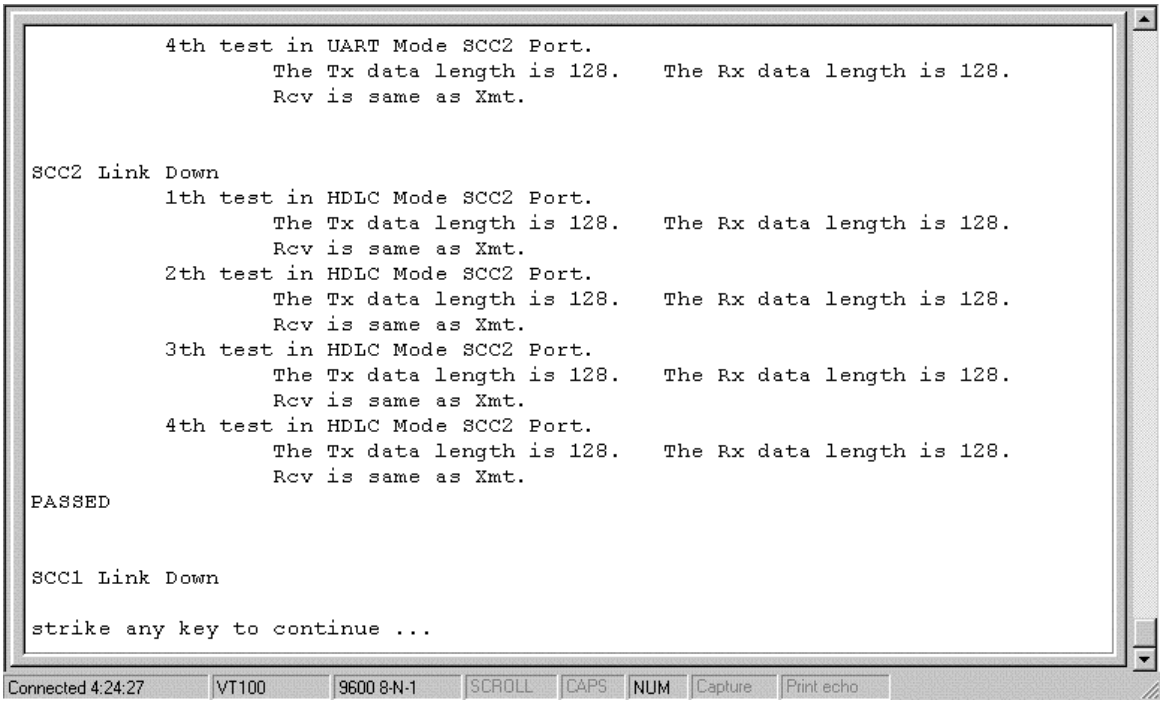
System LAN

The System LAN test is used to diagnose the LAN port. It can only be run if the LAN port is disabled in the **Interface Configuration** submenu.



System WAN

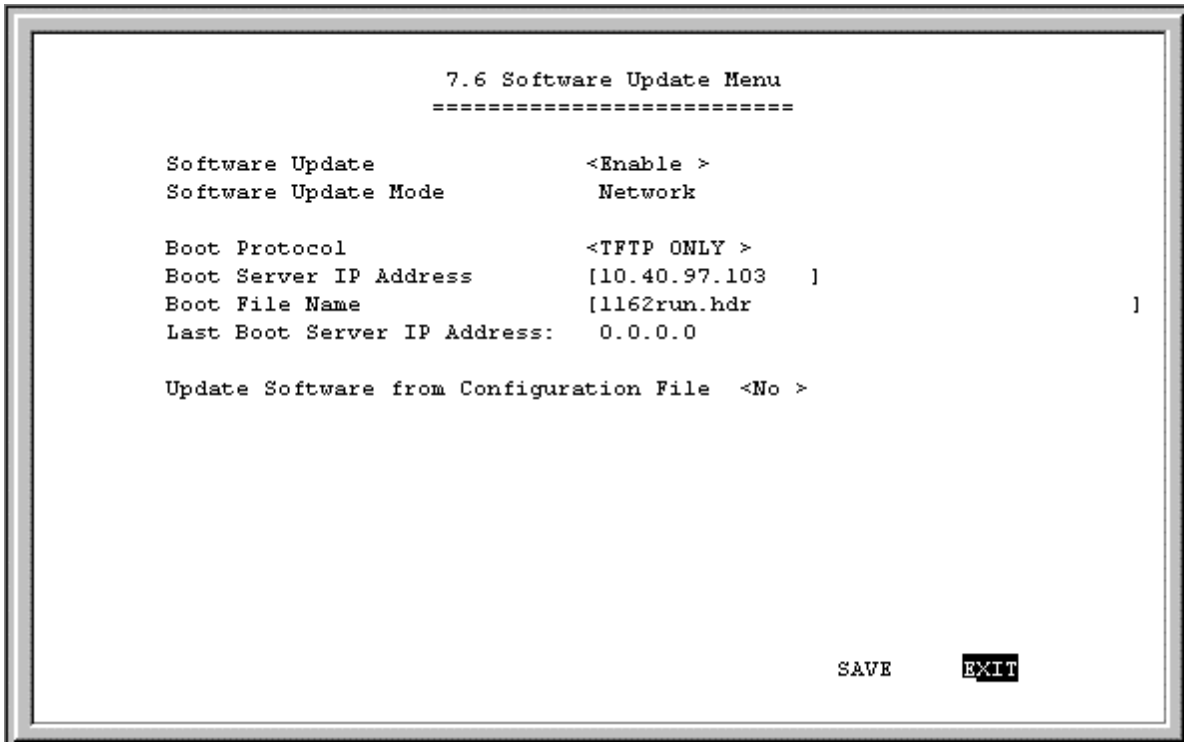
The System WAN test is used to diagnose the WAN port. It can only be run if the WAN port is disabled in the **Interface Configuration** submenu.



Software Update Menu

New routing software can be downloaded from a TFTP server.

If you do not have a TFTP server on your LAN, you can use the included Router Configuration Utility to upgrade the software. This Windows-based utility has a built-in TFTP emulator enabling you to use the computer (connected to the LAN and running the Configuration Utility) to upload the new software to the router.



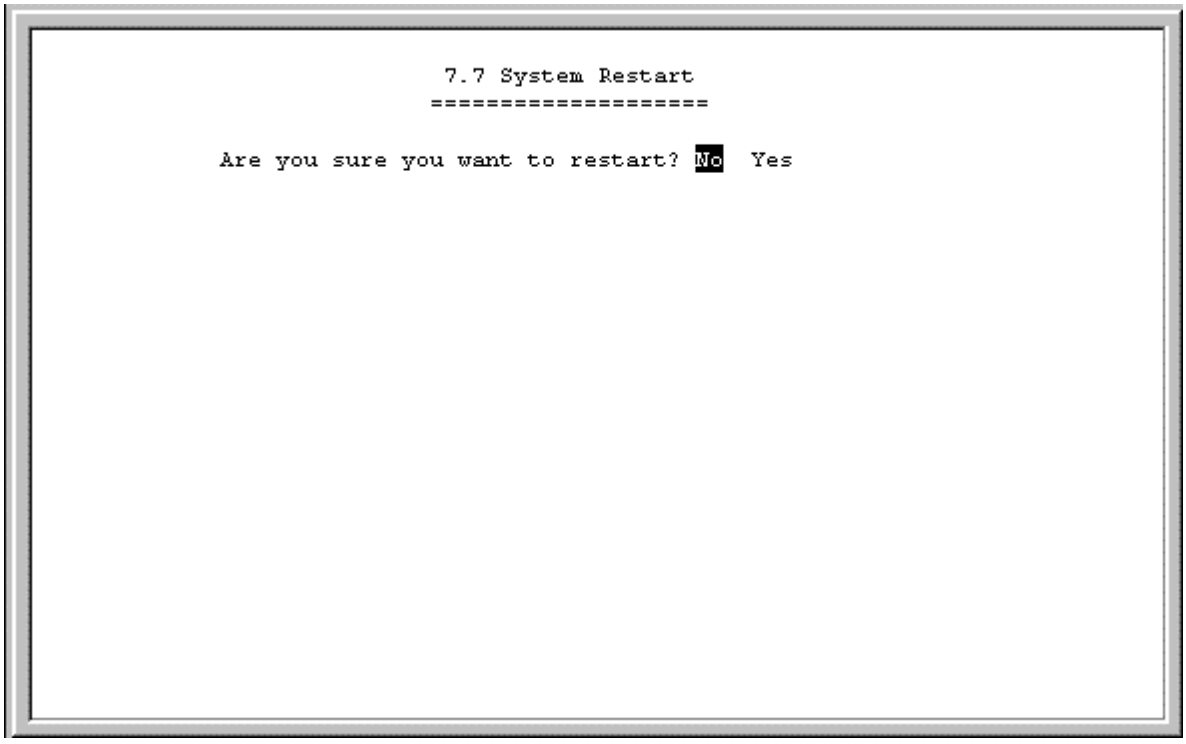
This is the same **Software Update Menu** as in the "*PROM System Configuration"* chapter's **Software Update Menu**. The parameters are described in that section.

Perform a **System Restart** after configuring these settings begins the software update procedure.

System Restart

The system restart function enables you to reset the DI-1162/DI-1162M without powering off. Some settings changes require a system restart in order for them to take effect.

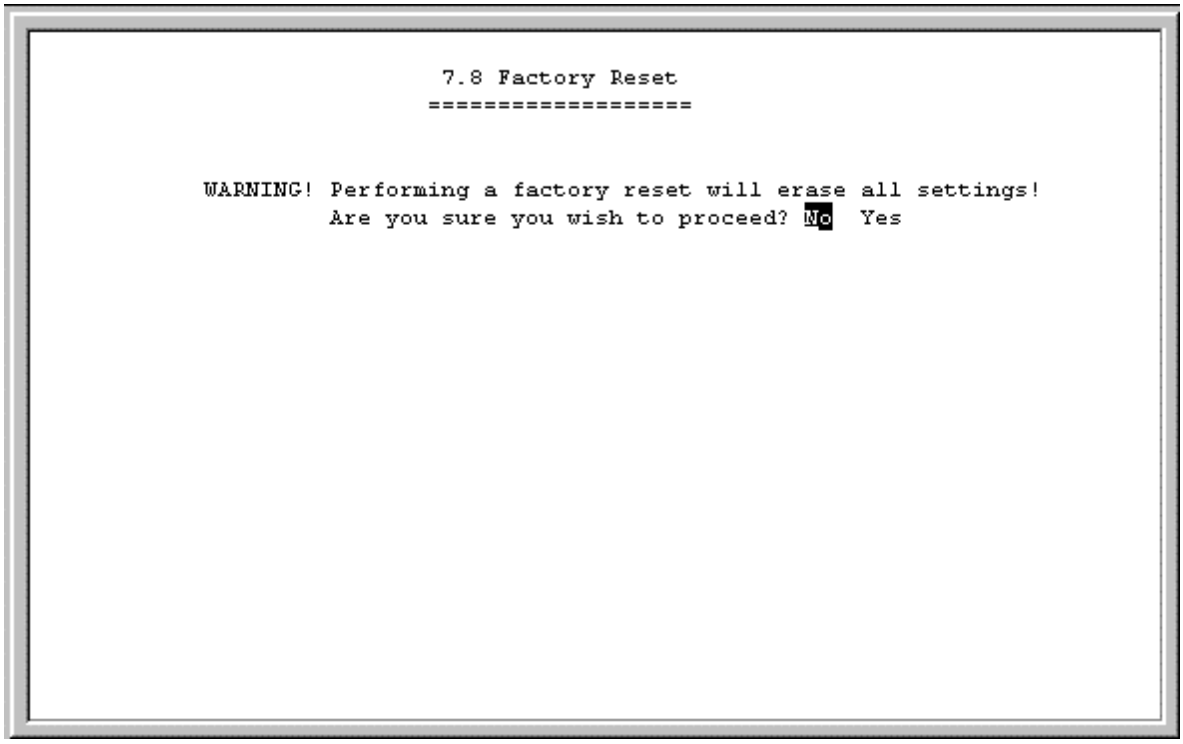
A system restart will not affect the router's settings, but will clear all tables including the routing table and all SNMP counters and tables. It is also used to initiate a software update.



Factory Reset

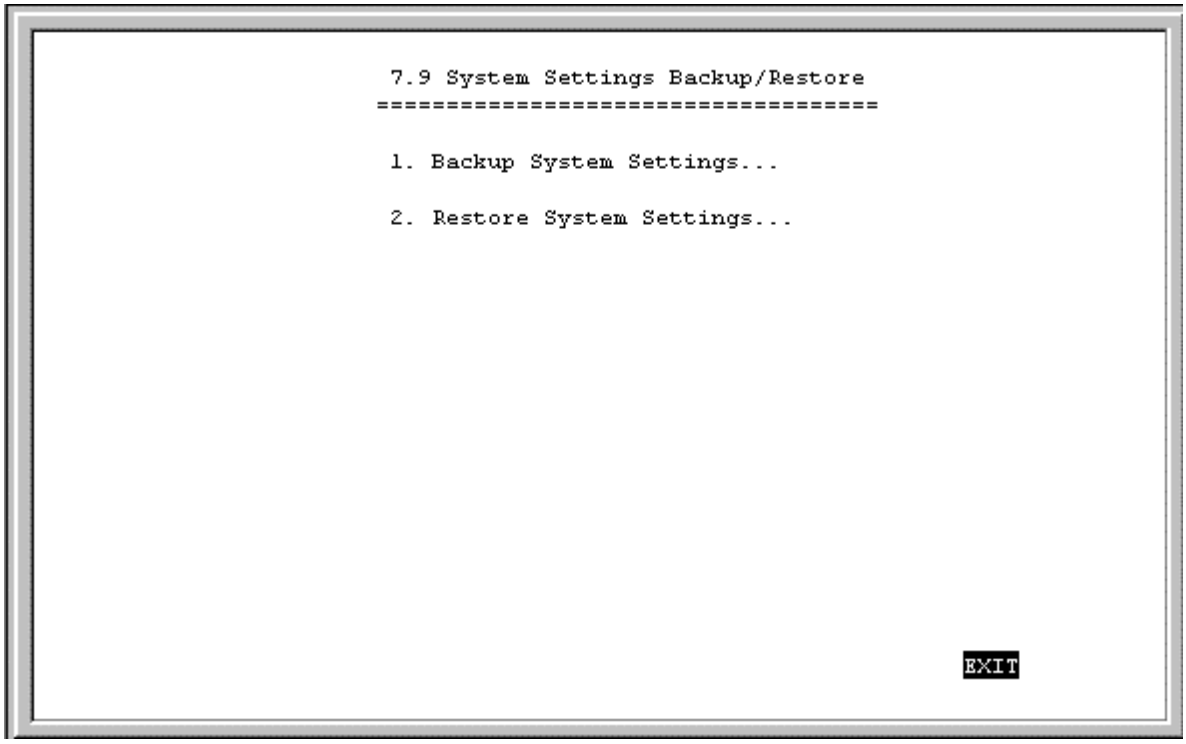
Performing a factory reset erases all settings and tables. All configuration changes ever made to the router will be deleted. The router will be set to the factory defaults it was shipped with and will no longer have an IP address.

Please make sure you wish to wipe out all settings and configure the router from scratch before you perform a factory reset.

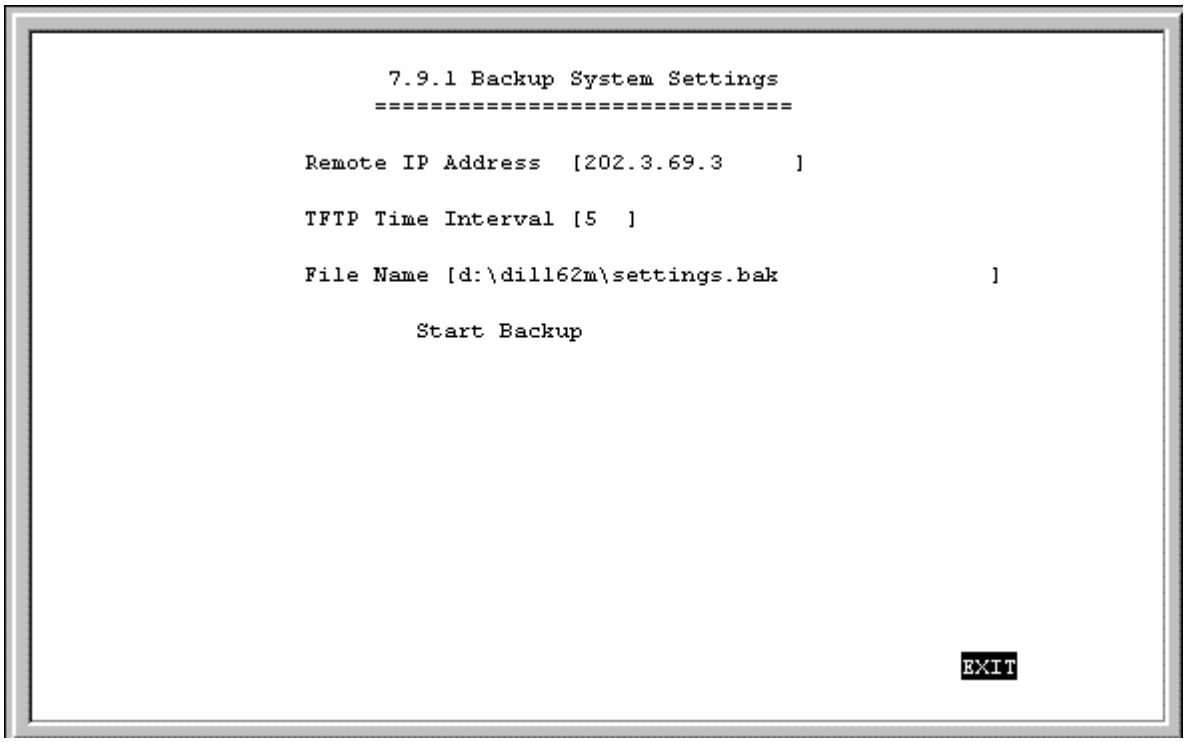


System Settings Backup/Restore

The backup and restore system settings functions are used to backup the router settings. The files created by this process is different than a configuration file or the software update file that are used in the **Software Update Menu**. The files defined here can be used as a backup for all the router settings and can be used to configure another DI-1162/DI-1162M with exactly the same settings, or as a backup before you make major changes to the configuration.



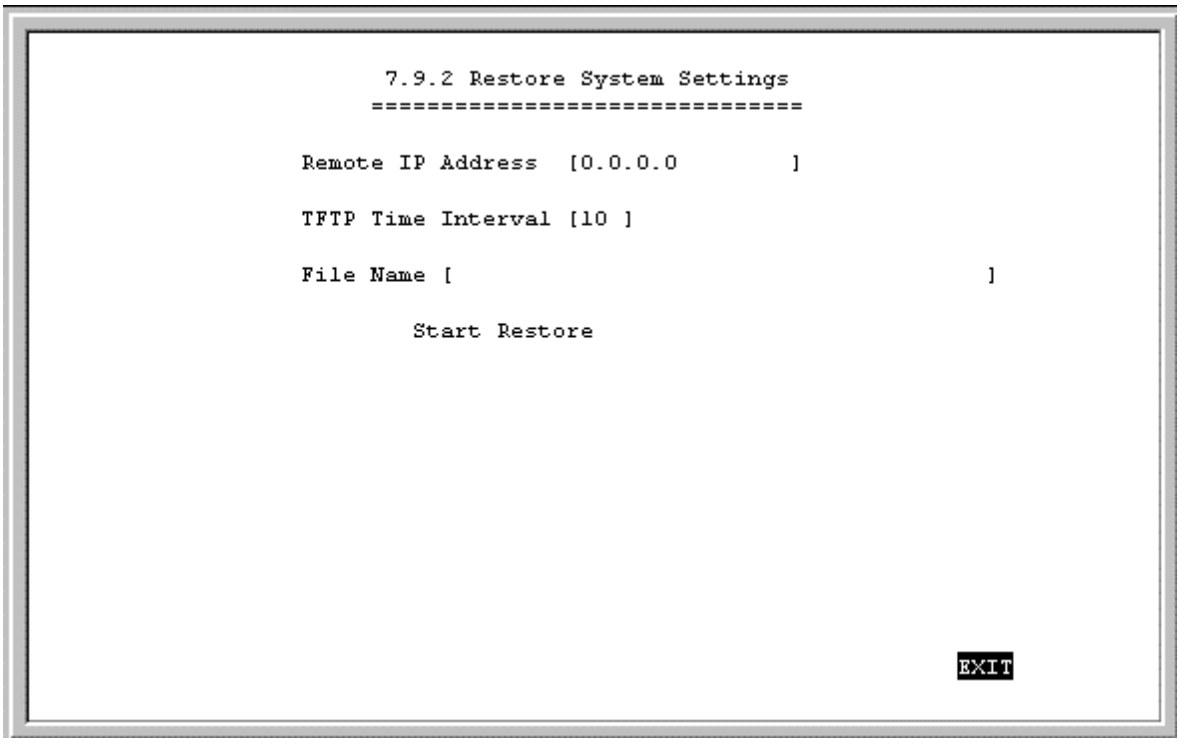
Backup System Settings



Items in the window are described below:

- **Remote IP Address** – This is the IP address of the TFTP server on which you wish to store the settings file.
- **TFTP Time Interval** – The time between requests to occupy TFTP server time. If the router doesn't receive a response (ACK) from the TFTP server within the time interval defined here, it will assume the request has been dropped and send another.
- **File Name** – Specifies the complete path and filename on the TFTP server for the settings file.
- **Start Backup** – Press this to begin the backup procedure.

Backup System Settings



Items in the window are described below:

- **Remote IP Address** – This is the IP address of the TFTP server on which you wish to store the settings file.
- **TFTP Time Interval** – The time between requests to occupy TFTP server time. If the router doesn't receive a response (ACK) from the TFTP server within the time interval defined here, it will assume the request has been dropped and send another.
- **File Name** – Specifies the complete path and filename on the TFTP server for the settings file.
- **Start Restore** – Press this to begin the restore procedure.

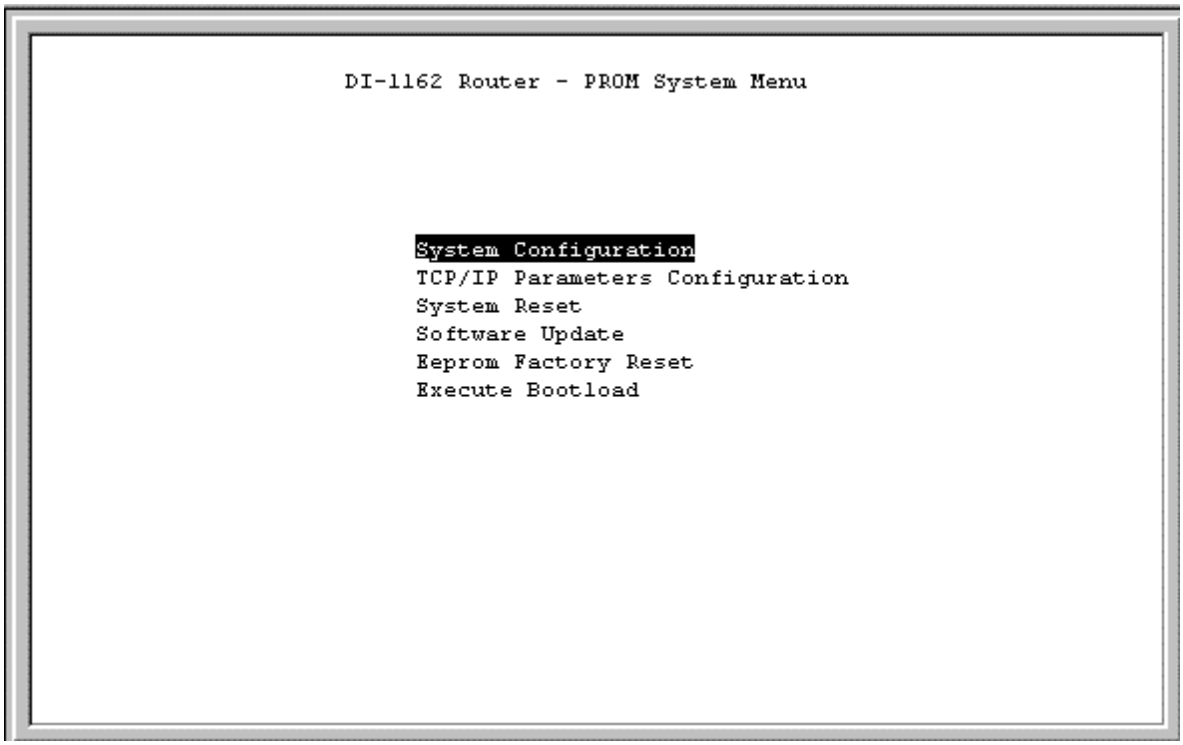
PROM System Configuration

The PROM program is run before the normal console (runtime) configuration program in the router's Flash Memory. Thus, the PROM System Configuration can be used if there are problems with the router's console program.

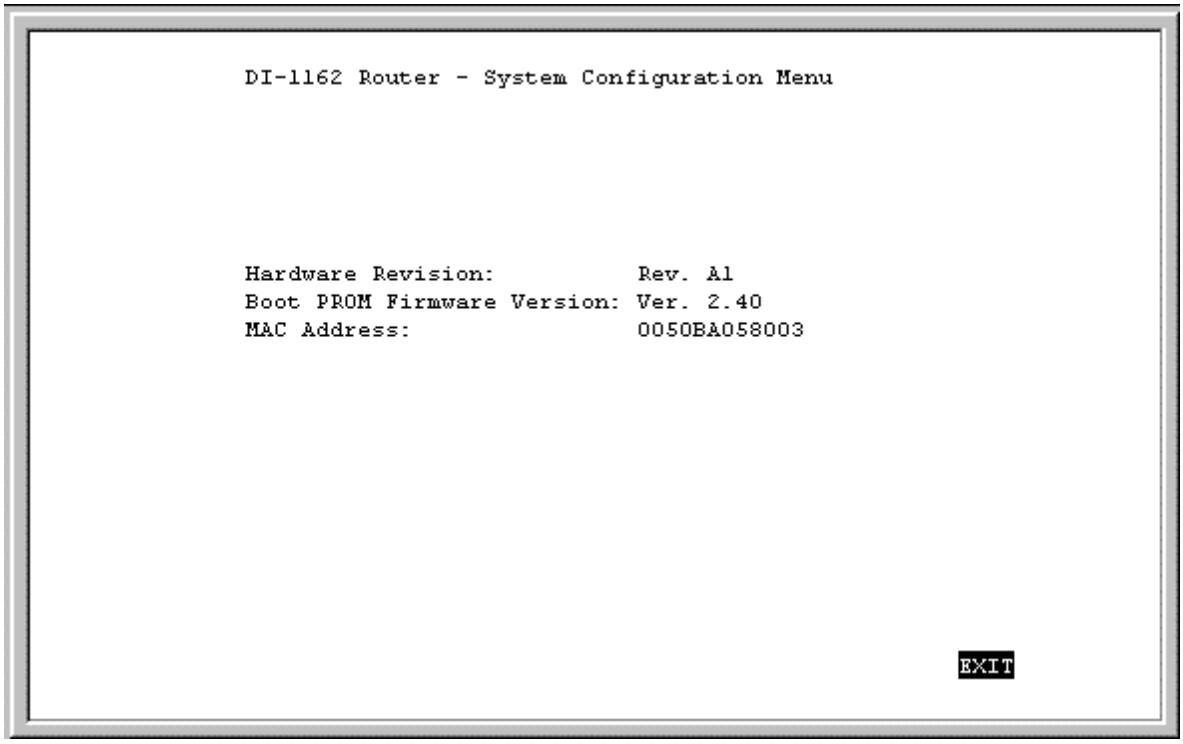
Specifically, the PROM Configuration program has procedures to initialize the administration parameters and the LAN IP address of the router in order to allow the console software in the router's flash memory to be replaced if it has been damaged or deleted.

PROM System Menu

To enter the **PROM System Menu**, press Ctrl-C during the router's POST procedure. The following menu will appear:



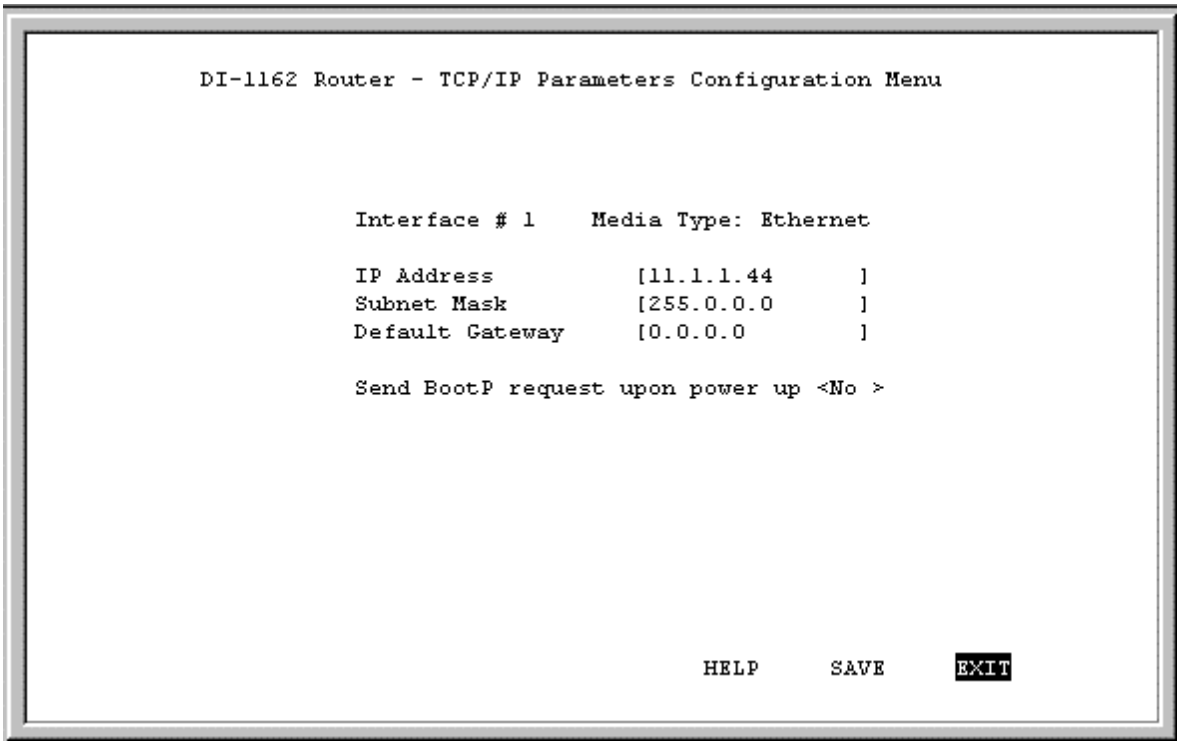
System Configuration Menu



The parameters are described as follows:

- **Hardware Revision –** This is the version ID of hardware used in this router.
- **Boot PROM Firmware Version –** This is the version ID of firmware used in this router.
- **MAC Address –** This is the physical address for this router.

TCP/IP Parameters Configuration Menu



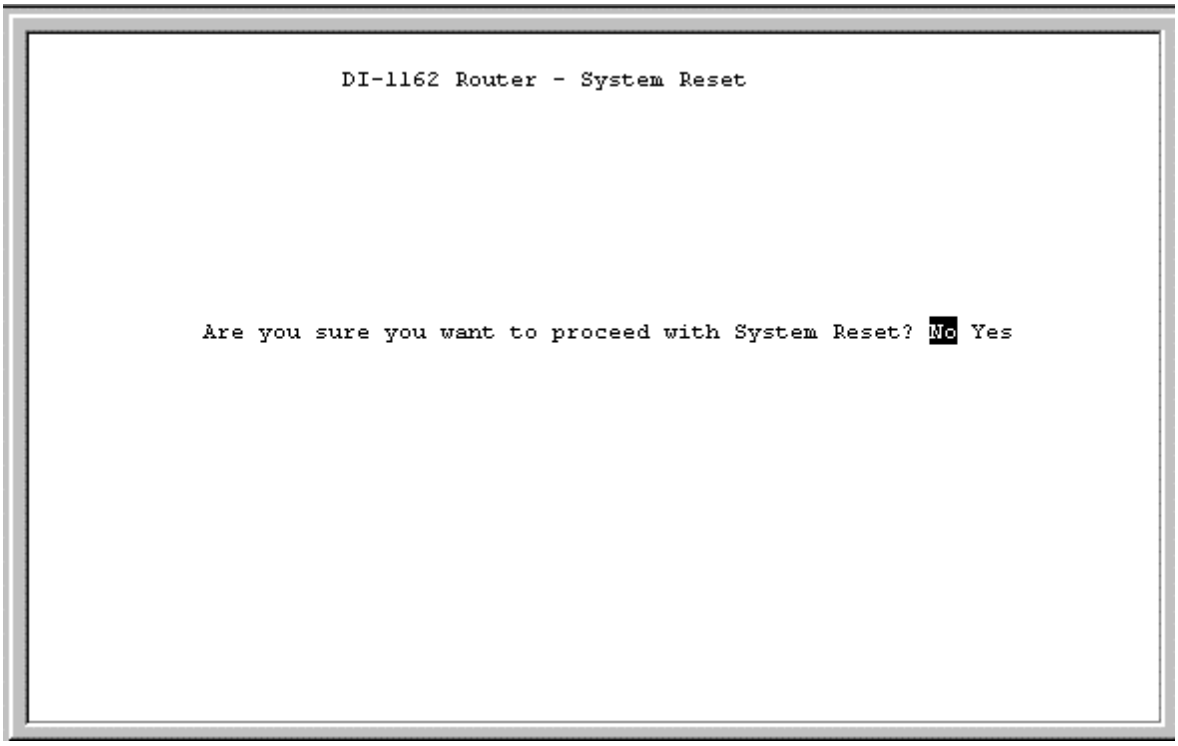
The parameters are described as follows:

- **Interface –** The LAN interface must use Ethernet/Fast Ethernet and is displayed here. This setting cannot be adjusted.
- **IP Address –** This is the router's IP Address for the LAN interface.
- **Subnet Mask –** This mask shows how the LAN is to be divided into network, subnet, and host parts.
- **Default Gateway –** This is the default gateway for the LAN. If this router will be the default gateway for the LAN, then the address should be 0.0.0.0.
- **Send BootP request upon power up –** If set to *Yes*, when the router boots up, it will attempt to acquire the path to the image file, the TFTP server IP Address and the routers own IP Address.

System Reset

The system reset function enables you to reset the DI-1162/DI-1162M without powering off. Some settings changes require a system reset in order for them to take effect.

A system reset will not affect the router's settings, but will clear all tables including the routing table and all SNMP counters and tables. It is also used to initiate a software update.



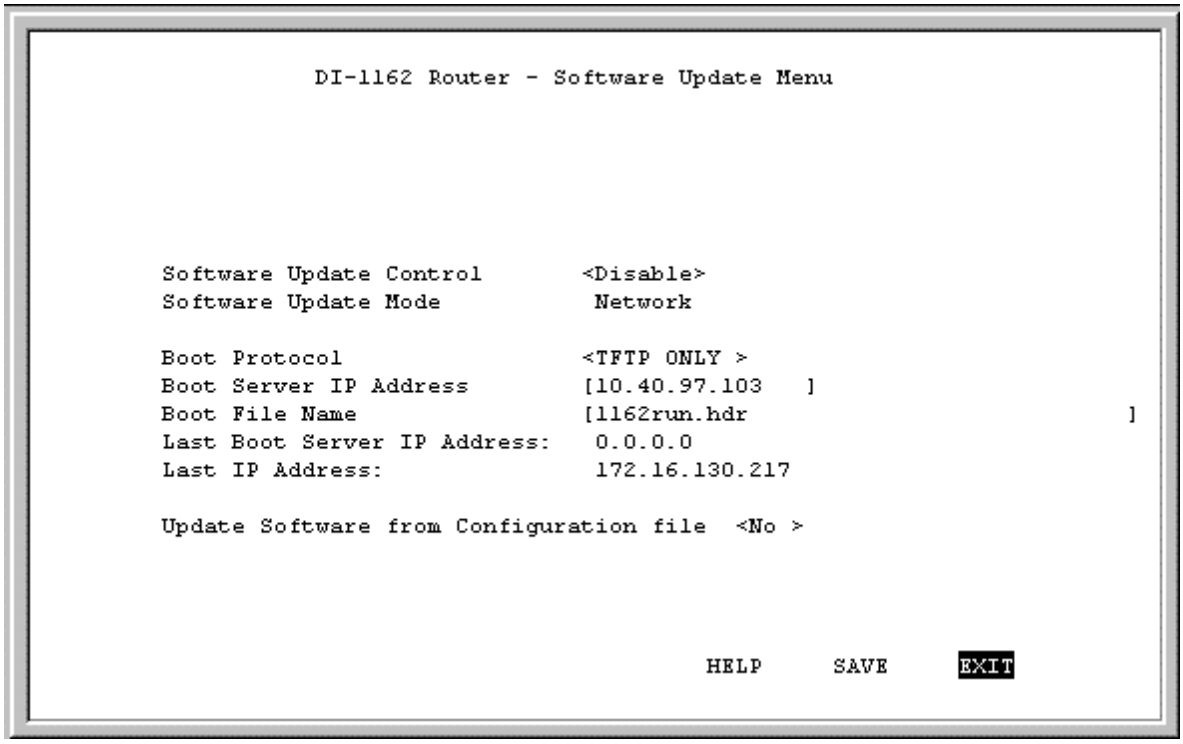
Software Update Menu

The Software Update option is used to change the software in the flash memory of the router. This is the runtime software that is used to configure the router and is described in full in the preceding chapter.

The runtime software should only be updated if you are encountering problems with your current runtime software or you are certain your runtime software is lacking functionality contained in a more recent version.

Downloading new software will only replace the runtime software and will not affect any configuration settings you have made. Upon running the new software, the router will be configured exactly as you had it before downloading the new software.

The runtime software (image file) must be stored on a TFTP server and accessed via the LAN.



Items listed in the above menu are described as follows:

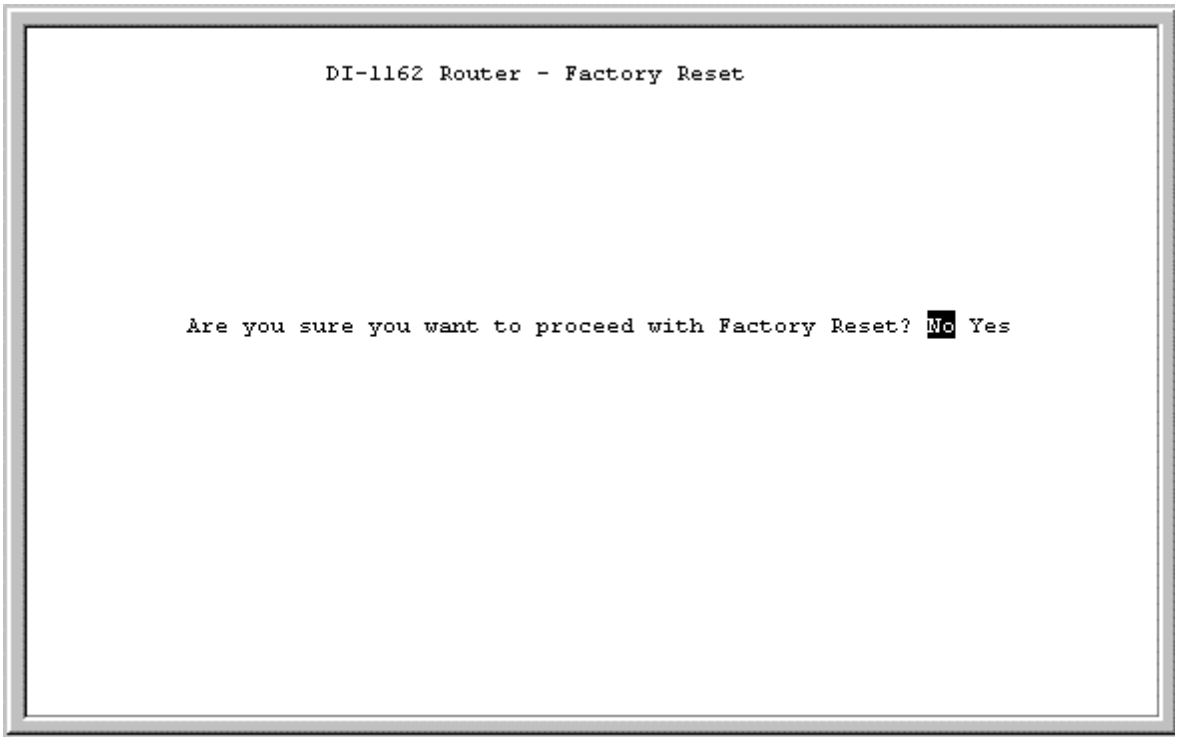
- **Software Update Control –** This toggles *Disable* and *Enable*.
- **Software Update Mode –** This specifies downloading the image file from a Network server on the local LAN.
- **Boot Protocol –** This setting is for a local network download and has two options *TFTP ONLY* and *BOOTP&TFTP*.
  - *TFTP ONLY* **–** A File Transfer Protocol. Using this setting assumes all other items on this screen have been filled out.
  - *BOOTP&TFTP* **–** BootP is run first and sends your router IP Addresses for the TFTP server and the router, and tells the router the path to the software update (image file). Then TFTP will be used to download the image file.
- **Boot Server IP Address –** This specifies the IP address of the server to be used to download the image file.
- **Boot File Name –** This specifies a complete path and filename on the TFTP server. If you choose to use a configuration file, this setting must show the path and filename to the configuration file. If you are not using a configuration file, this must show the path and filename to the software update image file.
- **Last Boot Server IP Address –** This shows the last boot server used to download an image file. This is for reference only.
- **Last IP Address –** This shows the last IP address used for the LAN interface. Again, this is for reference only. The LAN port must have an IP address in order to access the TFTP server via the LAN network.
- **Update Software from Configuration File –** Either *Yes* or *No*. If *Yes*, the software update procedure will try to access a configuration file located at the path defined in the above Boot File Name. Please ensure that the path and file name of the image file is listed in the configuration file. If set to *No*, the update procedure will try to find an image file at the Boot File Name path. Please see "*Appendix E – Configuration File"* for more information about configuration files.

After the parameters are set in the **Software Update Menu**, save the changes, exit, and perform a System Reset or Execute Bootload to begin the software download process.

After the new runtime software has been downloaded, the router will automatically start up using the new software with the Software Update Control setting disabled to avoid a downloading loop.

Factory Reset

Performing a factory reset erases all settings and tables. All configuration changes ever made to the router will be deleted. The router will be set to the factory defaults it was shipped with and will no longer have an IP address.



Please make sure you wish to wipe out all settings and configure the router from scratch before you perform a factory reset.

Execute Bootload

Choosing this option accepts the changes made in the PROM program and begins the router's startup sequence.

Executing a bootload can also begin the Software Update procedure, if enabled.

Using Telnet

The DI-1162/DI-1162M router can be configured and managed using telnet. Telnet accesses the same built-in configuration program as the RS-232 Diagnostic port console connection. As such, all settings that can be adjusted through the console can also be configured using Telnet.

Telnet Configuration

In order to use telnet, the DI-1162/DI-1162M router must first be configured using a console connected to the RS-232 Diagnostic port. Depending on the placement of the management station using telnet, the initial configuration requirements for the router are as follows:

Using Telnet via LAN

Preparing the router for management by telnet over the LAN only requires enabling the LAN port, enabling telnet, and assigning the LAN port an IP address. To do this:

1. Connect a console to the RS-232 Diagnostic port on the front panel of the router and run a terminal emulation program (for more information, see *Connecting the Console to the Router* and *Setting Up the Console* sections of this manual).

2. Enable the LAN port in the **Interface Configuration** submenu.

3. Assign an IP address to the LAN port in the **Network Configuration** submenu.

4. Enable Telnet in the **Advanced Functions** submenu.

5. Connect the router to the LAN.

The router can now be accessed via the LAN by the included Windows-based Configuration program, Telnet and SNMP management applications. For more detailed information regarding these procedures, please refer to the *Connecting the Router* section of this manual. For more information about the submenus, please refer to the *Configuration and Management* section of this manual.

Using Telnet via WAN

Preparing the router for management by telnet over WAN lines requires more initial configuring of the router via the console.

To do this, you must configure a WAN port for dial-in users. Please refer to *Step 3b - Configuring the WAN Ports for Dial-in, Dial-out and Leased Lines* section on page 10 of this manual.

System Timeout

When you are connected to your DI-1162/DI-1162M via Telnet, there is a system timeout (in the **System Information** submenu), adjustable to a maximum of 90 minutes. If you are logged onto the device and leave it inactive for this timeout period, the router will automatically disconnect you.

Using RADIUS Authentication

In addition to the dial-in 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 or Windows NT-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

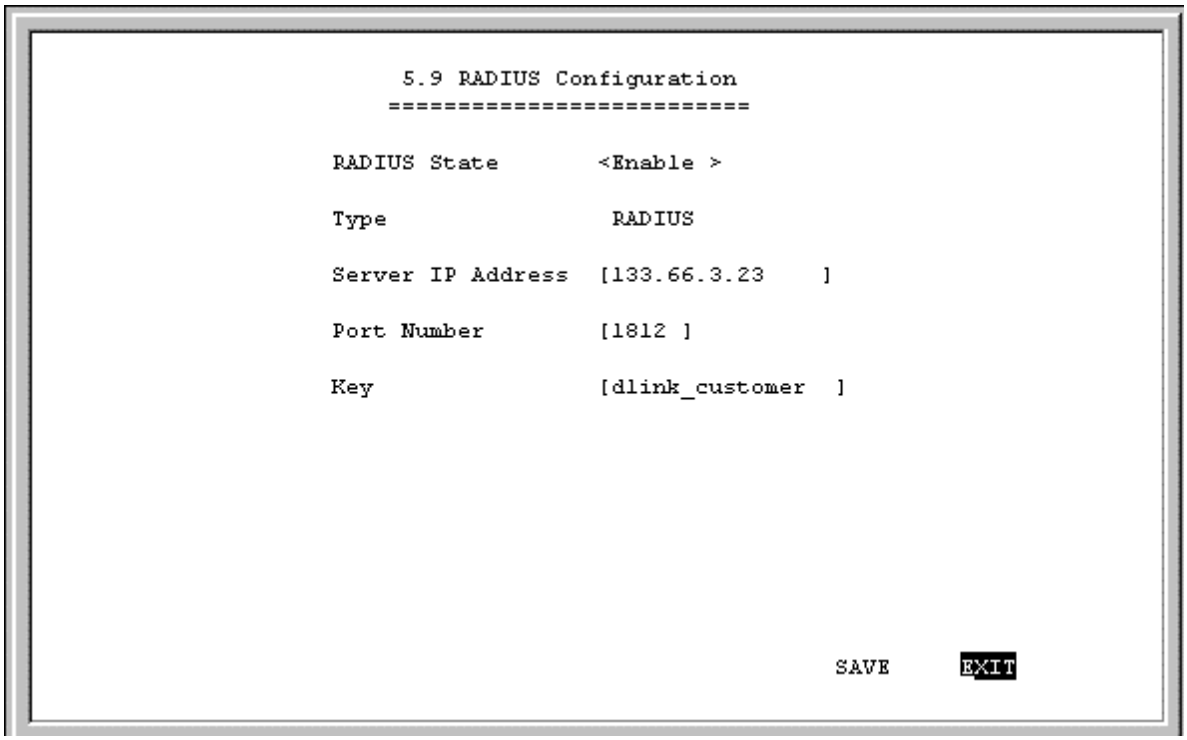
http://www.livingston.com/marketing/products/radius.html

or at:

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

Configuring the DI-1162/DI-1162M for RADIUS Authentication

To configure the DI-1162/DI-1162M to use the RADIUS server set up in the previous section, go to the **Main Menu** in the console program and choose **Advanced Functions** and then **RADIUS Configuration**.



Items in the above submenu are described as follows:

- **RADIUS State –** Enables or disables RADIUS.
- **Type –** Refers to the type of external password protocol. Currently, only RADIUS is supported.
- **Server IP Address –** This is the IP Address of your UNIX or NT-based RADIUS server.
- **Port –** The port number for the RADIUS server. The standard port number specified by RFC 1700 is 1812 (shown above).
- **Key –** This is a shared secret used to identify the DI-1162/DI-1162M as a valid RADIUS client.

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-1162/DI-1162M, 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-1162/DI-1162M will use it to authenticate all users instead of checking it's internal Dial-Up User Profile.

Adding Users to the RADIUS Database

The DI-1162/DI-1162M only uses the RADIUS database for user authentication; except for Password and User Name. Most standard RADIUS attribute fields are ignored by the DI-1162/DI-1162M.

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.

Appendix A – Cables and Connectors

RS-232 (EIA-574) for Diagnostic Port

Pin	Signal Name	Mnemonic	Source
1	Recv. Line Sig. Det. (DCD)	109	DCE
2	Received Data	104	DCE
3	Transmitted Data	103	DTE
4	DTE Ready (DTR)	108	DTE
5	Signal Ground	102	-
6	DCE Ready (DSR)	107	DCE
7	Request to Send	105/133	DTE
8	Clear to Send	106	DCE
9	Ring Indicator	125	DCE

End Connector: DB-9 Pin Male
Cable Length: 1.5 m

RS-232 (EIA-530) Cable for WAN Port

DB25 Female Pin Number	DB25 Male Pin Number	Signal Name	Mnemonic	Source
1	1	Protective Ground	-	-
2	2	TXD	BA	DTE
3	3	RXD	BB	DCE
4	4	RTS	CA	DTE
5	5	CTS	CB	DCE
6	6	DSR	CC	DCE
7	7	Signal Ground	AB	-
8	8	Rec. Line Signal Det.	CF	DCE
9	9	RXD CLK	DD	DCE
10	10	Rec. Line Signal Det.	CF	DCE
11	11	TXD CLK	DA	DTE
12	12	TXD CLK	DB	DCE
13	13	CTS	CB	DCE
14	14	TXD	BA	DTE
15	15	TXD CLK	DB	DCE
16	16	RXD	BB	DCE
17	17	RXD CLK	DD	DCE
18	18	Local Loopback	LL	DTE
19	19	RTS	CA	DTE
20	20	DTR	CD	DTE
21	21	Remote Loopback	RL	DTE
22	22	DSR	CC	DCE
23	23	DTR	CD	DTE
24	24	TXD CLK	DA	DTE
25	25	Test Mode	TM	DCE

End Connector: DB-25 Pin Female (ISO-2110)
DB-25 Pin Male (ISO-2110)
Cable Length: 1.5M

RS-449 Cable for WAN Port

DB25 Female Pin Number	DB37 Male Pin Number	Signal Name	Mnemonic	Source
1	1	Protective Ground	-	-
2	4	TXD	BA	DTE
3	6	RXD	BB	DCE
4	7	RTS	CA	DTE
5	9	CTS	CB	DCE
6	11	DSR	CC	DCE
7	19	Signal Ground	AB	-
8	13	Rec. Line Signal Det.	CF	DCE
9	26	RXD CLK	DD	DCE
10	31	Rec. Line Signal Det.	CF	DCE
11	35	TXD CLK	DA	DTE
12	23	TXD CLK	DB	DCE
13	27	CTS	CB	DCE
14	22	TXD	BA	DTE
15	5	TXD CLK	DB	DCE
16	24	RXD	BB	DCE
17	8	RXD CLK	DD	DCE
18	10	Local Loopback	LL	DTE
19	25	RTS	CA	DTE
20	12	DTR	CD	DTE
21	14	Remote Loopback	RL	DTE
22	29	DSR	CC	DCE
23	30	DTR	CD	DTE
24	17	TXD CLK	DA	DTE
25	18	Test Mode	TM	DCE

End Connector: DB-25 Pin Female (ISO-2110)
DB-37 Pin Male
Cable Length: 1.5 m

V.35 Cable for WAN Port

DB25 Female Pin Number	V.35 Male Pin Number	Signal Name	Mnemonic	Source
1	A	Protective Ground	-	-
2	P	TXD	103	DTE
3	R	RXD	104	DCE
4	C	RTS	105	DTE
5	D	CTS	106	DCE
6	E	DSR	107	DCE
7	B	Signal Ground	102	-
8	F	Rec. Line Signal Det.	109	DCE
9	X	RXD CLK	115	DCE
10				
11	W	TXD CLK	113	DTE
12	AA	TXD CLK	114	DCE
13				
14	S	TXD	103	DTE
15	Y	TXD CLK	114	DCE
16	T	RXD	104	DCE
17	V	RXD CLK	115	DCE
18				
19				
20	H	DTR	108	DTE
21				
22				
23				
24	U	TXD CLK	113	DTE
25				

End Connector: DB-25 Pin Female (ISO-2110)
V.35 Male 34 Pin (ISO-2593)
Cable Length: 1.5 m

Appendix B – Specifications

General	
Network Protocols:	IP (Internet Protocol)
WAN Protocols:	PPP (Point-to-Point Protocol) Multi-Link PPP, SLIP, HDLC, Frame Relay
Routing Protocols:	RIP 1 and RIP 2, DVMRP, IGMP, OSPF; IPX and Bridge (DI-1162M only)
Management:	Local RS-232 Console Port (out-of-band) Telnet (in-band) SNMP MIB II and Enterprise MIB
Memory: Flash Memory System Memory	 4MB 16 MB DRAM
No. of Ports and Type: WAN LAN Add-on Module Slot:	 2 DB-25 Ports 1 RJ-45 Port 1 LAN, 2 WAN, 1 ISDN (BRI)
WAN Interface: 2 EIA-530 DTE Ports	 Async/sync, V.35, RS-232, RS-449
WAN Speeds (max): Async Sync	 115.2 Kbps T1/E1 (2.048 Mbps)
LAN Interface: 1 RJ-45 Port	 10/100M Auto-negotiation Full/Half Duplex Ethernet/Fast Ethernet

Physical and Environmental	
Weight:	3.3 kg (7.26 lbs)
Dimensions (W x D x H):	441 x 236 x 55 mm (17 x 9.3 x 2 inches)
Operating Temperature:	0° to 50° C (32° to 122° F)
Humidity:	5% to 95% (non-condensing)
Power:	100 ~ 240 VAC 50 ~ 60 Hz
EMI:	FCC Class A, CE Mark Class A, BSMI Class A, C-Tick Class A
Safety:	UL (1950), CSA (950)

Appendix C - IP Concepts

This appendix describes some basic IP concepts, the TCP/IP addressing scheme and show how to assign IP Addresses.

When setting up the router, you must make sure all ports to be utilized on the router have valid IP addresses. Even if you will not use the WAN ports, you should, at the very least, make sure the LAN port is assigned a valid IP address. This is required for telnet, in-band SNMP management, and related functions such as “trap” handling and TFTP firmware download.

IP Addresses

The Internet Protocol (IP) was designed for routing data between network sites all over the world, and was later adapted to allow routing between networks (often referred to as “subnets”) within any site. IP includes a system by which a unique number can be assigned to each of the millions of networks and each of the computers on those networks. Such a number is called an IP address.

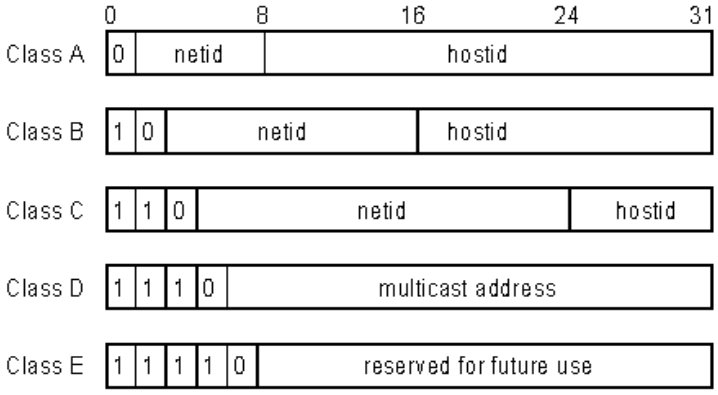
To make IP addresses easy to understand, the originators of IP adopted a system of representation called “dotted decimal” or “dotted quad” notation. Below are examples of IP addresses written in this format:

201.202.203.204 189.21.241.56 125.87.0.1

Each of the four values in an IP address is the ordinary decimal (base 10) representation of a value that a computer can handle using eight “bits” (binary digits — 1s and 0s). The dots are simply convenient visual separators.

Zeros are often used as placeholders in dotted decimal notation; 189.21.241.56 can therefore also appear as 189.021.241.056.

IP networks are divided into three classes on the basis of size. A full IP address contains a network portion and a “host” (device) portion. The network and host portions of the address are different lengths for different classes of networks, as shown in the table below.



Networks attached to the Internet are assigned class types that determine the maximum number of possible hosts per network. The previous figure illustrates how the net and host portions of the IP address differ among the three classes. Class A is assigned to networks that have more than 65,535 hosts; Class B is for networks that have 256 to 65534 hosts; Class C is for networks with less than 256 hosts.

IP Network Classes

Class	Maximum Number of Networks in Class	Network Addresses (Host Portion in Parenthesis)	Maximum Number of Hosts per Network
A	126	1(.0.0.0) to 126(.0.0.0)	16,777,214
B	16,382	128.1(.0.0) to 191.254(.0.0)	65,534
C	2,097,150	192.0.1(.0) to 223.255.254(.0)	254

Note: All network addresses outside of these ranges (Class D and E) are either reserved or set aside for experimental networks or multicasting.

When an IP address's host portion contains only zero(s), the address identifies a network and not a host. No physical device may be given such an address.

The network portion must start with a value from 1 to 126 or from 128 to 223. Any other value(s) in the network portion may be from 0 to 255, except that in class B the network addresses 128.0.0.0 and 191.255.0.0 are reserved, and in class C the network addresses 192.0.0.0 and 223.255.255.0 are reserved.

The value(s) in the host portion of a physical device's IP address can be in the range of 0 through 255 as long as this portion is not all-0 or all-255. Values outside the range of 0 to 255 can never appear in an IP address (0 to 255 is the full range of integer values that can be expressed with eight bits).

The network portion must be the same for all the IP devices on a discrete physical network (a single Ethernet LAN, for example, or a WAN link). The host portion must be different for each IP device — or, to be more precise, each IP-capable port or interface — connected directly to that network.

The network portion of an IP address will be referred to in this manual as a **network number**; the host portion will be referred to as a **host number**.

To connect to the Internet or to any private IP network that uses an Internet-assigned network number, you must obtain a registered IP network number from an Internet-authorized network information center. In many countries you must apply through a government agency, however they can usually be obtained from your Internet Service Provider (ISP).

If your organization's networks are, and will always remain, a closed system with no connection to the Internet or to any other IP network, you can choose your own network numbers as long as they conform to the above rules.

If your networks are isolated from the Internet, e.g. only between your two branch offices, you can assign any IP Addresses to hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP Addresses specifically for private (stub) networks:

Class	Beginning Address	Ending Address
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

It is recommended that you choose private network IP Addresses from the above list. 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*.

Subnet Mask

In the absence of subnetworks, standard TCP/IP addressing may be used by specifying subnet masks as shown below.

IP Class	Subnet Mask
Class A	255.0.0.0
Class B	255.255.0.0
Class C	255.255.255.0

Subnet mask settings other than those listed above add significance to the interpretation of bits in the IP address. The bits of the subnet mask correspond directly to the bits of the IP address. Any bit an a subnet mask that is to correspond to a net ID bit in the IP address must be set to 1.

Appendix D – IP Protocol and Port Numbers

Common Internet service protocols and IP port numbers.

IP Protocol Numbers

Protocol #	Protocol Name	Description
1	ICMP	Internet Control Message [RFC792]
2	IGMP	Internet Group Management [RFC1112]
6	TCP	Transmission Control [RFC793]
8	EGP	Exterior Gateway Protocol [RFC888,DLM1]
9	IGP	any private interior gateway [IANA] (used by Cisco for their IGRP)
17	UDP	User Datagram [RFC768,JBP]
46	RSVP	Reservation Protocol [Bob Braden]
88	EIGRP	EIGRP [CISCO,GXS]
115	L2TP	Layer Two Tunneling Protocol [Aboba]

IP Port Numbers

Service	TCP	UDP	Notes
FTP	21		File Transfer
Telnet	23		
SMTP	25		Simple Mail Transfer
DNS	53	53	Domain Name Server
Finger	79		
WWWHTTP	80		World Wide Web HTTP
POP3	110		Post Office Protocol – Version 3
NetBios- ns	137	137	NetBios Name Service
NetBios – dgm	138	138	NetBios Datagram Service
NetBios – ssn	139	139	NetBios Session Service
SNMP		161	
SNMP Trap		162	

Appendix E – Configuration File

The router can be configured when performing a Software Update through a configuration file.

The configuration file can hold many settings for the router including IP Addresses for all ports, path to the boot server, and various port settings.

The configuration file is very useful if you wish to update your software and keep all or most of your settings the same.

The configuration file should be saved with the extension .SYS in the same directory as the runtime image file (software update file).

An example configuration file is shown below. Please note that:

: Comment. This line describes the actual configuration in the next line. You can also use this feature to mask items you don't need to be configured (rather than deleting them).

Format: Keyword <Space> Parameter. For example the very last line:

ip-stat disable

ip-stat is the keyword as explained in the # (comment) line above as meaning IP routing statistics.

disable is the parameter you set.

Configuration File Example

```
# The system configuration file for D-Link DI-1162 Remote Access Router

# DI-1162 runtime image file name (software update path and file name)
di1162-image d:\project\di1162\runtime\image\1162run\1162run.hdr

# sysname (string name)
sysname DI-1162 Remote Access Router
# syscontact (string name)
syscontact Engineering Administrater
# syslocation (string name)
syslocation No 8 Lihsing Road VII 5th floor
# systimeout setting in minutes (0 means no timeout)
systimeout 10
# telnet stat (enable/disable)
telnet enable
# ip routing stack (enable/disable)
ip-routing enable

# interface decription (string name)
lan-port-1 System Lan Interface
# port stat (enable/disable)
port-stat enable
# ip address
ip-address 202.39.74.119
# subnet mask
ip-netmask 255.255.255.0
# routing protocol type (0:RIPv1, 1:RIPv2, 2:RIPv1&2)
routing-type 2
# routing operating mode (0:None, 1:Listen, 2:Talk, 3:Both)
operating-mode 0
# ip routing stat (enable/disable)
ip-stat enable

# interface decription (string name)
lan-port-2 Option Lan Interface
# port stat (enable/disable)
port-stat disable
# ip address
```

```
ip-address 10.19.88.1
# subnet mask
ip-netmask 255.255.255.0
# routing protocol type (0:RIPv1, 1:RIPv2, 2:RIPv1&2)
routing-type 0
# routing operating mode (0:None, 1:Listen, 2:Talk, 3:Both)
operating-mode 1
# ip routing stat (enable/disable)
ip-stat disable

# interface decription (string name)
wan-port-1 WAN SCC 1 Interface
# interface protocol type (0:SLIP, 1:HDLC, 2:SyncPPP, 3:AsyncPPP)
protocol-type 0
# modem initial string (initial string name, SLIP/AsyncPPP only)
modem-init AT&FS0=1X1
# dial phone number (phone number string, SLIP/AsyncPPP only)
phone-num 5779110-6403
# baud rate (baud rate, SLIP/AsyncPPP only)
# (0:9600, 1:19200, 2:38400, 3:57600, 4:115200)
baud-rate 0
# port stat (enable/disable)
port-stat disable
# ip address
ip-address 20.19.88.1
# subnet mask
ip-netmask 255.255.255.0
# routing protocol type (0:RIPv1, 1:RIPv2, 2:RIPv1&2)
routing-type 1
# routing operating mode (0:None, 1:Listen, 2:Talk, 3:Both)
operating-mode 2
# ip routing stat (enable/disable)
ip-stat disable

# interface decription (string name)
wan-port-2 WAN SCC 2 Interface
# interface protocol type (0:SLIP, 1:HDLC, 2:SyncPPP, 3:AsyncPPP)
protocol-type 1
# port stat (enable/disable)
port-stat disable
# ip address
ip-address 40.19.88.1
# subnet mask
ip-netmask 255.255.255.0
# routing protocol type (0:RIPv1, 1:RIPv2, 2:RIPv1&2)
routing-type 2
# routing operating mode (0:None, 1:Listen, 2:Talk, 3:Both)
operating-mode 3
# ip routing stat (enable/disable)
ip-stat disable
```

Index

D-Link Offices

AUSTRALIA — **D-LINK AUSTRALASIA**
Unit 16, 390 Eastern Valley Way Roseville, NSW 2069 Australia
TEL: 61-2-9417-7100 FAX: 61-2-9417-1077 TOLL FREE (Australia): 1800 177 100 TOLL FREE (New Zealand): 0800-900900
URL: www.dlink.com.au E-MAIL: support@dlink.com.au & info@dlink.com.au

CANADA — **D-LINK CANADA**
2180 Winston Park Drive, Oakville, Ontario, L6H 5W1 Canada
TEL: 1-905-829-5033 FAX: 1-905-829-5223 BBS: 1-965-279-8732 TOLL FREE: 1-800-354-6522
URL: www.dlink.ca FTP: ftp.dlinknet.com E-MAIL: techsup@dlink.ca

DENMARK — **D-LINK DENMARK**
Naverland 2 DK-2600 Glostrup Copenhagen, Denmark
TEL:45-43-969040 FAX:45-43-424347 URL: www.dlink.dk E-MAIL: info@dlink.dk

EGYPT — **D-LINK MIDDLE EAST**
7 Assem Ben Sabet Street, Heliopolis Cairo, Egypt
TEL: 202-245-6176 FAX: 202-245-6192 URL: www.dlink-me.com E-MAIL: support@dlink-me.com & fateen@dlink-me.com

FRANCE — **D-LINK FRANCE**
Le Florilege #2, Allee de la Fresnerie, 78330 Fontenay le Fleury, France
TEL: 33-1-3023-8688 FAX: 33-1-3023-8689 URL: www.dlink-france.com E-MAIL: info@dlink-france.fr

GERMANY — **D-LINK GERMANY**
Bachstrae 22, D-65830 Kriftel, Germany
TEL: 49-(0)6192-97110 FAX: 49-(0)6192-9711-11 URL: www.dlink.de BBS: 49-(0)6192-971199 (analog)
BBS: 49-(0)6192-971198 (ISDN) INFO: 00800-7250-0000 (toll free) HELP: 00800-7250-4000 (toll free)
REPAIR: 00800-7250-8000 E-MAIL: mbischoff@dlink.de & mboerner@dlink.de

INDIA — **D-LINK INDIA**
Plot No.5, Kurla-Bandra Complex Rd., Off Cst Rd., Santacruz (E) Bombay - 400 098 India
TEL: 91-22-652-6696 FAX: 91-22-652-8914 URL: www.dlink-india.com E-MAIL: service@dlink.india.com

ITALY — **D-LINK ITALY**
Via Nino Bonnet n.6/b, 20154 Milano, Italy
TEL: 39-02-2900-0676 FAX: 39-02-2900-1723 URL: www.dlink.it E-MAIL: info@dlink.it

JAPAN — **D-LINK TOKYO**
10F, 8-8-15 Nishi-Gotanda, Shinagawa-ku, Tokyo 141 Japan
TEL: 81-3-5434-9678 FAX: 81-3-5434-9868 URL: www.d-link.co.jp E-MAIL: kida@d-link.co.jp

SINGAPORE — **D-LINK INTERNATIONAL/D-LINK SINGAPORE**
1 International Business Park, #03-12 The Synergy, Singapore 609917
TEL : 65-774-6233 FAX: 65-774-6322 E-MAIL: info@dlink.com.sg URL: www.dlink-intl.com

SWEDEN — **D-LINK SWEDEN**
P. O. Box 15036, S-167 15 Bromma, Sweden
TEL: 46-(0)8564-61900 FAX: 46-(0)8564-61901 E-MAIL: info@dlink.se URL: www.dlink.dk

TAIWAN — **D-LINK TAIWAN**
2F, No. 119 Pao-Chung Rd, Hsin-Tien, Taipei, Taiwan, R.O.C.
TEL: 886-2-2910-2626 FAX: 886-2-2910-1515 URL: www.dlinktw.com.tw E-MAIL: dssqa@tsc.dlinktw.com.tw

U.K. — **D-LINK EUROPE/D-LINK U.K.**
4th Floor, Merit House, Edgeware Road, Colindale, London NW9 5AB U.K.
TEL: 44 (0) 20-8731-5555 FAX: 44 (0) 20-8731-5511 URL: www.dlink.co.uk E-MAIL: info@dlink.co.uk

U.S.A. — **D-LINK U.S.A.**
53 Discovery Drive, Irvine, CA 92618, USA
TEL: 1-949-788-0805 FAX: 1-949-753-7033 BBS: 1-949-455-1779 & 1-949-455-9616 INFO: 1-800-326-1688
URL: www.dlink.com E-MAIL: tech@dlink.com & support@dlink.com

Registration Card

Print, type or use block letters.

Your name: Mr./Ms_____
Organization: _____Dept. _____
Your title at organization:_____
Telephone:_____ Fax:_____
Organization's full address: _____
_____
Country: _____
Date of purchase (Month/Day/Year): _____

Product Model	Product Serial No.	* Product installed in type of computer (e.g., Compaq 486)	* Product installed in computer serial No.

(* Applies to adapters only)

Product was purchased from:
Reseller's name: _____
Telephone:_____ Fax:_____
Reseller's full address: _____
_____
_____

Answers to the following questions help us to support your product:

1. Where and how will the product primarily be used?
☐Home ☐Office ☐Travel ☐Company Business ☐Home Business ☐Personal Use

2. How many employees work at installation site?
☐1 employee ☐2-9 ☐10-49 ☐50-99 ☐100-499 ☐500-999 ☐1000 or more

3. What network protocol(s) does your organization use ?
☐XNS/IPX ☐TCP/IP ☐DECnet ☐Others_____

4. What network operating system(s) does your organization use ?
☐D-Link LANsmart ☐Novell NetWare ☐NetWare Lite ☐SCO Unix/Xenix ☐PC NFS ☐3Com 3+Open
☐Banyan Vines ☐DECnet Pathwork ☐Windows NT ☐Windows NTAS ☐Windows '95
☐Others_____

5. What network management program does your organization use ?
☐D-View ☐HP OpenView/Windows ☐HP OpenView/Unix ☐SunNet Manager ☐Novell NMS
☐NetView 6000 ☐Others_____

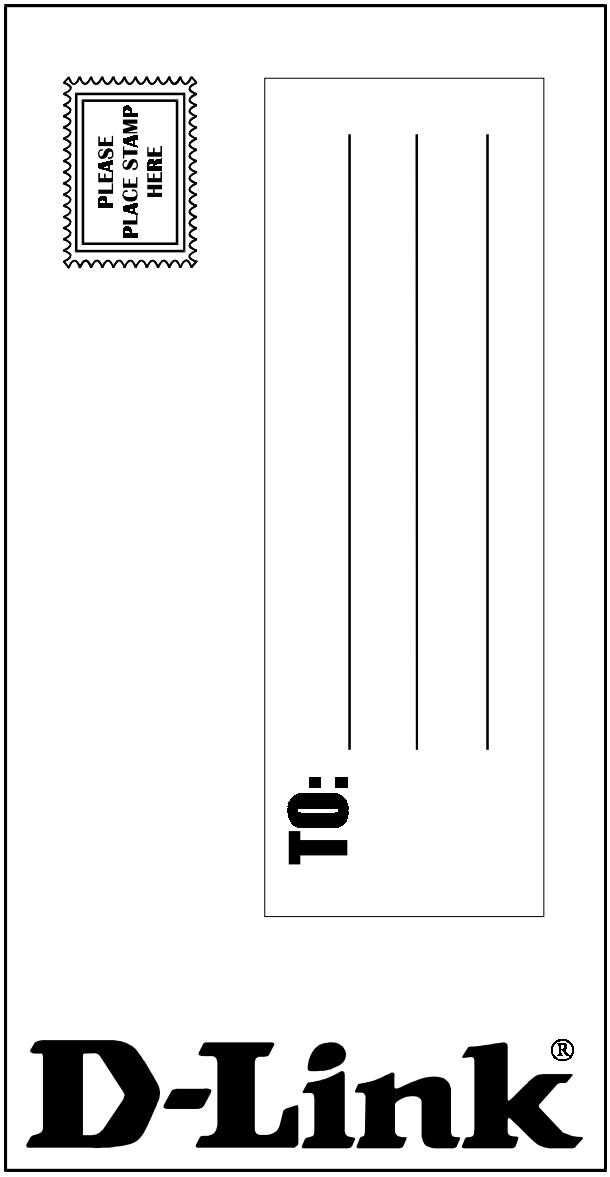
6. What network medium/media does your organization use ?
☐Fiber-optics ☐Thick coax Ethernet ☐Thin coax Ethernet ☐10BASE-T UTP/STP
☐100BASE-TX ☐100BASE-T4 ☐100VGAnyLAN ☐Others_____

7. What applications are used on your network?
☐Desktop publishing ☐Spreadsheet ☐Word processing ☐CAD/CAM
☐Database management ☐Accounting ☐Others_____

8. What category best describes your company?
☐Aerospace ☐Engineering ☐Education ☐Finance ☐Hospital ☐Legal ☐Insurance/Real Estate ☐Manufacturing
☐Retail/Chainstore/Wholesale ☐Government ☐Transportation/Utilities/Communication ☐VAR
☐System house/company ☐Other_____

9. Would you recommend your D-Link product to a friend?
☐Yes ☐No ☐Don't know yet

10.Your comments on this product?
_____


PLEASE
PLACE STAMP
HERE
TO:
D-Link®