Exhibit E   -   User's Manual

ISDN Router/Hub RA368

User's Guide

Version 1.0

Netgear

ISDN Router/Hub *RA368 WAN Bridge/Routers*

Incoming Call Support

In addition to making outgoing calls, the ISDN Router/Hub allows you to configure it as a remote access server for telecommuting employees.

Multiple Protocol Support

♦ TCP/IP (Transmission Control Protocol/Internet Protocol) network layer protocol.

♦ Novel IPX (Internetwork Packet eXchange) network layer protocol.

♦ Transparently bridging for unsupported network layer protocols.

♦ PPP/MP (Point-to-Point Protocol/Multilink Protocol) link layer protocol.

Integrated 4-Port Ethernet Hub

The built-in 4-port Ethernet 10Base-T hub saves you the cost and the clutter of an external hub.

Dial-On-Demand

The Dial-On-Demand feature allows the ISDN Router/Hub to automatically place a call to a remote gateway based on the triggering packet   destination without user intervention.

PPP Multilink

The ISDN Router/Hub can bundle multiple links in a single connection using PPP Multilink Protocol (MP). The number of links can be either statically configured or dynamically managed based on traffic demand.

Bandwidth-On-Demand

The ISDN Router/Hub dynamically allocates bandwidth by dialing and dropping connections according to traffic demand.

Full Network Management

♦ SNMP (Simple Network Management Protocol) support.

♦ Accessing SMT (System Management Terminal) through telnet connection.

♦ Web-based PWC (ISDN Router/Hub Web Configurator).

Chapter 1
Getting to Know Your Router/Hub

This chapter describes the key features and applications of your ISDN Router/Hub.

1.1   ISDN Router/Hub RA368 ISDN/Modem Bridge Router

The ISDN Router/Hub RA368 is an ISDN bridge/router with an integrated 4-port Ethernet 10Base-T hub and a 56K modem. The ISDN Router/Hub is ideal for everything from Internet browsing to receiving calls from remote dial-in users to making LAN-to-LAN connections to remote networks.

1.2   Features of ISDN Router/Hub RA368

The following are the key features of the ISDN Router/Hub RA368.

ISDN Basic Rate Interface (BRI) Support

The PRA368 supports a single BRI. A BRI offers two 64Kbps channels, which can be used independently for two destinations or be bundled to speed up data transfer.

Built-in V.90 56K Client Side Modem

The ISDN Router/Hub RA368 features a built-in V.90 56K high-speed client side modem. The built-in modem enables the ISDN Router/Hub to make/receive analog modem calls in addition to ISDN data calls.

Extensive Analog Phone Support

The ISDN Router/Hub is equipped with two standard phone jacks for you to connect analog devices such as telephones and FAX machines. It also supports supplementary services such as call waiting and 3-way conferencing.

Single User Account (SUA)

The SUA   (Single User Account) features allows multiple users to share a single user account.

ISDN Router/Hub *RA368 WAN Bridge/Routers*

Backup and Restore Configuration File via LAN or WAN

PCT (ISDN Router/Hub Configuration Transfer), the stand-alone Java-based utility, allows backup and restoration of the configuration file via LAN or WAN.

Upgrade PRA368 Firmware via LAN

PCT allows upgrading of the ISDN Router/Hub RA368 firmware over the local LAN.

Supplementary Voice Features

The ISDN Router/Hub supports the following Supplementary Voice Features on both of its Analog (POTS) Phone Ports:

♦ Call Waiting

♦ Three Way Calling (conference)

♦ Call Transfer

♦ Call Forwarding

Caller ID Display Services on Analog PSTN lines

The ISDN Router/Hub can send out CLID information on both POST ports. To use Caller ID Display you need a special telephone or display unit that can show and store incoming telephone numbers.

1.3   The Built-In Modem

The built-in V.90 modem is capable of maximum downloading speed of 56 kilobits per second (kbps). Please note that due to the local telephone regulations and the line quality of your local loop, the ISDN Router/Hub may or may not achieve the theoretical maximum throughput. Note also that the modem is a V.90 client; the maximum 56 kbps throughput is possible only when it connects to a V.90 server. When it connects to another V.90 client, the maximum throughput is 33.6 kbps in both directions.

The modem also supports V.42bis compression to speed up data transfer.

Logging and Tracing

♦ CDR (Call Detail Record) to help to analyze and manage the telephone bill.

♦ Built-in message logging and packet tracing.

♦ Unix syslog facility support .

RADIUS Support

RADIUS (Remote Authentication Dial-In User Service) is the most popular protocol for user authentication on dial-up lines. RADIUS support allows you to use an external server for unlimited number of users and the ease of centralized management.

PAP and CHAP Security

The ISDN Router/Hub supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure than PAP; however, PAP is readily available on more platforms.

DHCP Support

DHCP (Dynamic Host Configuration Protocol) allows the workstations on your LAN to obtain the configuration from the ISDN Router/Hub.

Call Control

Your ISDN Router/Hub provides budget management for outgoing calls and maintains a blacklist for unreachable phone numbers in order to save you the expense of unnecessary charges.

Data Compression

Your ISDN Router/Hub incorporates Stac data compression to speed up data transfer. Stac is the de facto standard of data compression over PPP links.

Networking Compatibility

Your ISDN Router/Hub is compatible with remote access products from other manufacturers such as Ascend, Cisco, and 3Com. Furthermore, it supports Microsoft Windows 95 and Windows NT remote access capability.

ISDN Router/Hub Web Configurator

The ISDN Router/Hub Web Configurator is a JAVA based utility designed to allow users to access the ISDN Router/Hub   management settings via a Worldwide Web browser.

ISDN Router/Hub *RA368 WAN Bridge/Routers*

Novell IPX routing, as well as transparent bridging for other network layer protocols. Your ISDN Router/Hub can also bundle multiple links in a single connection for greater bandwidth. A typical LAN-to-LAN application for your ISDN Router/Hub is shown below.
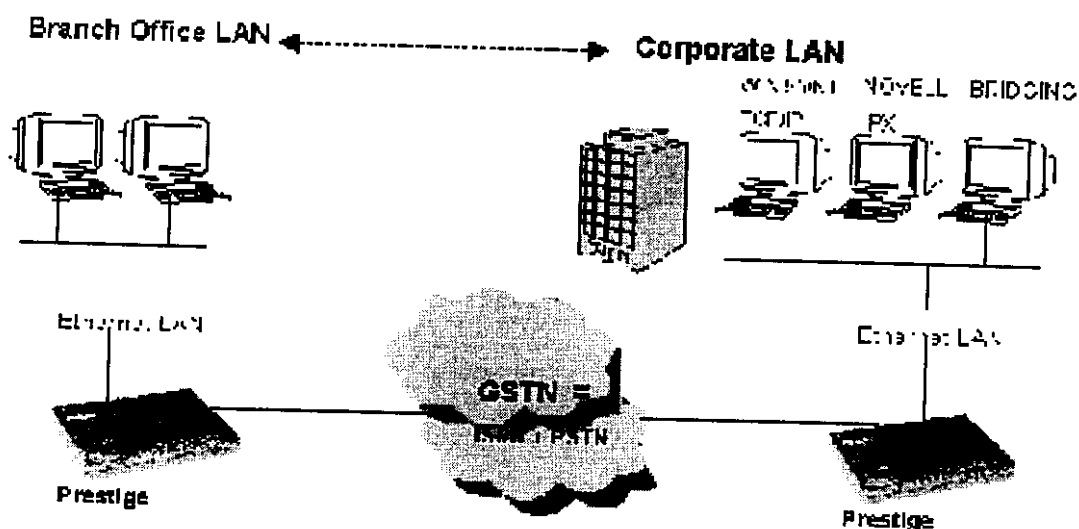
Figure 1-2 LAN-to-LAN Connection Application

1.4.3 Remote Access Server

Your ISDN Router/Hub allows remote users to dial-in and gain access to your LAN. This feature enables users that have workstations with remote access capabilities, e.g., Windows 95, to dial in to access the network resources without physically being in the office. Either PAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol) authentication can be used to control the access from the remote users. You can also use callback for security and/or accounting purposes.

1.4 Applications for ISDN Router/Hub RA368

The following sections show you the possible applications for your ISDN Router/Hub.

1.4.1 Internet Access

The ISDN Router/Hub is the ideal high-speed Internet access solution. Your ISDN Router/Hub supports the TCP/IP protocol, which the Internet uses exclusively. It is also compatible with access servers manufactured by major vendors such as Cisco and Ascend. A typical Internet Access application is shown below.
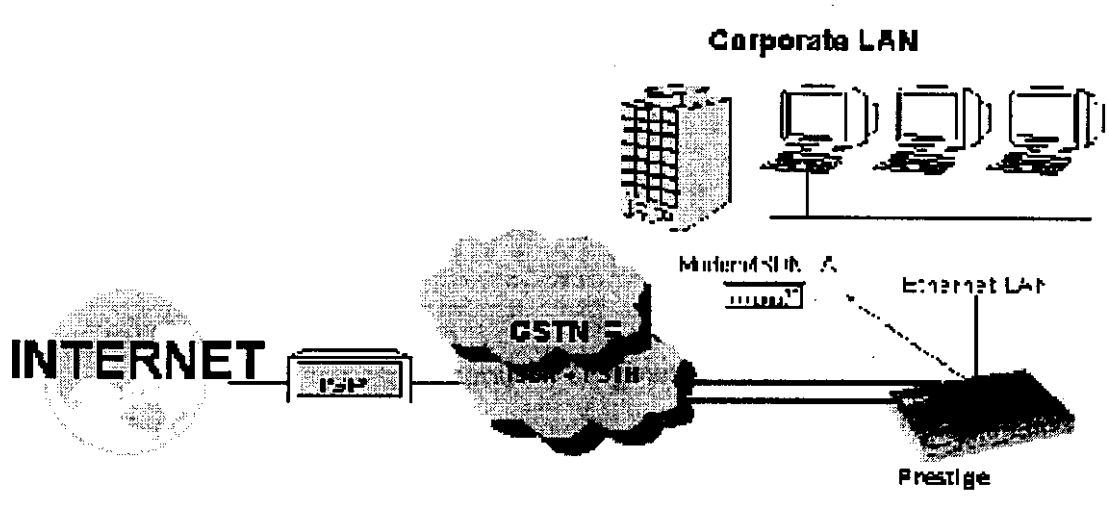
Figure 1-1 Internet Access Application

Internet Single User Account

For a SOHO (small office/Home Office) environment, your ISDN Router/Hub offers a Single User Account (SUA) feature that allows multiple users on the LAN (Local Area Network) to access the Internet concurrently for the cost of a single user. Single User Account address mapping can also be used for other LAN to LAN connections.

1.4.2 Multi-Protocol/Multilink LAN-to-LAN Connection

You can use the ISDN Router/Hub to connect two geographically dispersed networks over up to 128Kbps over a single ISDN BRI line. It incorporates PPP/MP (Point-to-Point Protocol/Multilink Protocol) to bundle two B channels in a BRI line. The ISDN Router/Hub supports TCP/IP and

---

Chapter 2
Hardware Installation & Initial Setup

This chapter shows you how to connect the hardware and the initial setup.

2.1.1 Front Panel LEDS

The LED indicators on the front panel indicate the router/hub functional status of the ISDN Router/Hub. The following table describes the LED functions:
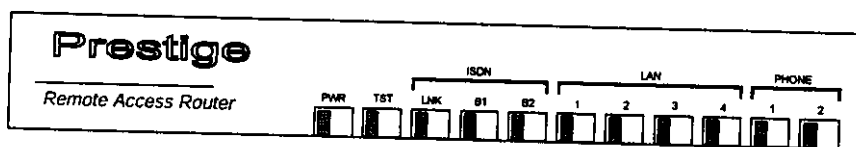
Figure 2-1 Front Panel

PWR	The PWR (power) LED is on when power is applied to the ISDN Router/Hub.
TST	A blinking TST (test) LED indicates the ISDN Router/Hub is functioning properly. A steady or an off TST indicates malfunction.
ISDN: LNK	The LNK (Link) LED is on when the ISDN Router/Hub is connected to an ISDN switch and the line has been successfully initialized.
ISDN: B1/B2	The B1/B2 LED is on when the corresponding B channel is in use.
LAN: 1 to 4	A steady LED indicates an active station is connected to the corresponding port. The LED blinks when the connected station is transmitting.
PHONE: 1/2	The LED is on when the device on the corresponding POTS port is in use.

Table 2-1 LED functions
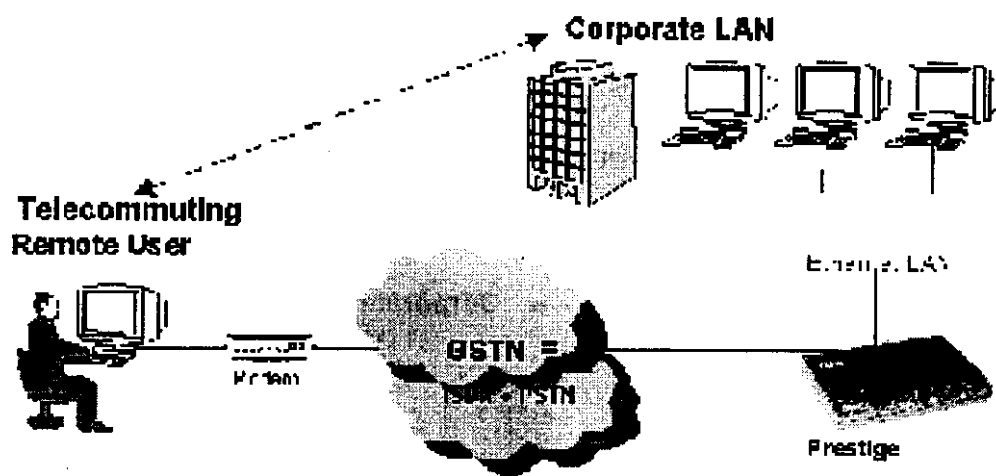
Figure 1-3 Telecommuting/Remote Access Server Application

ISDN Router/Hub *RA368 WAN Bridge/Routers*

2.2 ISDN Router/Hub RA368 Rear Panel and Connections

The figure below shows the rear panel of your ISDN Router/Hub 128MH and the connection diagram.
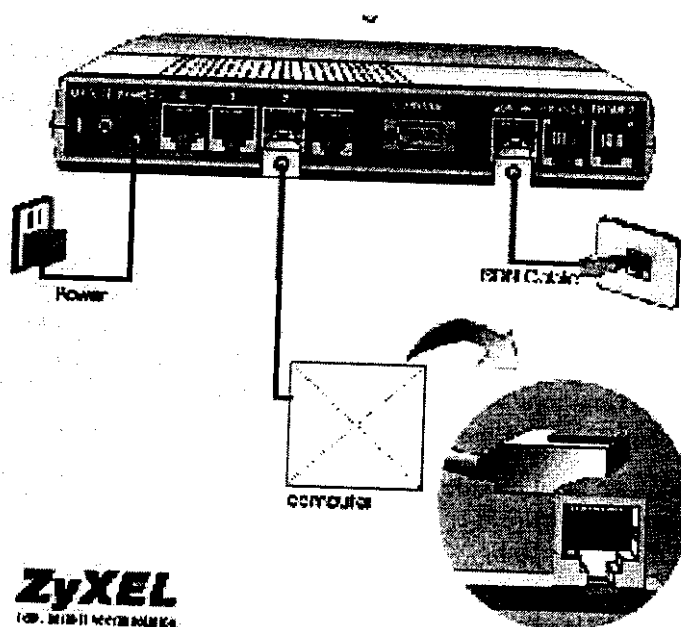
Figure 2-2 ISDN Router/Hub RA368 Rear Panel and Connections

This section outlines how to connect your ISDN Router/Hub 128MH to the LAN and to the ISDN network.

Step 1. Connecting the ISDN Line

Connect the ISDN Router/Hub to the ISDN network using the included ISDN (black) cable. Plug one end of the cable into the port labeled **ISDN BRI** and the other to the ISDN wall jack.

ISDN Router/Hub *RA368 WAN Bridge/Routers*

After the ISDN Router/Hub is properly set up, you can make future changes to the configuration through telnet connections.

Step 2. Connecting a Workstation to the ISDN Router/Hub

Connect a workstation to the built-in hub on the ISDN Router/Hub to create an Ethernet network. Connect one end of a straight through Ethernet cable to the NIC on the workstation and the other end to one of the 4 Ethernet ports. Ethernet 10Base-T networks use Unshielded Twisted Pair (UTP) cable with RJ-45 connectors that look like a bigger telephone plug with 8 pins.

Step 3. Connecting a Telephone/Fax to the ISDN Router/Hub

If you wish, you can connect regular telephones, fax machines or other analog devices to the ISDN Router/Hub. To connect an analog device, plug the end of the telephone cord from the device in either port **PHONE1** or **PHONE2** on the rear panel of the ISDN Router/Hub.

Step 4. Connecting the Power Adapter to your ISDN Router/Hub

Connect the power adapter to the port labeled **POWER** on the rear panel of your ISDN Router/Hub.

Step 5. Connecting the Console Port

For the initial configuration of your ISDN Router/Hub, you need to use a terminal emulator software on a workstation and connect it to the ISDN Router/Hub through the console port. Connect the 9-pin (smaller) end of the console cable to the console port of the ISDN Router/Hub and the 25-pin (bigger) end to a serial port (COM1, COM2 or other COM port) of your workstation. You can use an extension RS-232 cable if the enclosed one is too short.

After the initial setup, you can modify the configuration remotely through telnet connections. See *Chapter 12 - Telnet Configuration and Capabilities* for detailed instructions on using telnet to configure your ISDN Router/Hub.

2.3   Additional Installation Requirements

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

1. A computer with Ethernet 10Base-T NIC (Network Interface Card).

2. A computer equipped with communications software configured to the following parameters:

    ♦   VT100 terminal emulation.

    ♦   9600 Baud.

    ♦   No parity, 8 Data bits, 1 Stop bit.

ISDN Router/Hub *RA368 WAN Bridge/Routers*

2.5   Navigating the SMT Interface

The SMT (System Management Terminal) is the interface that you use to configure your ISDN Router/Hub.

Several operations that you should be familiar with before you attempt to modify the configuration are listed in the table below.

Table 2-2 Main Menu Commands

Operation	Press/<read>	Description
Move forward to another menu	[Enter]	To move forward to a sub-menu, type in the number of the desired sub-menu and press [Enter].
Move backward to a previous menu	[Esc]	Press the [Esc] key to move back to the previous menu.
Move the cursor	[Enter] or [Up]/[Down] arrow keys	Within a menu, press [Enter] to move to the next field. You can also use the [Up]/[Down] arrow keys to move to the previous and the next field, respectively.
Enter information	Fill in, or Press the [Space bar] to toggle	You need to fill in two types of fields. The first requires you to type in the appropriate information. The second allows you to cycle through the available choices by pressing the [Space] bar.
Required fields	<?>	All fields with the symbol <?> must be filled in order be able to save the new configuration.
N/A fields	<N/A>	Some of the fields in the SMT will show a <N/A>. This symbol refers to an option that is Not Applicable.
Save your configuration	[Enter]	Save your configuration by pressing [Enter] at the message [Press ENTER to confirm or ESC to cancel]. Saving the data on the screen will take you, in most cases to the previous menu.
Exit the SMT	Type 99, then press [Enter].	Type 99 at the Main Menu prompt and press [Enter] to exit the SMT interface.

2.4 Power On Your ISDN Router/Hub

At this point, you should have connected the console port, the ISDN BRI port, the Ethernet port and the power port to the appropriate devices or lines. You can now apply power to the ISDN Router/Hub by flipping the power switch to on (I is ON, O is OFF).

Step 1. *Initial Screen*

When you power on your ISDN Router/Hub, it performs several internal tests as well as line initialization. After the initialization, the ISDN Router/Hub asks you to press **Enter** to continue, as shown.

```
Copyright (c) 1994 - 1998 Netgear Communications Corp.
ethernet address: 00:a0:c5:98:23:12
Resetting ISDN firmware.(2) Netgear ISDN Router/Hub DSS1: V 099
....................
Press ENTER to continue...
```

Figure 2-3 Power-On Display

Step 2. *Entering Password*

The login screen appears after you press Enter, prompting you to enter the password, as shown below.

For your first login, enter the default password **1234**. As you type the password, the screen displays an (X) for each character you type.

Please note that if there is no activity for longer than 5 minutes after you log in, your ISDN Router/Hub will automatically log you out and will display a blank screen. If you see a blank screen, press [Enter] to bring up the login screen again.

```
                    Enter Password : XXXX
```

Figure 2-4 Login Screen

ISDN Router/Hub *RA368 WAN Bridge/Routers*

After you enter the password, the SMT displays the Main Menu, as shown below.

```
              Copyright (c) 1994 - 1998 Netgear Communications Corp.
                     ISDN Router/Hub 128IMH Main Menu

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

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



                     Enter Menu Selection Number:
```

Figure 2-5 SMT Main Menu
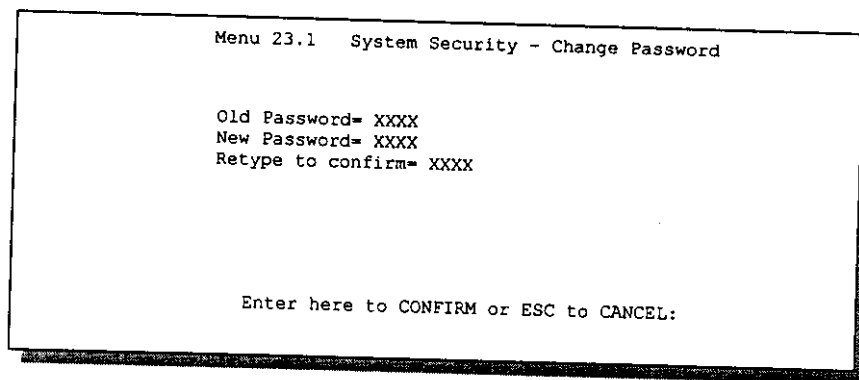
2.5.1 System Management Terminal Interface Summary

Table 2-3 Main Menu Summary

#	Menu Title	Description
1	General Setup	Use this menu to setup general information and to enable routing for specific protocols and bridging.
2	ISDN Setup	Use this menu to setup the ISDN.
3	Ethernet Setup	Use this menu to setup Ethernet.
4	Internet Access Setup	A quick and easy way to setup Internet connection.
11	Remote Node Setup	Use this menu to setup the Remote Node for LAN-to-LAN connection, including Internet connection.
12	Static Routing Setup	Use this menu to setup static route for different protocols.

ISDN Router/Hub *RA368 WAN Bridge/Routers*

When the Submenu 23.1- System Security-Change Password appears, as shown in the figure below, type in your existing system password, i.e., 1234, and press [Enter].

```
    Menu 23.1    System Security - Change Password


    Old Password= XXXX
    New Password= XXXX
    Retype to confirm= XXXX




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

Figure 2-7 Menu 23.1 - System Security - Change Password

Step 3.   Enter your new system password and press [Enter].

Step 4.   Re-type your new system password for confirmation and press [Enter].

Note that as you type a password, the screen displays a (X) for each character you type.

13	Default Dial-in Setup	Use this menu to setup default dial-in parameters so that your ISDN Router/Hub can be used as a dial-in server.
14	Dial-in User Setup	Use this menu to setup dial-in users.
15	SUA Server Setup	Use this menu to specify inside servers when SUA is enabled.
21	Filter Set Configuration	Use this menu to setup filters to provide security, call control, etc.
22	SNMP Configuration	Use this menu to setup SNMP related parameters
23	System Security	Use this menu to setup security related parameters.
24	System Maintenance	This menu provides system status, diagnostics, firmware upload, etc.
99	Exit	To exit from SMT and return to the blank screen.

2.6   Changing the System Password

The first thing your should do before anything else is to change the default system password by following the steps below.

Step 1.   Enter 23 in the Main Menu to open **Menu 23 - System Security** as shown below.

Step 2.   Enter 1 in Menu 23 to open **Menu 23.1 - System Security - Change Password.**

```
                    Menu 23 - System Security


               1. Change Password
               2. External Server




                  Enter Menu Selection Number: 1
```
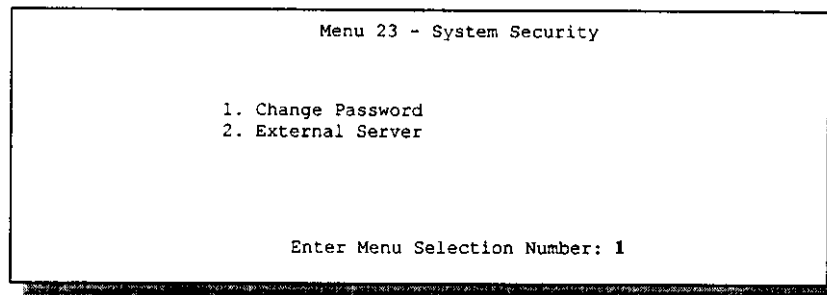
Figure 2-6 Menu 23 - System Security

ISDN Router/Hub *RA368 WAN Bridge/Routers*

Table 2-4 General Setup Menu Fields

Field	Description	Example
System Name	Choose a descriptive name for identification purposes. This name can be up to 8 alphanumeric characters long. Spaces are not allowed, but dashes and underscores "_" are accepted. This name can be retrieved remotely via SNMP, used for CHAP authentication, and will be displayed at the prompt in the Command Mode.	PRA368
Location (optional)	Enter the geographic location (up to 31 characters) of your ISDN Router/Hub.	MyHouse
Contact Person's Name (optional)	Enter the name (up to 8 characters) of the person in charge of this ISDN Router/Hub.	JohnDoe
Protocols:	Turn on or off routing for the individual protocols.	Press space-bar to toggle
Route IP	Set this field to **Yes** to enable IP routing. You must enable IP routing for Internet access.	**Yes/No**
Route IPX	Set this field **Yes** to enable IPX routing.	**Yes/No**
Bridge	Turn on/off bridging for protocols not supported (e.g., SNA) or not turned on in the previous Route fields.	**Yes/No**

Note on Bridging
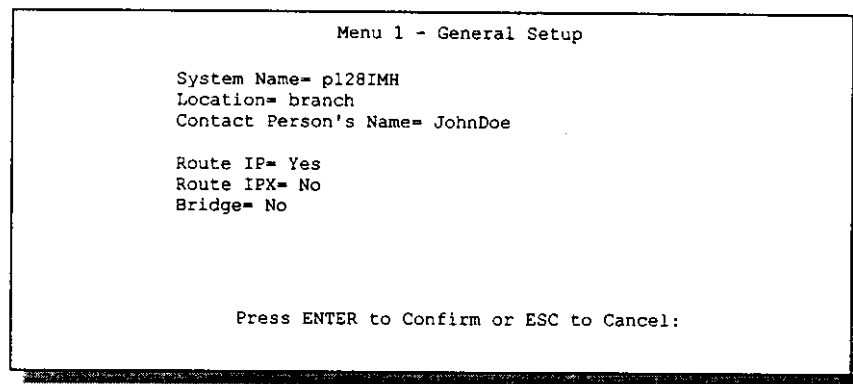
When bridging is enabled, your ISDN Router/Hub forwards any packet that it does not route. Without bridging, the packets that the ISDN Router/Hub does not route are simply discarded. Compared to routing, bridging generates far more traffic for the same network protocol and consumes more CPU cycles and memory.

2.7   General Setup

Menu 1 - General Setup contains administrative and system-related information.

To enter Menu 1 and fill in the required information, follow these steps:

Step 1.   Enter 1 in the Main Menu to open **Menu 1 – General Setup**.

Step 2.   The Menu 1 - General Setup screen appears, as shown below. Fill in the required fields marked [?] and turn on the individual protocols for your applications, as explained in the following table.

```
                        Menu 1 - General Setup

            System Name= p128IMH
            Location= branch
            Contact Person's Name= JohnDoe

            Route IP= Yes
            Route IPX= No
            Bridge= No




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

Figure 2-8 Menu 1 – General Setup

<u>ISDN Router/Hub *RA368 WAN Bridge/Routers*</u>

Call to **Ignore**, then the ISDN Router/Hub ignores all global calls. If **Analog Call Routing** is **Ignore** to begin with, then all analog calls, including global calls, are ignored.

2.8.5 Modem Calls

The built-in modem is internally connected to A/B adapter 2. If you wish to receive modem calls, you must set the **A/B Adapter 2 Accepts Modem Call** field to **Enable**. When this field is enabled, only the modem receives the incoming analog calls routed to A/B adapter 2 according to the description above; the external device will not ring. Note that this field only controls the incoming calls; you can still place outgoing modem calls even if this field is **Disable**.

2.8.6 PABX Outside Line Prefix

A PABX (Private Automatic Branch eXchange) generally requires you to dial a number (a single digit in most cases) when you need an outside line. If your ISDN Router/Hub is connected to a PABX, enter this number in **PABX Outside Line Prefix**, otherwise, leave it blank.

Please note that the PABX prefix is for calls initiated by the ISDN Router/Hub only. If you place a call from a device on either A/B adapter, you must dial the prefix by hand.

2.8.7 Outgoing Calling Party Number

If this field is not blank, the ISDN Router/Hub will use its value as the *calling party number* for "ISDN Data", "A/B Adapter 1" and "A/B Adapter 2" outgoing calls. Otherwise, the individual entries for "ISDNData", "A/B Adapter 1" and "A/B Adapter 2" will be used as the calling party number.You only need to fill in this field if your switch or PABX requires a specific calling party number for outgoing calls, otherwise, leave it blank. If you need to override the individual calling party number, enter Command Interpreter mode and issue the command:

```
isdn initstring set AT&ZOx=number
```

where x is 'I' for ISDN data calls, 'A' for A/B Adapter 1 and 'B' for A/B Adapter 2. For instance,

```
isdn initstring set AT&ZOI=100&ZOA=101&ZOB=102
```

2.8 European ISDN Setup Menus

Menu 2 is for you to enter the information about your ISDN line. Please note that the ISDN Router/Hub only accepts digits in phone number fields; please do no include   or spaces in these fields.

2.8.1 Switch Type

The only switch type supported in Europe is DSS-1.

2.8.2 MSN and Subaddress

Depending on your location, you may have Multiple Subscriber Number (MSN) where the telephone company gives you more than one number for your ISDN line. You can assign each number to a different port, e.g., the first number to data calls, the second to A/B adapter 1 and so on. Or the telephone company may give you only one number, but allow you to assign your own subaddresses to different ports, e.g., subaddress 1 to data calls and 2 to A/B adapter 1.

2.8.3 Incoming Call Routing

The **Incoming Phone Number Matching** setting governs how incoming calls are routed. If you select **Multiple Subscriber Number (MSN)** or **Called Party Subaddress**, a call (either ISDN data or analog) is routed to the port that matches the dialed number; if no match is found, the call is dropped.

If you select **Don't Care**, then all data calls are routed to the ISDN Router/Hub itself. Analog calls, however, are routed to either A/B adapter 1 or 2, or simply ignored, depending on the **Analog Call Routing** field.

2.8.4 Global Calls

A global call is an incoming analog call where the switch did not send the dialed number. This happens most often when the call originates from an analog telephone line.

If you specify explicit matching, i.e., **Incoming Phone Number Matching** is either MSN or Called Party Subaddress, then global calls are always ignored. If it is **Don't Care** and **Analog Call Routing** is either A/B Adapter 1 or 2, then the ISDN Router/Hub uses **Global Analog Call** to decide how to handle global calls. If you set **Global Analog Call** to **Accept**, then global calls are routed to the port according to the **Analog Call Routing** setting; if you set **Global Analog**

ISDN Router/Hub *RA368 WAN Bridge/Routers*

	another device on the S/T bus), then select **Switch/Unused.** The default is **Switch/Switch.**
ISDN Data & Subaddress	Enter the telephone number and the subaddress assigned to ISDN data calls for the ISDN Router/Hub. The maximum number of digits is 19 for the telephone number and 5 for the subaddress.
A/B Adapter 1 & Subaddress	Enter the telephone number and the subaddress assigned to A/B Adapter 1 (PHONE1).
A/B Adapter 2 & Subaddress	Same as above for A/B Adapter 2 (PHONE2).
PABX Outside Line Prefix	Enter the number for outside line access if the ISDN Router/Hub is connected to a PABX; otherwise, leave it blank. The maximum number of digits is 4.
Outgoing Calling Party Number	You only need to fill in this field if your switch requires a specific **Outgoing Calling Party Number**; otherwise, leave it blank.
Incoming Phone Number Matching	Determines how incoming calls are routed. The choices for this field are **Multiple Subscriber Number (MSN), Called Party Subaddress** and **Don't Care.**
Analog Call Routing	Select the destination for analog calls. The choices are **A/B Adapter 1, A/B Adapter 2** and **Ignore.** This field is only applicable when **Incoming Phone Number Matching** is **Don't Care.**
Global Analog Call	Select how to handle global analog calls. The choices are **Accept** and **Ignore.** This field is not applicable when the **Analog Call Routing** is **Ignore.**
Edit Advanced Setup	Select **Yes** and press **Enter** to go to the advanced setup submenu.

2.8.8 Advanced Setup

Select **Yes** in the **Advanced Setup** field of **Menu 2 – ISDN Setup** above to display menu 2.1 below.

ISDN Call Waiting

This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number. By default call waiting is disabled on both telephone ports, but can be enabled on either port from **Menu 2.1**

sets the calling party number to 100 for ISDN data calls, 101 for A/B adapter 1 and 102 for A/B adapter 2.

```
                          Menu 2 - ISDN Setup
           Switch Type: DSS-1(Taiwan)
           B Channel Usage= Switch/Switch


           ISDN Data      =                                    Subaddress=
           A/B Adapter 1 =                                     Subaddress=
           A/B Adapter 2 =                                     Subaddress=
           A/B Adapter 2 Accepts Modem Call= Disable


           PABX Outside Line Prefix =
           Outgoing Calling party Number =
           Incoming Phone Number Matching= Multiple Subscriber Number (MSN)
             Analog Call Routing= N/A
             Global Analog Call= N/A
         Edit Advanced Setup = No

           Press ENTER to Confirm or ESC to Cancel:

   Press Space Bar to Toggle.
```

Figure 2-9 Menu 2 – ISDN Setup

Table 2-5 Menu 2 – ISDN Setup

Switch Type	This field is fixed as DSS1.
B Channel Usage	In general, this is **Switch/Switch**. If you are only using one B channel (e.g., your ISDN Router/Hub is sharing the ISDN BRI line with

ISDN Router/Hub *RA368 WAN Bridge/Routers*

This section describes how to configure the Ethernet using Menu 3   Ethernet Setup. From the Main Menu, enter 3 to open Menu 3.

```
                    Menu 3 - Ethernet Setup


            1. General Setup
            2. TCP/IP and DHCP Setup
            3. Novell IPX Setup
            4. Bridge Setup




                   _____ ____ _____ _____.
```
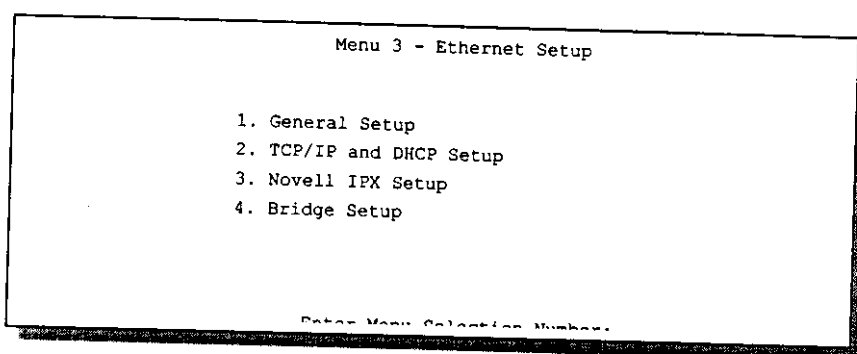
Figure 2-12 Menu 3 - Ethernet Setup

2.9.1 General Ethernet Setup

This menu allows you to specify the filter sets that you wish to apply to the Ethernet traffic. You seldom need to filter Ethernet traffic, however, the filter sets may be useful to block certain packets, reduce traffic and prevent security breaches.

```
                  Menu 3.1 - General Ethernet Setup

          Input Filter Sets:
            protocol filters= 2
               device filters=
          Output Filter Sets:
            protocol filters=
               device filters=

          Press ENTER to Confirm or ESC to Cancel:
```
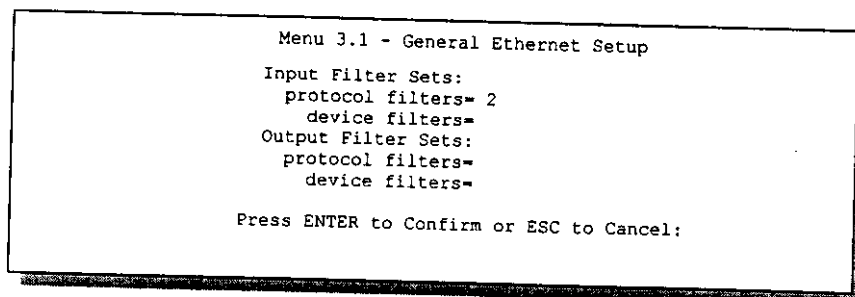
Figure 2-13 Menu 3.1 - General Ethernet Setup

If you need to define filters, please read *Chapter 9- Filter Set Configuration*, then return to this menu to define the filter sets.

How to use call waiting

The **Call Waiting** feature on your ISDN line works in exactly the same way it does on a regular analog line. After hearing a call waiting indicator tone, press and immediately release the flash button on your telephone. This puts your current call on hold and answers the incoming call.

Calling Line Indication

```
                Menu 2.1 - ISDN Advanced Setup

           Phone 1 Call Waiting- Disable
           Phone 2 Call Waiting= Disable
           Calling Line Indication- Enable
```

Figure 2-10 ISDN Advanced Setup

The **Calling Line Indication,** or Caller ID, governs whether the other party can see your number when you call. If set to **Enable**, the ISDN Router/Hub sends the caller ID and the party you call can see your number, otherwise, the caller ID is blocked.

When you are finished, press **ENTER** at the message: ress ENTER to confirm the ISDN Router/Hub uses the information that you entered to initialize the ISDN line. It should be noted that whenever the switch type is changed, the ISDN initialization takes slightly longer.

At this point, the ISDN Router/Hub asks if you wish to test your ISDN. If you select **Yes**, the ISDN Router/Hub will perform a loop-back test to check the ISDN line. If the loop-back test fails, please note the error message that you receive and take the appropriate troubleshooting action.

```
Setup LoopBack Test...

Dialing to 40000// ...

Sending and Receiving Data ...

Disconnecting...
```

Figure 2-11 Loopback test

2.9   Ethernet Setup
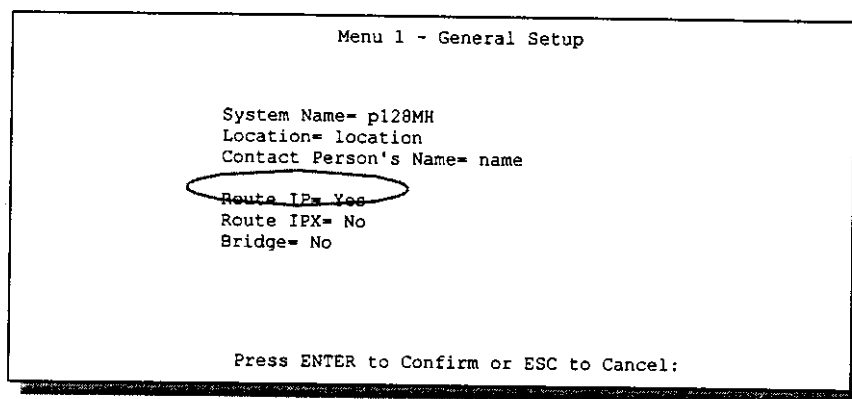
Chapter 3
Internet Access

This chapter shows you how to configure the LAN as well as the WAN of your ISDN Router/Hubfor Internet access.

3.1 Route IP Setup

The first step is to enable the IP routing in Menu 1 - General Setup.

To edit Menu 1, enter 1 in the Main Menu to select **General Setup** and press [Enter]. Set the Route IP field to **Yes** by pressing the space bar.

```
                    Menu 1 - General Setup


          System Name= p128MH
          Location= location
          Contact Person's Name= name

          Route IP= Yes
          Route IPX= No
          Bridge= No




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

Figure 3-1 Menu 1 – General Setup

3.2 TCP/IP Parameters

3.2.1 IP Address and Subnet Mask

Similar to the houses on a street that share a common street name, the machines on a LAN share one common network number, also.

2.10 Protocol Dependent Ethernet Setup

Depending on the protocols for your applications, you need to configure the respective Ethernet Setup, as outlined below.

- For TCP/IP Ethernet setup refer to *Chapter 3 - Internet Access Application.*

- For Novell IPX Ethernet setup refer to Section 7.4 - IPX Ethernet Setup in *Chapter 7 - Novell IPX Configuration for LAN-to-LAN.*

- For bridging Ethernet setup refer to *Chapter 8 - Bridge Configuration for LAN-to-LAN.*

ISDN Router/Hub *RA368 WAN Bridge/Routers*

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 (ignoring the trailing zero) and you must enable the Single User Account feature of the ISDN Router/Hub. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do *not* use any other number unless you are told otherwise. Let say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first 3 numbers specify the network number while the last number identifies an individual workstation on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, e.g., 192.168.1.1, for your ISDN Router/Hub.

The subnet mask specifies the network number portion of an IP address. Your ISDN Router/Hub will compute the subnet mask automatically based on the IP address that you entered. You don need to change the subnet mask computed by the ISDN Router/Hub unless you are instructed to do otherwise.

3.2.2 RIP Setup

RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. When set to both, the ISDN Router/Hub will broadcast its routing table periodically and incorporate the RIP information that it receives; when set to none, it will not send any RIP packets and will ignore any RIP packets received.

The **Version** field controls the format and the broadcasting method of the RIP packets that the ISDN Router/Hub sends (it recognizes both formats when receiving). **RIP-1** is universally supported; but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have a unusual network topology.

Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load

ISDN Router/Hub *RA368 WAN Bridge/Routers*

query to the real DNS server learned through IPCP and relays the response back to the workstation.

Please note that DNS proxy works only when the ISP uses the IPCP DNS server extensions. It does not mean you can leave the DNS servers out of the DHCP setup under all circumstances. If your ISP gives you explicit DNS servers, make sure that you enter their IP addresses in the **DHCP Setup** menu. This way, the ISDN Router/Hub can pass the DNS servers to the workstations and the workstations can query the DNS server directly without the ISDN Router/Hub intervention.

on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also.

By default, **RIP direction** is set to **Both** and the **Version** set to **RIP-1**.

3.2.3 DHCP Configuration

DHCP (Dynamic Host Configuration Protocol) allows the individual clients (workstations) to obtain the TCP/IP configuration at start-up from a centralized DHCP server. The ISDN Router/Hub has built-in DHCP server capability, enabled by default, which means it can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client.

IP Pool Setup

The ISDN Router/Hub is pre-configured with a pool of 32 IP addresses starting from 192.168.1.33 to 192.168.1.64. This configuration leaves 31 IP addresses (excluding the ISDN Router/Hub itself) in the lower range for other server machines, e.g., server for mail, FTP, telnet, web, etc., that you may have.

DNS Server Address

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa, e.g., the IP address of *www.Netgear.com* is 204.217.0.2. The DNS server is extremely important because without it, a user must know the IP address of a machine before s/he can access it. The DNS server addresses that you enter in the DHCP setup are passed to the client machines along with the assigned IP address and subnet mask.

There are two ways that an ISP disseminates the DNS server addresses. The first is for an ISP to tell a customer the DNS server addresses, usually in the form of an information sheet, when s/he signs up. If your ISP does give you the DNS server addresses, enter them in the **DNS Server** fields in **DHCP Setup**.

Some ISP choose to pass the DNS servers using the DNS server extensions of PPP IPCP (IP Control Protocol) after the connection is up. If your ISP did not give you explicit DNS servers, chances are the DNS servers are conveyed through IPCP negotiation. The ISDN Router/Hub supports the IPCP DNS server extensions through the DNS proxy feature.

If the **Primary** and **Secondary DNS Server** fields in **DHCP Setup** are not specified, i.e., left as 0.0.0.0, the ISDN Router/Hub tells the DHCP clients that it itself is the DNS server. When a workstation sends a DNS query to the ISDN Router/Hub, the ISDN Router/Hub forwards the

---

ISDN Router/Hub *RA368 WAN Bridge/Routers*

Follow the instructions in the following table on how to configure the DHCP fields.
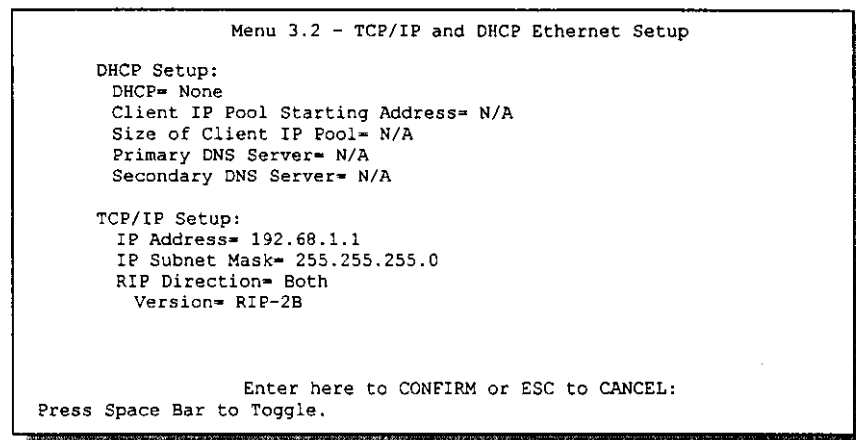
Table 3-1 DHCP Ethernet Setup Menu Fields

Field	Description	Example
DHCP Setup		
DHCP=	This field enables/disabled the DHCP server. If it is set to **Server**, your ISDN Router/Hub will act as a DHCP server. If set to **None**, DHCP server will be disabled.	**None** **Server** (default)
	When DHCP is used, the following four items need to be set:	
Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.	192.168.1.33
Size of Client IP Pool	This field specifies the size, or count, of the IP address pool.	32
Primary DNS Server Secondary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.	

3.3 TCP/IP Ethernet Setup and DHCP

You will now use Menu 3.2 to configure your ISDN Router/Hub for TCP/IP.

To edit Menu 3.2, select the menu option **Ethernet Setup** in the Main Menu. When Menu 3 appears, select the submenu option **TCP/IP and DHCP Setup** and press [Enter]. The screen now displays Menu 3.2 - TCP/IP and DHCP Ethernet Setup, as shown below.

```
                   Menu 3.2 - TCP/IP and DHCP Ethernet Setup

        DHCP Setup:
         DHCP= None
         Client IP Pool Starting Address= N/A
         Size of Client IP Pool= N/A
         Primary DNS Server= N/A
         Secondary DNS Server= N/A

        TCP/IP Setup:
         IP Address= 192.68.1.1
         IP Subnet Mask= 255.255.255.0
         RIP Direction= Both
           Version= RIP-2B



                   Enter here to CONFIRM or ESC to CANCEL:
        Press Space Bar to Toggle.
```

Figure 3-2 Menu 3.2 – TCP/IP and DHCP Ethernet Setup

ISDN Router/Hub *RA368 WAN Bridge/Routers*

3.4 Internet Access Configuration

Menu 4 allows you to enter the Internet Access information in one screen. Menu 4 is actually a simplified setup for one of the remote nodes that you can access in Menu 11. Before you configure your ISDN Router/Hub for Internet access, you need to collect your Internet account information from your ISP.

Use the table below to record your Internet Account Information.

Table 3-3 Internet Account Information

Internet Account Information	Write your account information here
IP Address of the ISP's Gateway (Optional)	✍
Telephone Number(s) of your ISP	✍
Login Name	✍
Password for ISP authentication	✍
(DNS server address(es) for your workstation	✍

Follow the instructions in the following table to configure TCP/IP parameters for the Ethernet port.

Table 3-2 TCP/IP Ethernet Setup Menu Fields

Field	Description	Example
TCP/IP Setup		
IP Address	Enter the IP address of your ISDN Router/Hub in dotted decimal notation	192.168.1.1 (default)
IP Subnet Mask	Your ISDN Router/Hub will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ISDN Router/Hub	255.255.255.0
RIP Direction	Press the space bar to select the RIP direction from **Both/In Only/Out Only.**	**Both** (default)
Version	Press the space bar to select the RIP version from **RIP-1/RIP-2B/RIP-2M.**	**RIP-1** (default)
When you have completed this menu, press [Enter] at the prompt [Press ENTER to Confirm to save your configuration, or press [Esc] at any time to cancel.		

ISDN Router/Hub *RA368 WAN Bridge/Routers*

		on the Single User Account feature. The default is **Yes.**
Telco options:	Transfer Type	This field specifies the type of connection between the ISDN Router/Hub and this remote node. Select **64K, Leased**, or **Modem.**
Multilink		The ISDN Router/Hub uses the PPP Multilink Protocol (PPP/MP) to bundle multiple links in a single connection to boost the effective throughput between two nodes. This option is only available if the transfer type is **64K.** See menu 11.2 for more details.
Idle Timeout		This value specifies the number of idle seconds that elapses before the remote node is automatically disconnected. Idle seconds is the period of time when no data is transmitted from your ISDN Router/Hub. Administrative packets such as RIP are not counted as data. The default is 300 seconds (5 minutes). *This option only applies when the ISDN Router/Hub initiates the call.*

At this point, the SMT will ask if you wish to test the Internet connection. If you select **Yes**, your ISDN Router/Hub will call the ISP to test the Internet connection. If the test fails, note the error message that you receive on the screen and take the appropriate troubleshooting steps.

From the Main Menu, enter option **Internet Access Setup** to go to Menu 4 - Internet Access Setup, as displayed below. The following table contains instructions on how to configure your ISDN Router/Hub for Internet access.

```
              Menu 4 - Internet Access Setup

     ISP's Name= myISP
      Pri Phone #= 1234
      Sec Phone #=
      My Login= JohnDoe
      My Password= *******
      Single User Account= Yes
        IP Addr= 0.0.0.0

      Telco Options:
         Transfer Type= 64K

      Multilink= Off
      Idle Timeout= 300


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

Figure 3-3 Menu 4 – Internet Access Setup

Table 3-4 Internet Access Setup Menu Fields

Field	Description
ISP Name	Enter the name of your Internet Service Provider, e.g., myISP. This information is for identification purposes only.
ISP IP Addr	Enter the IP Address of the remote gateway at the ISP site. If you don have this data, just leave it blank.
Pri Phone and Sec Phone Number	Both the Primary and the Secondary Phone number refer to the number that the ISDN Router/Hub dials to connect to the ISP.
My Login Name	Enter the login name given to you by your ISP.
My Password	Enter the password associated with the login name above.
Single User Account	Please see the following section for a more detailed discussion

ISDN Router/Hub *RA368 WAN Bridge/Routers*

The IP address for the SUA can be either fixed or dynamically assigned when a call is connected. In addition, you can designate servers, e.g., a web server and a telnet server, on your local network and make them accessible to the outside world.

If you do not define any server, SUA offers the additional benefit of firewall protection. If no server is defined, all incoming inquiries will be filtered out by your ISDN Router/Hub and thus preventing intruders from probing your network.

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

3.5.1 Advantages of SUA

In summary:

- SUA is a cost-effective solution for small offices with less than 20 hosts to access the Internet or other remote TCP/IP networks.

- SUA supports servers to be accessible to the outside world.

- SUA can provide firewall protection if you do not specify a server. All incoming inquiries will be filtered out by your ISDN Router/Hub.

- UDP and TCP packets can be routed. In addition, partial ICMP, including echo and trace route, is supported.

3.5 Single User Account

Typically, if there are multiple users on the LAN wanting to concurrently access the Internet, you will have to lease a block of legal, or globally unique, IP addresses from the ISP.

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

illustrates a typical Single User Account topology.
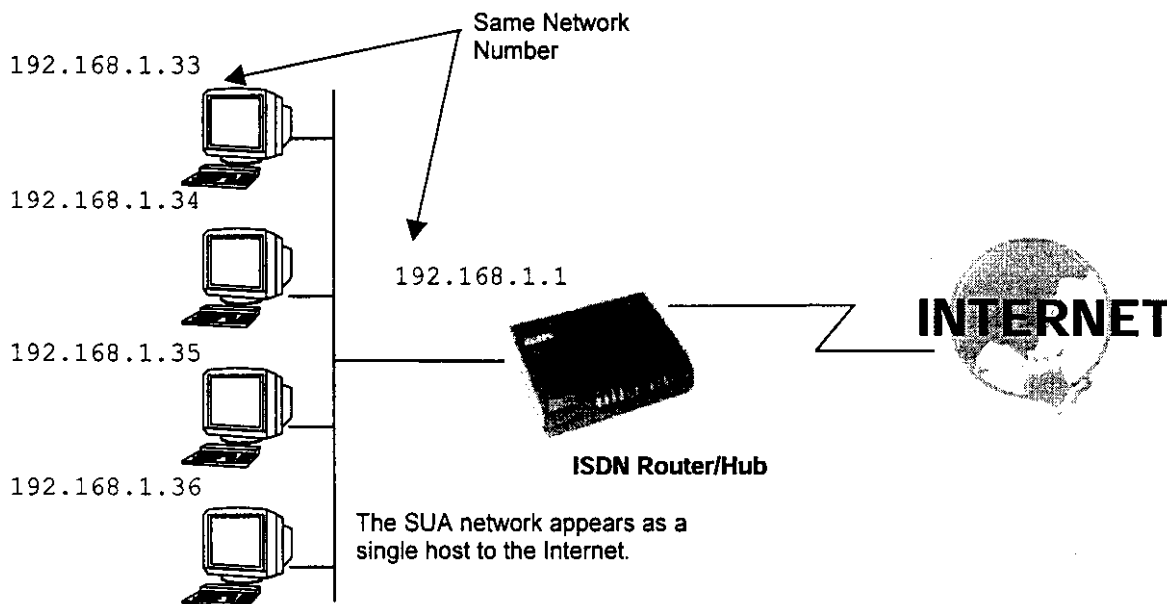
Figure 3-4 Single User Account Topology

The Single User Account feature may also be used on connections to remote networks other than the ISP. For example, this feature can be used to simplify the allocation of IP addresses when connecting branch offices to the corporate network.

ISDN Router/Hub *RA368 WAN Bridge/Routers*

3.6   Configuring Backup ISP Accounts

If you have more than one ISP account, you can configure the secondary ISP as a backup. You can switch to the backup ISP in the event that the primary ISP is out of service. The SUA feature can be enabled for all these accounts.

3.6.1 Configure a Backup ISP

To configure a backup ISP Account, follow these steps:

Step 1.   Configure your primary ISP using Menu 4, as described earlier in this chapter.

Step 2.   Enter Menu 11, then select an unused remote node.

Step 3.   In Menu 11.1, choose a name for your backup ISP account, then set the Active field to No, and enter your outgoing login name, password, and phone number(s). The Remote IP Address field should be set to **1.1.1.1**.

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

Step 5.   Save the new configuration.

Please note that the remote IP address of **1.1.1.1** is only a placeholder to avoid conflicting with that of the primary ISP, which is implicitly set at **0.0.0.0**. When the backup ISP is activated, the remote IP address of **1.1.1.1** combined with the subnet mask of **0.0.0.0** creates a default route that is equivalent to the one derived form the primary ISP.

3.6.2 To Switch ISP

Follow these steps when you need to switch from your primary ISP to a backup ISP:

Step 1.   Enter Menu 11 and select your Primary ISP.

Step 2.   In Menu 11.1, set the **Active** field to **No**.

Step 3.   Enter Menu 11 again and select your Backup ISP.

Step 4.   In Menu 11.1, set the **Active** field to **Yes**.

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

3.5.2 Single User Account Configuration

The steps for configuring your ISDN Router/Hub for Single User Account are identical to the conventional Internet access with the exception that you need to fill in two extra fields in Menu 4 - Internet Access Setup, as shown below.

```
                    Menu 4 - Internet Access Setup

              ISP's Name= myISP
              Pri Phone #= 1234
              Sec Phone #=
              My Login= JohnDoe
              My Password= ********
              Single User Account= Yes
                 IP Addr= 0.0.0.0
              Telco Options:
                 Transfer Type= 64K
              Multilink= Off
              Idle Timeout= 300



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

Figure 3-5 Menu 4 – Internet Access Setup for Single User Account

To enable the SUA feature in Menu 4, move the cursor to the **Single User Account** field and select **Yes** (or **No** to disable SUA). Then follow the instructions on how to configure the SUA fields.

Table 3-5 Single User Account Menu Fields

Field	Description
Single User Account	Select **Yes** to enable SUA.
IP Addr.	If your ISP did *not* assign you a static IP address, enter [0.0.0.0] here; otherwise, enter that IP address here.
Press [Enter] at the message [Press ENTER to Confirm ...] to save your configuration, or press [Esc] at any time to cancel.	

At this point, your ISDN Router/Hub will ask if you wish to test the Internet connection. If you select **Yes**, the ISDN Router/Hub will call the ISP and test the configuration. If the test fails, note the error messages on the screen and take the appropriate troubleshooting steps.

Chapter 4
Remote Node Configuration

A remote node is required for placing calls to a remote gateway. A remote node represents both the remote gateway and the network behind it across a WAN connection. Note that when you use Menu 4 to set up Internet access, you are actually configuring one of the remote nodes. Once a remote node is configured correctly, traffic to the remote network will trigger your ISDN Router/Hub to make a call automatically, i.e., Dial On Demand.

In this chapter, we will discuss the parameters that are protocol independent. The protocol-dependent configuration will be covered in subsequent chapters. For TCP/IP, *see Chapter 5*, for IPX, see *Chapter 6* and for Bridging, see *Chapter 7*.

4.1   Remote Node Setup

This section describes the protocol-independent parameters for a remote node.

4.1.1 Remote Node Profile

To configure a remote node, follow these steps:

Step 1.   From the Main Menu, select menu option **1. Remote Node Setup**

Step 2.   When Menu 11 appears, as shown below, enter the number of the remote node that you wish to configure.

ISDN Router/Hub *RA368 WAN Bridge/Routers*

```
                     Menu 11 - Remote Node Setup

              Menu 11 - Remote Node Setup

                1. remotenodename
                2. _____
                3. _____
                4. _____
                5. _____
                6. _____
                7. _____
                8. _____
                9. _____
               10. _____
               11. _____
               12. _____
                        Enter Node # to Edit:
```

Figure 4-1 Menu 11 – Remote Node Setup

When Submenu 11.1. - Remote Node Profile appearsfill in the fields as described in the table below to define this remote profile. The Remote Node Profile Menu Fields table shows how to configure the Remote Node Menu.

```
                 Menu 11.1 - Remote Node Profile

   Rem Node Name= remotenodename    Route= IP
   Active= Yes                      Bridge= No

   Call Direction= Outgoing         Edit PPP Options= No
   Incoming:                        Rem IP Addr= 0.0.0.0
      Rem Login= N/A                Edit IP/IPX/Bridge= No
      Rem Password= N/A             Telco Option:
      Rem CLID= N/A                    Allocated Budget(min)= 0
      Call Back= N/A                   Period(hr)= 0
   Outgoing:                           Transfer Type= 64K
      My Login= ChangeMe               Nailed-Up Connection= No
      My Password= ********         Session Options:
      Authen= CHAP/PAP                 Edit Filter Sets= No
      Pri Phone #= 1234                Idle Timeout(sec)= 300
      Sec Phone #=
                   Enter here to CONFIRM or ESC to CANCEL:
```

Figure 4-2 Menu 11.1 Remote Node Profile

Table 4-1 Remote Node Profile Menu Fields

Field	Description	Options
Rem Node Name	This is a required field [?]. Enter a descriptive name for the remote node, for example, Corp. This field can be up to eight characters. This name must be unique from any other remote node name or remote dial-in user name.	
Active	Press the space bar to toggle between **Yes** and **No**. Inactive nodes are displayed with a minus sign (-) at the beginning of the name in Menu 11.	Press space bar to toggle **Yes/No**
Call Direction	● If this parameter is set to **Both**, your ISDN Router/Hub can both place and receive calls to/from this remote node. ● If set to **Incoming**, your ISDN Router/Hub will not place a call to this remote node. ● If set to **Outgoing**, your ISDN Router/Hub will drop any incoming calls from this remote node. Several other fields in this menu depend on this parameter. For example, in order to enable **Callback**, the **Call Direction** must be **Both**.	**Both** **Incoming** **Outgoing**
Incoming: Rem Node Login Name	Enter the login name that this remote node will use when it calls your ISDN Router/Hub. The login name in this field combined with the Rem Node Password will be used to authenticate this node.	
Incoming: Rem Node Password	Enter the password used when this remote node calls your ISDN Router/Hub.	

ISDN Router/Hub *RA368 WAN Bridge/Routers*

Incoming:	Rem CLID	This field is applicable only if **Call Direction** is either **Both** or **Incoming**. Otherwise, an **N/A** appears in the field. This is the Calling Line ID (the telephone number of the calling party) of this remote node. If you enable the CLID Authen field in Menu 13 Default Dial In, your ISDN Router/Hub will check the CLID in the incoming call against the CLIDs in the database. If no match is found and CLID Authen is Required, the call will be dropped.	
Incoming:	Callback	This field is applicable only if **Call Direction** is **Both**. Otherwise, an **N/A** appears in the field. This field determines whether or not your ISDN Router/Hub will call back after receiving a call from this remote node. If this option is enabled, your ISDN Router/Hub will disconnect the initial call from this node and call it back at the Outgoing Primary Phone Number (see below).	**Enable** **Disable**
Outgoing:	My Login Name	This is a required field [?] if **Call Direction** is either **Both** or **Outgoing**. Enter the login name for your ISDN Router/Hub when it calls this remote node.	
Outgoing:	My Password	This is a required field [?] if **Call Direction** is either **Both** or **Outgoing**. Enter the password for your ISDN Router/Hub when it calls this remote node.	
Outgoing:	Authen	This field sets the authentication protocol used for outgoing calls. Options for this field are: ● **CHAP/PAP** - Your ISDN Router/Hub will accept either CHAP or PAP when requested by this remote node. ● **CHAP** - accept CHAP only. ● **PAP** - accept PAP only.	 **CHAP/PAP** **CHAP** **PAP**

Outgoing: Pri(mary) Sec(ondary) Phone Numbers	Your ISDN Router/Hub always calls this remote node using the Primary Phone number first for a dial-up line. If the Primary Phone number is busy or does not answer, your ISDN Router/Hub will dial the Secondary Phone number if available. Some areas require dialing the pound sign # before the phone number for local calls. A # symbol may be included at the beginning of the phone numbers as required.	
Route	This fields determines the protocols that your ISDN Router/Hub will route.	
Bridge	Bridging is used for protocols that the ISDN Router/Hub doe not support, e.g., SNA, or not turned on in the previous Route field. When bridging is enabled, your ISDN Router/Hub will forward any packet that it does not route to this remote node; otherwise, the packets are discarded. .	Press space bar to toggle **Yes/No**
Edit PPP Options	To edit the PPP options for this remote node, move the cursor to this field, use the space bar to select **Yes** and press [Enter]. This will bring you to Menu 11.2 - Remote Node PPP Options. For more information on configuring PPP options, see the section *Editing PPP Options.*	Press space bar to toggle **Yes** then press [Enter]
Rem IP Addr	This is a required field [?] if **Route** is set to **IP**. Enter the IP address of the remote gateway.	
Edit IP/IPX/Bridge Options	To edit the parameters, select **Yes** and press [Enter]. This will bring you to Menu 11.3 - Remote Node Network Layer Options. For more information on this screen, refer to the chapter pertaining to your specific protocol.	Press space bar to toggle **Yes** then press [Enter]

Telco Options:
 	
   Allocated Budget (min)
 	
   Period (hr)
	This field sets a ceiling for outgoing call time for this remote node. The default for this field is 0 for no budget control.
	
	This field sets the time interval to reset the above outgoing call budget control.
		Default = 0

Transfer Type	This field specifies the type of connection between the ISDN Router/Hub and this remote node. When set to **Leased**, the **Allocated Budget** and **Period** do not apply.	**64k/Modem/** **Leased**

ISDN Router/Hub *RA368 WAN Bridge/Routers*

Nailed-up Connection	This field specifies if you want to make the connection to this remote node a nailed-up connection. See below for more details.	**Yes/No**
Session Option: Edit Filter Sets	Use the space bar to toggle this field to Yes and press [Enter] to open Menu 11.5 to edit the filter sets. See the Remote Node Filter section for more details.	Default=Blank
Session Option: Idle Timeout (sec)	This value specifies the number of idle seconds that elapses before the remote node is automatically disconnected. Idle seconds is the period of time when no data is transmitted from your ISDN Router/Hub. Administrative packets such as RIP are not counted as data. The default is 300 seconds (5 minutes). *This option only applies when the ISDN Router/Hub initiates the call.*	Default=300sec
Once you have completed filling in Menu 11.1.1 Remote Node Profile, press [Enter] at the message [Press ENTER to Confirm to save your configuration, or press [Esc] at any time to cancel.		

4.1.2 Nailed-up Connection

A nailed-up connection is a dial-up line where the connection is always up regardless of traffic demand. The ISDN Router/Hub does two things when you specify a nailed-up connection. The first is that idle timeout is disabled. The second is that the ISDN Router/Hub will try to bring up the connection at power-on and whenever the connection is down.

A nailed-up connection can be very expensive for obvious reasons. Please do not specify a nailed-up connection unless your telephone company offers flat-rate service or you need a constant connection and the cost is of no concern.

4.1.3 Outgoing Authentication Protocol

Generally speaking, you should employ the strongest authentication protocol possible, for obvious reasons. However, some vendor   implementation includes specific authentication protocol in the user profile. It will disconnect if the negotiated protocol is different from that in the user profile, even when the negotiated protocol is stronger than specified. If you encounter the case where the peer disconnects right after a successful authentication, please make sure that you specify the correct authentication protocol when connecting to such an implementation.

4.1.4 PPP Multilink

The ISDN Router/Hub uses the PPP Multilink Protocol (PPP/MP) to bundle multiple links in a single connection to boost the effective throughput between two nodes. The bundle works best when the member links are of the same type of call (e.g., modem vs. ISDN) and at approximately the same speed.

Due to the fragmentation/reconstruction overhead associated with MP, you may not get a linear increase in throughput when a link is added.

The number of links in an MP bundle can be statically configured, or dynamically determined at runtime, as explained in the following section.

4.1.5 Bandwidth on Demand

The Bandwidth on Demand (BOD) feature adds or subtracts links dynamically according to traffic demand. After the initial call, the ISDN Router/Hub uses BAP (Bandwidth Allocation Protocol) to ask the peer for additional telephone number if BACP (Bandwidth Allocation Control Protocol) is negotiated. Otherwise, the ISDN Router/Hub uses the statically configured (primary and secondary) telephone numbers of the remote node.

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

Table 4-2 BTR v MTR for BOD

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

ISDN Router/Hub *RA368 WAN Bridge/Routers*

BTR & MTR Setting	No. of channel(s) used	Max No. of channel(s) used	Bandwidth on demand
BTR = 128, MTR = 128	2	2	Off

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

The **Target Utility** specifies the line utilization range at which you want the ISDN Router/Hub to add or subtract bandwidth. The range is 30 to 64 kbps (kilobits per second). The parameters are separated by a   For example,   0-60   means the add threshold is 30 kbps and subtract threshold is 60 kbps. The ISDN Router/Hub performs bandwidth on demand only if it initiates the call. Addition and subtraction are based on the value set in the **BOD Calculation** field. If this field is set to **Transmit or Receive**, then traffic in either direction will be included to determine if a link should be added or dropped. **Transmit** will only use outgoing traffic to make this determination and **Receive** will only use incoming traffic to make this determination.

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

The BOD configuration is through Menu 11.2 - Remote Node PPP Options.

4.1.6 Editing PPP Options

To edit the remote node PPP Options, move the cursor to the **Edit PPP Options** field in Menu 11.1 - Remote Node Profile, and use the space bar to select **Yes**. Press **Enter** to open Menu 11.2, as shown below.

```
                    Menu 11.2 - Remote Node PPP Options

            Encapsulation= Standard PPP
            Compression= No

            Multiple Link Options:
              BOD Calculation= Transmit or Receive
            Base Trans Rate(Kbps)= 64
            Max Trans Rate(Kbps)= 64
              Target Utility(Kbps)= 32-48
              Add Persist(sec)= 5
              Subtract Persist(sec)= 5



              Press ENTER to CONFIRM or ESC to CANCEL:
    Press Space Bar to Toggle.
```
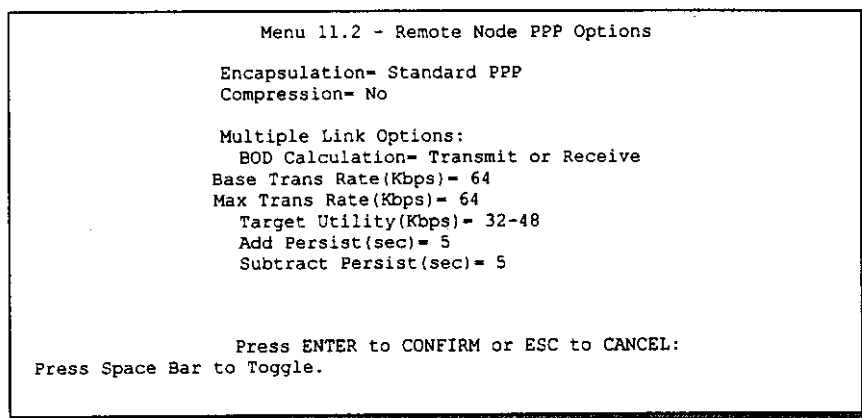
Figure 4-3 Menu 11.2 - Remote Node PPP Options

The following table describes the Remote Node PPP Options Menu, and contains instructions on how to configure the PPP options fields.

Table 4-3 Remote Node PPP Options Menu Fields

Field	Description	Option
Encapsulation	Select the CISCO PPP only when this remote node is a Cisco machine; otherwise, select the Standard PPP.	**Standard PPP** **CISCO PPP**
Compression	Turn on/off Stac Compression. The default for this field is **Off**.	**On/Off** (Default = **Off**)
Multiple Link Options:		
BOD Calculation	Select the direction of the traffic you wish to use in determining when to add or subtract a link. The default for this field is **Transmit or Receive**.	Default = **Transmit or Receive**
Base Trans Rate	Select the base data transfer rate for this remote node in Kbps. There are two choices for this field- **64** where only one channel is used or **128** where	**64/128**

ISDN Router/Hub *RA368 WAN Bridge/Routers*

	two channels are used as soon as a packet triggers a call	
Max Trans Rate	Enter the maximum data transfer rate allowed for this remote node. This parameter is in kilobits per second. There are two choices for this field- same as above.	**64/128**
Target Utility (kbps)	Enter the two thresholds separated by a [-] for subtracting and adding the second port.	Default=10-20
Add Persist	This parameter specifies the number of seconds where traffic is above the adding threshold before the ISDN Router/Hub will bring up the second link.	Default = 5 sec
Subtract Persist	This parameter specifies the number of seconds where traffic is below the subtraction threshold before your ISDN Router/Hub drops the second link.	Default = 5 sec
Once you have completed filling in Menu 11.2 - Remote Node PPP Options, press [Enter] at the message [Press ENTER to Confirm to save your configuration, or press [Esc] at any time to cancel.		

4.1.7 Remote Node Filter

Use **Menu 11.5 – Remote Node Filter** to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the ISDN Router/Hub and to prevent certain packets from triggering calls. You can specify up to 4 filter sets separated by comma, e.g., 1, 5, 9, 12, in each of the **filters** field. The default is no filters.

Note that spaces are accepted in this field. For more information on defining the filters, *see Chapter 9.* The ISDN Router/Hub comes with a prepackaged filter set, NetBIOS_WAN, that blocks NetBIOS packets. You can include this in the call filter sets if you wish to prevent NetBIOS packets from triggering calls to a remote node.

```
                    Menu 11.5 - Remote Node Filter

        Input Filter Sets:
          protocol filters=
            device filters=
        Output Filter Sets:
          protocol filters=
            device filters=
        Call Filter Sets:
          protocol filters= 1
            device filters=
```

Figure 4-4 Menu 11.5 – Remote Node Filter

Chapter 5
Remote Node TCP/IP Configuration

This chapter shows you how to configure the TCP/IP parameters of a remote node. A typical LAN-to-LAN application is to use your ISDN Router/Hub to connect a branch office to the headquarters, as depicted in the folllowing diagram.

5.1 LAN-to-LAN Application
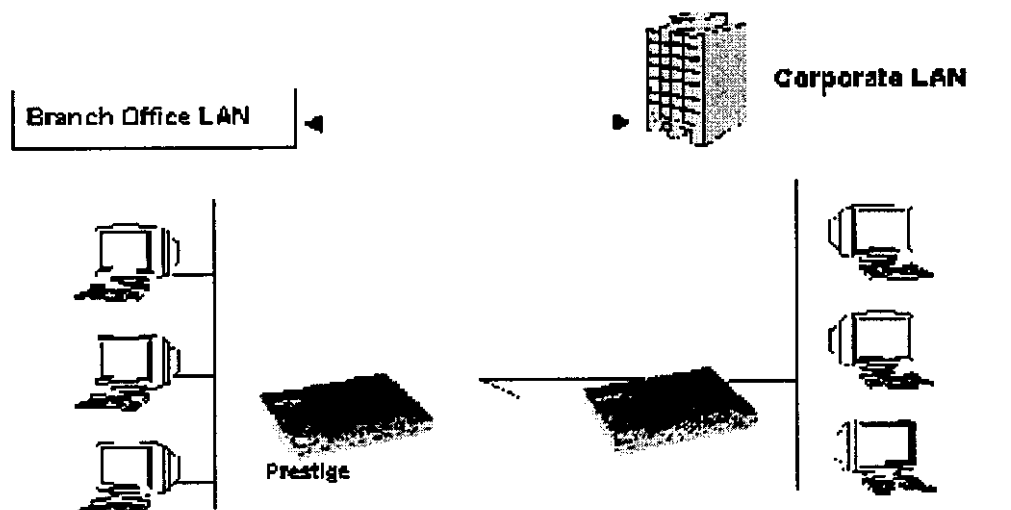
Figure 5-1 TCP/IP LAN-to-LAN Application

For the branch office, you need to configure a remote node in order to dial out to the headquarters. Additionally, you may also need to define static routes if some services reside beyond the immediate remote LAN.

ISDN Router/Hub *RA368 WAN Bridge/Routers*

5.1.1 Remote Node Setup

Follow the procedure in *Chapter 5 - Remote Node Configuration* to configure the protocol-independent parameters in Menu 11 - Remote Node Profile. For the TCP/IP parameters, follow the instructions below. If you are configuring your ISDN Router/Hub to receive incoming calls, you also need to set the default dial-in parameters in Menu 13.

Follow the steps below to edit Menu 11.3 - Remote Node Network Layer Options shown below.

In Menu 11.1, make sure **IP** is among the protocols in the Route field. (The Route field should display Route = IP or Route = IP + IPX.)

Move the cursor to the **Edit IP/IPX/Bridge** field, then press the space bar to toggle and set the value to **Yes**. Press [Enter] to open Menu 11.3 - Network Layer Options.

```
              Menu 11.3 - Remote Node Network Layer Options

     IP Options:                        IPX Options:
        Rem IP Addr: 0.0.0.0               Dial-On-Query= N/A
        Rem Subnet Mask= 0.0.0.0           Rem LAN Net #= N/A
        My WAN Addr= 0.0.0.0               My WAN Net #= N/A
        Single User Account= No           Hop Count= N/A
                                          Tick Count= N/A
        Metric= 2                         W/D Spoofing(min)= N/A
        Private= No                       SAP/RIP Timeout(min)= N/A
        RIP Direction= Both
           Version= RIP-2B                Bridge Options:
                                          Dial-On-Broadcast= N/A
                                          Ethernet Addr Timeout(min)= N/A


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

Figure 5-2 Menu 11.3- Remote Node TCP/IP Options

The following diagram explains the Sample IP Addresses to help you to understand the field of **My Wan Addr** in Menu 11.3.

Remote Network   **Local Network**
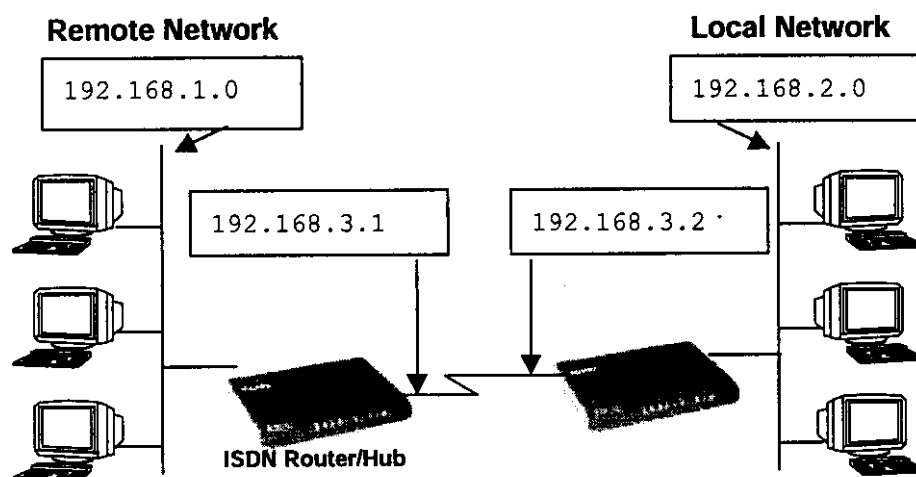
Figure 5-3 Sample IP Addresses for a TCPI/IP LAN-to-LAN Connection

To configure the TCP/IP parameters of a remote node, first configure the three fields in Menu 11 Remote Node Profile, as shown in the table below. For more details on the IP Option fields, refer to *Chapter 3 – Internet Access Application.*

Table 5-1 TCP/IP related fields in Remote Node Profile

Field	Description	Option
Route	Make sure **IP** is among the protocols in the **Route** field in the Remote Node Profile.	**IP**
Rem IP Address	Enter the IP address of the remote gateway in Remote Node Profile.	
Edit IP/IPX/Bridge	Press the space bar to select **Yes** and press **Enter** to go to Menu 11.3 - Remote Node Network Layer Options Menu.	**Yes** **(Yes/No)**

The following table shows the TCP/IP related fields in Menu 11.3 - Remote Node Network Layer Options.

Table 5-2 TCP/IP Remote Node Configuration

Rem IP Address	This will show the IP address you entered for this remote node in the previous menu.	
Rem IP Subnet Mask	Enter the subnet mask for the remote network.	
My WAN Addr	Some implementations, especially the UNIX derivatives, require the ISDN link to have a separate IP network number from the LAN and each end must have a unique address within the WAN network number. If this is the case, enter the IP address assigned to the ISDN port of your ISDN Router/Hub. Note that this is the address assigned to your local ISDN Router/Hub, not the remote router.	
Single User Account	Set this field to **Yes** to enable the Single User Account feature for your ISDN Router/Hub. Use the space bar to toggle between **Yes** and **No**. *See Chapter 3 - Internet Access Application* for more information on the Single User Account feature.	**Yes/No**
Metric	The metric represents the ost of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.	**1 to 15**
Private	This parameter determines if the ISDN Router/Hub will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and not included in RIP broadcast. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.	**Yes/No**
RIP	Press the space bar to select the **RIP direction** from **Both/In Only/Out Only**.	(Default=**Both**)
Version=	Press the space bar to select the RIP version from **RIP-1/RIP-2B/RIP-2M.**	RIP-1 (default)

> Once you have completed filling in the Network Layer Options Menu, press [Enter] to return to Menu 11. Press [Enter] at the message [Press ENTER to Confirm...] to save your configuration, or press [Esc] at any time to cancel.

5.1.2 Static Route Setup

Static routes tell the ISDN Router/Hub routing information that it cannot learn automatically through other means. This can arise in cases where RIP is disabled on the LAN or a remote network is beyond the one that is directly connected to a remote node.

Each remote node specifies only the network to which the gateway is directly connected, and the ISDN Router/Hub has no knowledge of the networks beyond. For instance, the ISDN Router/Hub
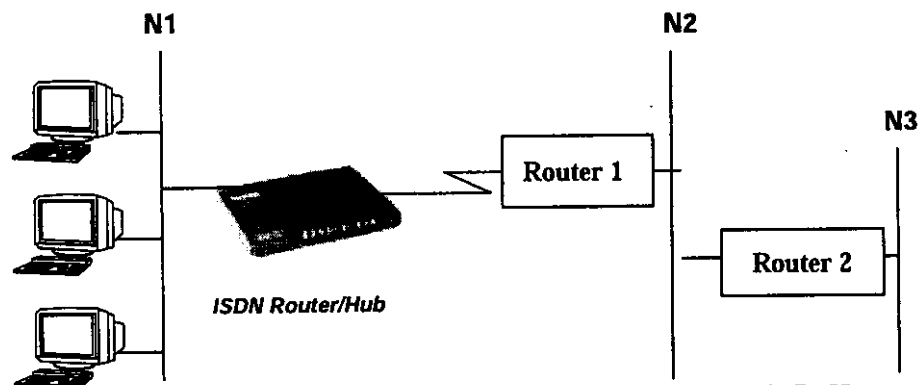
knows about network N2 in the following diagram through remote node R. However, the ISDN Router/Hub is unable to route a packet to network N3 because it doesn't know that there is a route through remote node R. The static routes are for you to tell the ISDN Router/Hub about the networks beyond the remote nodes.

Figure 5-4 Example of Static Routing Topology

To configure an IP static route, use Menu 12, Static Route Setup, as displayed below.

```
                        Menu 12 - Static Route Setup
```
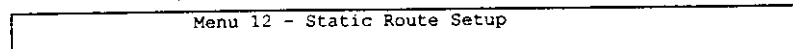
ISDN Router/Hub *RA368 WAN Bridge/Routers*

```
1. IP Static Route
2. IPX Static Route
3. Bridge Static Route

Please enter selection:
```

Figure 5-5 Menu 12 - Static Route Setup

From Menu 12, select one of the available IP static routes to open Menu 12.1 - IP Static Route
Setup, as shown below.

```
                Menu 12.1 - IP Static Route Setup

                1. _____
                2. _____
                3. _____
                4. _____
                5. _____
                6. _____
                7. _____
                8. _____




                Enter selection number:
```

Figure 5-6 Menu 12.1 - IP Static Route Setup

Choosing a static route to edit produces the following screen.

```
                Menu 12.1.1 - Edit IP Static Route

        Route #: 1
        Route Name= ?
        Active= No
        Destination IP Address= ?
        IP Subnet Mask= ?
        Gateway IP Address= ?
        Metric= 2
        Private= No

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

Figure 5-7Edit IP Static Route

The following table describes the fields for Menu 12.1.1 Edit IP Static Route Setup.

Table 5-3 Edit IP Static Route Menu Fields

Field	Description
Route Name	Enter a descriptive name for this route. This is for identification purpose only.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the subnet mask for this destination. Follow the discussion on IP subnet mask in this chapter.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your ISDN Router/Hub that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your ISDN Router/Hub; over WAN, the gateway must be the IP address of one of the remote nodes.
Metric	Same meaning as those in the Remote Node Setup.
Private	Same meaning as those in the Remote Node Setup.

Chapter 6
IPX Configuration

This chapter shows you how to configure the IPX parameters of the ISDN Router/Hub.

6.1 IPX Network Environment

Novell bundles the protocol stack, the server software and routing functionality in their NetWare server products. So a NetWare server is not only a file or print server, it is also a router.

6.1.1 Network and Node Number

Every IPX machine has a network number and a node number, together they form the complete address of the machine. The IPX network number is a 32-bit quantity and is usually expressed in 8 hexadecimal digits, e.g., 0893A8CF. The host number is a 48-bit quantity and usually is taken from the MAC (Media Access Control) address of the Ethernet hardware, so you don't have to explicitly configure the node number.

An IPX client obtains its network number from a server that has the network numbers statically configured. If there are multiple servers on a network, only one server need to have the network numbers configured, and all other stations (clients and servers) can obtain the network numbers from it. The server with configured network numbers is called a seed router.

If you have a NetWare server on the same LAN as the ISDN Router/Hub, we recommend that you set up a NetWare server as a seed router. Even though the ISDN Router/Hub is capable as a seed router, a NetWare server offers a much more extensive facility for network management.

6.1.2 Frame Types

IPX can run on top of four different frame types on the Ethernet. These frame types are 802.2, 802.3, Ethernet II (DIX), and SNAP (Sub-Network Access Protocol). Each frame type is a separate logical network, even though they exist on one physical cable.

Although there are four frame types available on the Ethernet, you should configure as few frame types as possible on your NetWare server and use automatic frame detection on the clients to simplify management and to reduce network overhead.

ISDN Router/Hub *RA368 WAN Bridge/Routers*

6.1.3 External Network Number

Each of the four logical networks (based on frame type) has its own external network number.

6.1.4 Internal Network Number

In addition to the external network numbers, each NetWare server has its own internal network number that is a virtual network to which the server is attached. It is important to remember that every network number must be unique for that entire internetwork, either internal or external.
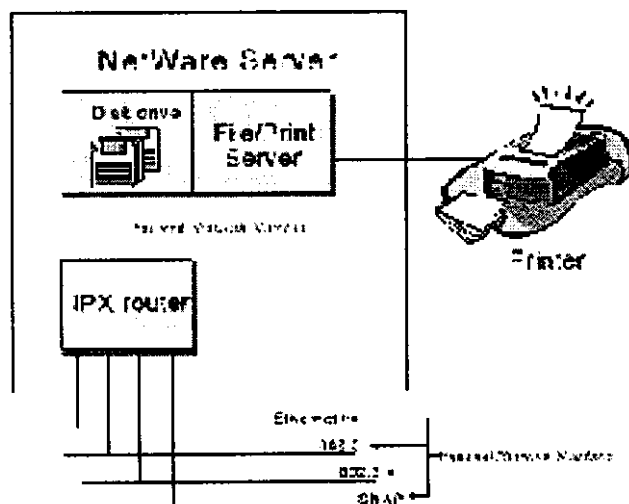
Figure 6-1 Netware Server

6.2   ISDN Router/Hub in an IPX Environment

There are two scenarios in which your ISDN Router/Hub is deployed, depending on whether there is a NetWare server on the LAN, as depicted in the following diagram.
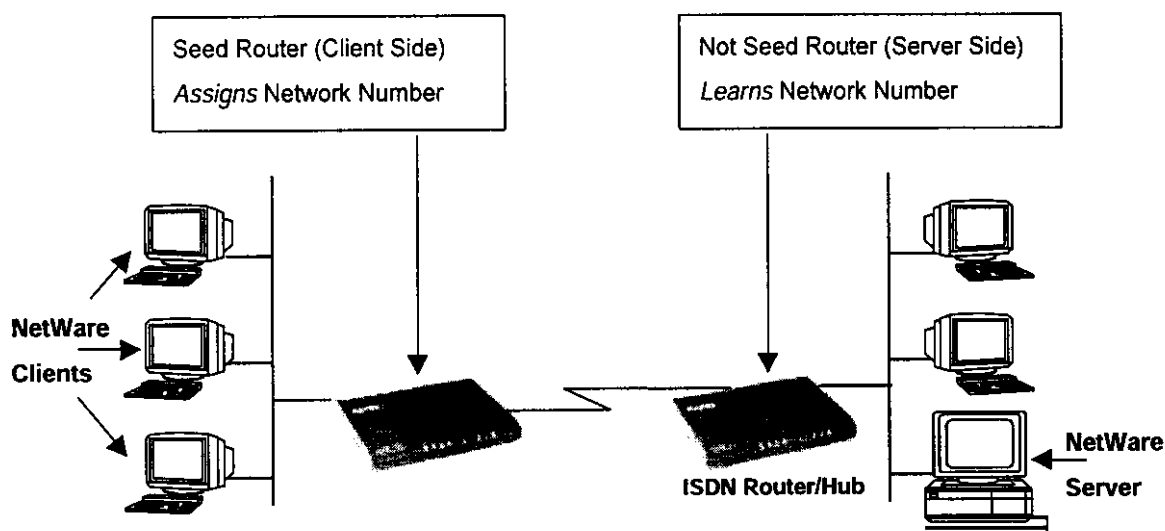
Figure 6-2 ISDN Router/Hub in an IPX Environment

6.2.1   ISDN Router/Hub on LAN with Server

If your ISDN Router/Hub is on a LAN with a seed router, you do not need to configure the LAN network numbers. Your ISDN Router/Hub will learn the network number from the seed router and add the routes to its routing table.

6.2.2   ISDN Router/Hub on LAN without Server

Each IPX network must have a seed router. If you only have NetWare clients on your network, then you must configure the ISDN Router/Hub as a seed router and set up unique network numbers for each frame type enabled using the Ethernet Setup Menu.

ISDN Router/Hub *RA368 WAN Bridge/Routers*

6.3   IPX Spoofing
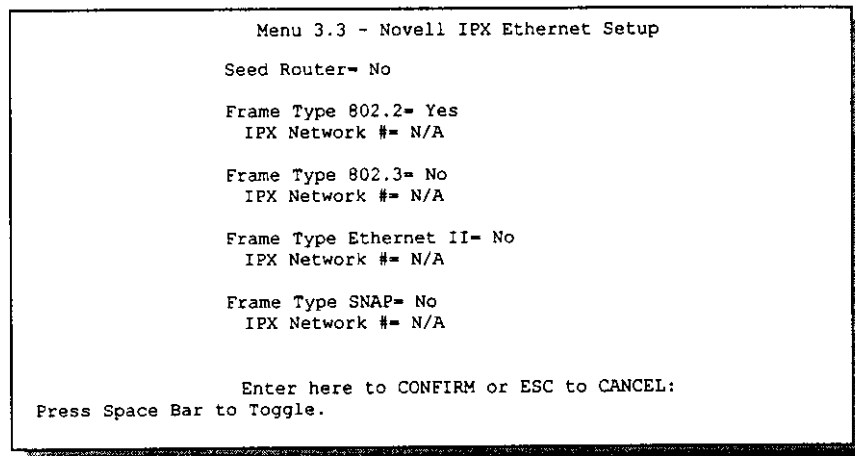
Your ISDN Router/Hub comes with several pre-defined call filters designed to prevent certain IPX packets from triggering a call to a remote node.

The built-in call filters are defined as follows:

- Block periodical RIP (Routing Information Protocol) and SAP (Service Advertising Protocol) response messages.

- Block NetWare serialization packets.

- Allow SAP and RIP inquiry packets.

6.4 IPX Ethernet Setup

From Menu 3 - Ethernet Setup, select option **Novell IPX Setup** to go to Menu 3.3 - Novell IPX Ethernet Setup as shown in the figure below.

```
                    Menu 3.3 - Novell IPX Ethernet Setup

              Seed Router- No

              Frame Type 802.2- Yes
                IPX Network #- N/A

              Frame Type 802.3- No
                IPX Network #- N/A

              Frame Type Ethernet II- No
                IPX Network #- N/A

              Frame Type SNAP- No
                IPX Network #- N/A


                    Enter here to CONFIRM or ESC to CANCEL:
        Press Space Bar to Toggle.
```

Figure 6-3 Menu 3.3 - Novell IPX Ethernet Setup

The following table describes the Novell IPX Ethernet Setup Menu.

Table 6-1 Novell IPX Ethernet Setup Fields

Field	Description	Options
Seed Router	Determine if your ISDN Router/Hub is to act as a seed router.	**Yes/No**
Frame Type	Enable/Disable the individual frame type. Remember to enable only the ones that are actually used on your network.	**802.2** **802.3** **Ethernet II** **SNAP**
IPX Network #	If your ISDN Router/Hub is a seed router, enter a unique network number for each frame type enabled.	
Press [Enter] at the message [Press ENTER to Confirm ...] to save your configuration, or press [Esc] at any time to cancel.		

ISDN Router/Hub *RA368 WAN Bridge/Routers*

6.5   LAN-to-LAN Application with Novell IPX

A typical LAN-to-LAN application is to use your ISDN Router/Hub to call from a branch office
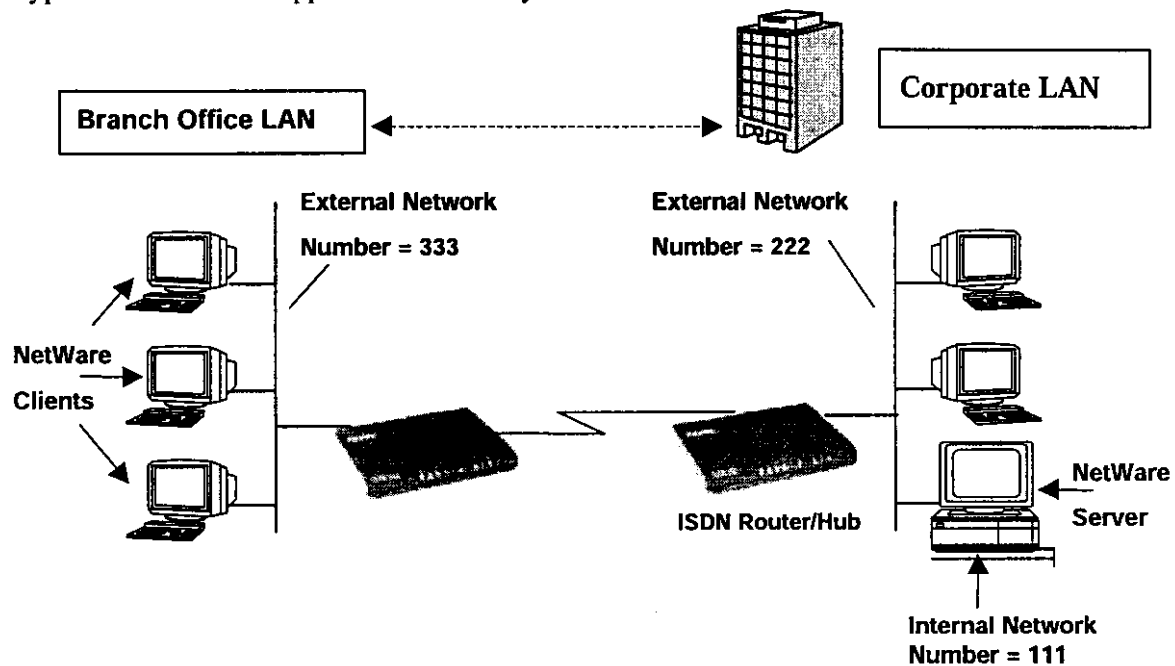
to the corporate headquarters to enable the stations in the branch office to access the NetWare servers at the headquarters, as depicted in the figure below.

Figure 6-4 LAN-to-LAN Application with Novell IPX

6.5.1 IPX Remote Node Setup

Follow the procedure in *Chapter 5* to configure the protocol-independent parameters in Menu 11.1 - Remote Node Profile. For the IPX-specific parameters in Menu 11.3 - Remote Node Network Layer Options, follow the instructions below. If you want the ISDN Router/Hub to receive incoming calls, you must also configure the default dial-in parameters in Menu 13.

To edit Menu 11.3 - Remote Node Network Layer Options shown below, follow these steps:

Step 1. In Menu 11.1, make sure **IPX** is among the protocols in the Route field. (The Route field should display Route = IPX or Route = IP + IPX.)

Step 2. Move the cursor to the **Edit IP/IPX/Bridge** field, then press the space bar to select **Yes** and press [Enter] to open Menu 11.3 - Network Layer Options.

```
              Menu 11.3 - Remote Node Network Layer Options


     IP Options:                         IPX Options:
       Rem IP Addr:                        Dial-On-Query= No
       Rem Subnet Mask= N/A                Rem LAN Net #= 00000000
       My WAN Addr= N/A                    My WAN Net #= 00000000
       Single User Account= N/A           Hop Count= 1
         Server IP Addr= N/A              Tick Count= 2
       Metric= N/A                        W/D Spoofing(min)= 3
       Private= N/A                       SAP/RIP Timeout(min)= 3
       RIP Direction= N/A
         Version= N/A                   Bridge Options:
                                          Dial-On-Broadcast= N/A
                                          Ethernet Addr Timeout(min)= N/A



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

Figure 6-5 Menu 11.3 - Remote Node Novell IPX Options

The table below describes the IPX-specific parameters of the remote node setup.

Table 6-2 Remote Node Novell IPX Options

Field	Description	Option
Dial-On-Query	This field is necessary for your ISDN Router/Hub on the client side. When set to **Yes**, any Get Service SAP or RIP broadcasts will trigger your ISDN Router/Hub to make a call to that remote node.	**Yes/No**
Rem LAN Net #	In this field, enter the internal network number of the NetWare server on the remote LAN.	
My WAN Net #	In this field, enter the network number of the ISDN link. If you leave this field as **00000000**, your ISDN Router/Hub will determine automatically the network number through negotiation with the PPP peer.	**00000000** (default)
Hop Count	This field indicates the number of intermediate networks that must be passed through to reach the remote node.	**1** (default)
Tick Count	This field indicates the time-ticks required to reach the remote node.	**2** (default)
W/D Spoofing (min)	This field is for the ISDN Router/Hub on the server side. Your ISDN Router/Hub can spoof a response to a server WatchDog request after the connection is dropped. In this field, type in the time (number of minutes) that you want your ISDN Router/Hub to spoof the WatchDog response.	
SAP/RIP Timeout (min)	This field indicates the amount of time that you want your ISDN Router/Hub to maintain the SAP and RIP entries learned from this remote node in its internal tables after the connection has been dropped. If this information is retained, then your ISDN Router/Hub will not have to get the SAP information when the line is brought back up. Enter the time (number of minutes) in this field.	
Once you have completed filling in the Network Layer Options Menu, press [Enter] to return to Menu 11.1. Then press [Enter] at the message [Press ENTER to Confirm] to save your configuration, press [Esc] to cancel.		

6.5.2 IPX Static Route Setup

Similar to IP, IPX static routes tell the ISDN Router/Hub how to reach servers beyond a remote node before a connection to that remote node is established.

From Menu 12, select two, then select one of the IPX Static Routes to open Menu 12.2.1 - Edit IPX Static Route, as shown below.

```
                  Menu 12.2.1 - Edit IPX Static Route

            Route #= 11
            Server Name= ?
            Active= Yes
            Network #= ?
            Node #= 000000000001
            Socket #= 0451
            Type #= 0004
            Hop Count= 2
            Tick Count= 3
            Gateway Node= 1



            Press ENTER to CONFIRM or ESC to CANCEL:
```

Figure 6-6 Menu 12.2 - Edit IPX Static Route

The following table contains the instructions on how to configure the Edit IP Static Route Menu.

Table 6-3 Edit IPX Static Route Menu Fields

Field	Description
Server Name	In this field, enter the name of the server. This must be the *exact* name configured in the NetWare server.
Network #	This field contains the internal network number of the remote server that you wish to access. [00000000] or [FFFFFFFF] are reserved.
Node #	This field contains the address of the node on which the server resides. If you are using a Novell IPX implementation, this value is [000000000001].
Socket #	This field contains the socket number on which the server will receive service requests. The default for this field is hex [0451].
Type #	This field identifies the type of service the server provides. The default for this field is hex [0004].
Gateway Node	In this field, enter the number of the remote node that is the gateway for this static route.
Hop Count and Tick Count	These two fields have the same meaning as those in the Ethernet setup.
Once you have completed filling in the menu, press [Enter] at the message [Press ENTER to Confirm to save your configuration, or press [Esc] to cancel to cancel.	

Chapter 7
Bridging Setup

This chapter shows you how to configure the bridging parameters of your ISDN Router/Hub.

7.1 Bridging in General

Bridging bases the forwarding decision on the MAC (Media Access Control), or hardware, address, while routing does it on the network layer (IP or IPX) address. Bridging allows the ISDN Router/Hub to transport packets of network layer protocols that the ISDN Router/Hub does not route, e.g., SNA, from one network to another. The caveat is that, compared to routing, bridging generates more traffic for the same network layer protocol, and it also demands more CPU cycles and memory.

For efficiency reason, do *not* turn on bridging unless you need to support protocols other than IP and IPX on your network. For IP and IPX, enable the respective routing if you need it; do not bridge what the ISDN Router/Hub can route.

7.2 Bridge Ethernet Setup

Basically, all non-local packets are bridged to the WAN; however, your ISDN Router/Hub applies special handling for certain IPX packets to reduce the number of calls, depending on the setting of the **Handle IPX** field.

From Menu 3 - Ethernet Setup, enter option **Bridge Setup** and Menu 3.5 - Bridge Ethernet Setup displays as shown below.

```
                   Menu 3.5 - Bridge Ethernet Setup


               Handle IPX= None




               Press ENTER to CONFIRM or ESC to CANCEL:
   Press Space Bar to Toggle.
```

Figure 7-1 Menu 3.5 - Bridge Ethernet Setup

The following table describes how to configure the **Handle IPX** field in Menu 3.5.

Table 7-1 Bridge Ethernet Setup Menu - Handle IPX Field Configuration

Handle IPX Field (Menu 3.5)	Description
None	When there is no IPX traffic on the LAN or when you do not want to apply any special handling for IPX.
Client	When there are only client workstations on the LAN. RIP and SAP (Service Advertising Protocol) response packets will not trigger calls.
Server	When there are only IPX servers on the LAN. No RIP or SAP packets will trigger calls. In addition, during the time when the line is down, your ISDN Router/Hub will reply to watchdog messages from the servers on behalf of remote clients. The period of time that your ISDN Router/Hub will do this is linked to the Ethernet Address Timeout parameter in each remote node (see Remote Node Configuration). When a remote Ethernet address is aged out, there is no need to maintain its connection to the IPX server.

Router/Hub

If there are both clients and servers on the LAN, and the local clients will access the remote servers, set this field to **Server** but turn on the **Dial-On-Broadcast** parameter in Menu 11.3 to allow the client queries to trigger calls.

7.2.1 Remote Node Bridging Setup

Follow the procedure in *Chapter 5* to configure the protocol-independent parameters in Menu 11.1 - Remote Node Profile. For bridging-specific parameters, you need to configure Menu 11.3 - Remote Node Network Layer Options.

To setup Menu 11.3 - Remote Node Network Layer Options, follow these steps:

Step 1.   In Menu 11.1, make sure the **Bridge** field is set to **Yes**.

```
             Menu 11.3 - Remote Node Network Layer Options

     IP Options:                      IPX Options:
       Rem IP Addr:                     Dial-On-Query= No
       Rem Subnet Mask= N/A             Rem LAN Net #= 00000000
       My WAN Addr= N/A                 My WAN Net #= 00000000
       Single User Account= N/A         Hop Count= 1
         Server IP Addr= N/A            Tick Count= 2
       Metric= N/A                      W/D Spoofing(min)= 3
       Private= N/A                     SAP/RIP Timeout(min)= 3
       RIP Direction= N/A
         Version= N/A                 Bridge Options:
                                        Dial-On-Broadcast= No
                                        Ethernet Addr Timeout(min)= 0



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

Step 2.   Move the cursor to the **Edit IP/IPX/Bridge** field, then press the space bar to select **Yes** and press [Enter] to open Menu 11.3 - Network Layer Options.

Figure 7-2 Menu 11.3 - Remote Node Bridging Options

ISDN Router/Hub *RA368 WAN Bridge/Routers*
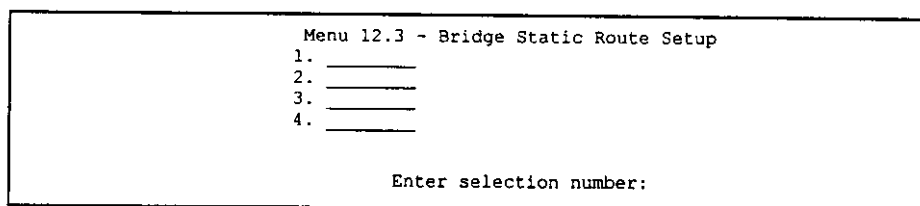
The following table describes the bridging-specific parameters in the Remote Node Profile and Network Layers menus.

Table 7-2 Remote Node Network Layers Menu Bridge Options

Field	Description
Bridge	Make sure this field is set to **Yes**.
Edit IP/IPX/Bridge	Press the space bar to change it to **Yes** and press Enter] to go to the Network Layer Options Menu.
Dial-On-Broadcast	This field is necessary for your ISDN Router/Hub on the caller side LAN. When set to **Yes**, any broadcasts coming from the LAN will trigger your ISDN Router/Hub to make a call to this remote node. If it is set to No, your ISDN Router/Hub will not make the outgoing call.
Ethernet Addr Timeout (min)	In this field, enter the time (number of minutes) that you wish your ISDN Router/Hub to retain the Ethernet Addr information in its internal tables while the line is down. If this information is retained, your ISDN Router/Hub will not have to recompile the tables when the line is brought back up.
Once you have completed filling in the Network Layer Options Menu, press [Enter] to return to Menu 11.1. Then press [Enter] at the message [Press ENTER to Confirm to save your configuration, or press [Esc] to cancel.	

7.3 Bridge Static Route Setup

Similar to network layer static routes, a bridging static route tells the ISDN Router/Hub about the route to a node before a connection is established. You configure bridge static routes in Menu 12.3.1, by pressing 3 in menu 12 and then selecting one of the bridge static routes as shown
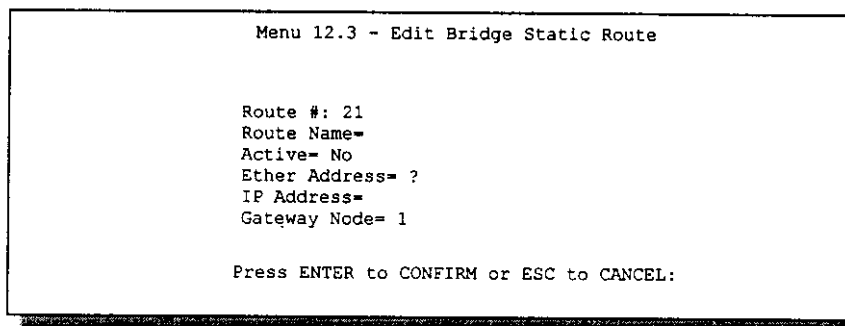
```
                  Menu 12.3 - Bridge Static Route Setup
            1. _____
            2. _____
            3. _____
            4. _____


                       Enter selection number:
```

below.

Figure 7-3 Menu 12.3 - Bridge Static Route Setup

```
                   Menu 12.3 - Edit Bridge Static Route



            Route #: 21
            Route Name=
            Active= No
            Ether Address= ?
            IP Address=
            Gateway Node= 1


            Press ENTER to CONFIRM or ESC to CANCEL:
```

Figure 7-4 Menu 12.3.1 - Edit Bridge Static Route

ISDN Router/Hub *RA368 WAN Bridge/Routers*

The following table describes the Bridge Static Route Menu.

Table 7-3 Bridge Static Route Menu Fields

Field	Description
Route Name	Enter a name for the bridge static route for identification purposes.
Active	Activate/deactivate the static route.
Ether Address	Enter the MAC address of the destination machine that you wish to bridge the packets to.
IP Address	If available, enter the IP address of the destination machine that you wish to bridge the packets to.
Gateway Node	Enter the number of the remote node that is the gateway of this static route. When a packet destination Ethernet (MAC) address matches the value entered above, it will trigger a call to this remote node.
Once you have completed filling in this menu, press [Enter] at the message [Press ENTER to Confirm to save your configuration, or press [Esc] to cancel.	

Chapter 8
Dial-in Server Configuration

You can configure your ISDN Router/Hub to receive calls from remote dial-in users, e.g., telecommuters, as well as remote nodes. There are several differences between dial-in users and remote nodes, as summarized in the table below.

Table 8-1 Remote Dial-in Users/Remote Nodes Comparison Chart

Remote Dial-in Users	Remote Nodes
Your ISDN Router/Hub will only answer calls from remote dial-in users; it will not make call to them.	Your ISDN Router/Hub can make calls to and receive calls from the remote node.
All remote dial-in users share one common set of parameters, as defined in the Default Dial In Setup (Menu 13).	Each remote node can have its own set of parameters such as Bandwidth On Demand, Protocol, Security, etc.

This chapter discusses how to setup default dial-in parameters for both remote node and remote dial-in users. The following sections give two examples of how your ISDN Router/Hub can be configured as a dial-in server.

Due to memory constraints, your ISDN Router/Hub can only store a finite number of users locally. If there are more remote dial-in users than what ISDN Router/Hub can support locally, you can use an external RADIUS server to provide authentication service. For details on using a RADIUS server, see the *Using RADIUS Authentication* section in *Chapter 11 - System Security.*

ISDN Router/Hub *RA368 WAN Bridge/Routers*

8.1 Remote Access Server

Telecommuting enables people to work at remote sites and yet still have access to the resources in the business office. Typically, a telecommuter will use a client workstation with TCP/IP and dial-out capabilities, e.g., a Windows PC or a Macintosh. For telecommuters to call in to your ISDN Router/Hub, you need to configure a dial-in user profile for each telecommuter. Additionally, you need to configure the Default Dial-In Setup to set the operational parameters for all dial-in users.
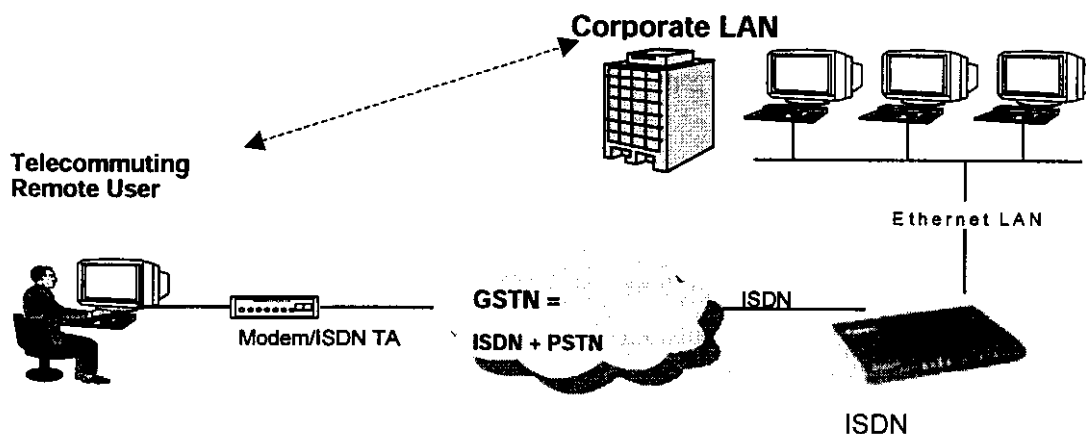
An example of remote access server for telecommuters is shown in .

Figure 8-1 Example of Telecommuting

8.2 LAN-to-LAN Server Application

Your ISDN Router/Hub can also be used as a dial-in server for LAN-to-LAN application to provide access for the workstations on a remote network. For your ISDN Router/Hub to be set up as a LAN-to-LAN server, you need to configure the Default Dial-In Setup to set the operational parameters for incoming calls. Additionally, you must create a remote node for the router on the remote network (*see Chapter 5 - Remote Node Configuration*).

An example of your ISDN Router/Hub being used as a LAN-to-LAN server is shown below.
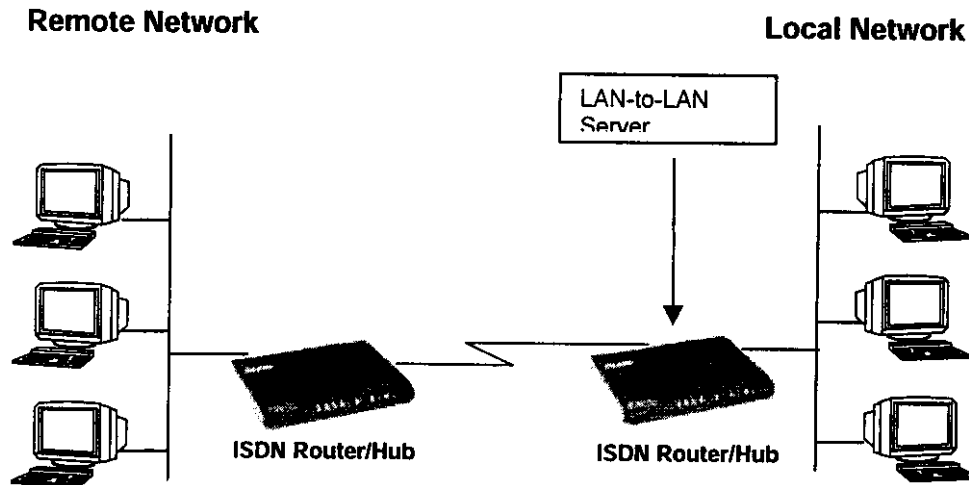
Figure 8-2 Example of a LAN-to-LAN Server Application

8.3 Default Dial-In Setup

This section covers the default dial-in parameters. The parameters in Menu 13 affect incoming calls from both remote dial-in users, and remote nodes until authentication is completed. Once authentication is completed and if it matches a remote node, your ISDN Router/Hub will use parameters from that particular remote node.

```
                    Menu 13 - Default Dial-in Setup

        Telco Options:                  IP Address Supplied By:
          CLID Authen= None                Dial-in User= Yes
                                           IP Pool= No
        PPP Options:                         IP Start Addr= N/A
          Recv Authen= CHAP/PAP              IP Count(1,2)= N/A
          Compression= Yes
          Mutual Authen= No             IPX Net Num Supplied By:
            PAP Login= N/A                IPX Pool= No
            PAP Password= N/A               IPX Start Net Num= N/A
          Multiple Link Options:            IPX Count(2,16)= N/A
            Max Trans Rate= 128
                                        Session Options:
        Callback Budget Management:       Edit Filter Sets= No
          Allocated Budget(min)=          Idle Timeout= 300
          Period(hr)=


                    Press ENTER to CONFIRM or ESC to CANCEL:
        Press Space Bar to Toggle.
```

Figure 8-3 Menu 13 – Default Dial-in Setup

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

The table below describes and contains information on how to configure each parameter in Menu 13   Default Dial-in Setup.

Table 8-2 Default Dial-in Setup Fields

Field	Description	Option
Telco Options: CLID Authen	This field sets the CLID authentication parameter for all incoming calls. There are three options for this field: ● **None** - No CLID is required. ● **Required** CLID must be available, or the ISDN Router/Hub will not answer the call. ● **Preferred** - If the CLID is available then CLID will be used; otherwise, authentication is performed in PPP negotiation.	**None** **Required** **Preferred**
PPP Options:		
Recv. Authen	This field sets the authentication protocol for incoming calls. For security reason, setting authentication to none is strongly discouraged. Options for this field are: ● **CHAP/PAP** - Your ISDN Router/Hub will try CHAP first, but PAP will be used if CHAP is not available. ● **CHAP** Use CHAP only. ● **PAP** Use PAP only. ● **None** Your ISDN Router/Hub tries to acquire CHAP/PAP first, but no authentication is required if CHAP/PAP is not available.	**CHAP/PAP** **CHAP** **PAP** **None**
Compression	Turn on/off Stac Compression. The default for this field is **Off**.	**On** **Off**
Mutual Authen	Some vendors, e.g., Cisco, require mutual authentication, i.e., the node that initiates the call will request a user name and password from the far end that it is dialing to. If the remote node requires mutual authentication, set this field to **Yes**.	**Yes/No**
PAP Login	This field is applicable only if the **Mutual Authen.** Field is set to **Yes**. Enter in the login name to be used to respond to the far end PAP authentication request. This field	

ISDN Router/Hub *RA368 WAN Bridge/Routers*

	does not apply to CHAP authentication.	
PAP Password	This field is applicable only if the **Mutual Authen.** Field is set to **Yes**. Enter in the PAP password to be used to respond to the far end authentication request. This field does not apply to CHAP authentication.	
Multiple Link Options:		
Max Trans Rate	Enter the maximum data transfer rate between your ISDN Router/Hub and the remote dial-in user. **64** - At most, one B channel is used. **128** - A maximum of two channels can be used.. When the ISDN Router/Hub calls back to the remote dial-in user, the maximum data transfer rate is always **64**.	**64/128**
Callback Budget Management:		
Allocated Budget (min)	This field sets the budget callback time for all the remote dial-in users. The default for this field is **0** for no budget control.	Default = **0**
Period (hr)	This field sets the time interval to reset the above callback budget control.	
IP Address Supplied By:		
Dial-in User	If set to **Yes**, the ISDN Router/Hub will allow a remote host to specify its own IP address. If set to **No**, the remote host must use the IP address assigned by your ISDN Router/Hub from the IP pool, configured below. This is to prevent the remote host from using an invalid IP address and potentially disrupting the whole network.	(Default = **Yes**) **Yes/No**
IP Pool	This field tells your ISDN Router/Hub to provide the remote host with an IP address from the pool. This field is required if **Dial-In IP Address Supplied By: Dial-in User** is set to **No**. You can configure this field even if Dial-in User is set to **Yes**, in which case your ISDN Router/Hub will accept the IP address if the remote peer specifies one; otherwise, an IP address is assigned from	**Yes/No** (Default = **No**)

	the pool.	
IP Pool: IP Start Addr	This field is applicable only if you selected **Yes** in the Dial-In IP Address Supplied By: IP Pool field. The IP pool contains contiguous IP addresses and this field specifies the first one in the pool.	
IP Count (1,2)	In this field, enter the number (**1** or **2**,) of addresses in the IP Pool. For example, if the starting address is 192.168.135.5 and the count is 2, then the pool will have 192.68.135.5 and 192.68.135.6	**1, 2**
IPX Net. Num. Supplied By:		
IPX Pool	This field tells your ISDN Router/Hub to provide the remote host with an IPX network number from the pool. Otherwise, your ISDN Router/Hub will generate a random IPX network number.	**Yes/No** (Default = **No**)
IPX Start Net Num	This field is applicable only if you selected **Yes** in the **Dial-In IPX Net. Num. Supplied By: IPX Pool** field. The IPX pool contains contiguous IPX network numbers and this field specifies the first one in the pool.	
IPX Count (2,16)	Enter the number (2 - 16) of network numbers in the IPX Pool. For example, if the starting number is 12345678, and the count is 2, then the IPX pool will have 12345678 and 12345679.	**2 to 16**
Session Options: Edit Filter Sets	Press **Yes**, then [Enter] to edit the filter sets. Keep in mind that the filter set(s) will only apply to remote dial-in users but not the remote nodes. Note that spaces and [-] symbol, are accepted in this field. For more information on customizing your filter sets, *see Chapter 9 - Filter Configuration*. The default is blank, i.e., no filters.	Default = blank
Once you have completed filling in Menu 13 - Default Dial-in Setup, press [Enter] at the message [Press ENTER to Confirm to save your configuration, or press [Esc] at any time to cancel.		

8.3.1 Default Dial-in Filter

Use **Menu 13.1 – Default Dial-in Filter** to specify the filter set(s) to apply to the incoming and outgoing traffic between all dial-in users and your ISDN Router/Hub. Note that the filter set(s) only applies to the dial-in users but not the remote nodes. You can specify up to 4 filter sets separated by comma, e.g., 1, 5, 9, 12, in each of the **filters** field. The default is no filters.

Spaces are accepted in this field. For more information on defining the filters, *see Chapter 9.*

```
                     Menu 13.1 - Default Dial-in Filter

          Input Filter Sets:
            protocol filters=
              device filters=
          Output Filter Sets:
            protocol filters=
              device filters=
```
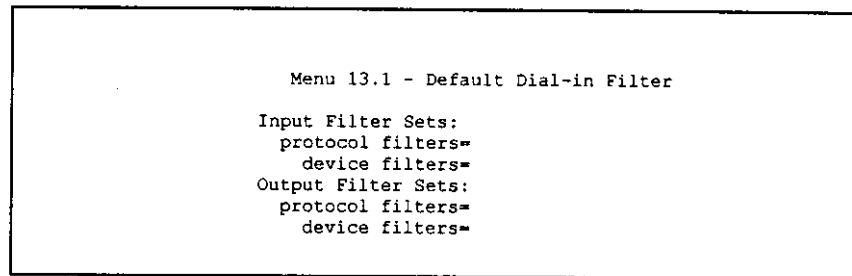
Figure 8-4 Default Dial-in Filter

8.4   Dial-In Users Setup

The following steps describe the setup procedure for setting up a remote dial-in user.

Step 1.   From the Main Menu, enter option 14 to go to Menu 14 - Dial-in User Setup, as shown in the figure below.

Figure 8-5 Menu 14 - Dial-in User Setup

```
                      Menu 14 - Dial-in User Setup                    n/ Router/Hub
            1. johndoe
            2. _____
            3. _____
            4. _____
            5. _____
            6. _____
            7. _____
            8. _____



                      Enter Menu Selection Number:
```

Step 2. Select one of the users by number, this will bring you to **Menu 14.1 - Edit Dial-in User**, as shown below.

```
                      Menu 14.1 - Edit Dial-in User

            User Name= ?
            Active= Yes
            Password= ?
            Callback= No
              Phone # Supplied by Caller= N/A
              Callback Phone #= N/A
            Rem CLID=
            Idle Timeout= 300




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

Figure 8-6 Edit Dial-in User

ISDN Router/Hub *RA368 WAN Bridge/Routers*

The following table provides instructions on how to fill in the Edit Dial-In User fields.

Table 8-3 Edit Dial-in User Menu Fields

Field	Description	Option
User Name	This is a required field. This will be used as the login name for authentication. Choose a descriptive word for login, for example, [johndoe].	
Active	You can disallow dial-in access to this user by setting this field to **Inactive.** Inactive users are displayed with a [-] (minus sign) at the beginning of the name in Menu 14.	**Active** **Inactive**
Password	Enter the password for the remote dial-in user.	
Callback	This field determines if your ISDN Router/Hub will allow call back to this user upon dial-in. If this option is enabled, your ISDN Router/Hub will call back to the user if requested. In such a case, your ISDN Router/Hub will disconnect the initial call from this user and dial back to the specified callback number (see below). ● **No** - The default is no callback. ● **Optional** - The user can choose to disable callback. ● **Mandatory** - The user can not disable callback.	Default=**No** **No** **Optional** **Mandatory**
Phone # Supplied by Caller	This option allows the user to specify the call back telephone number on a call-by-call basis. This is useful when your ISDN Router/Hub returns a call back to a mobile user at different numbers, e.g., a sales rep. In a hotel. ● If the setting is **Yes,** the user can specify and send to the ISDN Router/Hub the callback number of his/her choice. ● The default is **No,** i.e., your ISDN Router/Hub always calls back to the fixed callback number.	Default=**No** **Yes** **No**
Callback Phone #	If **Phone # Supplied by Caller** is **No,** then this is a required field. Otherwise, a **N/A** will appear in the field. Enter the telephone number to which your ISDN Router/Hub will call back.	

Table 8-4 Edit Dial-in User Menu Fields (continued)

Field	Description	Option
Rem CLID	If you enable CLID Authen field in Menu 13, then you need to specify the telephone number from which this user calls. Your ISDN Router/Hub wil check the CLID in the incoming call against the CLIDs in the database. If they do not match and CLID Authen is Required, your ISDN Router/Hub will not answer the call.	
Idle Time-out	Enter the idle time (in seconds). This time-out determines how long the dial-in user can be idle before your ISDN Router/Hub disconnects the call when the ISDN Router/Hub is calling back. Idle time is defined as the period of time where there is no data traffic between the dial-in user and your ISDN Router/Hub. The default is 300 seconds (5 minutes).	Default=300 seconds
Once you have completed filling in Menu 14.1 - Edit Dial-in User, press [Enter] at the message [Press ENTER to Confirm to save your configuration, or press [Esc] at any time to cancel.		

8.4.1 CLID Authentication

CLID (Calling Line IDentification) authentication affords you the security of limiting a user to only initiate connections from a fixed location. The ISDN Router/Hub uses the caller ID sent by the switch to match against the CLIDs in the database. Please note that for CLID authentication to work on the ISDN Router/Hub, your telephone company must support caller ID. You must also include the AT command in the [initAT] string in Menu 2 to enable caller ID detection on the modem.

8.4.2 Callback

Callback serves two purposes. One is security. When set to callback to a fixed number, an intruder will not gain access to your network even if he/she stole the password from your user, because the ISDN Router/Hub always calls back to the pre-configured number.

The other is ease of accounting. For instance, your company pays for the connection charges for telecommuting employees and you use your ISDN Router/Hub as the dial in server. When you turn on the callback option for the dial-in users, all usage is charged to the company instead of the employees, and your accounting department can avoid the hassles of accountability and reimbursement.

ISDN Router/Hub *RA368 WAN Bridge/Routers*

8.5   Multiple Servers behind SUA

If you wish, you can make inside servers for different services, e.g., web or FTP, visible to the outside users, even though SUA makes your whole inside network appear as a single machine to the outside world. A service is identified by the port number, e.g., web service is on port 80 and FTP on port 21.

As an example, if you have a web server at 192.168.1.2 and an FTP server 192.168.1.3, then you need to specify for port 80 (web) the server at IP address 192.168.1.2 and for port 21 (FTP) another at IP address 192.168.1.3.

Please note that a server can support more than one service, e.g., a server can provide both FTP and DNS service, while another provides only web service. Also, since you need to specify the IP address of a server in the ISDN Router/Hub, a server must have a fixed IP address and not be a DHCP client whose IP address potentially changes each time it is powered on.

In addition to the servers for specific services, SUA supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default server is not defined, the service request is simply discarded.

To make a server visible to the outside world, specify the port number of the service and the inside IP address of the server in **Menu 15, Multiple Server Configuration.**

8.5.1 Configuring a Server behind SUA

Follow the steps below to configure a server behind SUA:

1. Enter **15** in the main menu to go to menu 15, **Multiple Server Configuration.**

2. Enter an index number in menu 15 to go to menu 15.1, **SUA Server Configuration.**

3. Enter the service port number in the **Port #** field and the inside IP address of the server in the **IP Address** field.

4. Press **ENTER** at the   ress ENTER to confirm   prompt to save your configuration after you define all the servers or press **ESC** at any time to cancel.

```
              Menu 15 - Multiple Server Configuration
              Port #                 IP  Address
              ----                   ---------------

              1.Default
                                     0.0.0.0
              2. 0
                                     0.0.0.0
              3. 0
                                     0.0.0.0
              4. 0
                                     0.0.0.0
              5. 0
                                     0.0.0.0
              6. 0
                                     0.0.0.0
              7. 0
                                     0.0.0.0
              8. 0
                                     0.0.0.0


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

Figure 8-7 Multiple Server Configuration

The most often used port numbers are:

Table 8-5 Services vs. Port number

Services	Port Number
FTP (File Transfer Protocol)	21
Telnet	23
SMTP (Simple Mail Transfer Protocol)	25
DNS(Domain Name System)	53
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
PPTP (Point-to-Point Tunneling Protocol)	1723

Chapter 9
Advanced Phone Services

The ISDN Router/Hub RA368 supports a comprehensive set of advanced calling features known as Supplemental Services. These features include:

- Call Waiting

- Three Way Calling (conference)

- Call Transfer

- Call Forwarding

9.1   Getting Started

9.1.1 Things you need to know before you start using Supplemental Services.

♦ Additional Call Offering (ACO) is required on your ISDN line in order to use the Call Waiting feature. Flexible Calling is required on your ISDN line in order to use the Three-Way-Calling or Call Transfer features. You need to check with your telephone company to confirm if these services are available to you and if so, are there any additional charges for them.

♦ In some cases, your telephone company may only enable these features on your first directory (phone) number. In this case, you may want to request that the features be enabled on your second directory number as well.

9.2   Setting Up Supplemental Phone Service

All Supplemental Phone Services are enabled by default except for Call Waiting, which is disabled by default but can be enabled in **Menu 2.1- ISDN Advanced Setup. The Calling Line Indication,** or Caller ID, also in this menu decides whether the other party can see your number when you call. If set to **Enable** (default), the ISDN Router/Hub sends the caller ID and the party you call can see your number, otherwise, the caller ID is blocked.

ISDN Router/Hub *RA368 WAN Bridge/Routers*

9.3   The Flash Key

Flashing means to press the hook for a short period of time (a few hundred milliseconds) before releasing it. On newer telephones, there should be a   lash   key (button) that generates the signal electronically. If the flash key is not available, you can tap (press and immediately release) the hook by hand to achieve the same effect. However, using the flash key is preferred since the timing is much more precise. With manually tapping, if the duration is too long, it may be interpreted as hanging up by the ISDN Router/Hub.

9.4   Call Waiting

ISDN Call Waiting allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.

By default call waiting is disabled on both telephone ports, but can be enabled on either port from **Menu 2.1**.

9.4.1 How to use call waiting

The Call Waiting feature on your ISDN line works in exactly the same way as it does on a regular analog line (which almost everyone is familiar with). To put the current call on hold and answer the incoming call, press the flash key after hearing a call waiting indicator tone.

Dropping current call to switch to incoming/holding call.

After hearing a Call Waiting indicator tone, simply hang up the telephone and wait for the telephone to ring before answering the incoming/holding call.

Notes: An incoming caller receives a busy signal if

♦   You have two calls active (one active and one on hold, or both active using Three Way Calling) already.

♦   You are dialing a number on the B-Channel the incoming caller is attempting to reach, but have not yet established a connection.

9.5 Three way calling

The Three Way Call feature allows you to add a third party to an existing call. This service must be subscribed from your telephone company.

9.5.1 How To Use Three Way Calling

If you wish to call someone and conference him/her in with an existing call:

♦ Press the flash key to put the existing call on hold and receive a dial tone.

♦ Dial the third party   telephone number.

♦ When you are ready to conference the calls together, press the flash key again to establish a Three Way Conference Call.

Note: If you wish to cancel your attempt to establish the conference call because the third party line in busy or if they don't answer, simply hang-up the telephone and pick it back up after it starts ringing to return to the first caller.

To drop the last call added to the three-way-call:

Simply press the flash key. The last call that was added to the conference is dropped.

To drop yourself from the conference call:

If you hang up your telephone during a three-way-call and the two other callers remain on the line, the ISDN network will do an implicit transfer to directly connect the two remaining callers together.

9.6 Call Transfer

Call Transfer allows you to transfer an active call to a third party. This service must be subscribed from your telephone company.

9.6.1 How To Use Call Transfer

Transferring an active call to a third party:

♦ Once you have an active call (Caller A), press the flash key to put Caller A on hold and receive a dial tone.

♦ Dial the third party   telephone number (Caller B).

ISDN Router/Hub *RA368 WAN Bridge/Routers*

♦ When you are ready to conference the two calls together, press the flash key to establish a Three-Way-Conference call.

♦ Hang up the telephone. The ISDN network does an implicit transfer to directly connect Caller A with Caller B.

9.6.2 To Do A Blind Transfer:

♦ Once you have an active call (Caller A), press the flash key to put the existing call on hold and receive a dial tone.

♦ Dial the third party   telephone number (Caller B).

♦ Before Caller B picks up the call, you can transfer the call by pressing the flash key. The call is automatically transferred.

9.7   Call Forwarding

Call forwarding means the switch will ring another number at a place where you will be when someone dials your directory number.

There are two methods to activate call forwarding. The first is exactly the same as on an analog line, i.e., you pick up the handset and dial the access code assigned by your telephone company and the number that you want the calls forwarded.

The second is with the   hone flash commands where you pick up the handset and press the flash key before dialing the following:

Table 9-1 Phone Flash Commands

Command	Meaning
*20*forward-number#	Activate CFB (Call Forwarding Busy)
*21*forward-number#	Activate CFU (Call Forwarding Unconditional)
*22*forward-number#	Activate CFNR (Call Forwarding No Reply)
#20#	Deactivate CFB

#21#	Deactivate CFU
#22#	Deactivate CFNR

Either method should work fine, and you can use whichever one you are most comfortable with.

Chapter 10
Filter Configuration

10.1 About Filtering

Your ISDN Router/Hub uses filters to decide whether or not to allow passage of a data packet and/or to make a call. There are two types of filters: data filters and call filters.

Data filters screen the data to determine if the packet should be allowed to pass. Data filters are further divided into incoming and outgoing filters, depending on the direction of the packet relative to a port. Call filters are used to determine if a packet should be allowed to trigger a call.

Outgoing packets must pass through the data filters before they encounter the call filters. Call filters are divided into two groups, the built-in call filters and user-defined call filters. Your ISDN Router/Hub has built-in call filters that prevent administrative, e.g., RIP and SAP (Service Advertising Protocol), packets from triggering calls. These filters are always enabled and not accessible to you. Your ISDN Router/Hub applies the built-in filters first and then the user-defined call filters, if applicable, as illustrated in the figure below, *Figure 10-1 Outgoing Packet Filtering Process.*

ISDN Router/Hub *RA368 WAN Bridge/Routers*
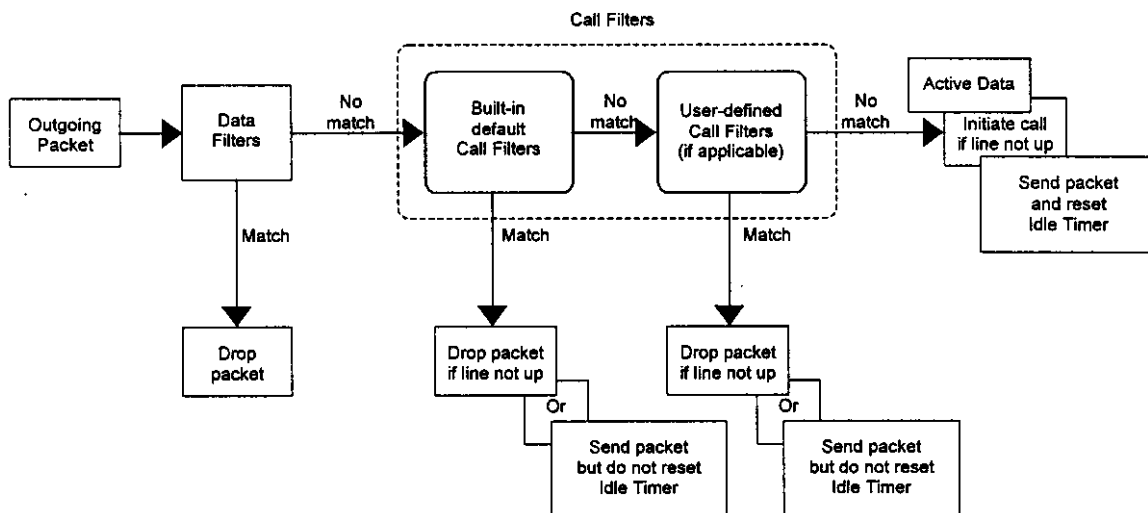
Figure 10-1 Outgoing Packet Filtering Process

For incoming packets, your ISDN Router/Hub applies data filters only. Packets are processed depending upon whether a match is found. The following sections describe how to configure filter sets.

The Filter Structure of the ISDN Router/Hub

A filter set consists of one or more filter rules. Usually, you would group related rules, e.g., all the rules for NetBIOS, into a single set and give it a descriptive name. The ISDN Router/Hub allows you to configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the system.

You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port.

10.2 Configuring a Filter Set

To configure a filter sets, follow the procedure below:

Step 1. Select option **21. Filter Set Configuration** from the Main Menu to open Menu 21.

```
                    Menu 21 - Filter Set Configuration

    Filter                              Filter
    Set #        Comments               Set #         Comments
    ------    -------------------       ------     -------------------
    1         _____       7          _____
    2         _____       8          _____
    3         _____       9          _____
    4         _____       10         _____
    5         _____       11         _____
    6         _____       12         _____


              Enter Filter Set Number to Configure=
              Edit Comments=
              Press ENTER to CONFIRM or ESC to CANCEL:
```

Figure 10-2 Menu 21 - Filter Set Configuration

Step 2. Select the filter set you wish to configure (no. 1-12) and press [Enter].

Step 3. Enter a descriptive name or comment in the Edit Comments field and press Enter.

Step 4. Press [Enter] at the message: [Press ENTER to confirm] to open Menu 21.1 - Filter Rules Summary.

ISDN Router/Hub *RA368 WAN Bridge/Routers*

```
                    Menu 21.1 - Filter Rules Summary

 # A Type                       Filter Rules                      M m n
 - - ----   --------------------------------------------- ---------- - - -
 1 N
 2 N
 3 N
 4 N
 5 N
 6 N


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

```

Figure 10-3 Menu 21.1 - Filter Rules Summary

10.2.1 Filter Rules Summary Menu

This screen shows the summary of the existing rules in the filter set. The following tables contain a brief description of the abbreviations used in Menu 21.1.

Table 10-1 Abbreviations Used in the Filter Rules Summary Menu

Abbreviations	Description	Display
#	Refers to the filter rule number (1-6).	
A	Refers to Active.	[Y] means the filter rule is active. [N] means the filter rule is inactive.
Type	Refers to the type of filter rule. This shows GEN for generic, IP for TCP/IP and IPX for Novell IPX.	[GEN] for Generic [IP] for TCP/IP [IPX] for Novell IPX

Table 10-2 Abbreviations Used in the Filter Rules Summary Menu (continued)

Abbreviations	Description	Display
Filter Rules	The filter rule parameters will be displayed here (see below).	
M	Refers to More.	[Y] means there are more rules to check. [N] means there are no more rules to check.
m	Refers to Action Matched.	[F] means to forward the packet. [D] means to drop the packet. [N] means check the next rule.
n	Refers to Action Not Matched	[F] means to forward the packet. [D] means to drop the packet. [N] means check the next rule.

The protocol dependent filter rules abbreviation are listed as follows:

● If the filter type is IP, the following abbreviations listed in the following table will be used.

Table 10-3 Abbreviations Used If Filter Type Is IP

Abbreviation	Description
Pr	Protocol
SA	Source Address
SP	Source Port number
DA	Destination Address
DP	Destination Port number

ISDN Router/Hub *RA368 WAN Bridge/Routers*

● If the filter type is IPX, the following abbreviations listed in the following table will be used.

Table 10-4 Abbreviations Used If Filter Type Is IPX

Abbreviation	Description
PT	IPX Packet Type
SS	Source Socket
DS	Destination Socket

● If the filter type is GEN (generic), the following abbreviations listed in the following table will be used.

Table 10-5 Abbreviations Used If Filter Type Is GEN

Abbreviation	Description
Off	Offset
Len	Length

Refer to the next section for information on configuring the filter rules.

10.3 Configuring a Filter Rule

To configure a filter rule, enter its number in Menu 21.1 - Filter Rules Summary and press Enter to open Menu 21.1.1 for the rule.

There are three types of filter rules: TCP/IP, IPX and Generic. Depending on the type of rule, the parameters below the type will be different. Use the space bar to select the type of rule that you wish to create in the Filter Type field and press Enter to open the respective menu.

The network layer (TCP/IP and IPX) filters are collectively called protocol filters. When NAT/SUA (Network Address Translation/Single User Account) is enabled, the inside IP address and port number are replaced on a connection-by-connection basis, which makes it impossible to know the exact address and port on the wire. Therefore, the ISDN Router/Hub applies the protocol filters to the   ative IP address and port number before NAT/SUA for outgoing packets and after NAT/SUA for incoming packets. On the other hand, the generic, or device, filters are applied to the raw packets that appear on the wire.

To speed up filtering, all rules in a filter set must be of the same class, i.e., protocol filters or generic filters. The class of a filter set is determined by the first rule that you create. When applying the filter sets to a port, separate menu fields are provided for protocol and device filter sets. If you include a protocol filter set in a device filters field or vice versa, the ISDN Router/Hub will warn you and will not allow you to save.

10.3.1 TCP/IP Filter Rule

This section shows you how to configure a TCP/IP filter rule. TCP/IP rules allow you to base the rule on the fields in the IP and the upper layer protocol, e.g., UDP and TCP, headers.

To configure a TCP/IP rules, select TCP/IP Filter Rule from the Filter Type field and press Enter to open Menu 21.1.1 - TCP/IP Filter Rule, as shown below.

```
               Menu 21.1.1 - TCP/IP Filter Rule

       Filter #: 1,1
       Filter Type= TCP/IP Filter Rule
       Active= No
       IP Protocol= 0       IP Source Route= No
       Destination: IP Addr=
                    IP Mask=
                    Port #= 0
                    Port # Comp= None
            Source: IP Addr=
                    IP Mask=
                    Port #= 0
                    Port # Comp= None
       TCP Estab= N/A
       More= No            Log= None
       Action Matched= Check Next Rule
       Action Not Matched= Check Next Rule

          Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
```

Figure 10-4 Menu 21.1.1 - TCP/IP Filter Rule

The following table describes how to configure your TCP/IP filter rule.

Table 10-6 TCP/IP Filter Rule Menu Fields

Field	Description	Option
Active	This field activates/deactivates the filter rule.	**Yes/No**
IP Protocol	Protocol refers to the upper layer protocol, e.g., TCP is 6, UDP is 17 and ICMP is 1. This value must be between 0 and 255	0-255
IP Source Route	If Yes, the rule applies to packet with IP source route option; else the packet must not have source route option. The majority of IP packets do not have source route.	**Yes/No**
Destination: IP Addr	Enter the destination IP Address of the packet you wish to filter. This field is a don -care if it is 0.0.0.0.	IP address
Destination: IP Mask	Enter the IP subnet mask to apply to the Destination: IP Addr.	Subnet mask
Destination: Port #	Enter the destination port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is a don -care if it is 0.	0-65535
Destination: Port # Comp	Select the comparison to apply to the destination port in the packet against the value given in Destination: Port #.	**None/Less/Greater/ Equal/Not Equal]**
Source: IP Addr	Enter the source IP Address of the packet you wish to filter. This field is a don -care if it is 0.0.0.0.	IP Address
Source: IP Mask	Enter the IP subnet mask to apply to the Source: IP Addr.	IP Mask
Source: Port #	Enter the source port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is a don - care if it is 0.	0-65535
Source: Port # Comp	Select the comparison to apply to the source port in the packet against the value given in Source: Port #.	**Yes/No**
TCP Estab	This field is applicable only when IP Protocol field is 6, TCP. If yes, the rule matches only established TCP connections; else the rule matches all TCP packets.	**Yes/No**
More	If yes, a matching packet is passed to the next filter rule before an action is taken; else the packet is disposed of	**Yes / N/A**

ISDN Router/Hub *RA368 WAN Bridge/Routers*

Field	Description	Option
	according the action fields. If More is **Yes**, then Action Matched and Action Not Matched will be **N/A**.	
Log	Select the logging option from the following: ● **None** No packets will be logged. ● **Action Matched** - Only packets that match the rule parameters will be logged. ● **Action Not Matched** - Only packets that do not match the rule parameters will be logged. ● **Both** All packets will be logged.	**None** **Action Matched** **Action Not Matched** **Both**
Action Matched	Select the action for a matching packet.	**Check Next Rule** **Forward** **Drop**
Action Not Matched	Select the action for a packet not matching the rule.	**Check Next Rule** **Forward** **Drop**
Once you have completed filling in Menu 21.1.1 - TCP/IP Filter Rule, press [Enter] at the message [Press Enter to Confirm] to save your configuration, or press [Esc] to cancel. This data will now be displayed on Menu 21.1 - Filter Rules Summary.		

10.3.2 Generic Filter Rule

This section shows you how to configure a generic filter rule. The purpose of generic rules is to allow you to filter non-IP/IPX packets. For IP and IPX packets, it is generally easier to use the IP and IPX rules directly.

For generic rules, the ISDN Router/Hub treats a packet as a byte stream as opposed to an IP or IPX packet. You specify the portion of the packet to check with the Offset (from 0) and the Length fields, both in bytes. The ISDN Router/Hub applies the Mask (bit-wise ANDing) to the data portion before comparing the result against the Value to determine a match. The Mask and Value are specified in hexadecimal numbers. Note that it takes two hexadecimal digits to represent a byte, so if the length is 4, the value in either field will take 8 digits, e.g., FFFFFFFF.

To configure a generic rule, select Generic Filter Rule in the Filter Type field and press Enter to open Menu 21.1.2 - Generic Filter Rule, as shown below.

```
            Menu 21.1.2 - Generic Filter Rule


       Filter #: 1,1
       Filter Type= Generic Filter Rule
       Active= No
       Offset= 0
       Length= 0
       Mask= N/A
       Value= N/A
       More= No           Log= None
       Action Matched= Check Next Rule
       Action Not Matched= Check Next Rule



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

Figure 10-5 Menu 21.1.2 - Generic Filter Rule

ISDN Router/Hub *RA368 WAN Bridge/Routers*

The table below describes the fields in the Generic Filter Rule Menu.

Table 10-7 Generic Filter Rule Menu Fields

Field	Description	Default
Offset	Enter the starting byte of the data portion in the packet that you wish to compare. The range for this field is from 0 to 255.	Default = 0
Length	Enter the byte count of the data portion in the packet that you wish to compare. The range for this field is 0 to 8.	Default = 0
Mask	Enter the mask (in Hexadecimal) to apply to the data portion before comparison.	
Value	Enter the value (in Hexadecimal) to compare with the data portion.	
Once you have completed filling in Menu 21.1.2 - generic Filter Rule, press [Enter] at the message [Press Enter to Confirm] to save your configuration, or press [Esc] to cancel. This data will now be displayed on Menu 21.1 - Filter Rules Summary.		

10.4 Novell IPX Filter Rule

This section shows you how to configure an IPX filter rule. IPX filters allow you to base the rules on the fields in the IPX headers.

To configure an IPX rules, select IPX Filter Rule from the Filter Type field and press Enter to open Menu 21.1.3 IPX Filter Rule, as shown in the figure below.

```
                    Menu 21.1.3 - IPX Filter Rule

            Filter #: 1,1
            Filter Type= IPX Filter Rule
            Active= No
            IPX Packet Type=
            Destination:   Network #=
                           Node #=
                           Socket #=
                           Socket # Comp= None
                  Source:  Network #=
                           Node #=
                           Socket #=
                           Socket # Comp= None
            Operation= N/A
            More= No            Log= None
            Action Matched= Check Next Rule
            Action Not Matched= Check Next Rule

            Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
```

Figure 10-6 Menu 21.1.3 - IPX Filter Rule

ISDN Router/Hub *RA368 WAN Bridge/Routers*

The table below describes the IPX Filter Rule.

Table 10-8 IPX Filter Rule Menu Fields

Field	Description
IPX Packet Type	Enter the IPX packet type (1-byte in hexadecimal) you wish to filter. The popular types are (in hexdecimal): 01 - RIP 04 - SAP 05 - SPX (Sequenced Packet eXchange) 11 - NCP (Netware Core Protocol) 14 - Novell NetBIOS
Destination/Source Network #	Enter the destination/source network numbers (4-byte in hexadecimal) of the packet that you wish to filter.
Destination/Source Node #	Enter in the destination/source node number (6-byte in hexadecimal) of the packet you wish to filter.
Destination/Source Socket #	Enter the destination/source socket number (2-byte in hexadecimal) of the packets that you wish to filter.
Destination/Source Socket # Comp	Select the comparison you wish to apply to the destination/source socket in the packet against that specified above.
Operation	This field is applicable only if one of the Socket # fields is 0452 or 0453 indicating SAP and RIP packets. There are seven options for this field that specify the type of the packet. ● None. ● RIP Request. ● RIP Response. ● SAP Request. ● SAP Response. ● SAP Get Nearest Server Request. ● SAP Get Nearest Server Response

Once you have completed filling in Menu 21.1.3 - IPX Filter Rule, press [Enter] at the message [Press Enter to Confirm] to save your configuration, or press [Esc] to cancel. This data will now be displayed on Menu 21.1 - Filter Rules Summary.

Chapter 11
SNMP Configuration

11.1 About SNMP

SNMP (Simple Network Management Protocol) is a protocol for network management and monitoring. Your ISDN Router/Hub supports SNMP agent functionality, which allows a manager station to manage and monitor the ISDN Router/Hub through the network. Keep in mind that SNMP is only available if TCP/IP is configured on your ISDN Router/Hub.

11.2 Configuring SNMP

To configure SNMP, select option **SNMP Configuration** from the Main Menu to open Menu 22 - SNMP Configuration, as shown in the figure below. The   ommunity for Get, Set and Trap fields is simply SNMP   terminology for password.

```
                    Menu 22 - SNMP Configuration


        SNMP:
          Get Community= public
          Set Community= public
          Trusted Host= 0.0.0.0
          Trap:
            Community= public
            Destination= 0.0.0.0


        Press ENTER to Confirm or ESC to Cancel:
```
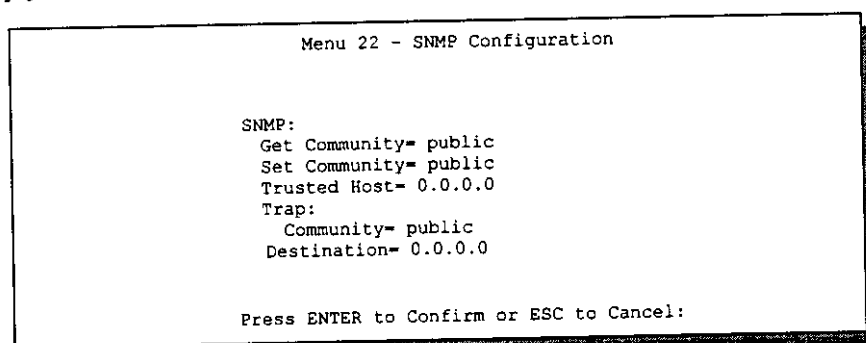
Figure 11-1 Menu 22 - SNMP Configuration

ISDN Router/Hub *RA368 WAN Bridge/Routers*

The following table describes the SNMP configuration parameters.

Table 11-1 SNMP Configuration Menu Fields

Field	Description	Default
Get Community	Enter the get community, which is the password for the incoming Get- and GetNext- requests from the management station.	public
Set Community	Enter the set community, which is the password for incoming Set- requests from the management station.	public
Trusted Host	If you enter a trusted host, your ISDN Router/Hub will only respond to SNMP messages from this address. If you leave the field blank (default), your ISDN Router/Hub will respond to all SNMP messages it receives, regardless of source.	blank
Trap: Community	Enter the trap community, which is the password sent with each trap to the SNMP manager.	public
Trap: Destination	Enter the IP address of the station to send your SNMP traps to.	blank
Once you have completed filling in Menu 22 - SNMP Configuration, press [Enter] at the message [Press Enter to Confirm] to save your configuration, or press [Esc] to cancel.		
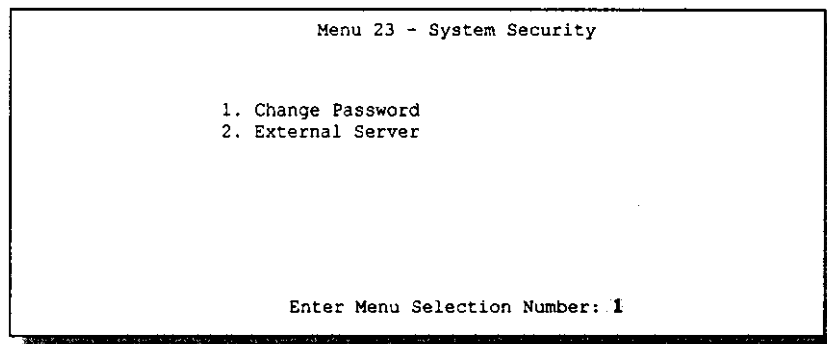
Chapter 12
System Security

This chapter covers Menu 23, which is for you to change the system password and to configure an external authentication server.

12.1 Changing the System Password

To change the system password, following steps below:

Step 1.   Select option **System Security** in the Main Menu to open Menu 23   System Security as shown below.
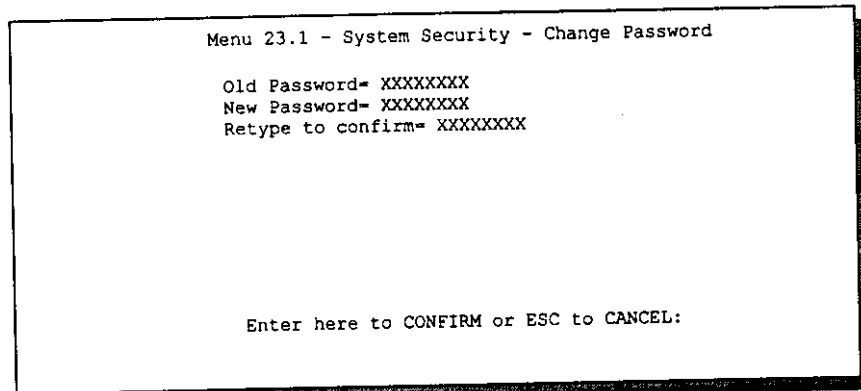
```
                    Menu 23 - System Security


            1. Change Password
            2. External Server






              Enter Menu Selection Number: 1
```

Figure 12-1 Menu 23 - System Security

Step 2. From the System Security Menu, select option **Change Password** to open Menu 23.1 - System Security - Change Password.

Step 3. Enter your existing system password and press [Enter].

```
           Menu 23.1 - System Security - Change Password

           Old Password= XXXXXXXX
           New Password= XXXXXXXX
           Retype to confirm= XXXXXXXX




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

Figure 12-2 Menu 23.1 - System Security - Change Password

Step 4. Enter your new system password and press [Enter].

Step 5. Re-type your new system password for confirmation and press [Enter].

As you enter the password, the screen displays an (X) for each character you type.

12.2 Using RADIUS Authentication

Your ISDN Router/Hub has a built-in dial-up user list; however, the number of users that can be stored locally is limited due to memory constraints. If you have more users than what the ISDN Router/Hub can store locally, use an external RADIUS (Remote Authentication Dial-In User Service) server that provides authentication service for unlimited number of users.

12.2.1 Installing a RADIUS Server

To use RADIUS authentication, you need to have a UNIX or Windows NT machine on your network as the RADIUS server, as well as the RADIUS software itself.

You can obtain the RADIUS server software, along with documentation, at

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

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

After you install the server software, you will need to edit the `dictionary` file in the RADIUS configuration directory (usually `/etc/raddb`). Using any text editor, add the following lines to the `dictionary` file:
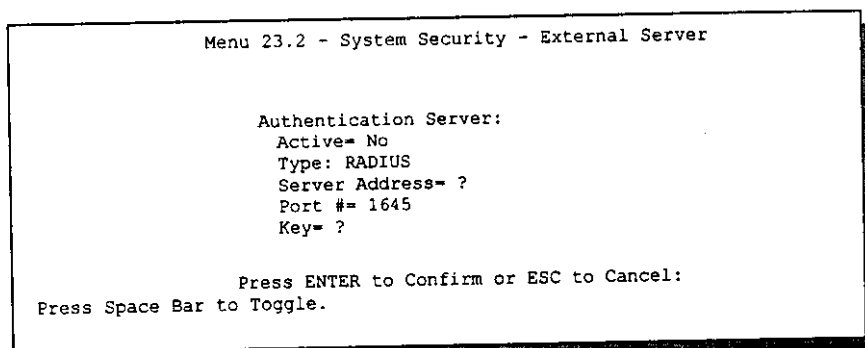
```
# Netgear   proprietary attributes
ATTRIBUTE   Netgear-Callback-Option   192   integer
VALUE       Netgear-Callback-Option   None        0
VALUE       Netgear-Callback-Option   Optional    1
VALUE       Netgear-Callback-Option   Mandatory   2

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

These changes add the support for CLID authentication, as described in the section below.

ISDN Router/Hub *RA368 WAN Bridge/Routers*

12.2.2 RADIUS Server Configuration

To configure the RADIUS server, select option 23, System Security, from the Main Menu to open Menu 23 - System Security. Select option 2, External Server from this menu to open Menu 23.2 - System Security - External Server, shown below.

```
                 Menu 23.2 - System Security - External Server


                      Authentication Server:
                       Active= No
                       Type: RADIUS
                       Server Address= ?
                       Port #= 1645
                       Key= ?

                      Press ENTER to Confirm or ESC to Cancel:
        Press Space Bar to Toggle.
```

Figure 12-3 Menu 23.2 - System Security - External Server

The fields in the System Security - External Server Menu are listed in the following table.

Table 12-1 System Security - External Server Menu Fields

Field	Description	Default
Active	Determines whether the external security facility is enabled. If No, only the built-in dial-up user list will be used. If Yes, the built-in dial-up user list will be searched first, then the external authentication server.	
Type	Determines the type of the external authentication server. At present only RADIUS is supported.	
Server Address	The IP address of the RADIUS server.	
Port #	The IP port number used by the authentication server. The default is port 1645.	[1645]
Key	A assword used to authenticate your ISDN Router/Hub to the RADIUS service. Please note that this is between the ISDN Router/Hub and the server; it has nothing to do with the dial-in users.	

12.2.3 The Key Field

The   ey   or password, must match that in the `client` file in the RADIUS server `/etc/raddb` directory, as shown in the following example:

```
# Client Name        Key
#-----------------------
192.168.1.1          1234
```

After you configure a RADIUS server, your ISDN Router/Hub will use it to authenticate all users that it can not find in its internal dial-up user list (*see* Menu 14)

12.2.4 Adding Users to the RADIUS Database

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

```
Joeuser   Password =   oepassword"
```

ISDN Router/Hub *RA368 WAN Bridge/Routers*

12.2.5 Using RADIUS Authentication for CLID

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

```
5551212    Password =   etgear-CLID"
User-Name =   oeuser"
Netgear-Callback-Option = Mandatory
Netgear-Callback-Phone-Source = Preconfigured
Dialback-No =    551212"
```

Note that if CLID is turned off in your ISDN Router/Hub, you need to have a separate user record for `joeuser` so the regular user name/password mechanism still works.

Chapter 13
Telnet Configuration and Capabilities

13.1 About Telnet Configuration

Before the ISDN Router/Hub is properly setup for TCP/IP, the only option for configuring it is through the console port. Once your ISDN Router/Hub is configured, you can use telnet to configure it remotely as shown below.
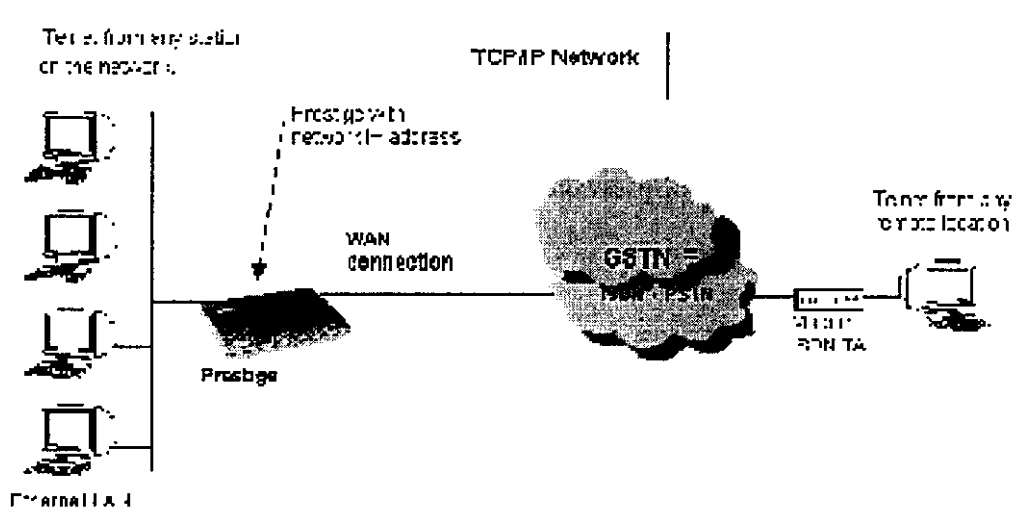
Figure 13-1 Telnet Configuration on a TCP/IP Network

If your ISDN Router/Hub is configured for IPX but not IP routing in Menu 1, telnet is still available provided you assign the ISDN Router/Hub a correct IP address and subnet mask. When IP routing is disabled, the ISDN Router/Hub can still function as a host.

13.2 Telnet Under SUA

When Single User Account (SUA) is enabled and an inside server is specified, telnet connections from the outside will be forwarded to the inside server. So to configure the ISDN Router/Hub via

ISDN Router/Hub *RA368 WAN Bridge/Routers*

telnet from the outside, you must first telnet to the inside server, and then telnet from the server to the ISDN Router/Hub using its inside LAN IP address. If no insider server is specified, telnet to the SUA   IP address will connect to the ISDN Router/Hub directly.

13.3   Telnet Capabilities

13.3.1 Single Administrator

To prevent confusion and discrepancy on the configuration, your ISDN Router/Hub only allows one administrator to log in at any time. Your ISDN Router/Hub also gives priority to the console port over telnet. If you have already connected to your ISDN Router/Hub via telnet, you will be logged out if another user logs in to the ISDN Router/Hub via the console port.

13.3.2 System Timeout

There is a system timeout of 5 minutes (300 seconds) for either the console port or telnet. Your ISDN Router/Hub will automatically log you out if you do nothing in this timeout period, except when it is continuously updating the status in Menu 24.1.
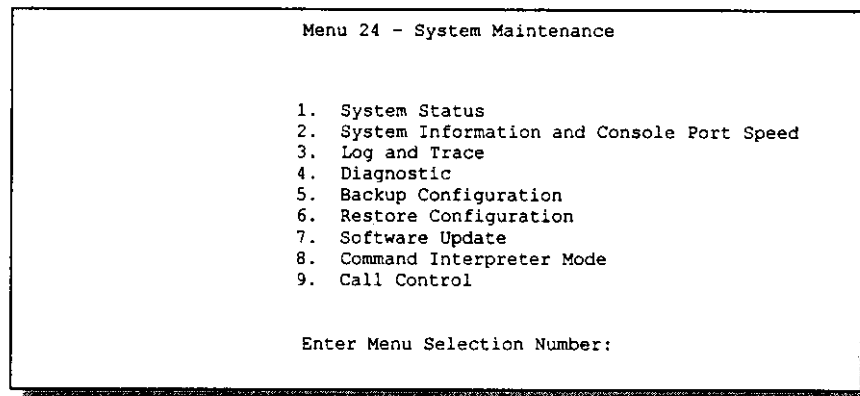
Chapter 14
System Maintenance

This chapter covers the diagnostic tools that help you to maintain your ISDN Router/Hub. These tools include updates on system status, port status, log and trace capabilities and upgrades for the system software. This chapter describes how to use these tools in detail.

Select menu 24 in the main menu to open Menu 24 - System Maintenance, as shown below.

Figure 14-1 Menu 24 - System Maintenance

```
                    Menu 24 - System Maintenance


            1.  System Status
            2.  System Information and Console Port Speed
            3.  Log and Trace
            4.  Diagnostic
            5.  Backup Configuration
            6.  Restore Configuration
            7.  Software Update
            8.  Command Interpreter Mode
            9.  Call Control


            Enter Menu Selection Number:
```

ISDN Router/Hub *RA368 WAN Bridge/Routers*

14.1 System Status

The first selection, System Status, gives you information on the version of your system firmware and the status and statistics of the ports, as shown in below. System Status is a tool that can be used to monitor your ISDN Router/Hub. Specifically, it gives you information on your system software version, ISDN telephone line status, number of packets sent and number of packets received.

To get to the System Status, select number **24** to go to **Menu 24 - System Maintenance.** From this menu, select number **1, System Status.** There are five commands in **Menu 24.1 - System Maintenance - Status.** Entering **1** disconnects the current B1 channel call; **2** disconnects the current B2 channel call, **3** resets the counters, **4** drops both B1 and B2 and **ESC** takes you back to the previous screen.

The table below describes the fields present in **Menu 24.1 - System Maintenance - Status.** It should be noted that these fields are READ-ONLY and are meant to be used for diagnostic purposes.

```
                     Menu 24.1 -- System Maintenance   Status

  Chan   Link      Type      TXPkts  RXPkts   Errors      CLU     ALU     Up Time
   --    Down      0Kbps        0       0        0         0%      0%      0:00:00
   --    Down      0Kbps        0       0        0         0%      0%      0:00:00
     Total Outcall Time:          0:00:00

     Ethernet:                        WAN:
       Status: 4 Port Hub               Chan 1 IP Addr:
       TX Pkts: 230                     Chan 2 IP Addr:
       RX Pkts: 0                       Port 1 CLID:
       Collisions: 0                    Port 2 CLID:

     LAN Packet Which Triggered Last Call:

                          Press Command:
       COMMANDS: 1-Drop B1  2-Drop B2  3-Reset Counters  4-Drop All   ESC-Exit
```

Figure 14-2 Menu 24.1 - System Maintenance – Status

The following table describes the fields present in Menu 24.1 - System Maintenance - Status.

Table 14-1 System Maintenance - Status Menu Fields

Field	Description
Chan	Shows statistics for **B1** and **B2** channels respectively. This is the information displayed for each channel:
Link	Shows the name of the remote node or the user the channel is currently connected to or the status of the channel (Idle, Calling or Answering).
Type	The current connecting speed (**56K** or **64K**).
TXPkt	The number of transmitted packets on this channel.
RXPkt	The number of received packets on this channel.
Error	The number of error packets on this channel.
CLU	(Current Line Utilization) percentage of current bandwidth used on this channel
ALU	(Average Line Utilization) a 5-second moving average of channel usage for this channel.
Up Time	Time this channel has been connected to the current remote node.
Total Outgoing call Time	Shows the total outgoing call time for both **B1** and **B2** channels since the system has been powered up.
Ethernet	
Status	Shows the current transmission speed and mode of the LAN.
TX Pkt	The number of transmitted packets to LAN.
RX Pkt	The number of received packets from LAN.
Collision	Number of collisions.
WAN	

ISDN Router/Hub *RA368 WAN Bridge/Routers*

CHAN 1 IP Addr	Refers to the IP address of the ISDN Router/Hub on Channel 1.
CHAN 2 IP Addr	Refers to the IP address of the ISDN Router/Hub on Channel 2.
Port 1 CLID	Shows the Caller ID of the peer on Port 1.
Port 2 CLID	Shows the Caller ID of the peer on Port 2.
LAN Packet Which Triggered Last Call	Shows the first 48 octets of the LAN packet that triggered the last outgoing call.

```
LAN Packet Which Triggered Last Call: (Type IP)
45 00 00 3C 02 12 00 00 3B 01 36 49 00 00 00 00 C0 44 87 22 08 00 62 2B 20 04 00
00 00 08 A9 D0 C0 44 87 22 00 01 02 03 04 05 06 07 08 09 0A 0B
```

┌─────────────────────┐
│ Source IP Address   │
└─────────────────────┘

┌────────────────────────┐
│ Source MAC Address   │
└────────────────────────┘

```
LAN Packet Which Triggered Last Call: (Type Raw)
FF FF 00 22 00 11 00 00 00 00 FF FF FF FF FF FF 04 52 00 00 00 00 00 40 95 90 04
B9 40 08 00 03 02 78 01 A5 A5 A5 A5 A5 A5 A5 A5
```
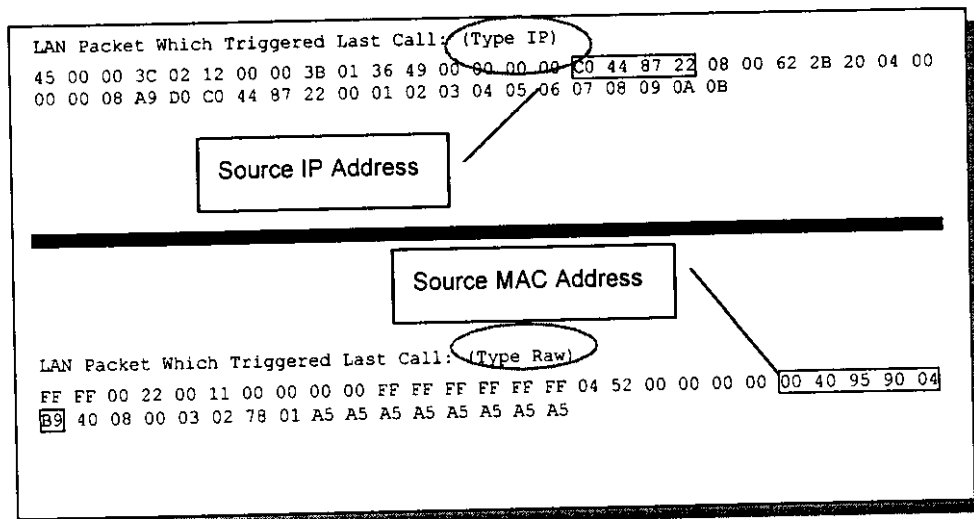
Figure 14-3 LAN Packet That Triggered Last Call

The figure above shows two examples of triggering packets from the LAN: the first of an ICMP ping packet (Type: IP) and the second a SAP broadcast packet (Type: Raw). With this information, you can determine the workstation from the source IP address or the source MAC address of the packet.

14.1.1 System Information

```
            Menu 24.2.1   System Maintenance - Information

       Name:

       Routing: IP

       RAS S/W Version: V2.21B01 | 11/6/98
       ISDN F/W Version: V 099

       Country Code: 238


       LAN

           Ethernet Address:00:a0:c5:02:34:56
           IP Address: 192.168.1.1
           IP Mask: 255.255.255.0
           DHCP: Server

           Press ESC or RETURN to Exit:
```

Figure 14-4 System Maintenance - Information

ISDN Router/Hub *RA368 WAN Bridge/Routers*

Table 14-2 Fields in System Maintenance

Field	Description
Name	displays the system name of your ISDN Router/Hub. This information can be modified in **Menu 1 - General Setup**.
Routing	refers to the routing protocol used.
RAS S/W Version	refers to the version of the ZyNOS software.
ISDN F/W Version	refers to the version of the ISDN firmware.
Country Code	refers to the one byte country code value (in decimal notation),
Ethernet Address	refers to the Ethernet MAC (Media Access Control) of your ISDN Router/Hub.
IP Address	This is the IP address of the ISDN Router/Hub in dotted decimal notation.
IP Mask	This shows the subnet mask of the ISDN Router/Hub.
DHCP	This field shows the DHCP setting (**None** or **Server**) of the ISDN Router/Hub.

14.1.2 Console Port Speed

You can set up different port speeds for the console port through Menu 24.2.2   Console Port Speed. Your ISDN Router/Hub supports 9600 (default), 19200, 38400, 57600, and 115200bps for the console port. Use the space bar to select the desired speed in Menu 24.2.2, as shown below.
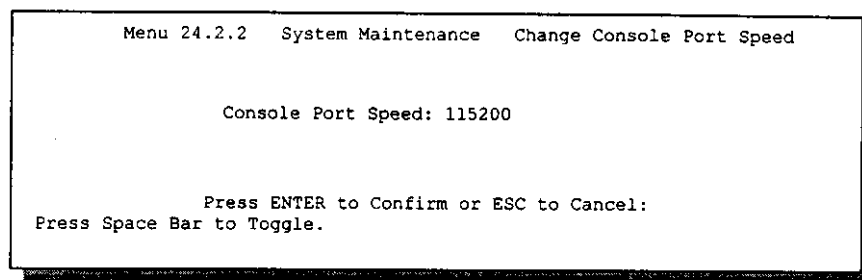
```
      Menu 24.2.2   System Maintenance   Change Console Port Speed


              Console Port Speed: 115200



              Press ENTER to Confirm or ESC to Cancel:
   Press Space Bar to Toggle.
```

Figure 14-5 Menu 24.2.2 – System Maintenance – Change Console Port Speed

14.2 Log and Trace

There are two logging facilities in the ISDN Router/Hub. The first is the error logs and trace records that are stored locally. The second is the UNIX syslog facility for message logging.

14.2.1 Viewing Error Log
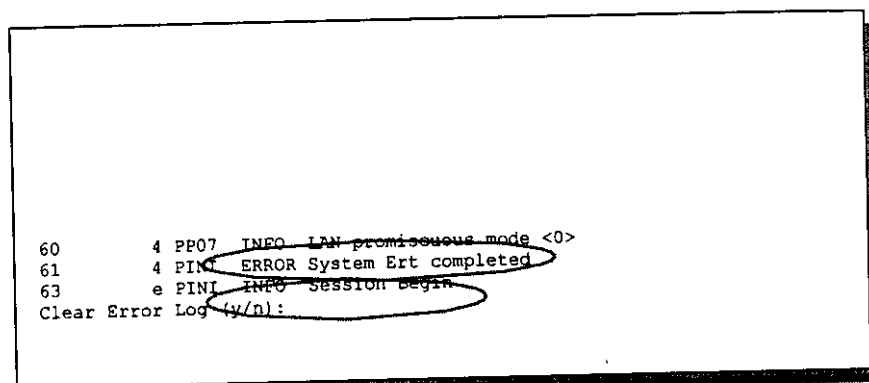
The first place you should look for clues when something goes wrong is the error/trace log. Follow the procedure below to view the local error/trace log:

Step 1.   Select option 24 from the Main Menu to open Menu 24 - System Maintenance.

Step 2.   From Menu 24, select option 3 to open Menu 24.3 - System Maintenance - Log and Trace.

Step 3.   Select the first option from Menu 24.3 - System Maintenance - Log and Trace to display the error log in the system.

After the ISDN Router/Hub finishes displaying, you will have the option to clear the error log.

ISDN Router/Hub *RA368 WAN Bridge/Routers*

Examples of typical error and information messages are presented in the figure below.

```
60          4 PP07  INFO  LAN promiscuous mode <0>
61          4 PIN   ERROR System Ert completed
63          e PIN   INFO  Session begin
Clear Error Log (y/n):
```

Figure 14-6 Examples of Error and Information Messages

14.2.2 Syslog And Accounting

The ISDN Router/Hub uses the UNIX syslog facility to log the CDR (Call Detail Record) and system messages to a syslog server. Syslog and accounting can be configured in Menu 24.3.2 - System Maintenance - Syslog and Accounting, as shown below.

```
      Menu 24.3.2 -- System Maintenance - Syslog and Accounting

                  Syslog:
                  Active- No
                  Syslog IP Address- ?
                  Log Facility- Local 1




                  Press ENTER to Confirm or ESC to Cancel:
      Press Space Bar to Toggle.
```

Figure 14-7 Menu 24.3.2 - System Maintenance - Syslog and Accounting

You need to configure the following 3 parameters described in the table below to activate syslog.

Table 14-3 System Maintenance Menu Syslog Parameters

Parameter	Description
Active	Use the space bar to turn on or off syslog.
Syslog IP Address	Enter the IP Address of your syslog server.
Log Facility	Use the space bar to toggle between the 7 different Local options. The log facility allows you to log the message in different files in the server. Please refer to your UNIX manual for more detail.

Your ISDN Router/Hub sends three types of syslog messages: call information messages (i.e. CDR), error information messages and session information messages. Some examples of these syslog messages are shown below:

1. Call Information Messages:

ISDN Router/Hub *RA368 WAN Bridge/Routers*

```
line 1 channel 1, call 41, C01, Incoming Call, 40001
line 1 channel 1, call 41, C01, ANSWER Connected, 49K 40001
line 1 channel 1, call 41, C01, Incoming Call, Call Terminated
```

2. Error Information Messages:

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

3. Session Information Messages:

```
line 1, channel 1, call 41, I01, IPCP up, myISDN Router/Hub
line 1, channel 1, call 41, I01, IPCP down, myISDN Router/Hub
```

14.3 Diagnostic

The diagnostic facility allows you to test the different aspects of your ISDN Router/Hub to determine if it is working properly. Menu 24.4 allows you to choose among various types of diagnostic tests to evaluate your system, as shown below.

```
            Menu 24.4 - System Maintenance - Diagnostic

WAN                                     System
   1.   Hang Up B1 Call                    21. Reboot System
   2.  Hang Up B2 Call                     22. Command Mode
   3.   Reset ISDN
   4.   ISDN Connection Test
   5.   Manual Call

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

                    Enter Menu Selection Number:
            Select WAN Port-
            Manual Call Remote Node- N/A
            Host IP Address- N/A
```

Figure 14-8 Menu 24.4 - System Maintenance - Diagnostic

Follow the procedure below to get to Diagnostic

Step 1. From the Main Menu, select option 24 to open Menu 24 - System Maintenance.

Step 2. From this menu, select option 4. Diagnostic. This will open Menu 24.4 - System Maintenance - Diagnostic.

ISDN Router/Hub *RA368 WAN Bridge/Routers*

The following table describes the diagnostic tests available in Menu 24.4 for your ISDN Router/Hub and the connections.

Table 14-4 System Maintenance Menu Diagnostic

Field	Description
Hang Up B1 Call	This tool hangs up the B1 channel. This is only applicable if the B1 channel is currently in use.
Hang Up B2 Call	This tool hangs up the B2 channel. This is only applicable if the B2 channel is currently in use.
Reset ISDN	This command re-initializes the ISDN link to the telephone company.
ISDN Connection Test	You can test to see if your ISDN line is working properly by using this option. This command triggers the ISDN Router/Hub to perform a loop-back test to check the functionality of the ISDN line. If the test is not sucessful, note the error message that you receive and consult your network administrator.
Manual Call	This provides a way for you to place a call to a remote node manually. This tests the connectivity to that remote node. When you use this command, you see traces displayed on the screen showing what is happening during the call setup and protocol negotiation. Below is an example of a successful connection.
Internet Setup Test	This test checks to see if your Internet access configuration has been done correctly. When this option is chosen, the ISDN Router/Hub places a manual call to the ISP remote node. If everything is working properly, you will receive an appropriate response. Otherwise, note the error message and consult your network administrator.
Ping Host	This diagnostic test pings the host, which determines the functionality of the TCP/IP protocol on both systems and the links in between.
Reboot System	This option reboots the ISDN Router/Hub.
Command Mode	This option allows you to enter the command mode. This mode allows you to diagnose and test your ISDN Router/Hub using a

	specified set of commands.

The following figure shows an example of a successful connection after selecting option **Manual Call** in Menu 24.4.

Figure 14-9 Trace Display for a Successful Manual Call

```
Start dialing for node <1>
### Hit any key to continue. ###
Dialing chan<2> phone<last 9-digit>:12345
Call CONNECT speed<64000> chan<2> prot<1>
LCP up
CHAP send response
CHAP login to remote OK!
IPCP negotiation started
IPCP up
```

This figure shows a trace example where authentication failed.

```
Strat dialing for node <1>
### Hit any key to continue. ###
Dialing chan<2> phone<last 9-digit>:23456
Call CONNECT speed<64000> chan<2> prot<1>
LCP up
CHAP send response
***Login to remote failed. Check name/passwd.
Receive Terminal REQ
IPCP down
Line Down chan<2>
```

Figure 14-10 Trace Display for a Failed Authentication

ISDN Router/Hub *RA368 WAN Bridge/Routers*

14.4 Backup Configuration

Option 5 from Menu 24 - System Maintenance allows you to backup the current ISDN Router/Hub configuration to your workstation. Backup is highly recommended once your ISDN Router/Hub is functioning properly.

You must perform the backup and restore through the console port. Any serial communications program should work fine; however, you must use XMODEM protocol to perform the download/upload.

Please note that terms ownload and pload are relative to the workstation. Download means to transfer from another machine to the workstation, while upload means from your workstation to another machine.

14.5 Restore Configuration

Selecting option 6 from Menu 24 - System Maintenance to restore the configuration from your workstation to the ISDN Router/Hub. Again, you must use the console port and XMODEM protocol to restore the configuration.

Keep in mind that the configuration is stored in the flash ROM in the ISDN Router/Hub, so even if power failure should occur, your configuration is safe.

14.6 Firmware Update

Menu 24.7 -- System Maintenance - Upload Firmware allows you to upgrade the firmware and the configuration file via the console port. Note that this function erases the old data before installing the new one; please do not attempt to update unless you have the new firmware at hand. There are 2 components in the system: the router firmware and the configuration file, as shown below.

```
     Menu 24.7 -- System Maintenance - Upload Firmware

         1. Upload Router Firmware
         2. Upload Router Configuration File




         Enter Menu Selection Number:
```
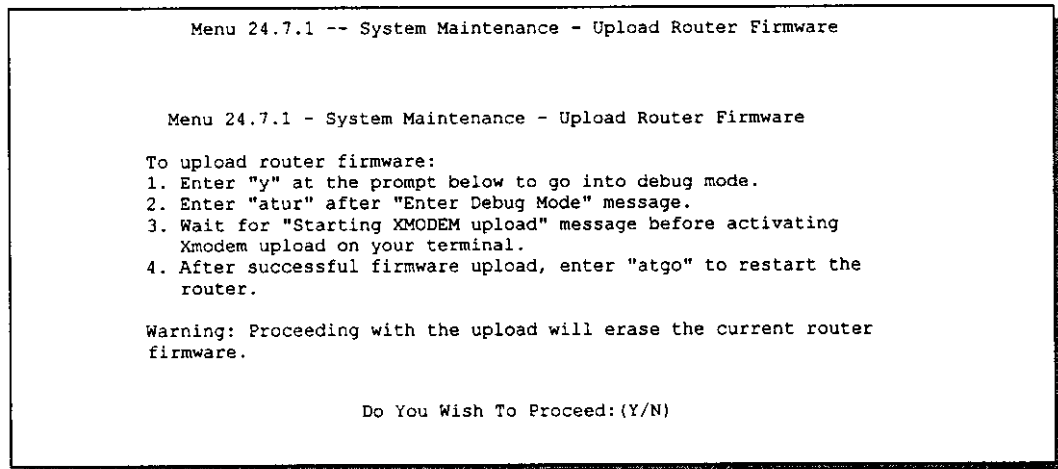
Maintenance

Figure 14-11 Menu 24.7 - System Maintenance - Upload Firmware

14.6.1 Upload Router Firmware

The firmware is the program that controls the functions of the ISDN Router/Hub. Menu 24.7.1 shows you the instructions for uploading the firmware. If you answer yes to the prompt, the ISDN Router/Hub will go into debug mode. Follow the procedure below to upload the firmware:

1. Enter "atur after the "Enter Debug Mode message.

2. Wait for the "Starting XMODEM upload message before activating Xmodem upload on your terminal.

3. After successful firmware upload, enter "atgo to restart the ISDN Router/Hub.

```
        Menu 24.7.1 -- System Maintenance - Upload Router Firmware



     Menu 24.7.1 - System Maintenance - Upload Router Firmware

To upload router firmware:
1. Enter "y" at the prompt below to go into debug mode.
2. Enter "atur" after "Enter Debug Mode" message.
3. Wait for "Starting XMODEM upload" message before activating
   Xmodem upload on your terminal.
4. After successful firmware upload, enter "atgo" to restart the
   router.

Warning: Proceeding with the upload will erase the current router
firmware.


              Do You Wish To Proceed:(Y/N)
```

Figure 14-12 Menu 24.7.1 - Uploading Router Firmware

14.6.2 Uploading Router Configuration File

The configuration data, system-related data, the error log and the trace log are all stored in the configuration file. Please be aware that uploading the configuration file replaces everything contained within.

ISDN Router/Hub *RA368 WAN Bridge/Routers*

Menu 24.7.2 shows you the instructions for uploading the configuration file. If you answer yes to the prompt, the ISDN Router/Hub will go into debug mode. Follow the procedure below to upload the configuration file:

1. Enter "atur3 after the "Enter Debug Mode message.

2. Wait for the "Starting XMODEM upload message before activating Xmodem upload on your terminal.

3. After successful firmware upload, enter "atgo to restart the ISDN Router/Hub.

If you replace the current configuration file with the default configuration file, i.e., pRA368.rom, you will lose all configurations that you had before and the speed of the console port will be reset to the default of 9600 bps with 8 data bit, no parity and 1 stop bit (8n1) . You will need to change your serial communications software to the default before you can connect to the ISDN Router/Hub again. The password will be reset to the default of 1234, also.

```
Menu 24.7.2 - System Maintenance - Upload Router Configuration File




        To upload router configuration file:
        1. Enter "y" at the prompt below to go into debug mode.
        2. Enter "atur3" after "Enter Debug Mode" message.
        3. Wait for "Starting XMODEM upload" message before activating
           Xmodem upload on your terminal.
        4. After successful firmware upload, enter "atgo" to restart the
           router.

        Warning:
        1. Proceeding with the upload will erase the current router
           configuration file.
        2. The router's console port speed (Menu 24.2.2) may change
           when it is restarted; please adjust your terminal's speed
           accordingly. The password may change (menu 23), also.
      .  3. When uploading the DEFAULT configuration file, the console
           port speed will be reset to 9600 bps and the password to
           "1234".
                    Do You Which To Proceed:(Y/N)
```

Figure 14-13 Menu 24.7.2 - System Maintenance - Upload Router Configuration File

14.6.3 TFTP Transfer

In addition to the direct console port connection, the ISDN Router/Hub supports the up/downloading of the firmware and the configuration file using TFTP (Trivial File Transfer Protocol) over LAN. Even though TFTP should work over WAN as well, it is not recommended because of the potential data corruption problem.

To use TFTP, your workstation must have both telnet and TFTP clients. To transfer the firmware and the configuration file, follow the procedure below:

Step 1. Use telnet from your workstation to connect to the ISDN Router/Hub and log in. Because TFTP does not have any security check, the ISDN Router/Hub records the IP address of the telnet client and accepts TFTP requests only from this address.

Step 2. Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.

Step 3. Enter command "sys stdio 0 to disable SMT timeout, so the TFTP transfer will not be interrupted.

ISDN Router/Hub *RA368 WAN Bridge/Routers*

Step 4. Launch TFTP client on your workstation and connect to the ISDN Router/Hub. Set the transfer mode to binary before starting data transfer.

Step 5. Use the TFTP client to transfer files between the ISDN Router/Hub and the workstation. The file name for the firmware is "ras and for the configuration file, "rom-0 (rom-zero, not capital o).

If you upload the firmware to the ISDN Router/Hub, it will reboot automatically when the file transfer is completed.

Note that the telnet connection must be active and the SMT in CI mode before and during the TFTP transfer. For details on TFTP commands, please consult the documentation of your TFTP client program. For UNIX, use "get to transfer from the ISDN Router/Hub to the workstation, "put the other way around, and "binary to set binary transfer mode.

14.6.4 Boot module commands

ISDN Router/Hub boot module commands are shown below. For ATBAx, x denotes the number preceeding the colon to give the baud rate following the colon in the list of numbers that follows; e.g. ATBA3 will give a baud of 9.6 kbps. ATSE displays the seed that is used to generate a password to turn on the debug flag in the firmware. The ATSH command shows product related information such as boot module version, vendor name, product model, RAS code revision, ISDN code revision, etc.
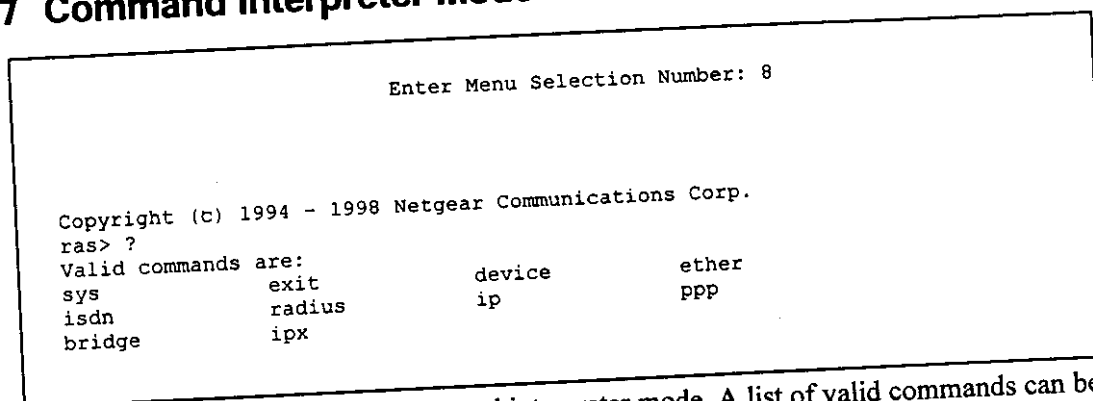
```
======= Debug Command Listing =======

ATHE      print help

ATGO      boot system

ATUR      upload RAS code

ATUR3     upload RAS configuration file

ATBAx     change baud rate. 1:38.4,2:19.2,3:9.6,4:57.6,5:115.2

ATTD      download configuration to PC

ATSE      display seed for password generation

ATSH      display Revision and etc
```

Figure 14-14 Boot module commands

Hardware Installation & Initial Setup

ISDN Router/Hub *RA368 WAN Bridge/Routers*

14.7 Command Interpreter Mode

```
                        Enter Menu Selection Number: 8




Copyright (c) 1994 - 1998 Netgear Communications Corp.
ras> ?
Valid commands are:
sys             exit           device         ether
isdn            radius         ip             ppp
bridge          ipx
```

This option allows you to enter the command interpreter mode. A list of valid commands can be found by typing [help] at the command prompt. For more detailed information, check the Netgear Web site or send e-mail to the Netgear Support Group.

Figure 14-15 Command mode

14.8 Call Control

The ISDN Router/Hub provides four call control functions: call control parameters, blacklist, budget management andcall history..

Call control parameters allows you to set a dial out time limit, the number of times a number should be called before it is added to the blacklist and the interim between calls.

The budget management function allows you to set a limit on the total outgoing call time of the ISDN Router/Hub over a period of time. When the total outgoing call time exceeds the limit, the current call will be dropped and any future outgoing calls will be blocked.
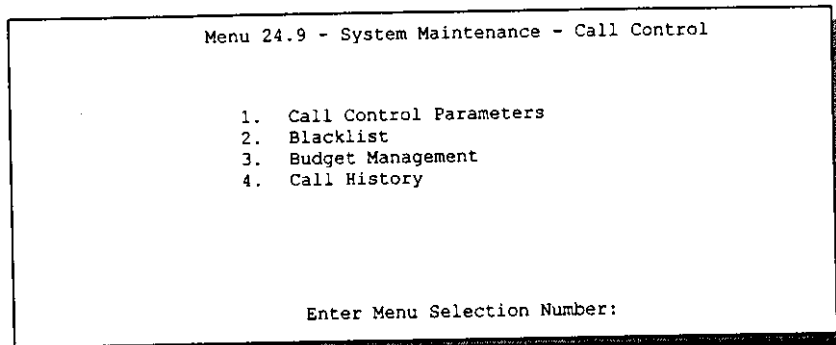
The blacklist function prevents the ISDN Router/Hub from re-dialing to an unreachable phone number. It is a list of phone numbers, up to a maximum of 14, to which the ISDN Router/Hub will not make an outgoing call. If the ISDN Router/Hub tries to dial to a phone number and fails a certain number of times (configurable in Menu 24.9.1), then the phone number is put in the

System Maintenance

Router/Hub

blacklist. You will have to enable the number manually before the ISDN Router/Hub will dial that number again.

Call history chronicles preceding incoming and outgoing calls.

To enter the call control menu, select option **9. Call Control** in Menu 24 to go to Menu 24.9 - System Maintenance - Call Control, as shown in the table below.

```
            Menu 24.9 - System Maintenance - Call Control



             1.   Call Control Parameters
             2.   Blacklist
             3.   Budget Management
             4.   Call History




             Enter Menu Selection Number:
```

Figure 14-16 Menu 24.9 - System Maintenance - Call Control

14.8.1 Call Control Parameters

```
                  Menu 24.9.1 - Call Control Parameters

                  Dialer Timeout:
                    Digital Call(sec)= 30

                  Retry Counter= 0
                  Retry Interval(sec)= N/A
      Press ENTER to confirm or ESC to Cancel:
```

Figure 14-17 Call Control Parameters

ISDN Router/Hub *RA368 WAN Bridge/Routers*

Table 14-5 Call Control Parameters Fields

Field	Description
Dialer Timeout: Digital Call (sec)	The ISDN Router/Hub will timeout if it can not set up an outgoing digital call within the timeout value. The default is **30**.
Retry Counter	How many times a busy or o answer telephone number is retried before it is put on the blacklist. The default is **0** and the blacklist control is not enabled.
Retry Interval (sec)	Elapsed time after a call fails before another call may be retried. This applies before a telephone number is blacklisted.

14.8.2 Blacklist

The phone numbers on the blacklist are numbers that the ISDN Router/Hub had problems connecting in the past. The only operation allowed is for you to take a number off the list by entering its index number.

Menu 24.9.2 shows the list of telephone numbers that have been blacklisted.

```
                        Menu 24.9.2 - Blacklist

              Phone Number
              1.
              2.
              3.
              4.
              5.
              6.
              7.
              8.
              9.
              10.
              11.
              12.
              13.
              14.
                        Remove Selection(1-14):
```

Figure 14-18 Menu 24.9.2 - Blacklist

ISDN Router/Hub *RA368 WAN Bridge/Routers*

14.8.3 Budget Management

Menu 24.9.3 shows the budget management statistics for outgoing calls.

```
                         Menu 24.9.3 - Budget Management

                              Connection Time/Total Budget    Elapsed Time/Total Period
          Remote Node              No Budget                       No Budget
     1.  isp1                         ---                             ---
     2.  --------                     ---                             ---
     3.  --------                     ---                             ---
     4.  --------                     ---                             ---
     5.  --------                     ---                             ---
     6.  --------                     ---                             ---
     7.  --------                     ---                             ---
     8.  --------                     ---                             ---
     9.  --------                     ---                             ---
    10.  --------                     ---                             ---
    11.  --------                     ---                             ---
    12.  --------                                                  No Budget
    13.  Dial-in User             No Budget



                          Reset Node (0 to update screen):
```

Figure 14-19 Menu 24.9.3 - Budget Management

The total budget is the time limit on the accumulated time for outgoing call to a remote node or for calling back to the dial-in users collectively. When this limit is reached, the call will be dropped and further outgoing calls to that remote node or dial-in user (callback) will be blocked. After each period, the total budget is reset. The default for the total budget is 0 minutes and the period is 0 hours, meaning no budget control. You can reset the accumulated connection time in this menu by entering the index of a remote node or the dial-in users. The budget and the reset period can be configured in the Menu 11 and 13 for a remote node and for the dial-in user, respectively.

14.8.4 Call History

Router/Hub

This is the fourth option in Call Control and relays information about past incoming and outgoing calls.

```
                        Menu 24.9.4 - Call History

Phone Number    Dir     Rate      #call        Max        Min        Total
    1.                                                 .
    2.
    3.
    4.
    5.        .
    6.
    7.
    8.
    9.
   10.


Enter Entry to Delete(0 to exit):
```

Figure 14-20 Call History

Table 14-6 Call History Fields

Field	Description
Phone Number	This is the telephone number of past incoming and outgoing calls.
Dir	This shows whether the call was incoming or outgoing.
Rate	This is the transfer rate of the call.
#call	This is the number of calls made to or received from that

ISDN Router/Hub *RA368 WAN Bridge/Routers*

	telephone number.
Max	This is the length of time of the longest telephone call.
Min	This is the length of time of the shortest telephone call.
Total	This is the total length of time of all the telephone calls to/from that telephone number.