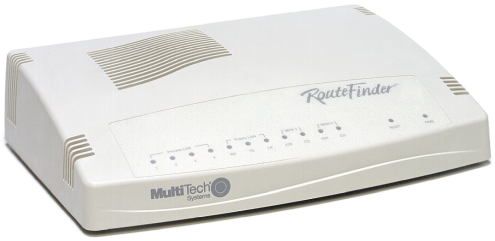
RouteFinder™

Model RF500S
Broadband Router



User Guide

MultiTech® Systems

User Guide

Broadband Router
Model RF500S
PN S000125D Revision D

Copyright

Record of Revisions

Revision	Date	Description
A	10/09/00	Manual updated for release in MTS case. All pages at Software Version 7.12
B	10/05/01	Manual updated to include a section on using an Internet browser to configure your RouteFinder, a clarification of the FDX/COL LED's function, a new FAQ section, and minor edits. All pages at Software Version 7.26
C	01/03/02	All pages at Software Version 7.29
D	07/17/02	Changed RF500S back panel graphics

Patents

This device is covered by one or more of the following patents: 6,219,708; 6,031,867; 6,012,113; 6,009,082; 5,905,794; 5,864,560; 5,815,567; 5,815,503; 5,812,534; 5,809,068; 5,790,532; 5,764,628; 5,764,627; 5,754,589; D394,250; 5,724,356; 5,673,268; 5,673,257; 5,644,594; 5,628,030; 5,619,508; 5,617,423; 5,600,649; 5,592,586; 5,577,041; 5,574,725; D374,222; 5,559,793; 5,546,448; 5,546,395; 5,535,204; 5,500,859; 5,471,470; 5,463,616; 5,453,986; 5,452,289; 5,450,425; D361,764; D355,658; D355,653; D353,598; D353,144; 5,355,365; 5,309,562; 5,301,274. Other Patents Pending

Trademarks

Trademark of Multi-Tech Systems, is the Multi-Tech logo. Windows, Windows 95, 98, Me, NT and 2000 are trademarks of Microsoft. All other trademarks are owned by their respective companies.

World Headquarters

Multi-Tech Systems, Inc.
2205 Woodale Drive
Mounds View, Minnesota 55112 U.S.A.
(763) 785-3500 or (800) 328-9717
U. S. FAX (763) 785-9874
Technical Support (800) 972-2439
Internet Address: http://www.multitech.com

Contents

RouteFinder™

Chapter 1

Introduction

MultiTech® Systems

Chapter 1 - Introduction

Welcome to the world of broadband connectivity to the Internet.

The Multi-Tech Broadband RouteFinder connects a cable modem or DSL modem to an Ethernet LAN to provide high-speed broadband access to the Internet for up to 253 users. The Broadband Router features a built-in 4-port 10/100M bps switch, one asynchronous port for backup Internet access or dial-in remote access, firewall services, and network security. This product is ideal for any business looking for cost-effective broadband access to the Internet for every user on the LAN or for the home user looking to share their DSL cable connection.

Connects up to 253 internal IP addresses to the Internet with broadband speed. With the RouteFinder, up to 253 users are connected to the Internet with only one IP account. The WAN Ethernet port has a bandwidth of 10M bps which is 179 times faster than a 56K modem and can support DSL or cable speeds of up to 4M bps.

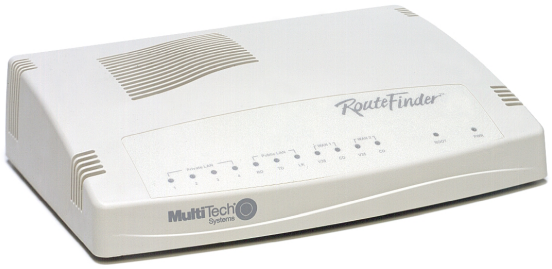
Built-in 10/100 Switch. The integrated 4-port 10/100 switch eliminates the need for an additional hub or switch to connect users not on a LAN. It ensures high-speed transmission and can serve as a completely dedicated full duplex backbone.

Network Security. The RouteFinder uses the NAT protocol to provide security from hackers attempting to access the office LAN without the extra cost of a firewall. It implements firewall and gateway security for LAN-based resources. Additionally, the RouteFinder supports Internet access restriction by IP address, client protocols or port number.

Dial Backup or Dial-in RAS Port. The RouteFinder also provides an additional asynchronous port that, when connected to a dial-up modem or ISDN terminal adapter, can serve as a backup resource for Internet access if your cable or DSL service goes down. It can also serve as dial-in remote access for your telecommuters or mobile users.

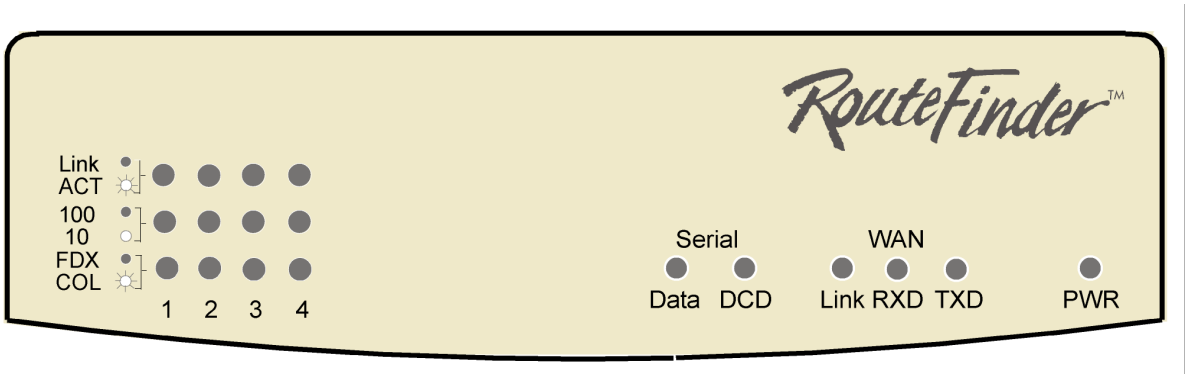
Virtual Server Support. In addition to providing shared Internet access, the RouteFinder can support Web, FTP or other Internet servers. Once configured, the RouteFinder accepts only unsolicited IP packets addressed to the Web, FTP, or other specified servers.

LAN Segmentation. For added LAN security, the RouteFinder can be used to segment the LAN by connecting the corporate servers to one RouteFinder Ethernet port and the Internet servers to the other Ethernet port. This configuration puts the corporate servers behind a firewall and the Internet servers outside the firewall. To continue to provide Internet access, connect a modem or ISDN terminal adapter to the RouteFinder's asynchronous port.



The RouteFinder RF500S

RF500S Front Panel



LAN LEDs

Link/ACT Lights when the LAN client is correctly connected to the Ethernet port. Blinks when the LAN client is correctly connected to the Ethernet port.

100 Lights when the LAN client is connected at 100MB. Off when the LAN client is connected at 10MB.

FDX/COL Lights when the LAN client is connected as full duplex. Off when the LAN client is connected as half duplex. Blinks when there are collisions on the network.

Serial LEDs

Data Blinks when the Serial async port is receiving or transmitting data.

DCD Lights when the Serial async port is properly connected to a remote site.

WAN LEDs

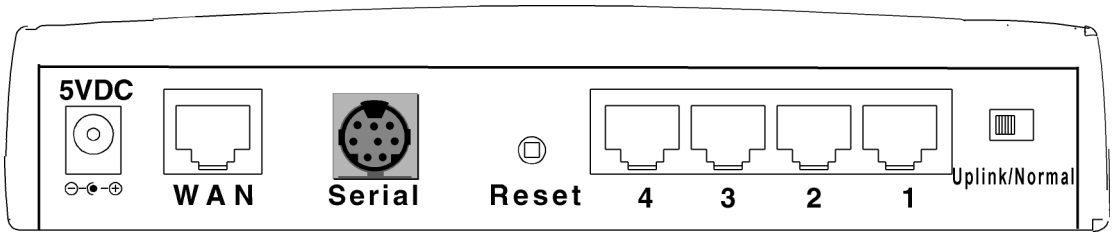
Link Lights when a successful connection to the 10BaseT WAN is established.

RXD Lights when the LAN port is receiving data.

TXD Lights when the LAN port is transmitting data.

Power Lights when power is being supplied to the router.

Back Panel



Power 5VDC Connect one end of the power cord to power socket and the other end to the power outlet.

10 BT WAN The WAN port is used to connect the router to a DSL or Cable modem.

ASYNC The Serial async port connects the router to a standard modem (optional).

Reset The Reset button is used to reset the router to factory defaults.

10/100 BT LAN The 4-10/100 ports are used to connect the router to LAN client workstations. If the RF500S is set to use the Uplink feature, the number 1 LAN port is inactive as a LAN port.

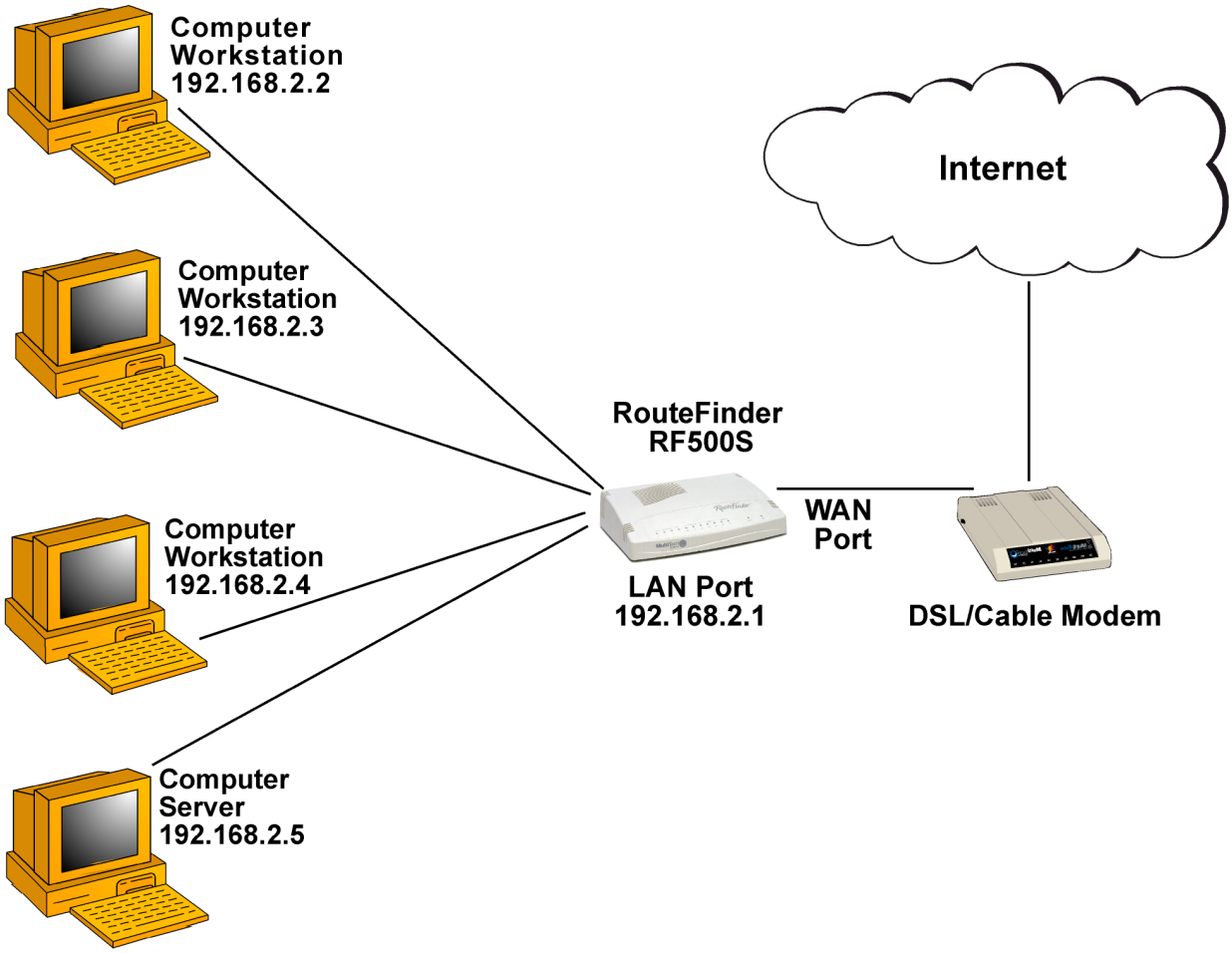
Uplink/Normal Slide the switch to the Uplink position to use the number 1 LAN 10/100 port to expand your network by connecting a network cable to another router, switch or hub. To connect the number 1port to a LAN client workstation, slide the switch to the Normal position.

Application Examples

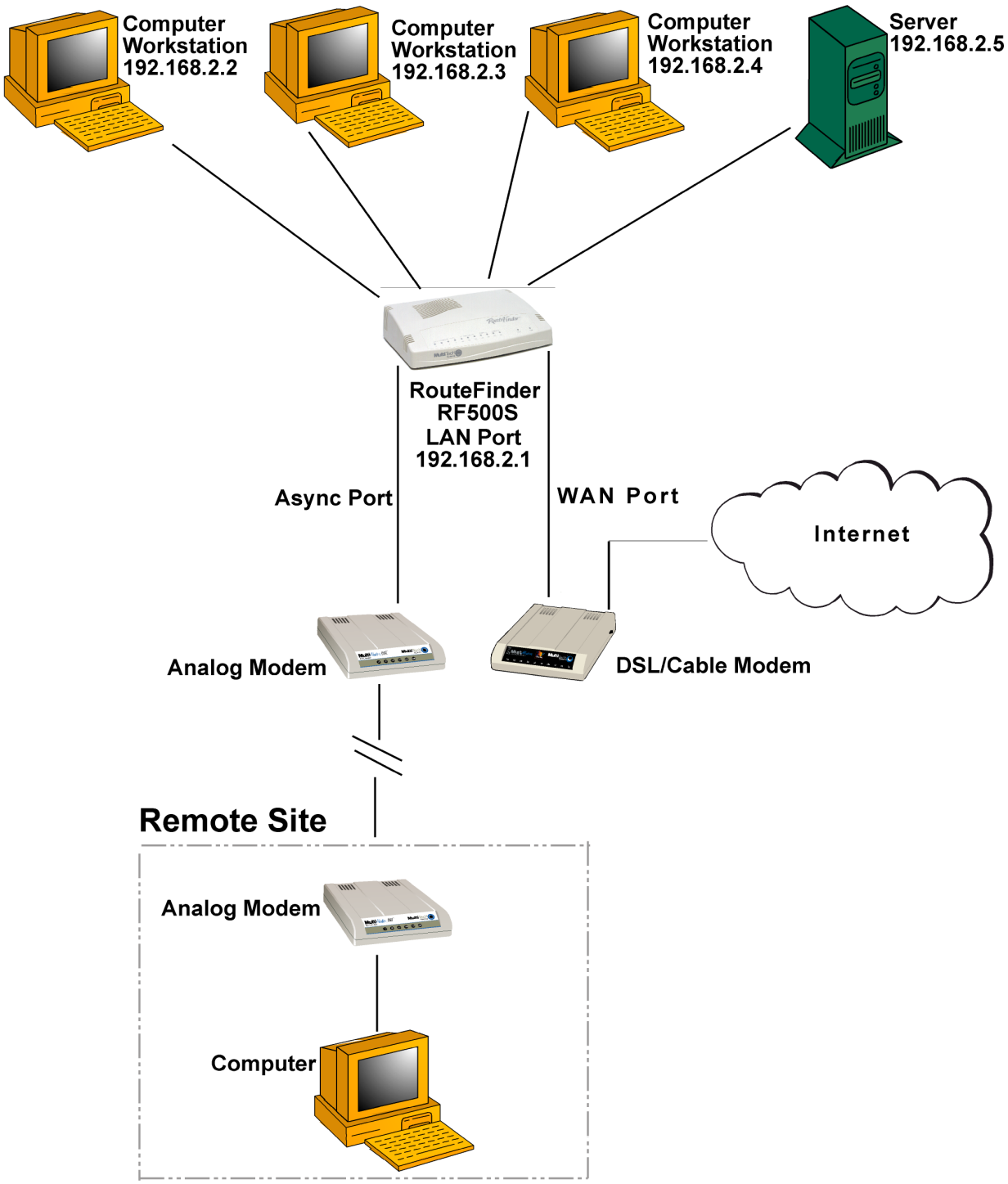
The following examples provide information about RF500S typical applications. The three examples include:

1. Connecting a local LAN to Internet.
2. Connecting a local LAN to the Internet and setting up a remote site.
3. Setting up a LAN to LAN via the Async Port.

Example 1 – Connecting a Local LAN to the Internet

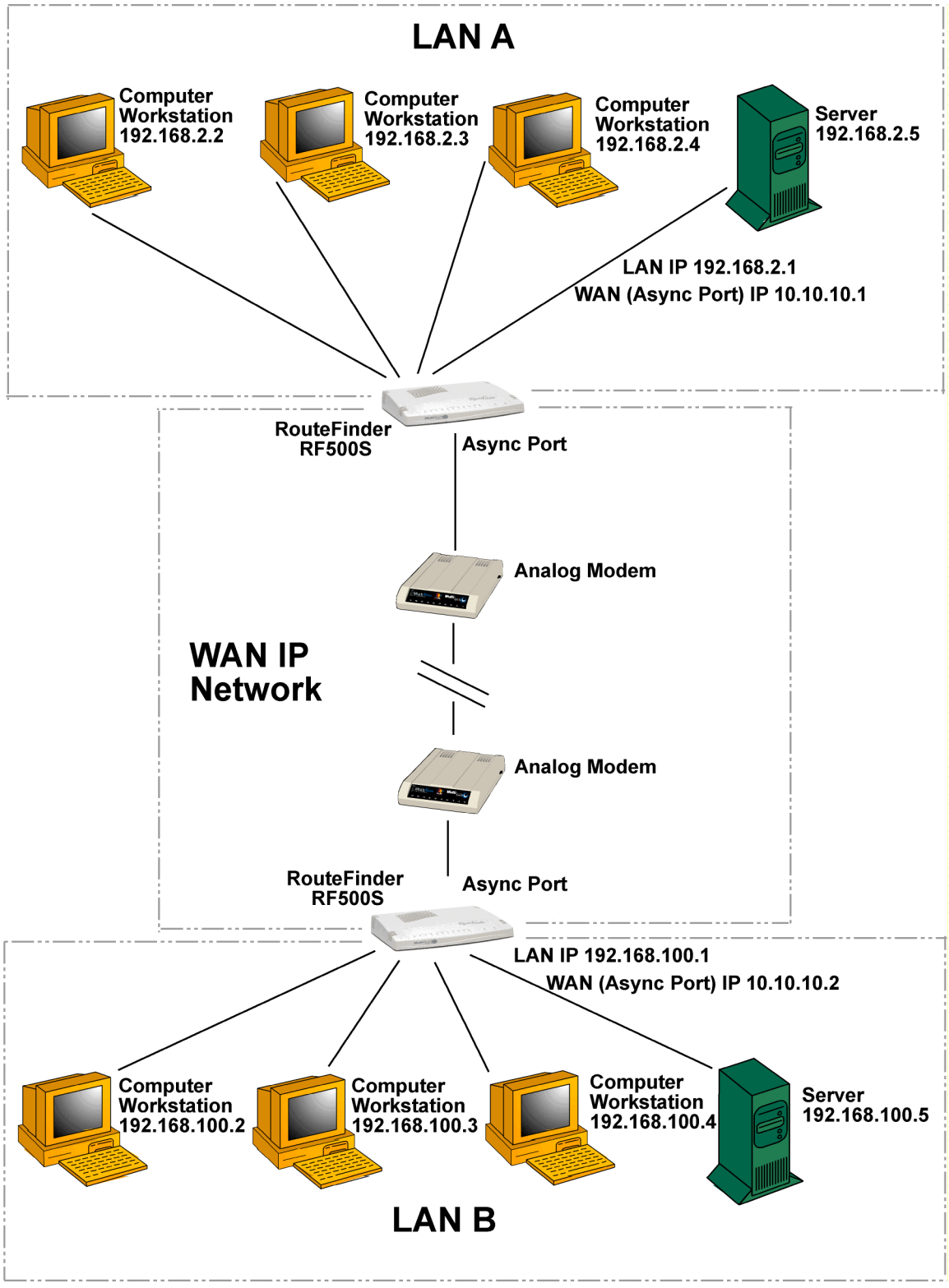


Example 2 – Local LAN to Internet / Remote Site



Example 3 – LAN to LAN via an Async Port

Note: Set the modem type to leased line.



Setup for Example 3

The setup describes the RF500S used as routers to route IP traffic between two LANs.

Network Addresses

LAN A IP Network Address: 192.168.2.x
WAN IP Network Address: 10.10.10.x
LAN B IP Network Address: 192.168.100.x
Note: Between LAN A and LAN B Are Two RF500S RouteFinders and One 56K

LAN A

RF500S WAN Ethernet port in this case is not used
95/98 Workstation has IP Address: 192.168.2.2
RF500S 10/100 Ethernet port has IP Address: 192.168.2.1
RS232 WAN port has local IP Address: 192.168.100.1
RS232 WAN port has remote IP Address: 192.168.100.2

LAN B

RF500S WAN Ethernet port in this case is not used
95/98 Workstation has IP Address: 10.10.10.2
RF500S 10/100 Ethernet port has IP Address: 10.10.10.1
RS232 WAN port has local IP Address: 192.168.100.2
RS232 WAN port has remote IP Address: 192.168.100.1

RF500S Setup for LAN A

1. Bring up the RouteFinder Manager program
2. Select the RF500S from the **Available Devices** list
3. Click the **General Settings** button. The General Settings main screen displays.

LAN Ethernet Segment

Set Server IP Address: 192.168.2.1

Set Server IP Netmask: 255.255.255.0

WAN Ethernet Segment

Uncheck NAT

Uncheck PPOE

Async Port Setup

Check IP Routing

Click the **PPP Settings** button. The **IP Routing Settings** screen displays.

IP Routing Settings Screen

Uncheck IP Routing (so NAT is disabled)

Enter the Phone Number of the modem on the other side

Enter the User Name and Password if you want authentication (the RF500S on the other side needs to be setup properly for this)

Enter the External (port) IP: 192.168.100.1

Check **Assign Remote Site an IP Address** and enter the IP Address: 192.168.100.2

Check Allow Remote Dial-in

Click the **Remote Authentication Settings** button if you want to authenticate with user name and password. The **Remote Connection Authentication** screen displays.

Remote Connection Authentication Screen

If you check PAP, then check Use Local Settings and enter the Remote User Name and **Remote Password**.

Click the **OK** button and return to the RouteFinder Manager main menu.

4. On the RouteFinder Manager main menu, click the **Port Settings** button to setup your modem.

   Click the **Dialup/Hangup Setting** button to enable/disable dial-on-demand.

   Click the **OK** button to return to the RouteFinder Manager main screen.

5. On the RouteFinder Manager main screen, click the **Routing Settings** button.

   Add the Default Gateway as 192.168.100.2 and the Interface as Async Port

6. Click **Save** and **Exit**

Workstation Setup for LAN A

Set IP Address to 192.168.2.2
Set Default Gateway to 192.168.2.1

RF500S Setup for LAN B

1. Bring up the RouteFinder Manager program
2. Select the RF500S from the **Available Devices** list
3. Click the **General Settings** button

LAN Ethernet Segment

Set Server IP Address: 10.10.10.1
Set Server IP Netmask: 255.255.255.0

WAN Ethernet Segment

Uncheck NAT
Uncheck PPOE

Async Port Setup

Check IP Routing

Click the **PPP Settings** button. The **IP Routing Settings** screen displays.

IP Routing Settings Screen

Uncheck IP Routing (so NAT is disabled)

Enter the Phone Number of the modem on the other side

Enter the User Name and Password if you want authentication (the RF500S on the other side needs to be setup properly for this)

Enter the External (port) IP: 192.168.100.2

Check **Assign Remote Site an IP Address** and enter the IP Address: 192.168.100.1

Check Allow Remote Dial-in

Click the **Remote Authentication Settings** button if you want to authenticate with user name and password. The **Remote Connection Authentication** screen displays.

Remote Connection Authentication Screen

If you check **PAP**, then check **Use Local Settings** and enter the **Remote User Name** and **Remote Password**.

Click the **OK** button and return to the RouteFinder Manager main menu.

4. On the RouteFinder Manager main menu, click the **Port Settings** button to setup your modem.
   Click the **Dialup**/Hangup Setting button to enable/disable dial-on-demand.
   Click the OK **button** to return to the RouteFinder Manager main menu.
5. On the RouteFinder Manager main menu, click the **Routing Settings** button.
   Add the Default **Gateway** as 192.168.100.1 and the **Interface as Async Port**
6. Click **Save** and **Exit**

Workstation Setup for LAN B

Set IP Address to 10.10.10.2

Set Default Gateway to 10.10.10.1

Once Setup Is Complete

You can try to ping 10.10.10.1 on the LAN A workstation. This will cause the RF500S on LAN A to dial and connect to the RF500S on LAN B. Once both modems are connected, you will see all the ping responses.

You can also bring up the RouteFinder Monitor program to see the activities on the Async Port.

Specifications

Hardware	ARM RISC CPU32 bit, 40MHZ 4MB DRAM and 512k Flash ROM UART Serial port controller
LAN Ports	Number of Ports: 4 Interface: 10Base T/100BaseTX, - One port can be used for uplink Standard: 802.3
WAN Ports	1 x 10BaseT 1 x RS232 (V.24) DTE Speed: Up to 460K asynchronous
Protocols	**Security:** PAP/CHAP, MSCHAP, NAT Firewall, RADIUS and Callback for remote access. **Network:** TCP/IP, IPX, DHCP, PPP, PPPoE **Filtering:** Protocol, port number, URL address and IP address
LED Indicators	1 indicator for Power On 3 indicators for WAN function (LINK, TxD, RxD) 2 indicators for Serial Async function (DATA, DCD) 3 indicators for each of 4 LAN ports functions (LINK/ACT, 100, FDX/COL)
Power Output	5VDC, 1000mA
Dimensions	230mm(L) x 152mm(W) x 39.5mm (H) 9.06 " (L) x 5.98 " (W) x 1.55" (H)
Weight	380g 13 oz.
Memory	RAM: 4MB Flash ROM: 512k
Temperature	**Temperature Range:** 32 - 120 degrees F (0 - 50 degrees C) **Humidity:** 25-85% non-condensing
Approvals	FCC Part 15 & CE Mark
Warranty	2-year warranty

RouteFinder™

Chapter 2

Hardware Installation

MultiTech® Systems

Chapter 2 - Hardware Installation

Safety

1. Never install telephone wiring during a lightning storm.
2. Never install telephone jacks in a wet location unless the jack is specifically designed for wet locations.
3. This product is to be used with UL and cUL listed computers.
4. Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
5. Avoid using a telephone during an electrical storm. There may be a remote risk of electrical shock from lightening.
7. Do not use the telephone to report a gas leak in the vicinity of the leak.
8. To reduce the risk of fire, use only No. 26 AWG or larger Telecommunications line Cord.
9. Use only the power source supplied with your product or an equivalent power source supplying the minimum power requirements.

Unpacking the RF500S

The RF500S shipping box contains the following items:

- System CD
- Power Source
- The RouteFinder RF500S
- The RF500S RouteFinder Quick Start Guide
- A serial cable

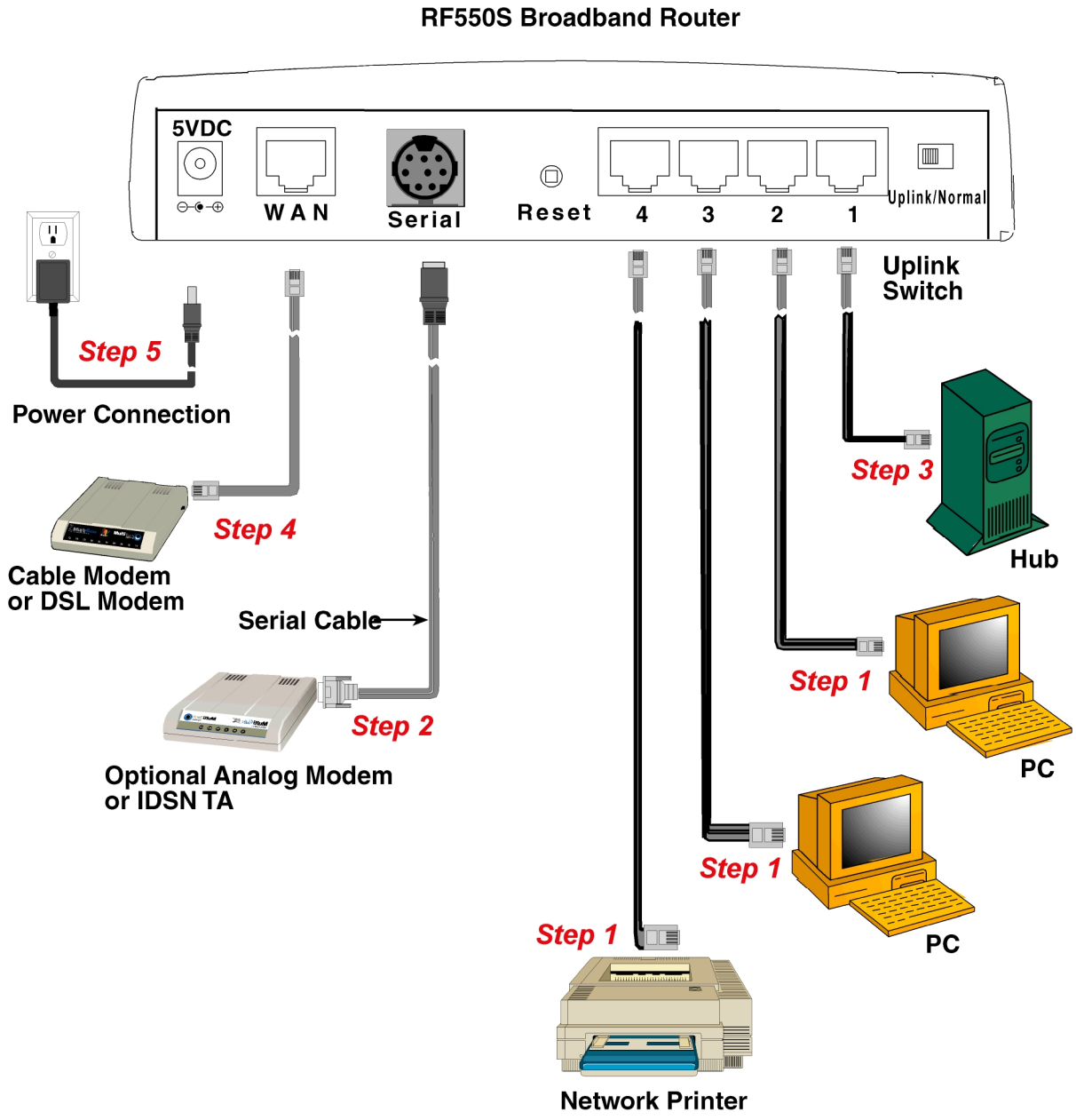
If any items are missing or damaged, please contact Multi-Tech Systems.

Requirements

- Intel 486 or higher processor.
- 10/100 BaseT cable to connect the RF500S to the network.
- One DSL or Cable Modem.
- A networked computer with Windows 95/98/Me/2000, Windows NT 3.5 or higher and TCP/IP protocol installed (or a non-Windows system with TCP/IP properly installed to enable Telnet configuration).
- Any PPP supported communication application for Dial-In operation.
- TCP/IP installed and configured on each workstation accessing the Internet.

Cabling

Cabling your RouteFinder requires making the appropriate connections to PCs, Cable or DSL modem, analog modem or ISDN TA (optional), AC power, and the RouteFinder. Then, after your device is properly cabled, you will have to configure your RouteFinder. Follow the instructions provided in the Web Browser Configuration and Management chapter.



Cabling Directions

Before beginning, turn the power off on all network devices (PCs, Cable/xDSL modems, analog modems, ISDN TAs, and the router).

1. Connect the Ethernet port of each PC or network device to one of the 4 LAN ports.

   Important: If you are using the Uplink option, Port Number 1 cannot be used as a LAN port).
2. If you are using an analog modem, connect it to the Serial Async port.
3. If you are using the Uplink option to connect to another network segment, slide the **Uplink/Normal** switch into the Uplink position. Connect the LAN cable to LAN Port Number 1. Plug the other end of the LAN cable into another hub, router, or switch.

   Note: If you are not using the Uplink feature, place the switch in the Normal position.
4. Connect a network cable from the cable or DSL modem to the 10 BT WAN port.
5. Connect the provided power supply cable to the 5VDC power port on the back of the router. Plug the power supply into an AC power outlet as shown above.

Power and Reset Button

1. Power on your cable or DSL modem.
2. If you are using an analog modem or ISDN TA, power on the device.
3. Press and hold the RouteFinder's Reset button for 3 seconds to restore the default settings.

You are ready to configure software for your RouteFinder and network PCs.

RouteFinder™

Chapter 3

Web Browser Configuration And Management

MultiTech® Systems

Chapter 3 – Configure and Manage Using a Web Browser

Overview of Configuration and Management

The RF500S can be configured and managed using one of two methods.

1. **Using a Web Browser:** Launch your Web browser and type the device IP address http://192.168.2.1 in the browser address box. This IP address is the default value of your gateway. Press **Enter**. The RouteFinder wizard main screen displays.

   This chapter walks you through the Web browser method of configuring and managing your RF500S.

OR

2. **Using Multi-Tech Software:** Install the Multi-Tech software, which consists of the RouteFinder Setup Wizard, the RouteFinder Manager, and the RouteFinder Monitor.

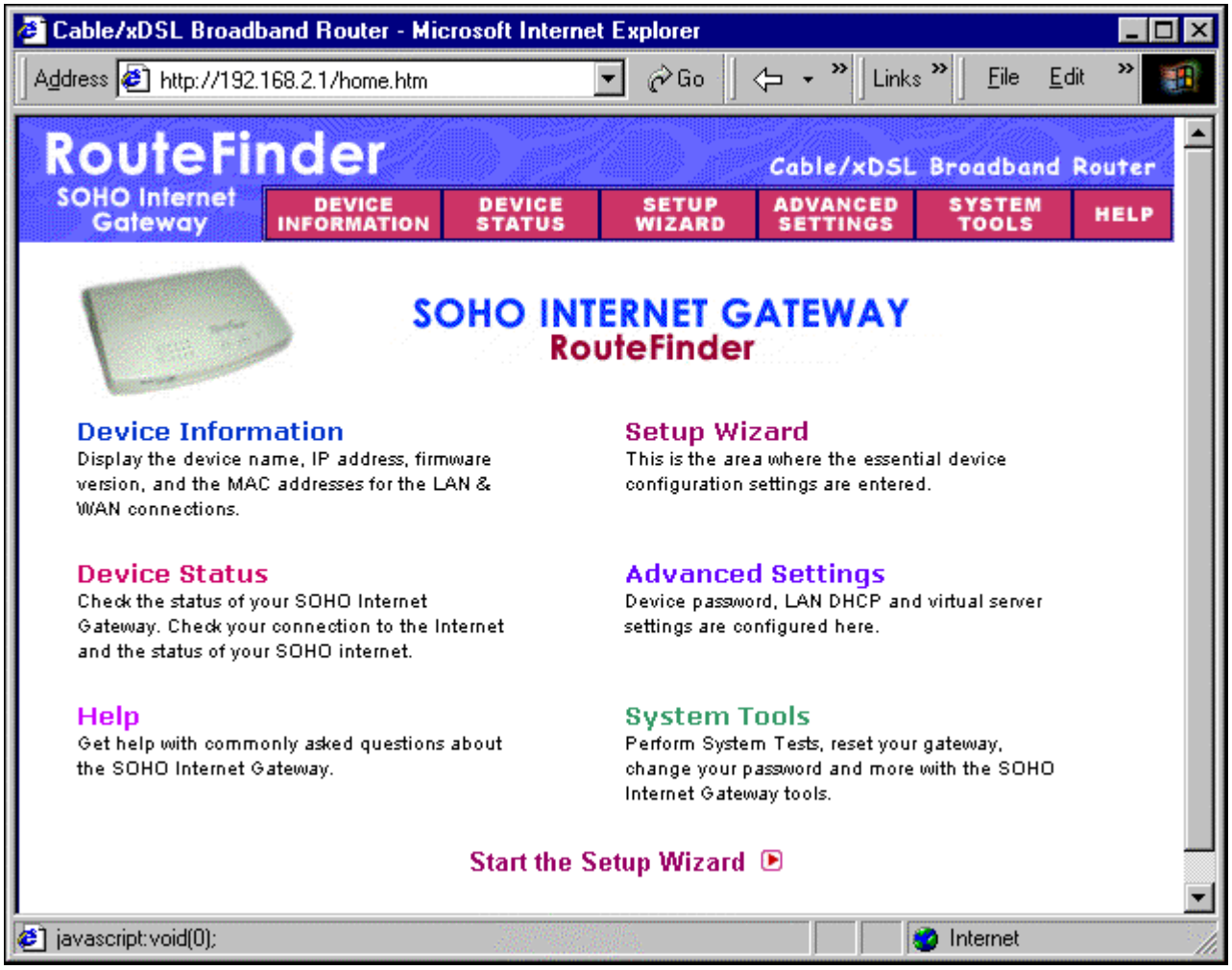
   This method of configuring and managing your RF500S is documented in Chapters 4, 5, and 6. The software is included on the system CD packaged with your RouteFinder.

Using the Web Browser

Launch your Web browser and type the device IP address **(http:// 192.168.2.1)** in the browser's address box. This IP address is the default value of your gateway. Press **Enter**.

Note: Make sure your PC's address is in the same network as the router's. In Windows 95/98/Me you can type **WINIPCFG**. In Windows 2000/NT, you can type **IPCONFIG**.

The main menu displays. It contains the setup, configuration, management, and display functions for your RouteFinder and home Internet gateway.

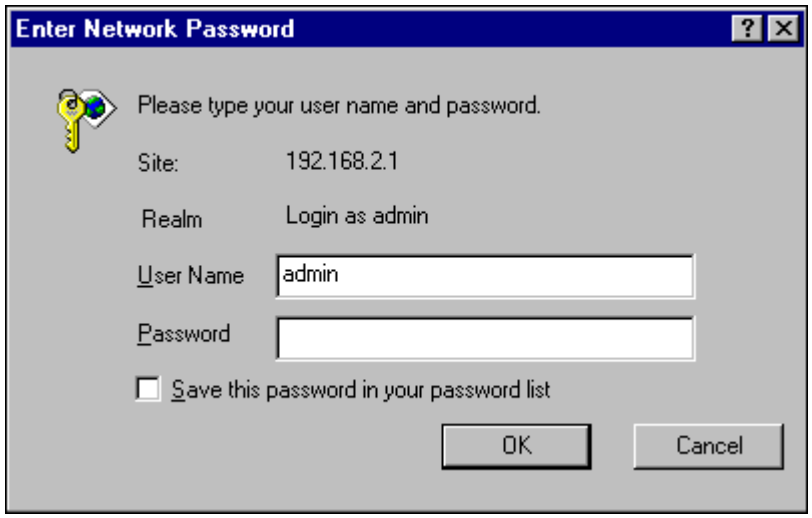


Setup Wizard

To access, click the **Setup Wizard** button on the main screen.

The **Setup Wizard** is a step-by-step process for configuring your RouteFinder.

The **Enter Network Password** screen displays. Type **admin** (the default user name) in the user name box and leave the password box empty. Click **OK**.



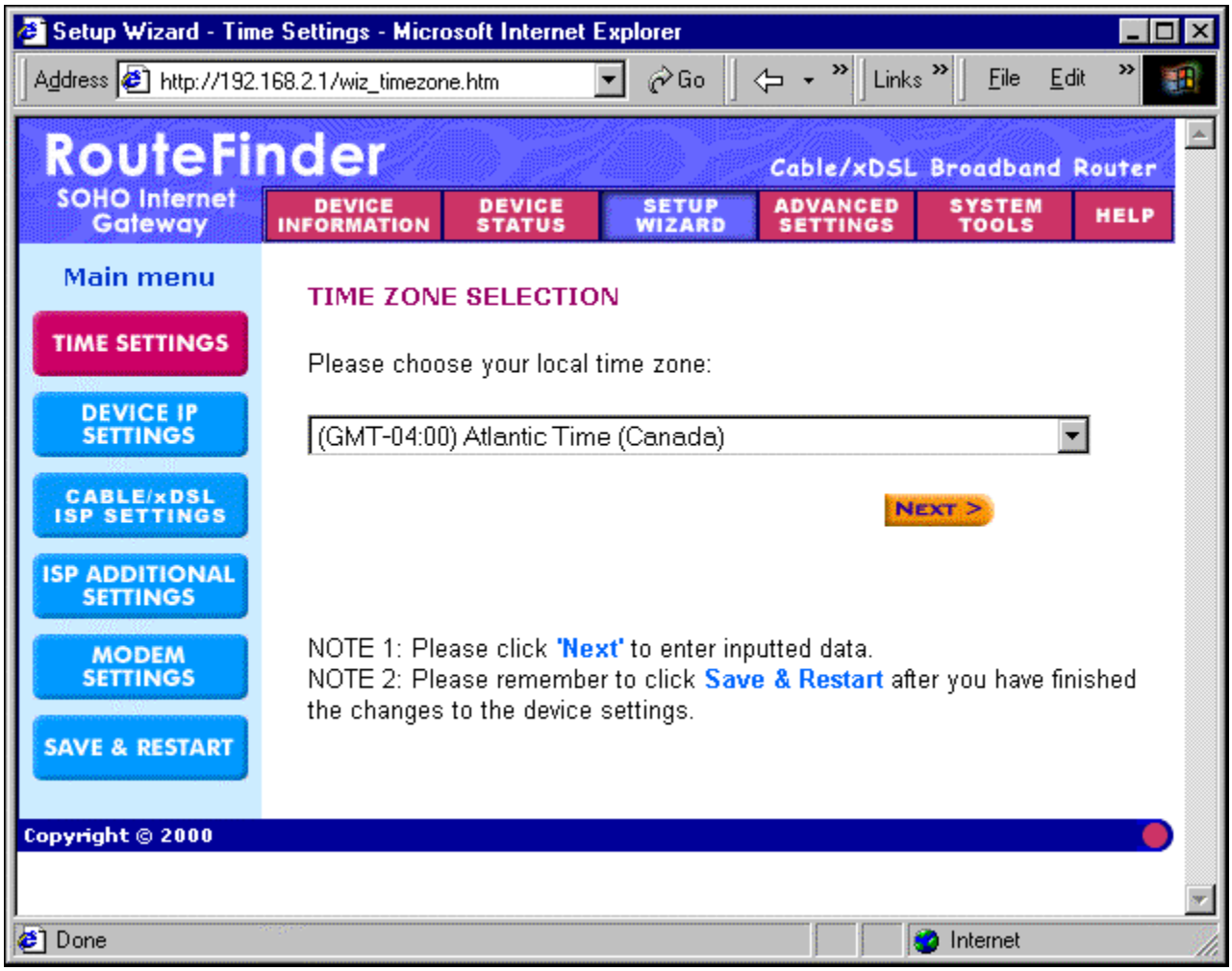
Note: For information on how to change your password, see the ISP Additional Settings section.

The **Setup Wizard** screen then displays.

Setup Wizard Screen

SETUP WIZARD – Time Zone Selection

Choose the local time zone (see screen above). Select the time zone, and then click the **Next** button to continue. You can also click the buttons on the left side of the screen. These buttons are useful when you want to change the information on individual screens or to choose your own setup order.



SETUP WIZARD – Device IP Settings

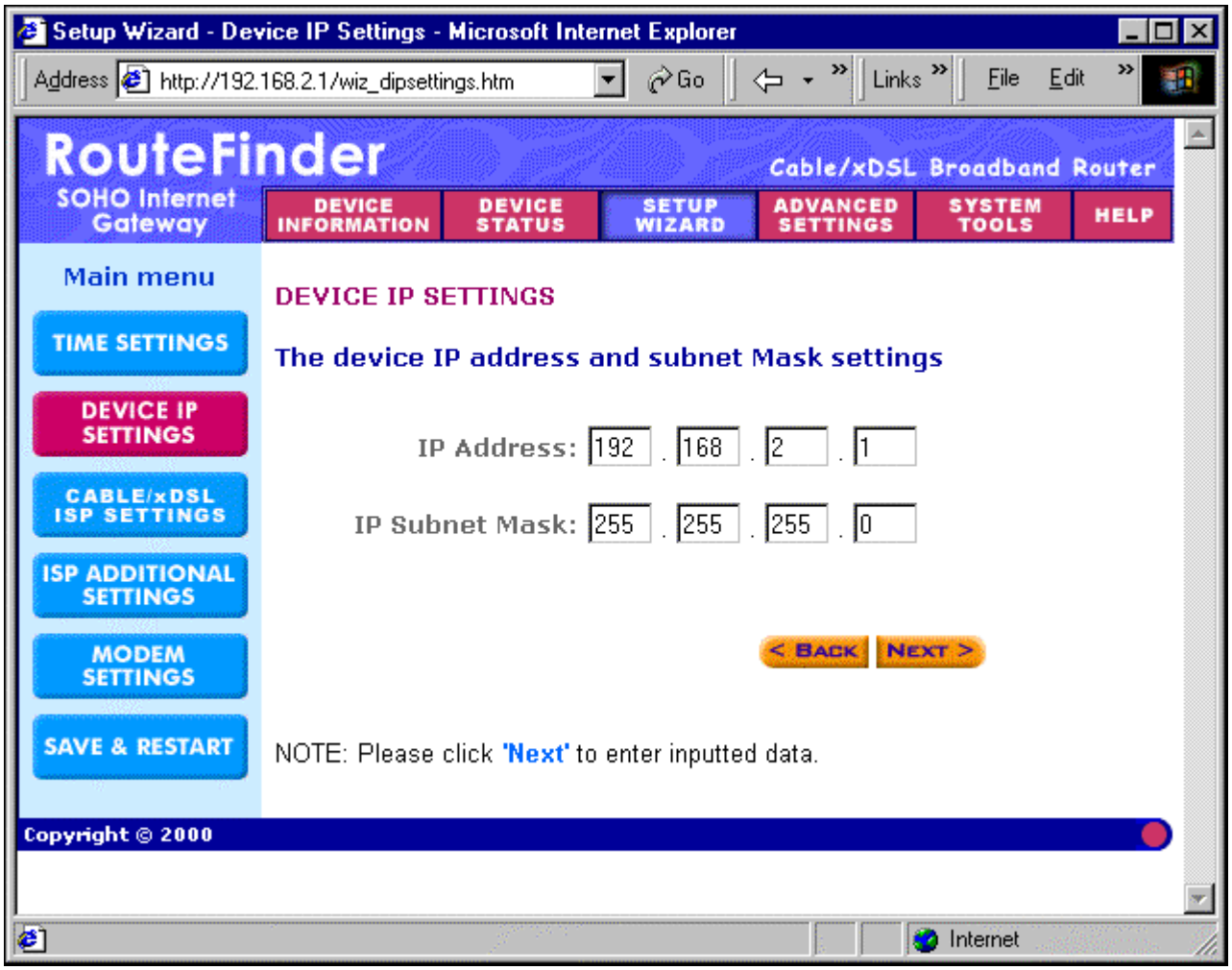
You must set your Internet gateway an IP address on your network. This is **not** the IP address from your ISP but the local internet LAN IP address. The IP address 192.168.2.1 is the default value of your gateway.

Device IP Address

The internal LAN IP address of your Internet gateway.

Device IP Subnet Mask

The subnet mask can usually be left as its default entry 255.255.255.0



SETUP WIZARD – Cable/xDSL ISP Settings

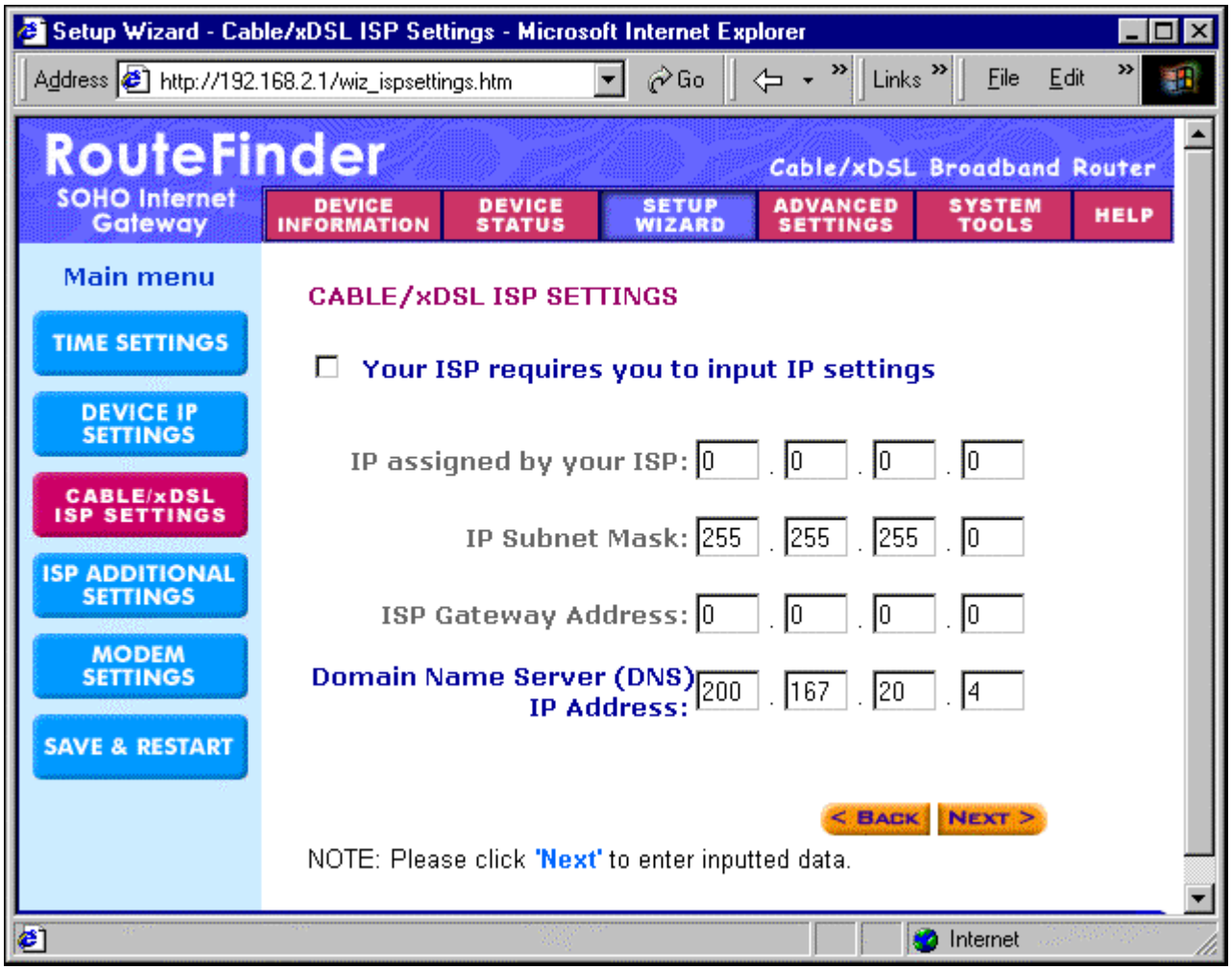
If you would like to establish Cable/xDSL ISP settings, you have to enable this function by configuring this screen. Some ISPs may give you Static IP settings. If this is the case for your ISP, then you need to:

Enter the IP address that is assigned by your ISP.

Enter the IP subnet mask.

Enter the ISP gateway address.

Enter the DNS IP address.



SETUP WIZARD – ISP Additional Settings (PPPoE Settings)

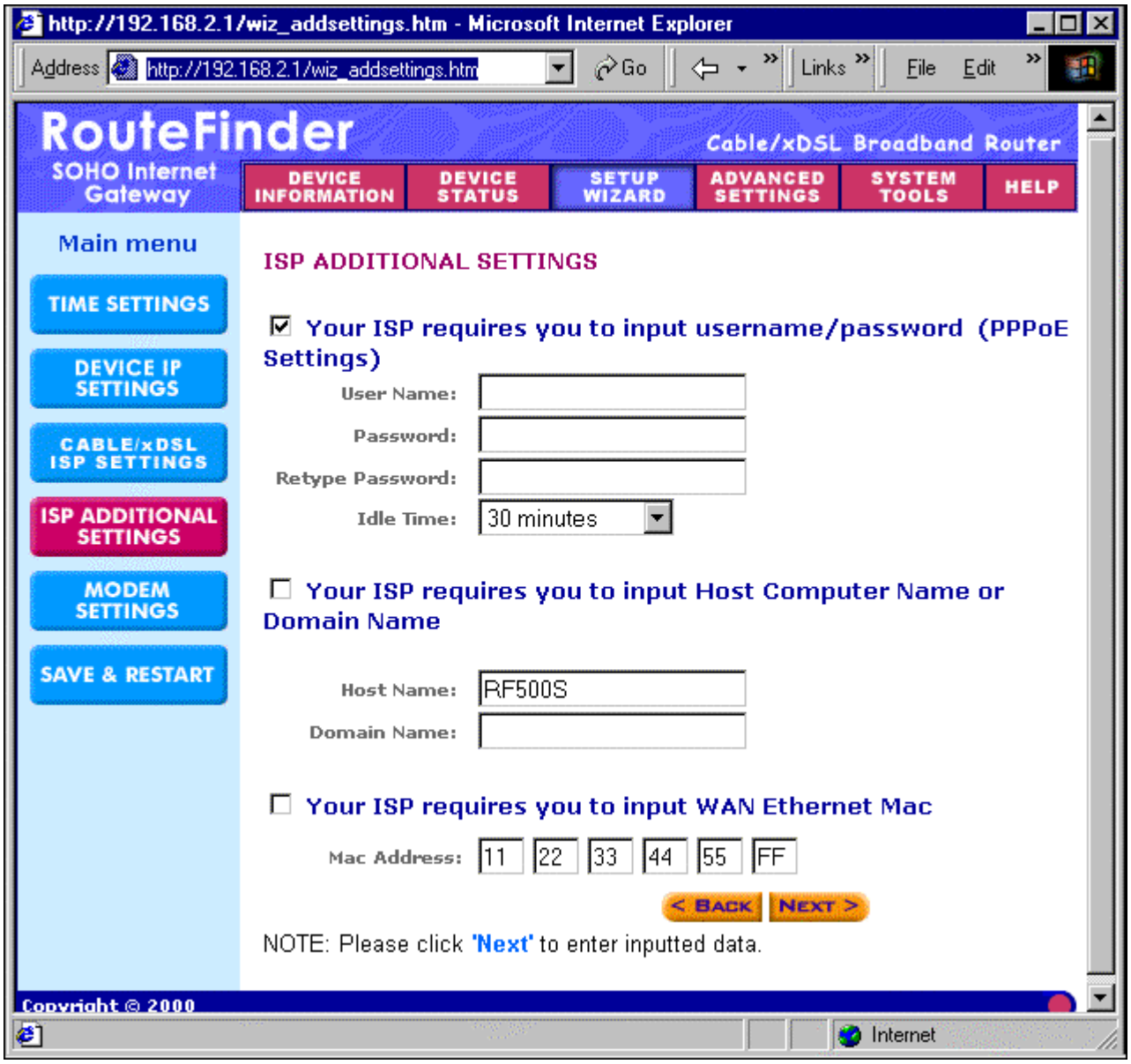
Some ISPs use this protocol for authentication purposes. If applicable:

Enter the **User Name** of your ISP account.
Enter the **Password** of your ISP account.
To verify your password, **Retype the Password** of your ISP account.

Some ISPs require additional information; if this is the case:

Enter the **Host Name** to authenticate the user.
Enter the LAN card **MAC address**.

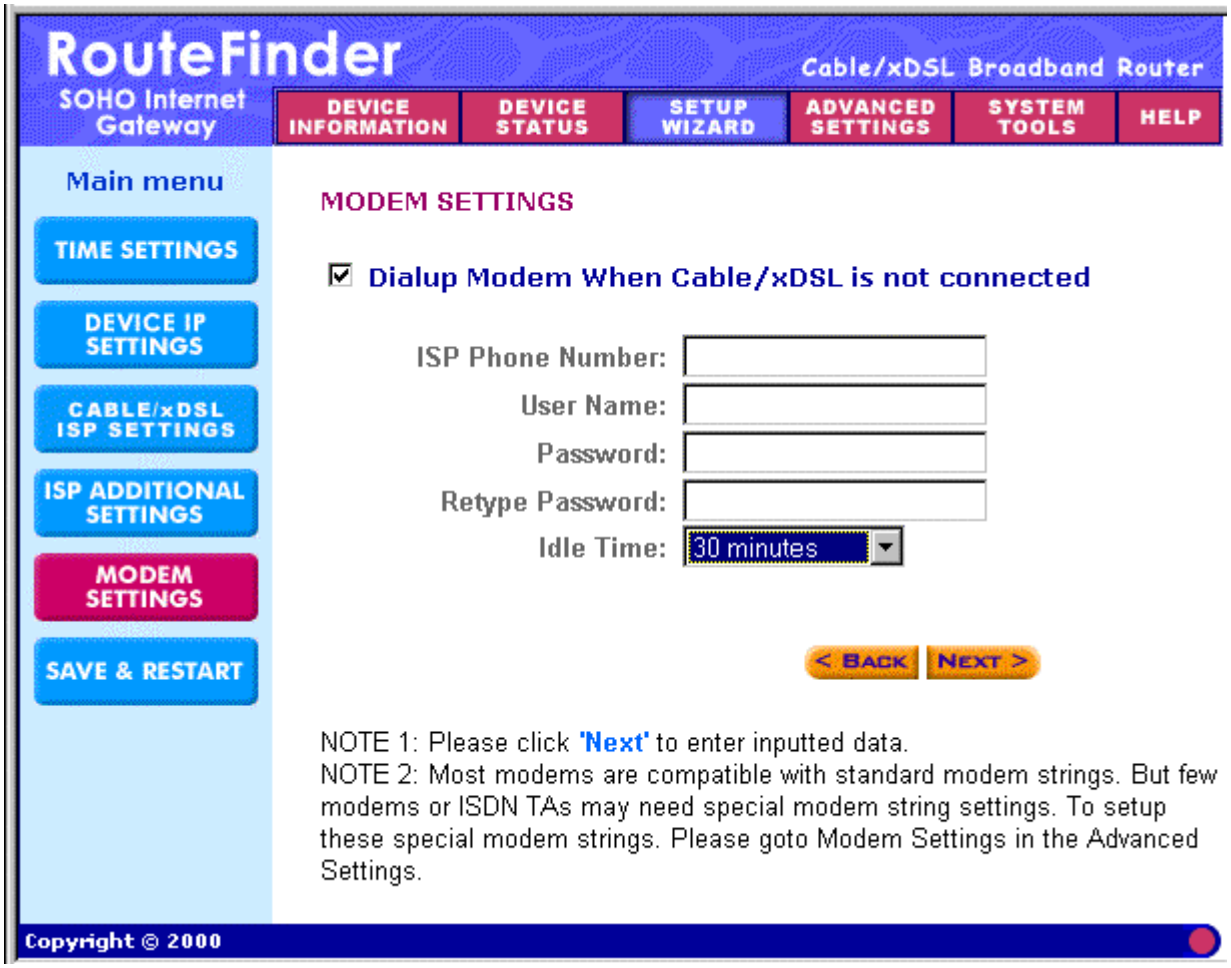
Note: Some ISPs may recognize your LAN card MAC address as a legal user. In this case, you have to copy the LAN card MAC address in the MAC address field.
For Windows 95/98, you can run **WINIPCFG** to see the LAN card MAC address.
For Windows 2000/NT, you can run **IPCONFIG/ALL** to see the LAN card MAC address.



SETUP WIZARD – Modem Settings

A modem can be used as a dialup backup to the Cable/xDSL connection. If you would like to use a modem backup, enable the modem settings function. Check the **Dialup Modem When Cable/xDSL Is Not Connected** box. Then input the ISP account settings.

Note: If you change the baud rate settings, please check the initial string. (You can refer to your modem manual or TA.)



SETUP WIZARD – Save and Restart

After you have finished making all the changes on the various pages, click **Save & Restart** to save the settings and restart the device**.** After restarting, the device will function according to the saved settings.

During the save and restart process, system messages will let you know that you have successfully configured the settings for the device and saved the settings.

During the startup process, the LEDs of the device will blink. Please **wait** until the blinking of the device stops before proceeding.

Device Information

Click the **Device Information** button. The **Device Information** screen displays the current settings of the RF500S.

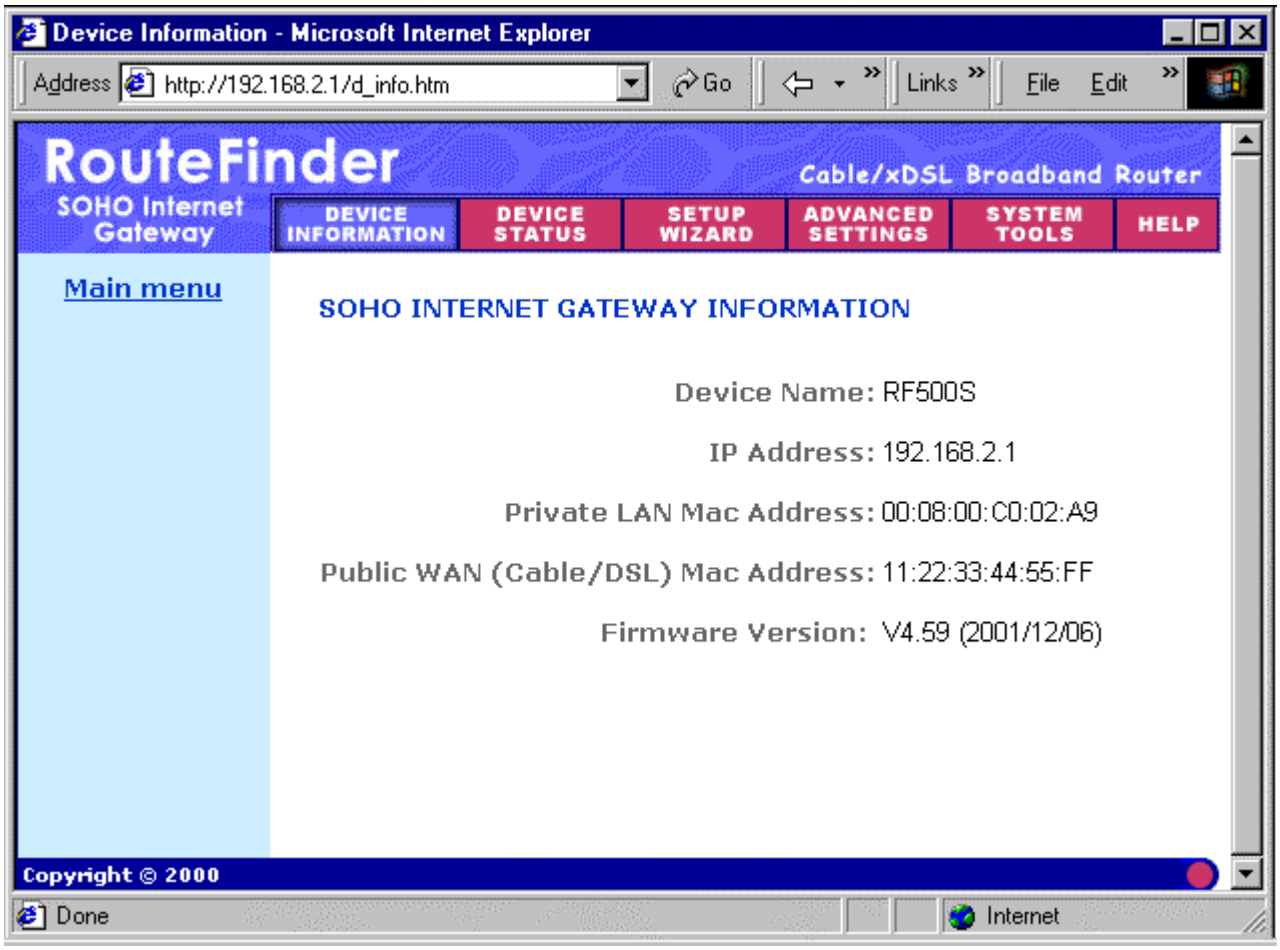
Device Name – The host name of the Internet gateway.

IP Address – The IP address of the Internet gateway.

Private LAN Mac Address – The Mac address of the Internet gateway LAN Ethernet port. This address cannot be changed; it is assigned by Multi-Tech.

Public WAN (Cable/xDSL) Mac Address – The Mac Address of the WAN Ethernet port. This address cannot be changed; it is assigned by Multi-Tech.

Firmware – The current firmware's version number and its release date.



Device Status

Click the **Device Status** button. The Device Status screen displays.

The **Device Status** screen displays the status of the current connection. It shows the status of the Cable/xDSL modem and the Modem Backup. It also shows the IP Address, the LAN Mac Address, and the WAN Mac Address.

WAN Ethernet – This describes the current connection status of the Cable/xDSL Modem. When the Cable/xDSL is connected, the screen displays a message **Cable/xDSL: Active.**

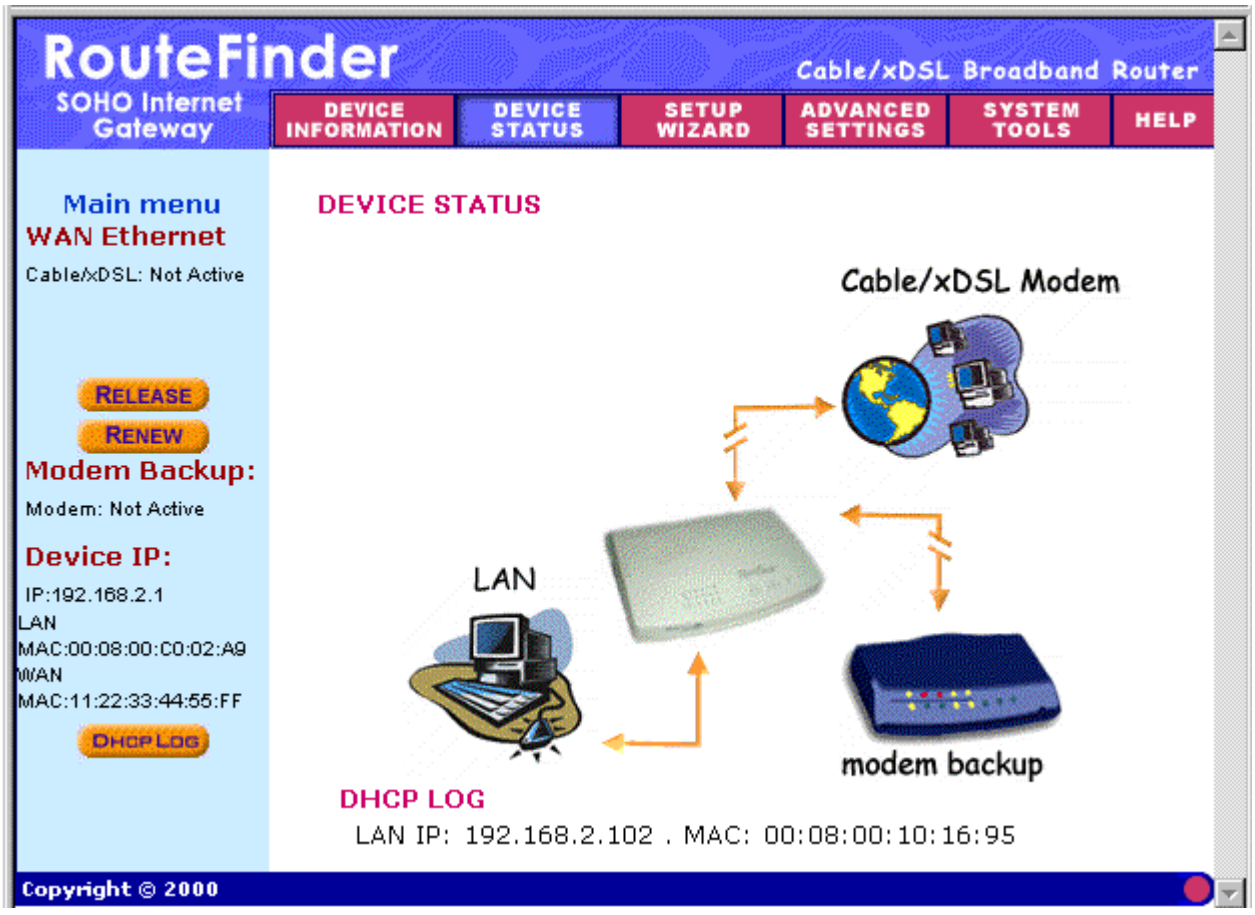
Release Button – Click this button to disconnect the Cable/xDSL modem from the RF500S.

Renew Button – Click this button to re-connect the Cable/xDSL modem to the RF500S.

Modem Backup – A modem can be used as a dialup backup for the Cable/xDSL modem. If this modem is the current connection, the screen displays a message **Modem: Active**.

Device IP - Shows the Device IP address, private LAN MAC address, and public WAN MAC address of the home Internet gateway.

DHCP Log Button – Click this button to view the current DHCP client information. The log will display at the button of the screen.



Advanced Settings

Click the **Advanced Settings** button. The DHCP Server Settings screen displays.

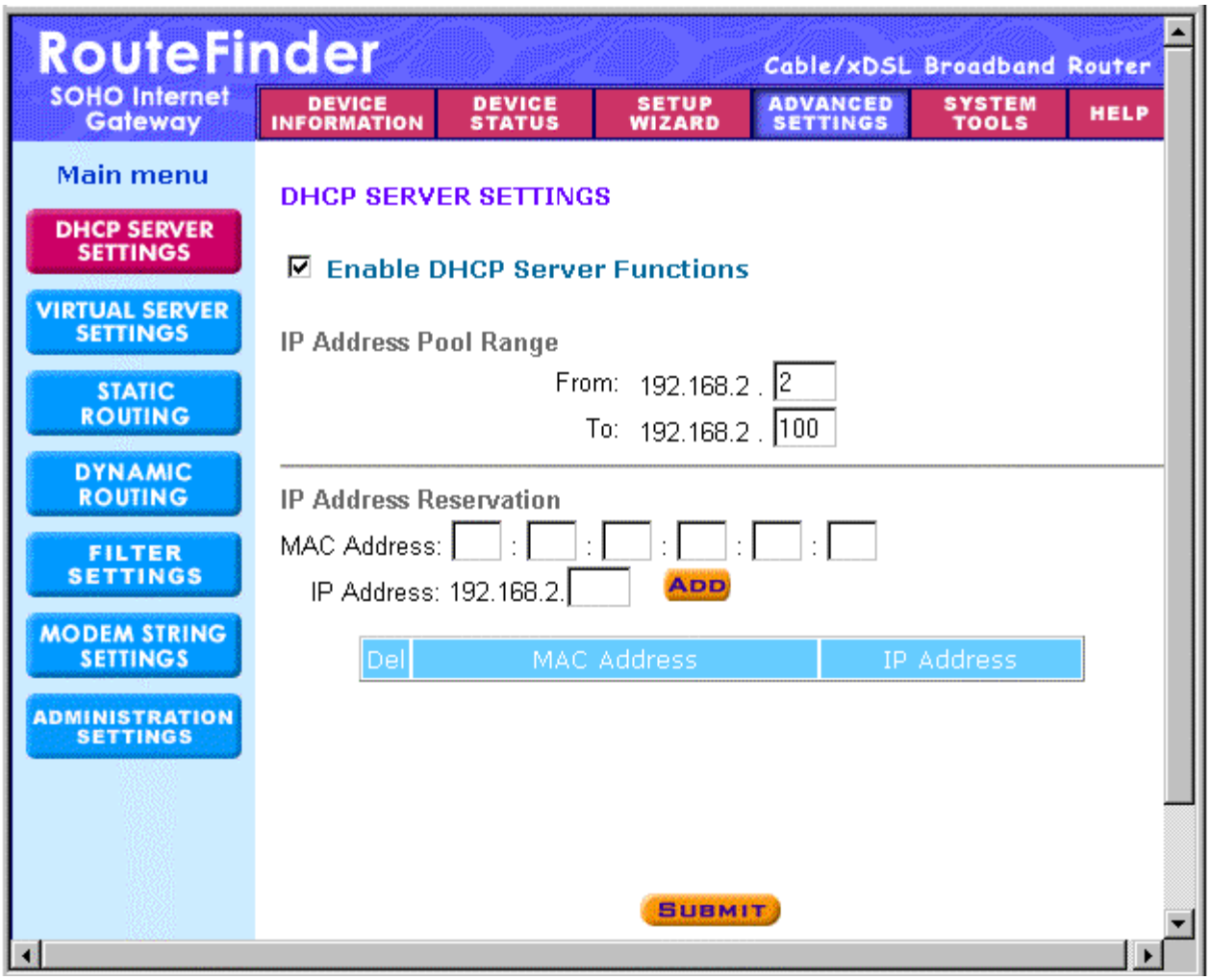
Advanced Settings options will establish DHCP server settings, virtual server settings, a static routing table, dynamic settings, modem string settings, administrative settings.

DHCP Server Settings

The **DHCP Server** is enabled by default. If you would like to disable it, uncheck the **Enable DHCP Server Functions** box.

IP Address Pool Range - Assign the range of the IP addresses that will automatically be assigned to the clients of your network. The default settings are **192.168.2.2** to **192.168.2.100**.

IP Address Reservation - Assign computers on your network the same static IP address every time the computer is turned on.

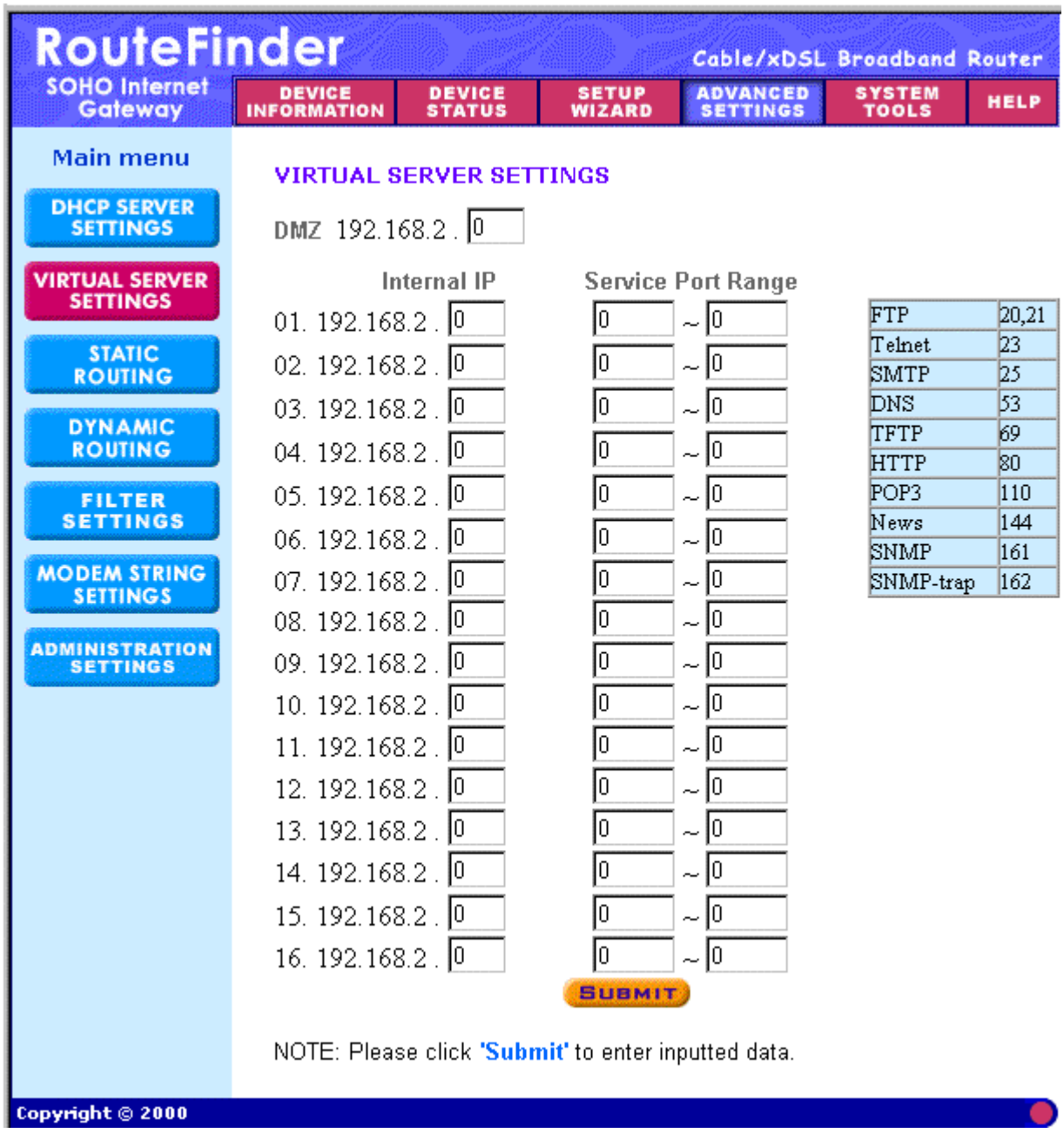


ADVANCED SETTINGS – Virtual Server Settings

To access this screen, click the **Virtual Server Settings** button on the left side of the screen. Virtual Server Settings allow clients on the Internet to access your LAN via the Internet. You can use the IP mapping function to access an FTP server or Telnet server, etc. on your LAN via your ISP Internet connection.

If applicable, enter a DMZ address.

Enter the Internal IP number and the Service Port Range for each client. See the **Typical Applications** section in this guide for examples of VPN Server Settings and their corresponding applications. Click the **Submit** button when finished.



ADVANCED SETTINGS – Static Routing

Routing is the process of moving packets of data from source to destination. Use this screen to create a routing table to connect your network to another, or to connect subnets within your network.

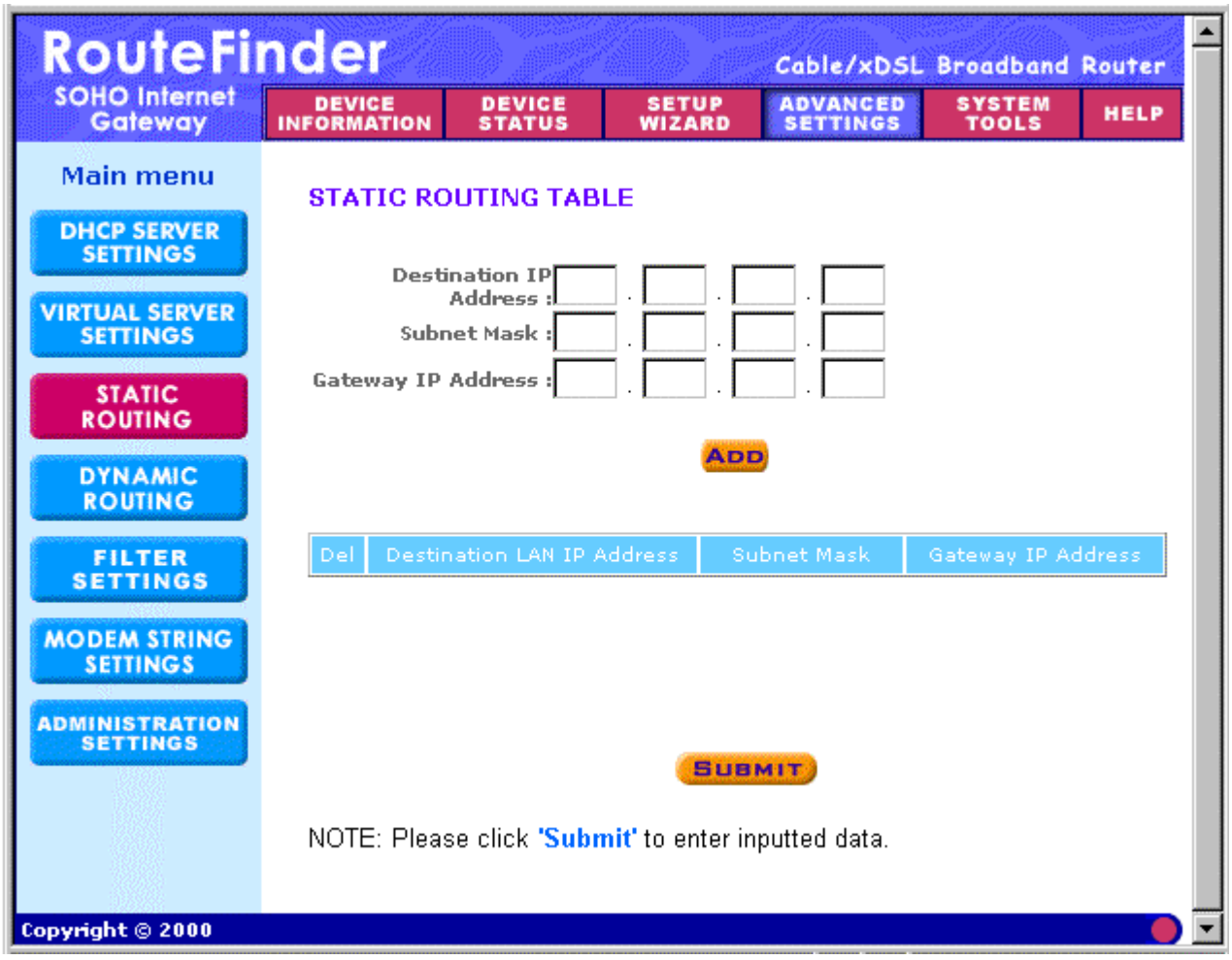
1. To access this screen, click the **Static Routing** button on the left side of the screen. The **Static Routing Table** screen displays.
2. Enter the details for each entry in the routing table. Click the **Add** button after each entry.

   Destination IP Address – The address of the remote network to which you want to assign a static route.

   Subnet Mask – The Subnet Mask of your network IP address.

   Gateway IP Address – The IP address of the interface used to link to the remote network.

   The entries display on the lower half of the screen. To change an entry, click the Delete **(Del)** button, and then re-enter the information.
3. When the table is complete, click the **Submit** button.



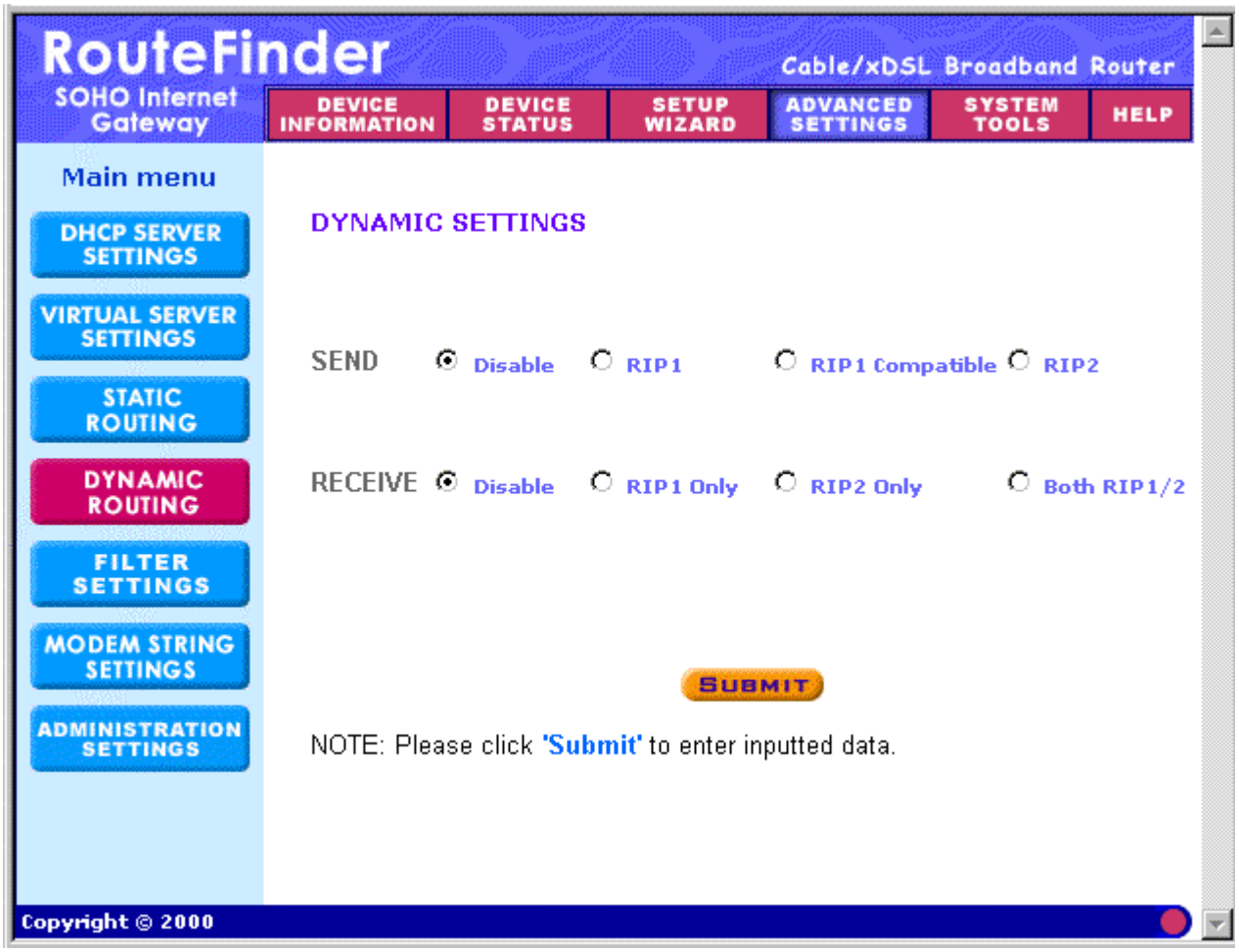
ADVANCED SETTINGS – Dynamic Routing

Dynamic Routing is disabled when Static Routing is used. You will have to disable Static Routing in order to choose one of the dynamic routing protocols. The Dynamic Routing protocol adjusts automatically to the changes in the network topology or traffic.

1. To access this screen, click the **Dynamic Routing** button on the left side of the screen. The **Dynamic Settings** screen displays.
2. Click the radio buttons for the **Send** and **Receive** settings desired. To change these settings before submitting them, simply re-check the desired ones.

   Send – Choose the protocol you want to use to **transmit** the network data. The recommended setting is **Disable**.

   Receive – Choose the protocol you want the RF500S to **receive** network data. The recommended setting is **Disable**.
3. Click the **Submit** button to accept these settings.



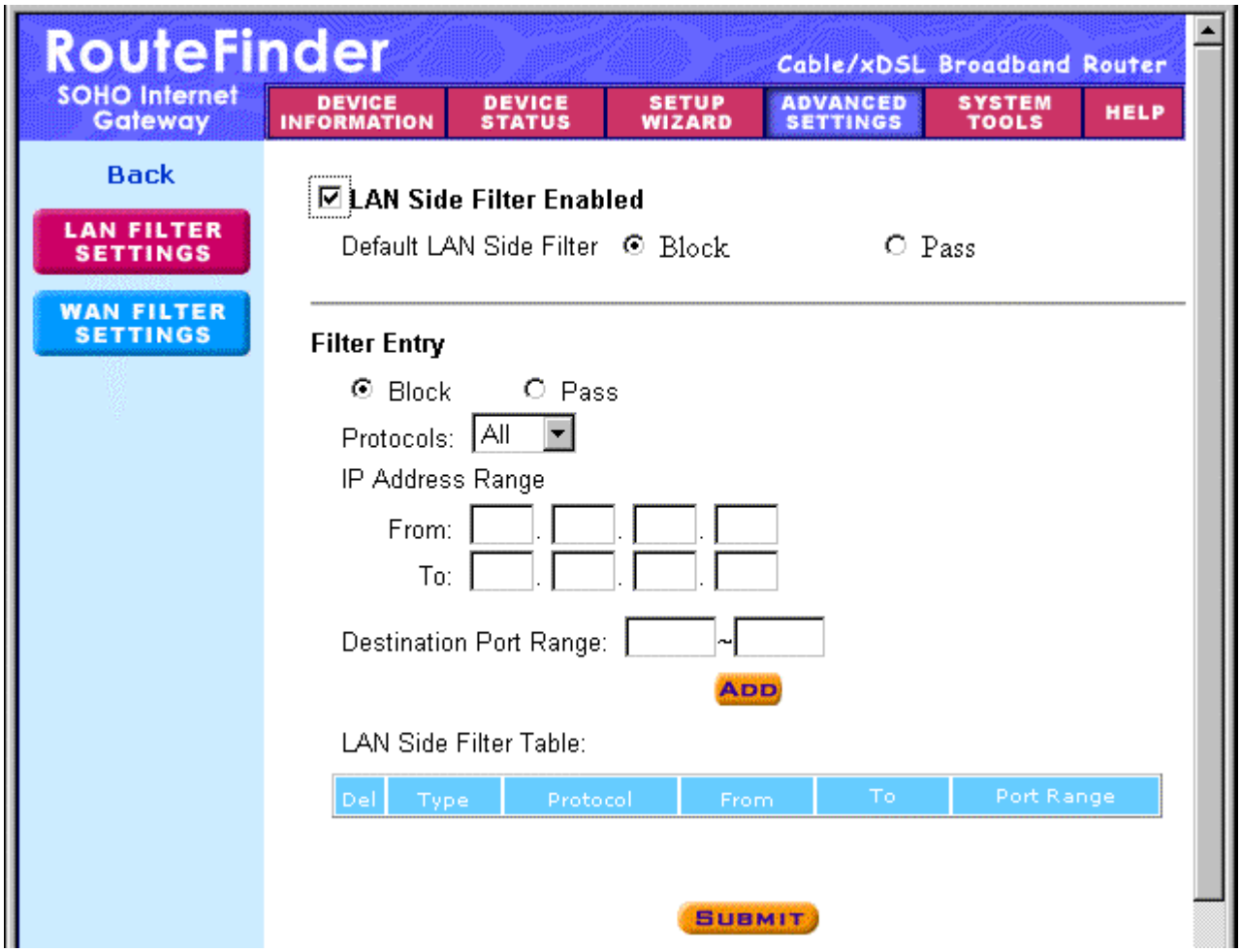
ADVANCED SETTINGS – Filter Settings

The **LAN Filter Settings** function allows the network administrator to define whether local users have the permission to access the Internet.

1. To access this screen, click the **Filter Settings** button on the left side of the **Advanced Settings** screen.
2. Check the **LAN Side Filter Enabled** box to begin a list of users and permissions.
3. Select the LAN side filter: **Block** or **Pass**.
4. Select the client filter settings: **Block** or **Pass**.
5. Select the protocol to be used from the **Protocol** drop-down list box.
6. Enter the client **IP Address Range** and **Destination Port Range**.
7. Click the **Add** button. The entry displays on the lower part of the screen.
8. Continue adding table entries. When complete, click the **Submit** button.

Example - To prevent the local users in IP address range 101 to 200 from accessing port 80 (HTTP), set up the following parameters:

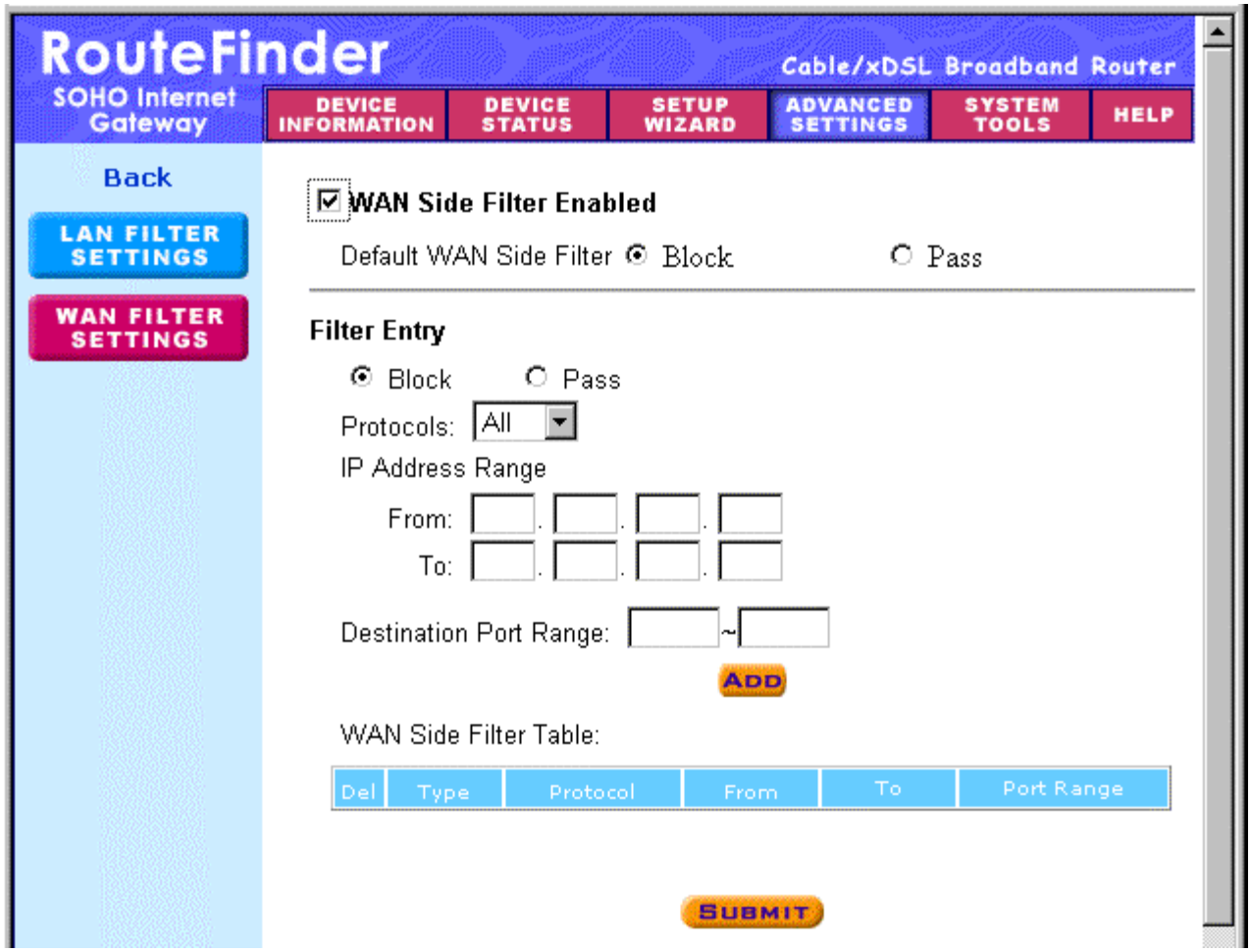
LAN Side Filter Enabled: **Enabled**	Protocol: **TCP**
Default LAN Side Filter: **Pass**	IP Address Range: **101 - 200**
Filter: **Block**	Destination Port Range: **80 - 80 (HTTP)**



ADVANCED SETTINGS – WAN Filter Settings

The **WAN Filter Settings** function allows the network administrator to define whether remote/outside users have the permission to access the local network. To activate, check the **WAN Side Filter Enabled** box. Then define the policy.

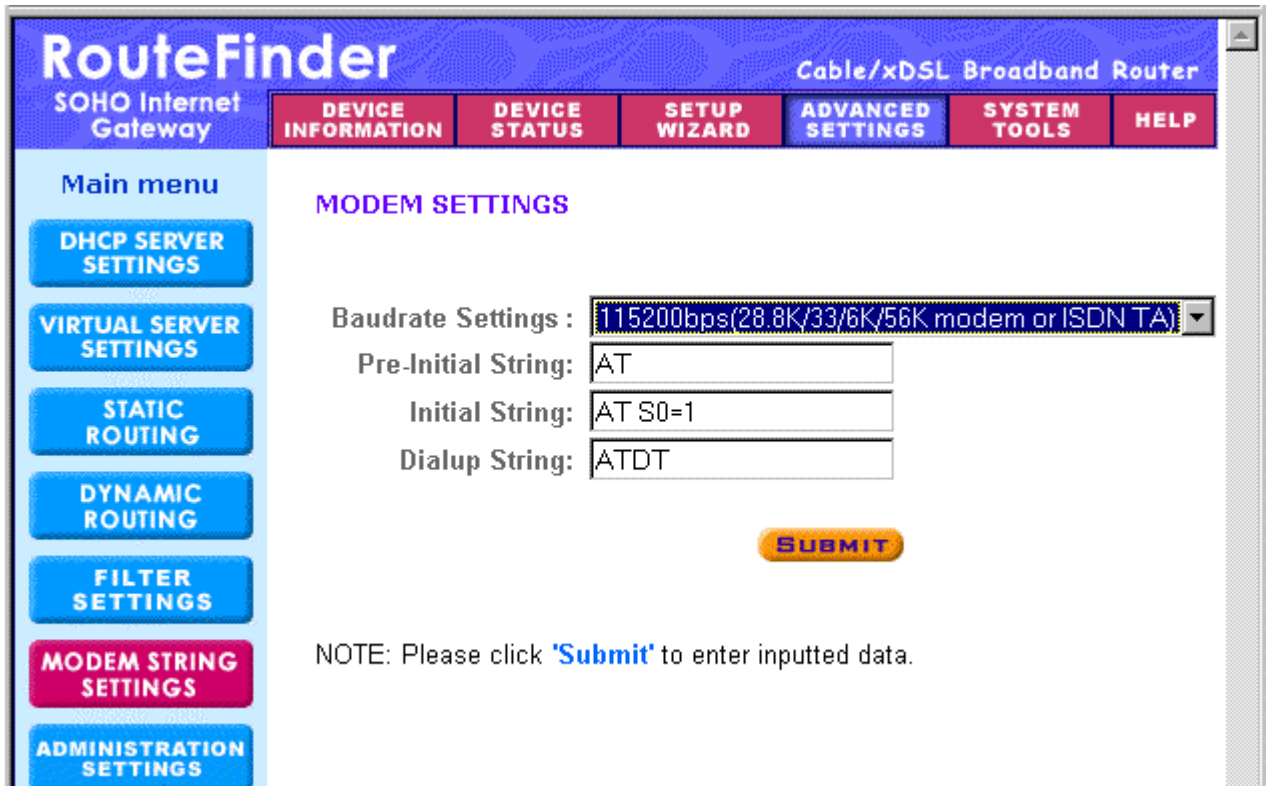
1. To access this screen, click the **Filter Settings** button on the left side of the **Advanced Settings** screen. Then click the **WAN Filter Settings** button on the left side of the screen. The **WAN Filter Settings** screen displays.
2. Check the **WAN Side Filter Enabled** box to begin a list of users and permissions.
3. Select the WAN side filter: **Block** or **Pass**.
4. Select the client filter settings: **Block** or **Pass**.
5. Select the protocol to be used from the **Protocol** drop-down list box.
6. Enter the client **IP Address Range** and **Destination Port Range**.
7. Click the **Add** button. The entry displays on the lower part of the screen.
8. Continue adding table entries. When complete, click the **Submit** button.



ADVANCED SETTINGS – Modem String Settings

Use the **Modem String Settings** screen to establish settings for your modem and to set the baud rate.

1. To access this screen, click the **Modem String Settings** button on the left side of the **Advanced Settings** screen. The **Modem Settings** screen displays.
2. Select the baud rate from the drop-down list box. If you want to change the baud rate, check the initial string. Refer to the manual that accompanied your modem or TA.
3. Enter the Pre-Initial, Initial, and Dialup Strings.
4. When finished, click the **Submit** button to accept these settings.



ADVANCED SETTINGS – Administrative Settings

Use this screen to change your RF500S password, set the HTTP port number, set remote user configuration, and establish system log settings.

1. To access this screen, click the **Administrative Settings** button on the left side of the **Advanced Settings** screen.
2. **Password:** To set a new password, type the new one in the **New Password** box and re-type it for verification in the **Retype Password** box. If you do not want to change any other item on this screen, click the **Submit** button to accept the password change.

   Important: It is important to remember your password. If for any reason you lose or forget it, press the small reset button on the back of the RF500S. Hold the reset button until the serial LEDs of the RF500S blink, and then release the reset button. This reset action will re-initialize the settings. However, all configurations, including the password, will be reset. You will have to reconfigure all of your RF500S settings.
3. **System Administration:** The settings in this portion of the screen can be used to give a remote user(s) the ability to configure and administrate the RF500S through the Internet. The default IP address of the remote administration host is **0.0.0.0**. This address means that any remote user can access and manage the RF500S.

   HTTP Port Number: The default value is 80.

   Allow Remote User to Configure the Device Check Box: To give remote users the ability to configure and administrate the RF500S, you have to check this box.

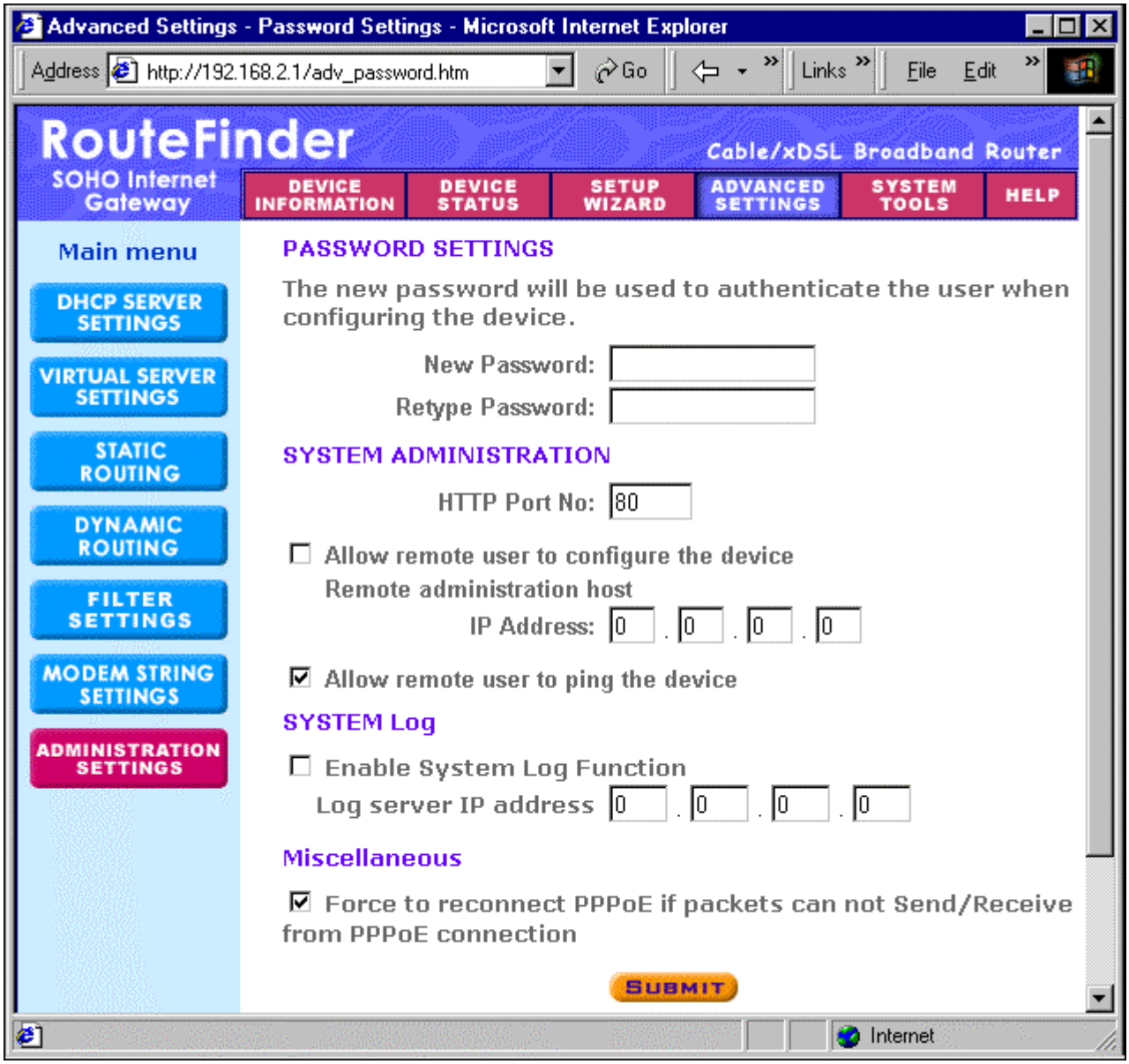
   IP Address: Type the RF500S WAN IP address into the browser of any or a specific PC on the network.

   http://192.168.100.1:1023

   http://<WAN **IP Address>: <Port Number>**

   Important: Once the HTTP port number (**NOT Port 80**) is changed and the users of the LAN terminal want to configure the RF500S, the users have to type the LAN IP address **with** the port number: 192.168.2.3.:1023
4. If you want to allow a remote user to **PING** the device, check the corresponding box. See information about PING in the Appendix D.
5. If you want to enable the system log function, check the corresponding box, and enter the **Log Server IP Address**.
6. If you want enable a **Detail Debug IPSec Log**, check the corresponding box.

7. When you have completed the screen, click the **Submit** button.



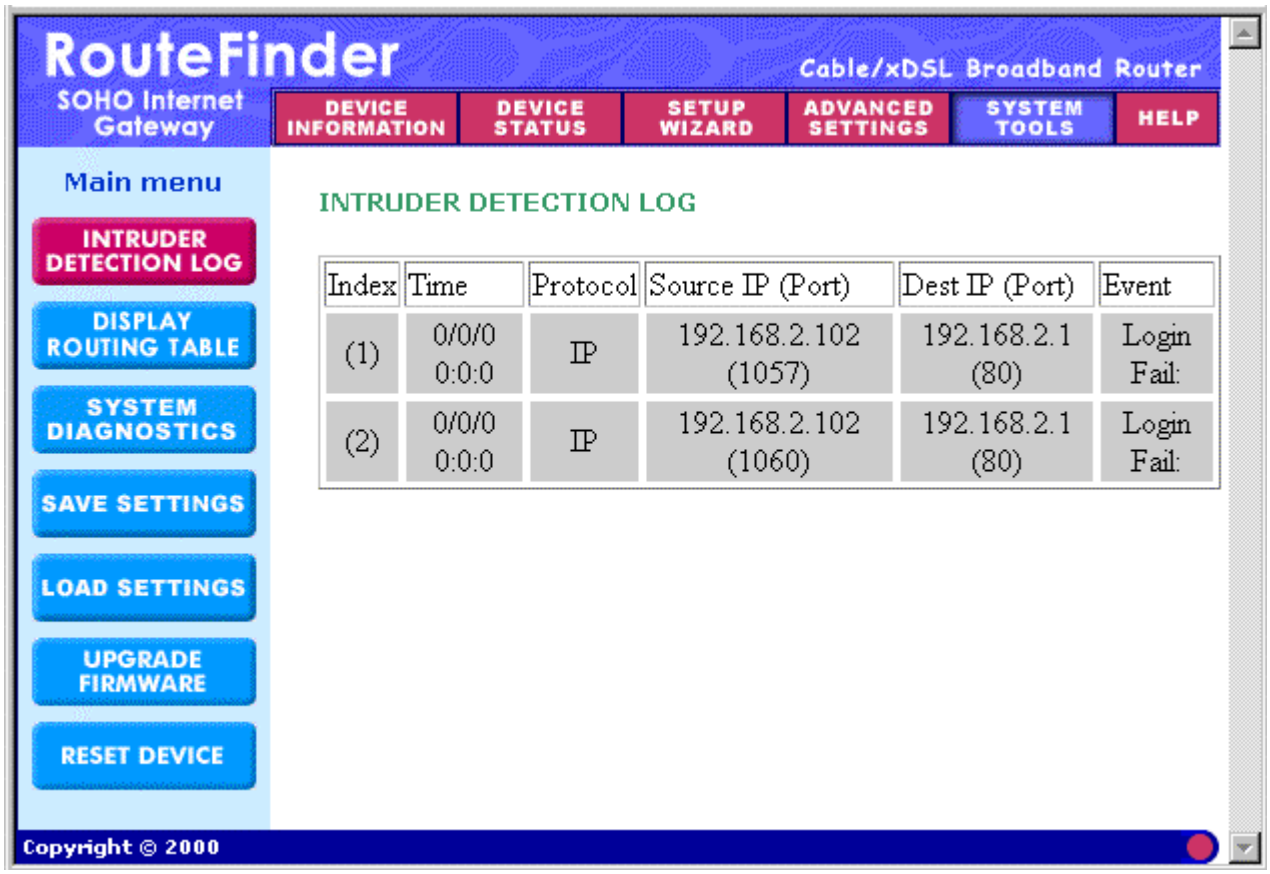
System Tools

Click the **Systems Tools** button on the Main Menu. The **Intruder Detection Log** displays first.

System Tools allow you to view the Intruder Detection Log, the Routing Table, and a System Diagnosis screen. You can also choose to save your settings, load the RF500S default settings, upgrade firmware, and reset the device.

Intruder Detection Log

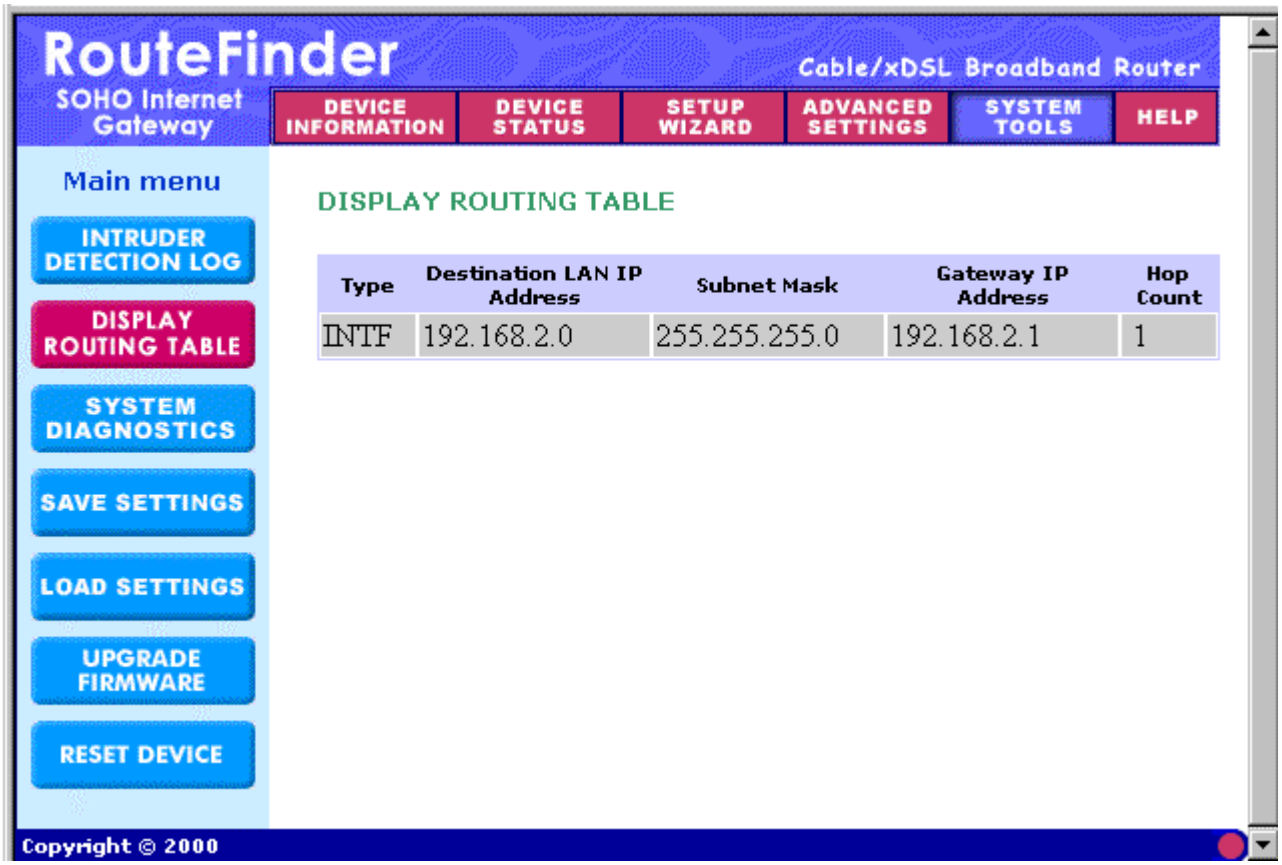
The event messages show the possible hacker attacks that have occurred on your Internet gateway. Up to 32 hacker attacks may be logged in this manner.



SYSTEM TOOLS – Display Routing Table

This table shows the current routing configuration that you setup on the Routing Table screen.

1. To access this screen, click the **Display Routing Table** button from the **System Tools** screen. The **Display Routing Table** screen displays.
2. To exit this screen, select another button on the left side of the screen.



SYSTEM TOOLS – System Diagnosis

When selected, the **System Diagnosis** function performs a check-up on your RF500S to make sure that everything is functioning properly.

SYSTEM TOOLS – Saving Your Settings to a File

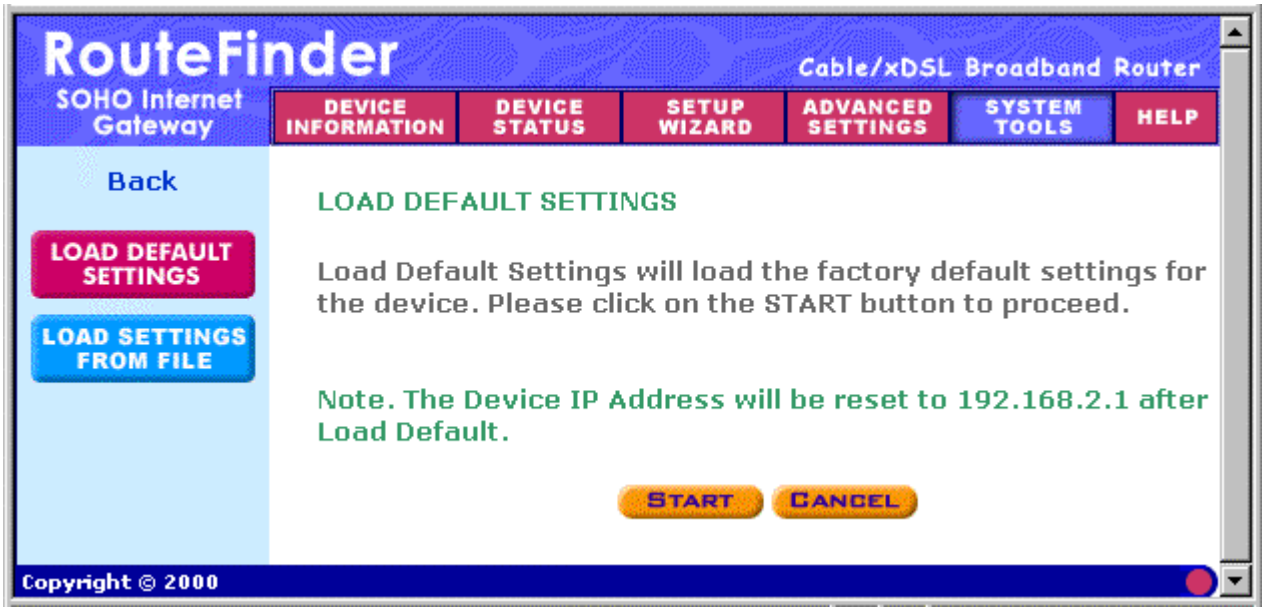
Use this screen to save your configuration settings to a file. This will provide a backup of your settings in case, for some reason, you have to reset your RF500S.

1. Click the **Save File** button in the middle of the screen.
2. Then click **Save This File to Disk** in the browsing wizard.

SYSTEM TOOLS – Load Default Settings

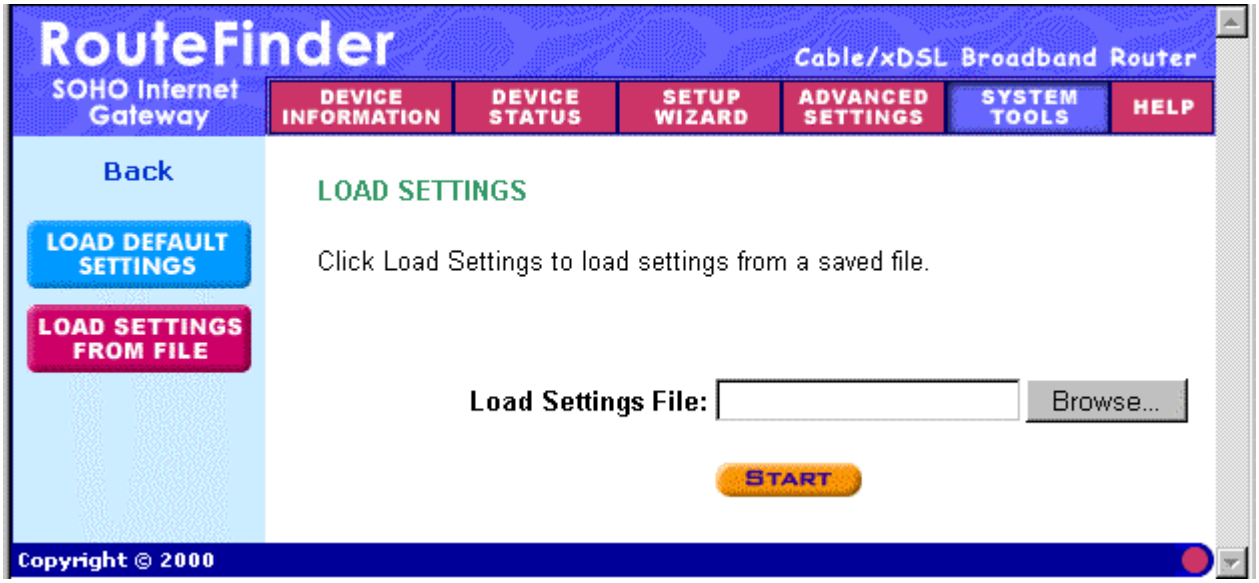
Use this screen to load the original RF500S factory defaults.

1. To access this screen, click the **Load Default Settings** button from the **System Tools** screen. The **Load Default Settings** screen displays.
2. Click the **Start** button to load the default settings.



SYSTEM TOOLS – Load Settings from a File

1. To load settings from a file, click the **Load Settings From File** button. The screen displays.
2. Select the browse button to locate the file.
3. When the file is located, click the **Start** button.



SYSTEM TOOLS – Upgrade Firmware

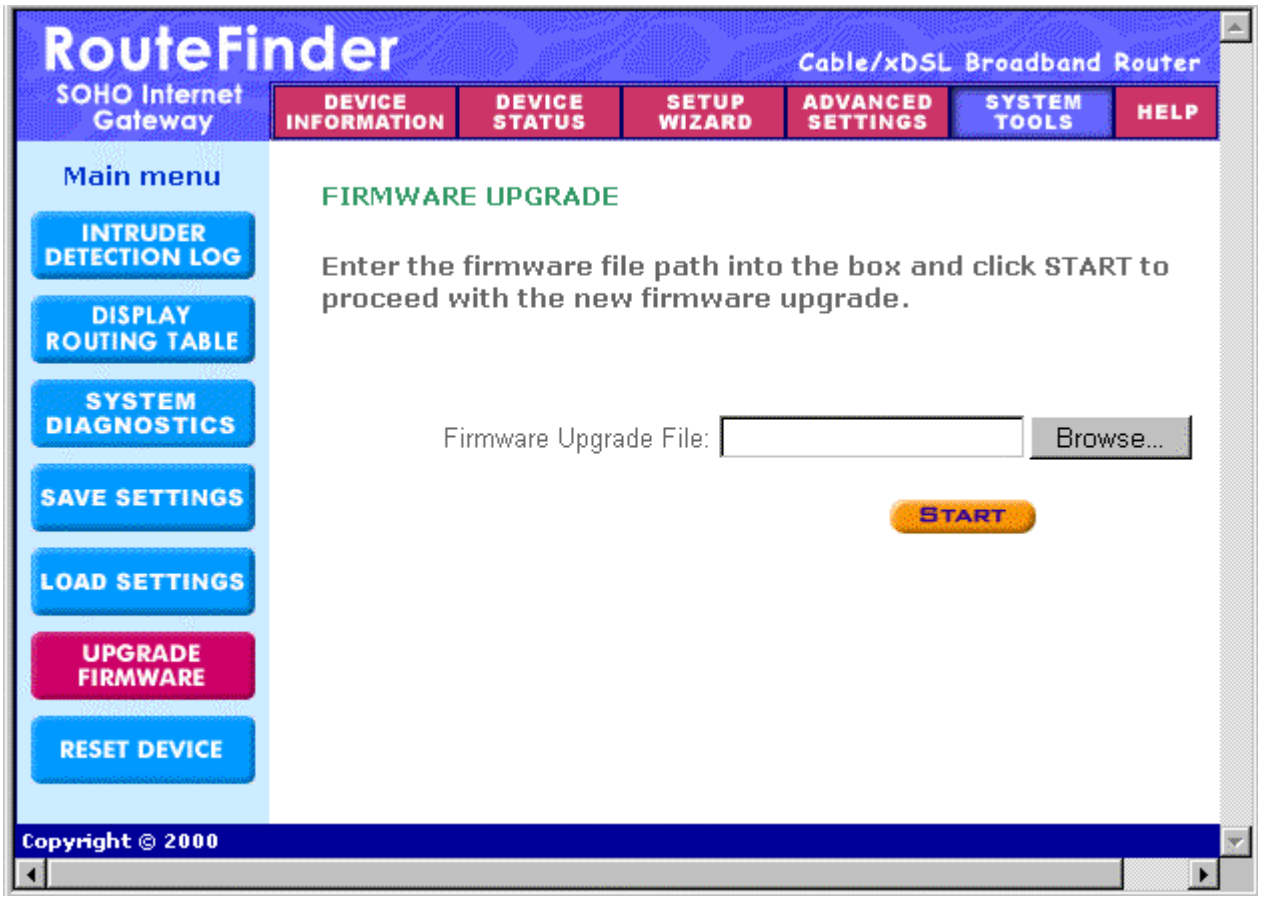
The **Upgrade Firmware** option allows you to upgrade the newest firmware to your RF500S.

How will I be notified of new router firmware upgrades?

All Multi-Tech firmware upgrades are posted on the Multi-Tech Web site at www.multitech.com, where they can be downloaded for free.

Your RouterFinder does NOT need the latest firmware upgrade if your Internet connection is already successful, as firmware upgrades will not increase your connection speed or enhance your Router's performance.

1. To access this screen, click the **Upgrade Firmware** button from the **System Tools** screen. The **Upgrade Firmware** screen displays.
2. Use the browse button to locate the file.
3. Click the **Start** button.
4. To exit this screen, select another option or return to the Main Menu.



SYSTEM TOOLS – Reset Device

Resetting the device will restart it.

1. To access this screen, click the **Reset Device** button from the **System Tools** screen. The **Reset Device** screen displays.
2. Click on the **Start** button to reset the device. Hold the reset button until the serial LEDs of the RF500S blink, and then release the reset button.

RouteFinder™

Chapter 4

Software Installation and Configuration

MultiTech® Systems

Chapter 4 - Software Installation and Configuration

Software Description

The RouteFinder software includes the RouteFinder Setup Wizard, the RouteFinder Manager, and the RouteFinder Monitor.

RouteFinder Setup Wizard
The RouteFinder Setup Wizard provides a step-by-step process to assist you in entering all the basic settings needed to configure your RF500S for general use. All settings that are entered in the Setup Wizard can be found in their respective menus in the RouteFinder Manager.

RouteFinder Manager
RouteFinder Manager is the main program used to configure all settings for your RF500S. Complete information about options within the RouteFinder Manager can be found in the RouteFinder Manager chapter in this User Guide.

RouteFinder Monitor
RouteFinder Monitor is a multi-purpose utility designed to let you know the status of your RF500S connection. The monitor offers the ability to point and click on an event to access troubleshooting procedures. Refer to the RouteFinder Monitor chapter in this User Guide for more information.

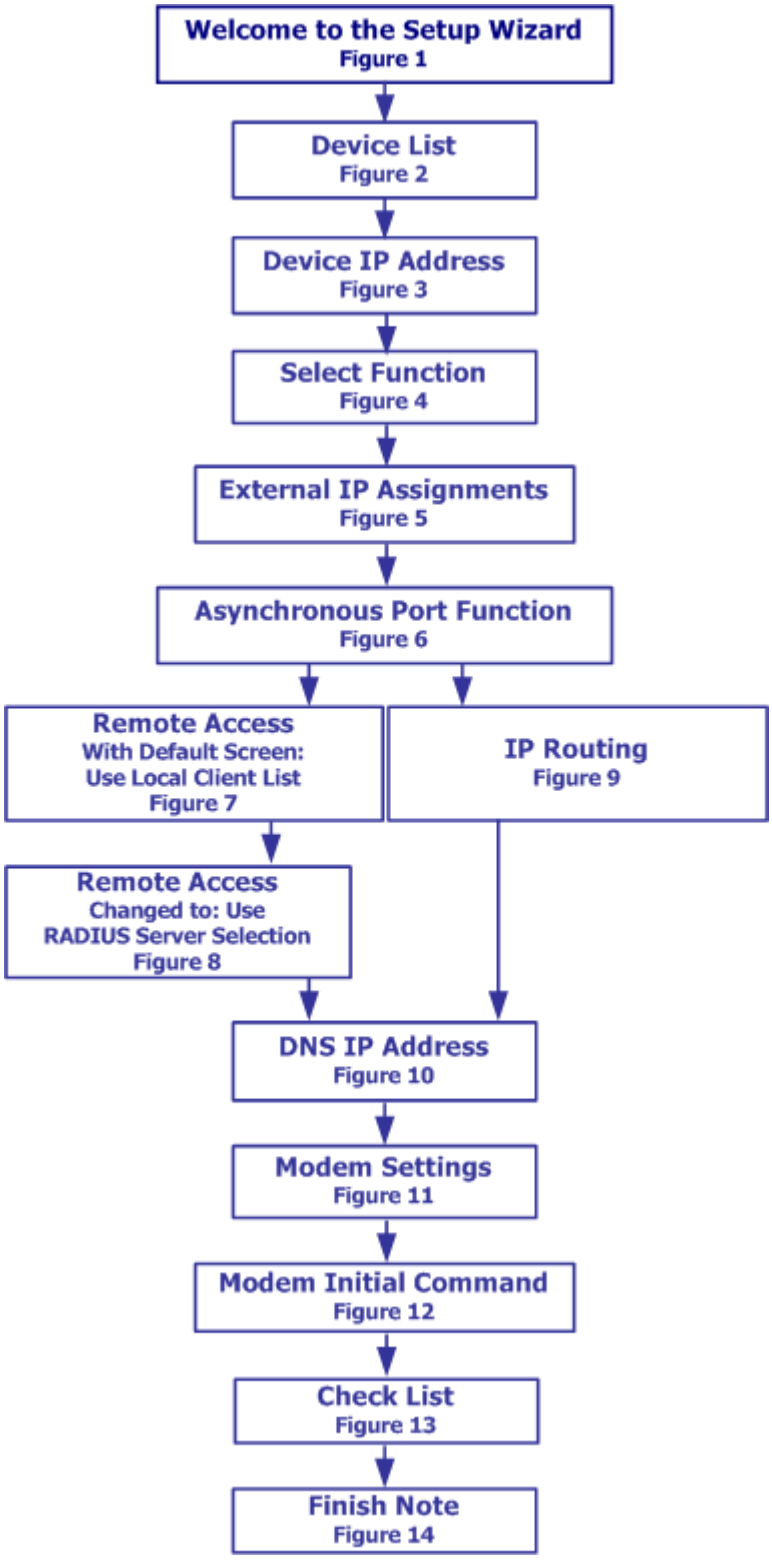
Software Installation Steps

1. Insert the RF500S System CD into your computer's CD-ROM drive. The RF500S System CD screen appears.

   Note: If Autorun is disabled on your computer, use Windows Explorer to view the contents of the CD. **Double-click** the CD icon to display the RF500S System CD main screen.

2. Click **Install Software**.
3. Follow the on-screen instructions to install the software.
4. When the software installation completes, the **Setup Wizard** screen displays.

RouteFinder Wizard Screen Flow



Using the RouteFinder Setup Wizard

Notes:

Before beginning this procedure, ensure that your RF500S is properly connected to the network and is powered on.

Before running the Setup Wizard, it is strongly recommended that you exit all Windows programs.

After the software is installed, you may return to this RouteFinder Setup Wizard at any time, by clicking **Start** | **Programs** | **RouteFinder Manager** | **RouteFinder Wizard**.

Figure 1 – Welcome to the Setup Wizard

1. Click OK to move to the next screen.

2. **The Device List screen displays. The Setup Wizard automatically checks your network for available network devices and displays them on the screen.**

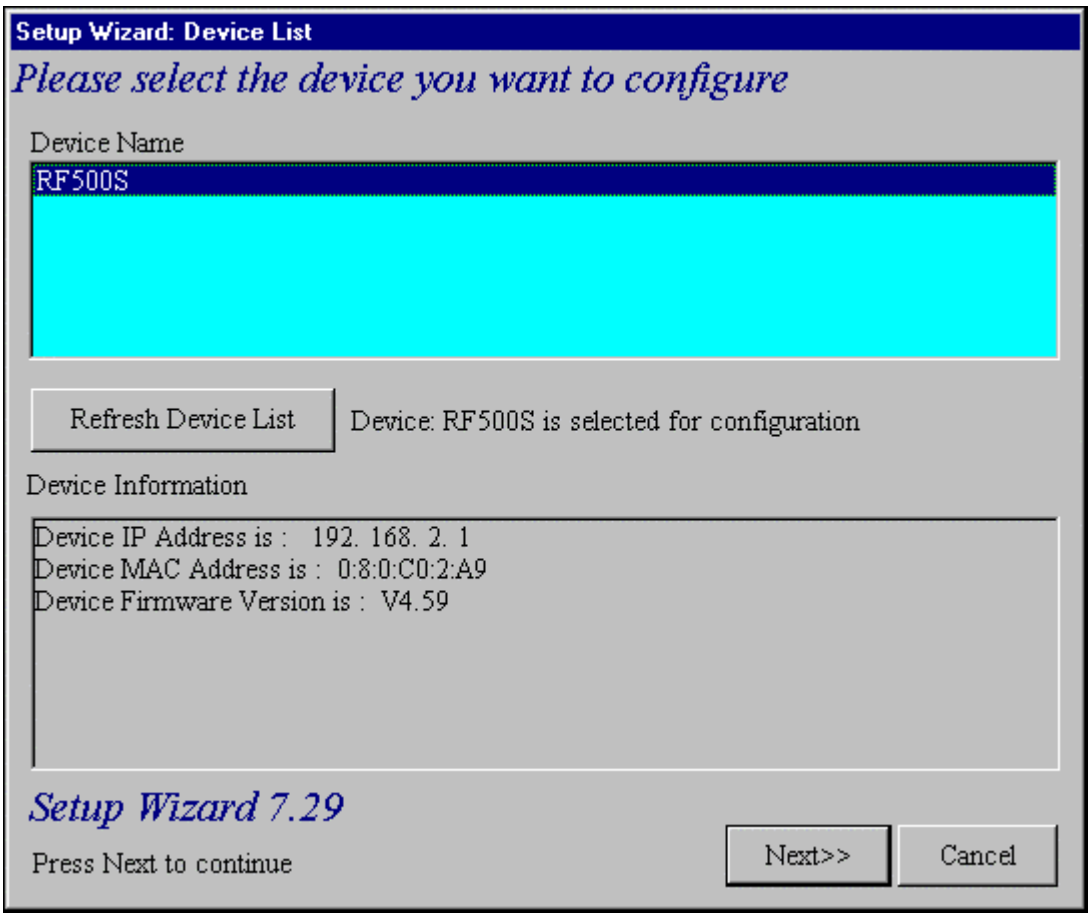


Figure 2 – Device List

Select the device you wish to configure from the **Device Name** list.

Record the values presented in the **Device Information** panel for later reference.

Device IP Address _____

Device MAC Address _____

Device Firmware Version _____

Click **Next>>**.

Note: If a message appears indicating the device is not found, or you do not see the device you are attempting to configure listed, click the **Refresh Device List** button.

3. The Device IP Address screen displays.

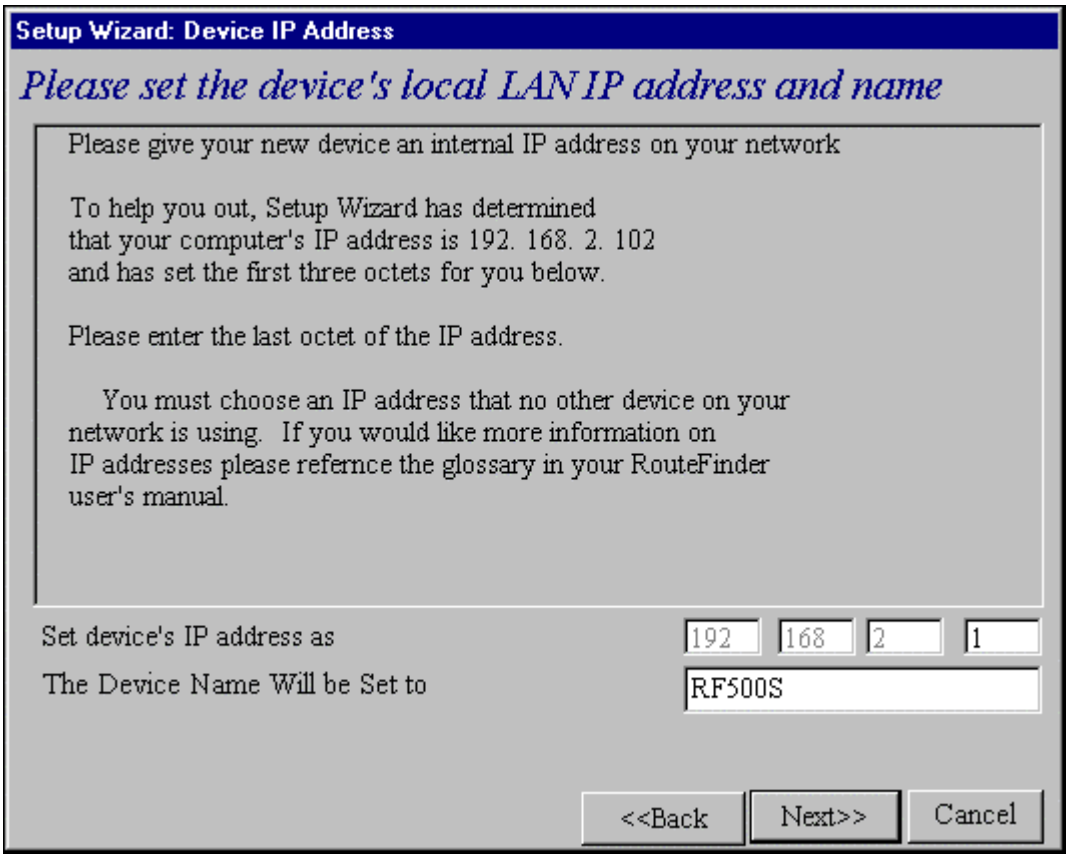


Figure 3 – Device IP Address

- Enter your local internal network's IP address for this device.

  The Setup Wizard will automatically detect the first three octets of your local IP address. You must enter the last octet only.

- If you wish, you can change the network name of your RouteFinder. If your ISP requires your device to have a name, you may use the value entered in this field.

- Click **Next>>** to continue. The device will search the network to ensure that the IP address is valid. This may take several seconds.

Note: If your ISP provided you with an IP address, **do not** enter that address in this field. Enter the IP address for this device on your local network. Refer to the Glossary in this User Guide for additional information on IP addressing.

4. The Select Function screen displays.

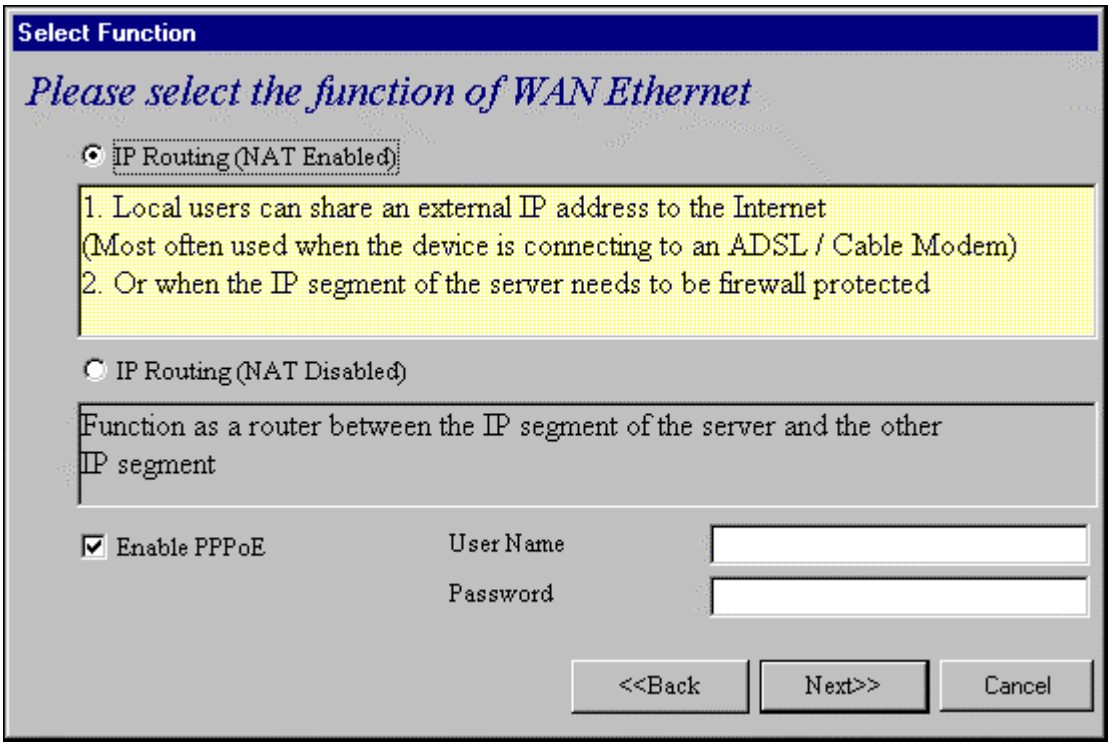


Figure 4 – Select Function

Select the function of the WAN Ethernet port by choosing **IP Routing (NAT Enabled)** or **IP Routing (NAT Disabled)**. If you are using NAT Enabled, you may also select **Enable PPPoE**.

- Select **IP Routing (NAT Enabled)** to allow local LAN clients to share one external IP address for accessing the Internet. This option is most often used when the RF500S is connected to a DSL or cable modem, or when the IP segment of the server needs firewall protection.

- Select **IP Routing (NAT Disabled)** to allow the RF500S to function as a router between IP segments. This option is ideal for organizations needing to segment workgroups.

- Select **Enable PPPoE** to use the RF500S with a time-base, rather than fixed-cost DSL modem connection. Enter the User Name and Password provided by your ISP. This option is most often used when connecting via DSL to the Internet.

  Note: Enable PPPoE is valid only when IP Routing (NAT Enabled) is selected.

  Click **Next>>**.

5. **The External IP Assignment screen displays.**

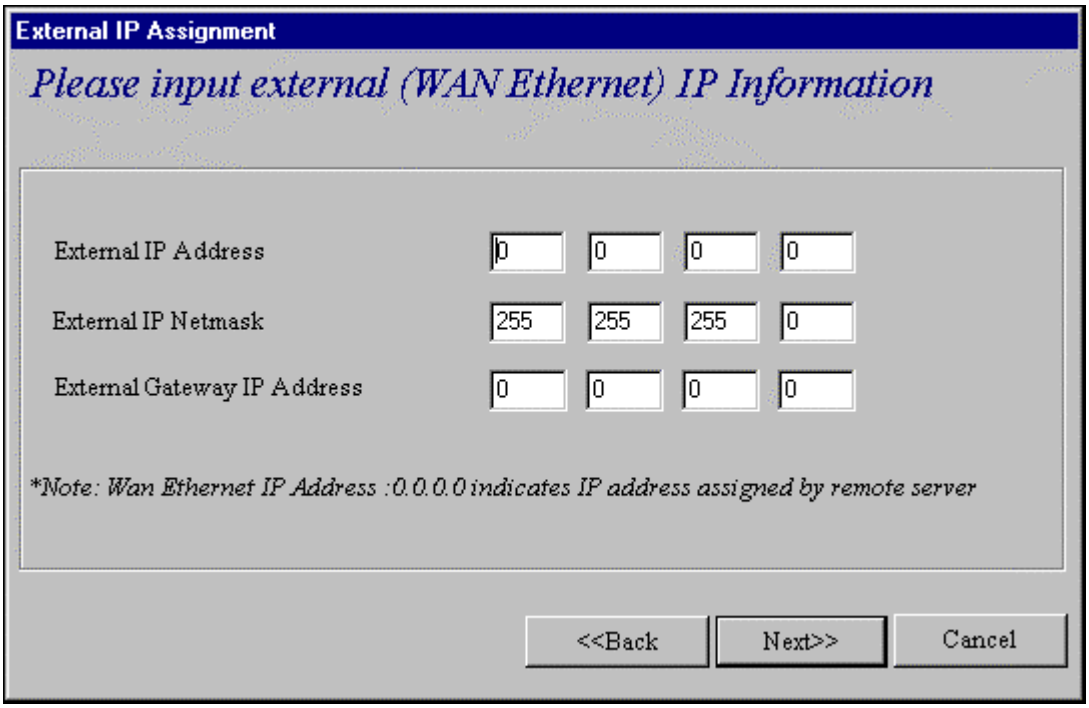


Figure 5 – External IP Assignments

Enter the WAN Ethernet IP address information **provided by your ISP** or other external network administrator.

- In the **External IP Address** box, enter the WAN Ethernet IP Address.
- In the **External IP Netmask** box, enter the Netmask of the WAN Ethernet IP Segment (for Class C networks, the Netmask is generally set to 255.255.255.0).
- In the **External Gateway IP Address** box, enter the IP address of the Gateway to the destination network.

Note: If your ISP uses dynamic IP addressing (DHCP), leave the External IP address and the External Gateway IP address at the default values of 0.0.0.0. Set the External IP Netmask to the default value of 255.255.255.0.

Click **Next>>**.

6. **The Asynchronous Port Function screen displays. Select Remote Access, IP Routing(NAT Enabled) or IP Routing (NAT Disabled).**

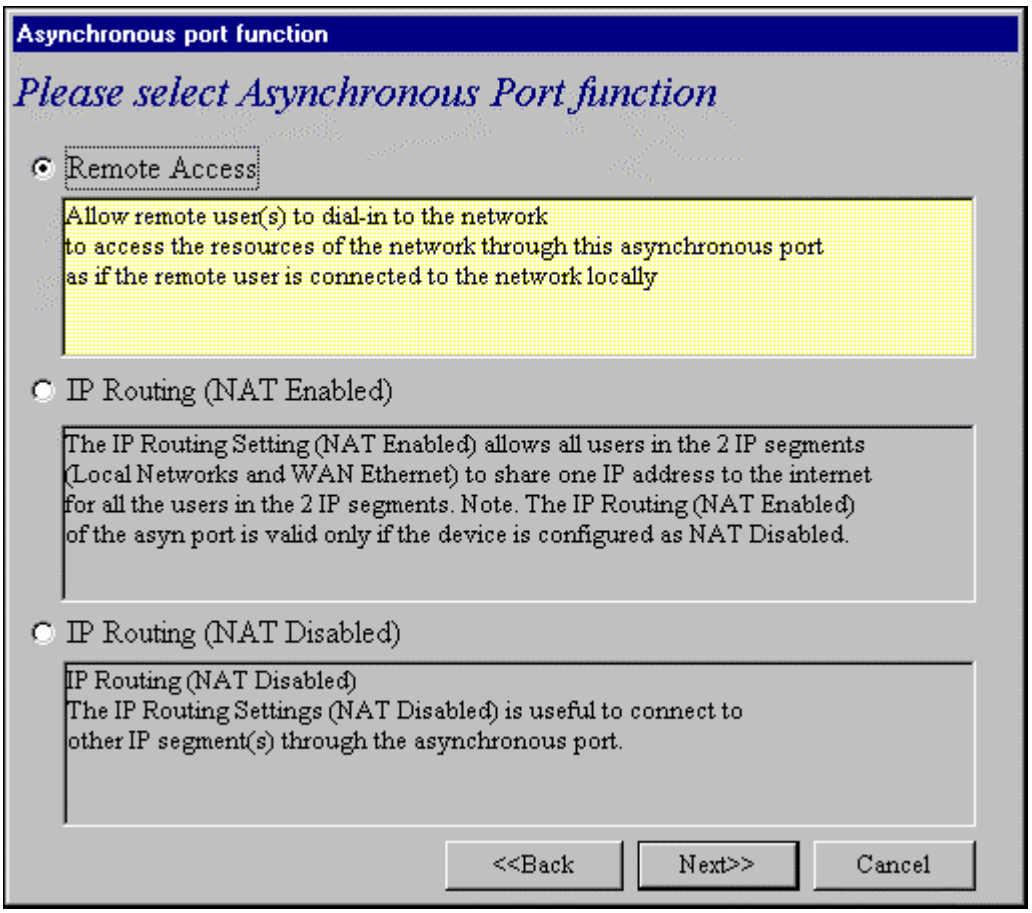


Figure 6 – Asynchronous Port Function

- Select **Remote Access** to allow remote users to dial-in to the network to access resources as if the remote user is connected to the network locally. Continue with the **Remote Access** instructions.

- Select **IP Routing (NAT Enabled)** to allow all users in the two IP segments (LAN and WAN Ethernet) to share one IP address to the Internet. You may also select this option to use the serial async port for dial backup in the event the DSL or cable modem becomes unavailable.

- Select **IP Routing (NAT Disabled)** to connect other IP segments through the serial async port.

Note: The IP Routing (NAT Enabled) feature of the serial async port is valid only if the WAN port is configured as NAT Disabled.

Click **Next>>**.

7a. If you selected Remote Access Selection from the Asynchronous Port Function screen, the Remote Access screen displays.

You must define the location of your remote user account database by selecting **Use Local Client List** or **Use RADIUS Server**.

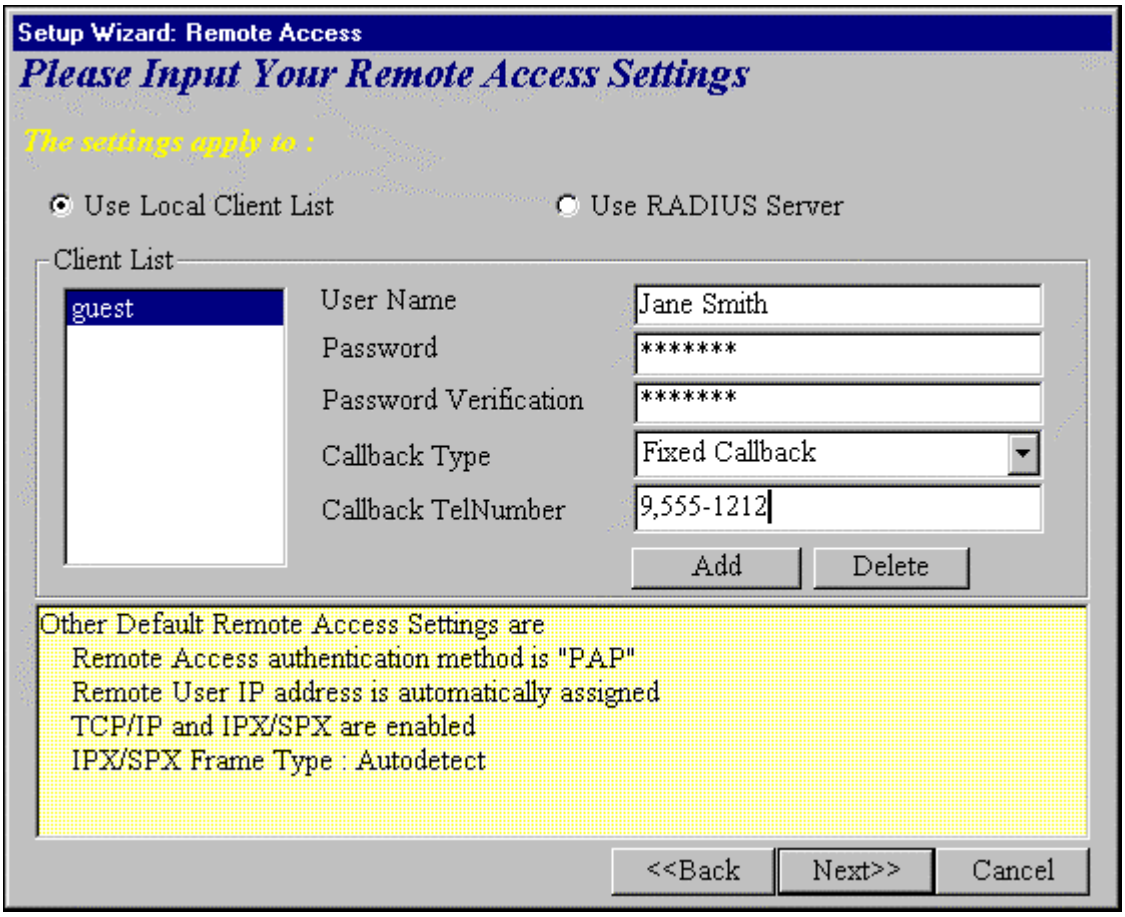


Figure 7 – Remote Access with Default Screen: Use Local Client List

Use Local Client List

Note: The Local Client List allows you to add a maximum of 64 users.

The Local Client List is an authentication database of user names, passwords and dial-in options for each remote user. Enter the following information for each client:

- **User Name** to authenticate the remote dial-in user.
- **Password** to authenticate the remote dial-in user. Passwords are limited to 16 characters.
- Re-enter the remote dial-in user's password for **Verification**.
- Select one of the following three Callback Types for each remote client:
  - **No Callback:** This option allows the remote user to immediately connect to the network after being authenticated. **No Callback** is the default.
  - **Fixed Callback:** This option allows you to specify a fixed callback telephone number for the user. After the PPP negotiation, the device will disconnect, and then callback the telephone number you entered in the callback

telephone number field. This option is best used for clients requiring callback security while dialing-in from the same location each time.

- **Variable Callback:** This option is for remote users who travel or dial-in from various locations and need callback security. It allows clients to specify the callback telephone number each time they connect to the network.

Click **Add** after entering information for each Local Client.

Click **Next>>** and continue with Step 10 when all users have been added.

Use RADIUS Server

Select this option if you would like your remote clients to be authenticated on a RADIUS server.

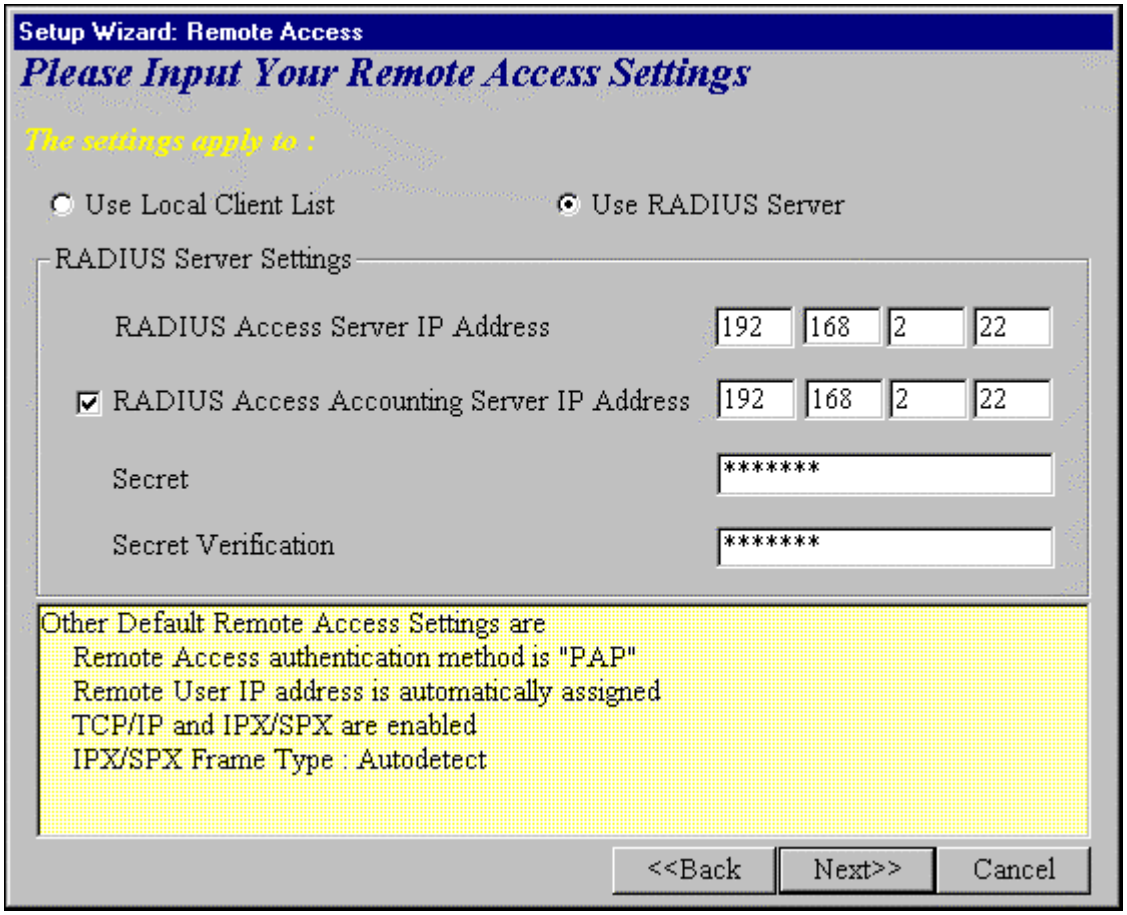


Figure 8 – Remote Access – Changed to: Use RADIUS Server Selection

You must enter the following RADIUS Server Settings:

- Enter the IP address of the **RADIUS Access Server**.
- Enter the IP address of the **RADIUS Accounting Server**.
- Enter your **Secret** RADIUS code or password.
- For **Secret Verification**, re-enter your code or password.

Note: In most cases, the RADIUS Access Server and the RADIUS Accounting Server are the same server, so the IP addresses will also be the same.

Click **Next>>** and continue with Step 8.

7b. If you selected IP Routing (NAT Enabled or Disabled) from the Asynchronous Port Function screen, the IP Routing screen displays.

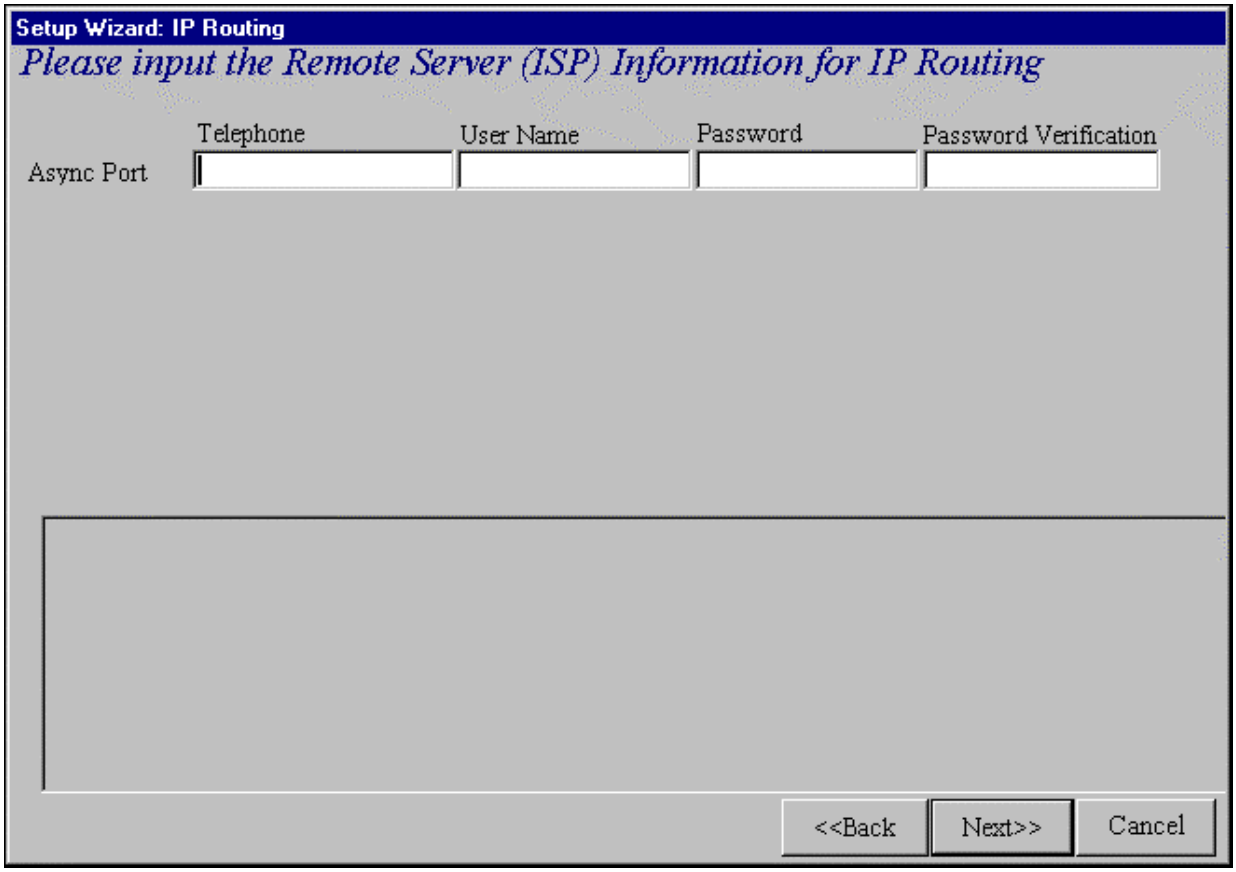


Figure 9 – IP Routing

Enter the information required to dial-up and login to your ISP's remote server:

- Enter the **Telephone** number used to dial your remote server (ISP).

  Note: If you must dial a number to get an outside line (e.g., 9, or 0), enter the required number plus a **w** (wait) or a comma in the **Telephone** box. (e.g., 9w555-2323 or 9,,5552323). Each comma provides a 3-4 second delay.

- Enter the **User Name** for your remote server or ISP account.
- Enter the **Password** for your remote server or ISP account.
- For **Password Verification**, re-enter the password for your remote account.

Click **Next>>**.

8. The DNS IP Address screen displays.

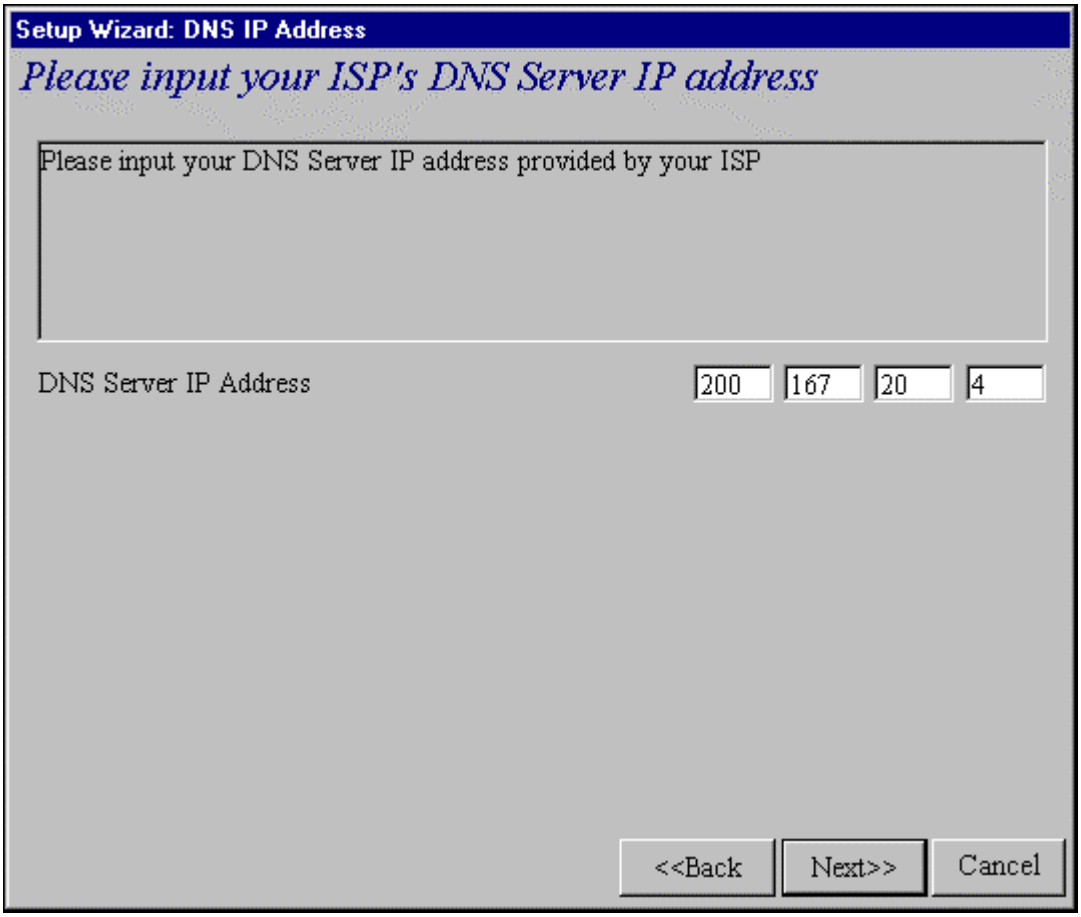


Figure 10 – DNS IP Address

Enter your ISP's DNS Server IP address. If you are not sure of the IP address, contact your ISP. Refer to the Glossary for more information about the DNS Server.

Click **Next>>**.

9. The Modem Settings screen displays.

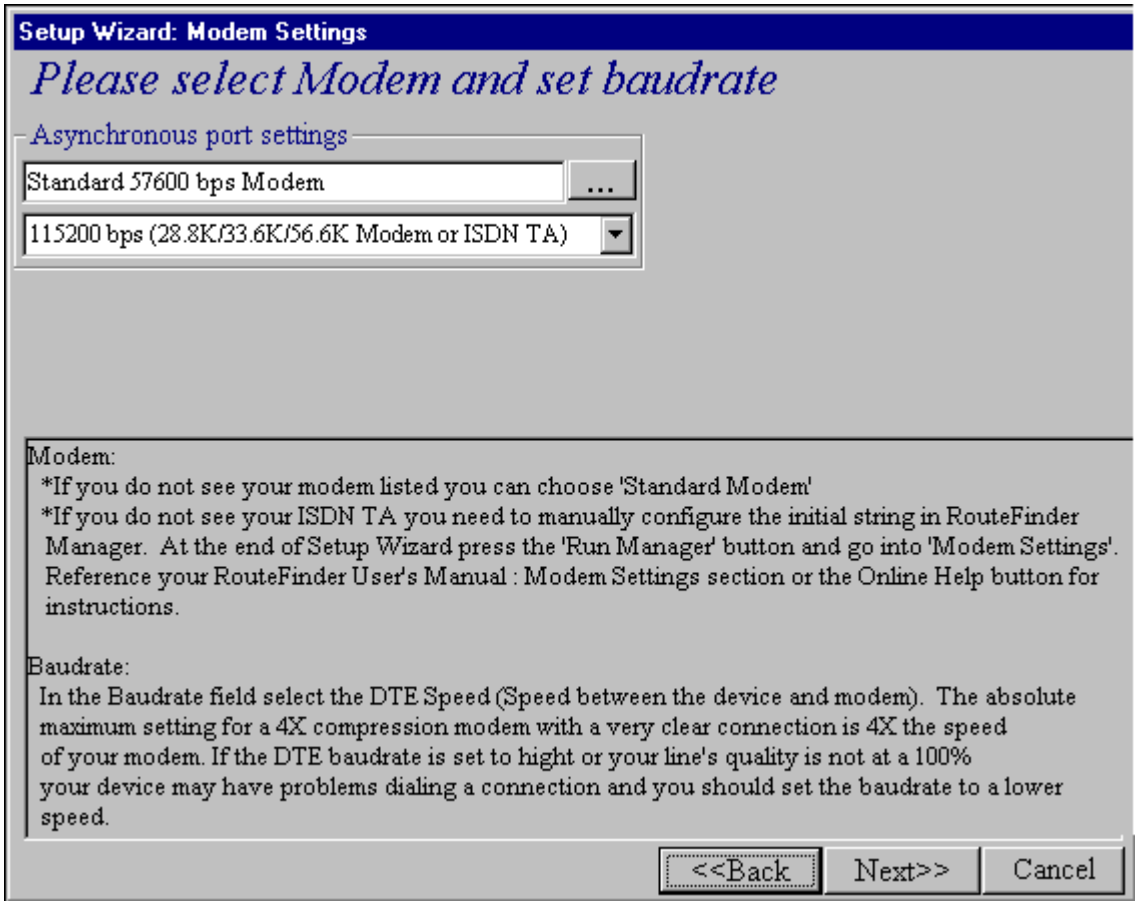


Figure 11 – Modem Settings

Select your **modem** from the **Asynchronous Port Settings** drop-down list box.

The Modem Initial Command screen displays. If you do not have a device attached to the serial async port, use the default modem values.

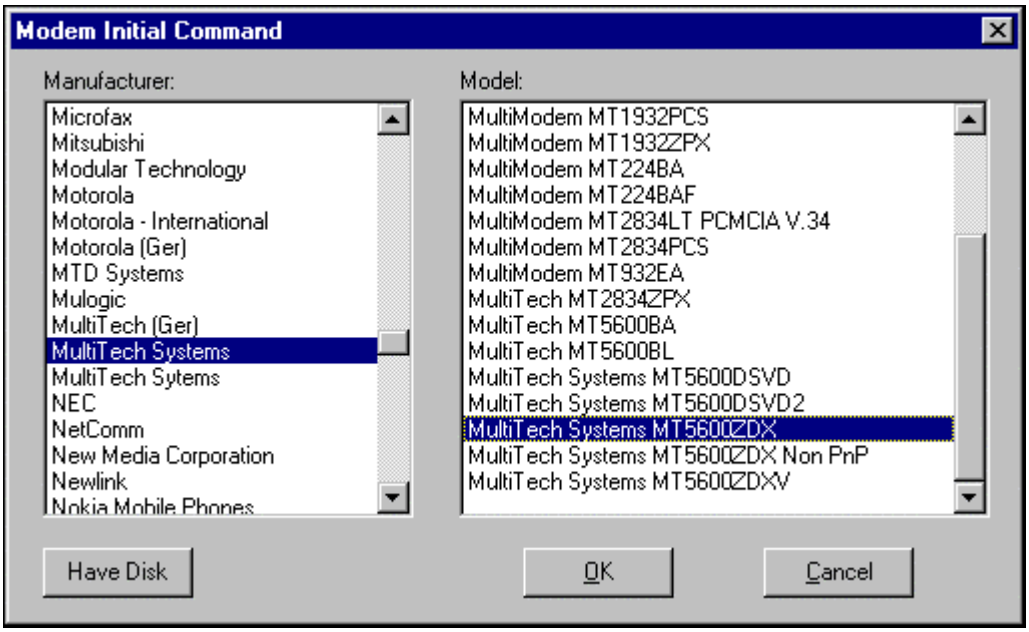


Figure 12 – Modem Initial Command

- Select your modem manufacturer, and then select the model from the list provided. Once chosen, the system loads modem information.
- Click **OK**

Notes:

If your modem is not listed and you have a driver disk, click **Have Disk...** to install your modem.

This setting configures the initial string of the asynchronous port on the RF500S so that it will know how to communicate with your modem.

If you are using an analog modem and your modem is not included in the selection list, in most cases, Standard Modem will work.

If you are using an ISDN TA, refer to the ISDN TA's User Guide for information on the initialization and hang up strings.

Use RouteFinder Manager to enter modem strings.

10. **After the modem is selected, the Modem Setting screen re-displays.**

Select the DTE speed (i.e., the speed of communication between the asynchronous port of the RF500S and the modem) from the drop-down list box. For DCE speed compression modems, this value can normally be set to about 4 times the speed of your modem. Keep in mind that if you set the baud rate too high, the dial-up connection may fail.

Note: You may need to set a lower baud rate since the theoretical maximum connection speed may not be attainable due to variations in quality of phone line and ISP connections.

Click **Next>>** to complete the basic configuration.

11. The Check List screen summarize your configuration selections.

You should read it to make sure that all values have been correctly entered. If you find an incorrect setting, click **<<Back** to return to the screen containing the error and correct it. When complete, use the **Next>>** button to return to this **Check List** screen.

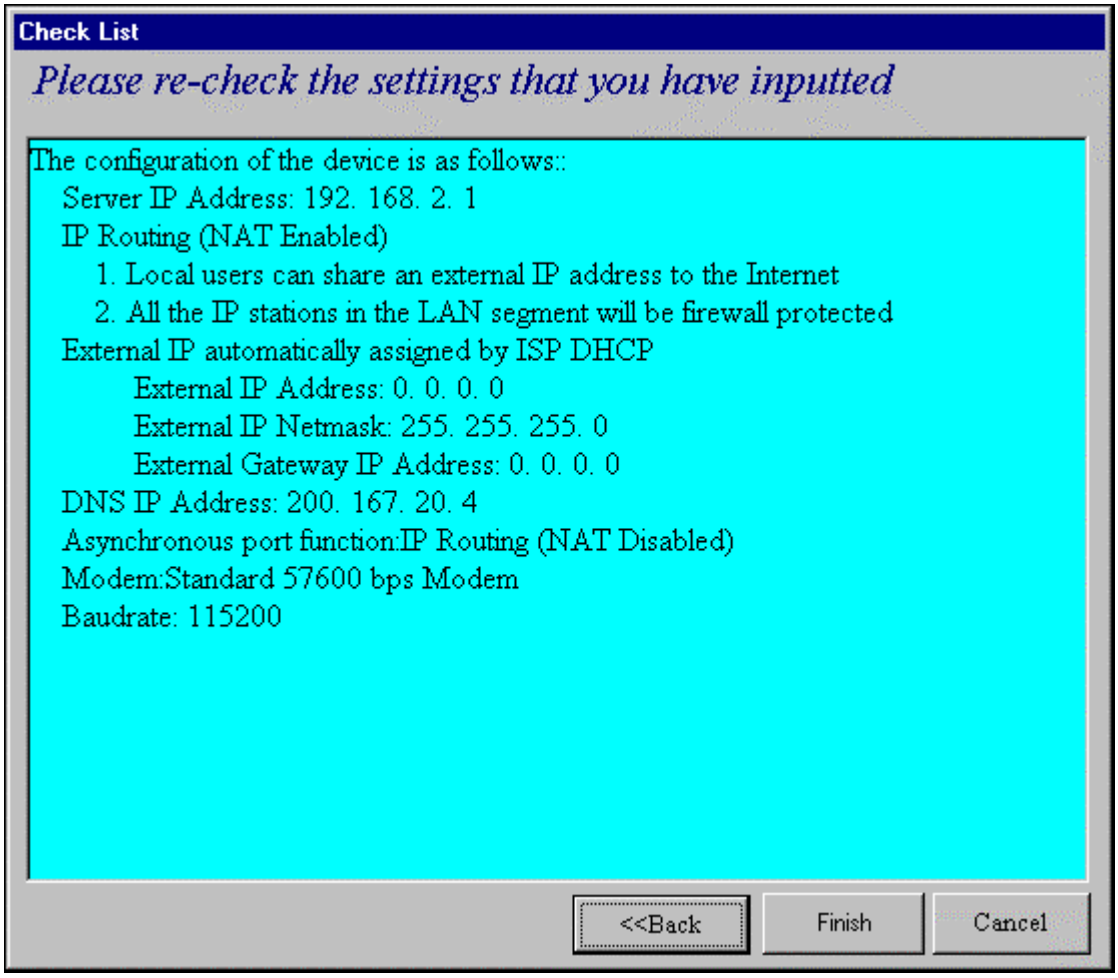


Figure 13 – Check List

Click **Finish** to complete the configuration. The **Note** screen displays indicating that you have completed the Setup Wizard.

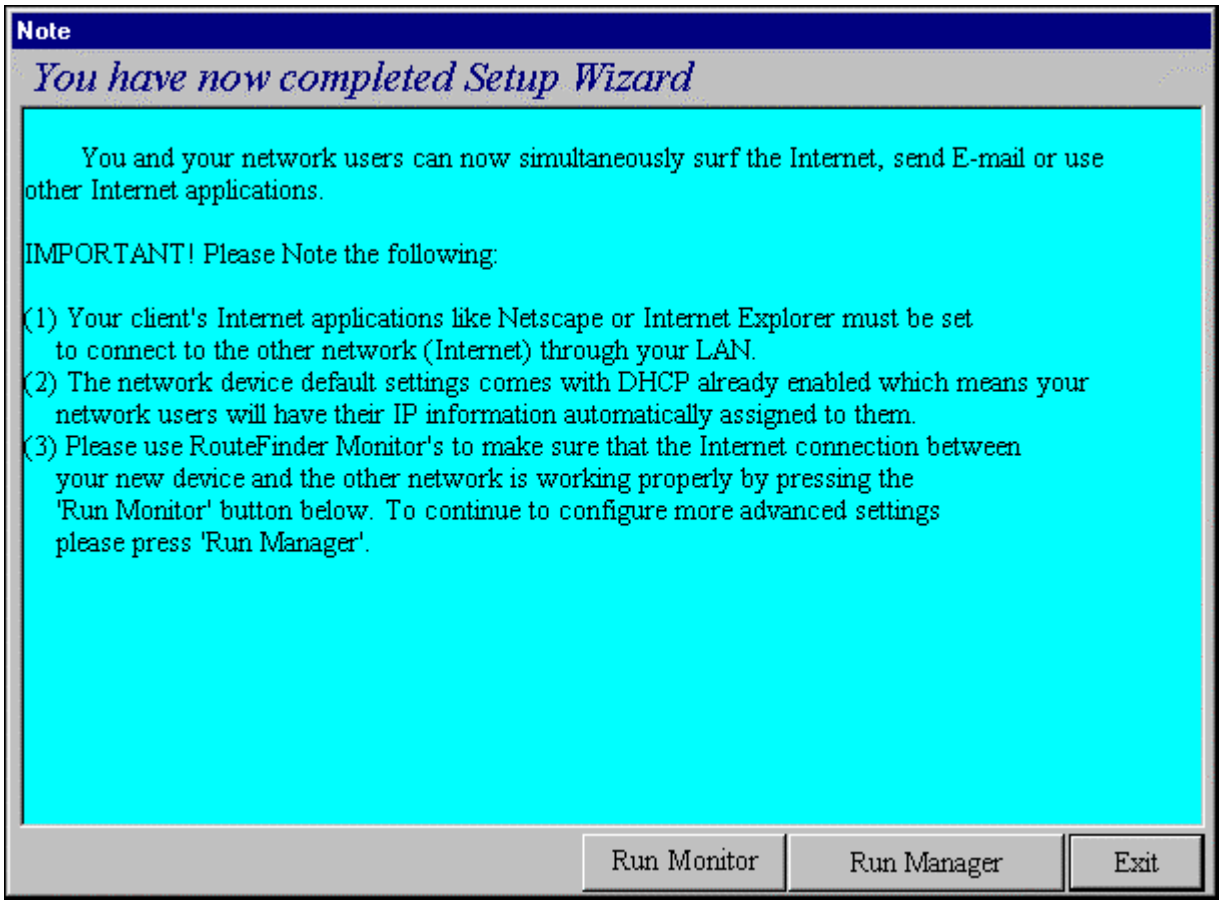


Figure 14 – Finish Note

- Read the **IMPORTANT** information contained in the screen.
- Click the **Run Monitor** button (recommended), or the **Run Manager** or **Exit** buttons.

Testing Your Connection

When you click the **Run Monitor** button, the RouteFinder Monitor program loads.

1. To test your current settings, select **Test Connection**. Select **Connect Port 1** to test the WAN port. Select **Connect Port 2** to test the serial async port. The monitor activity will appear in the display window. Refer to the RouteFinder Monitor chapter in this User Guide for additional information about the monitoring capabilities of the RF500S.
2. After successfully using the Test Connection option in Run Monitor, refer to the LAN Client Settings chapter of this User Guide to continue with your installation by configuring your LAN workstations.

Note: If a problem occurs while testing your connection, or you need to configure more advanced options for your RouteFinder, use RouteFinder Manager by selecting **Programs | RouteFinder Manager.**

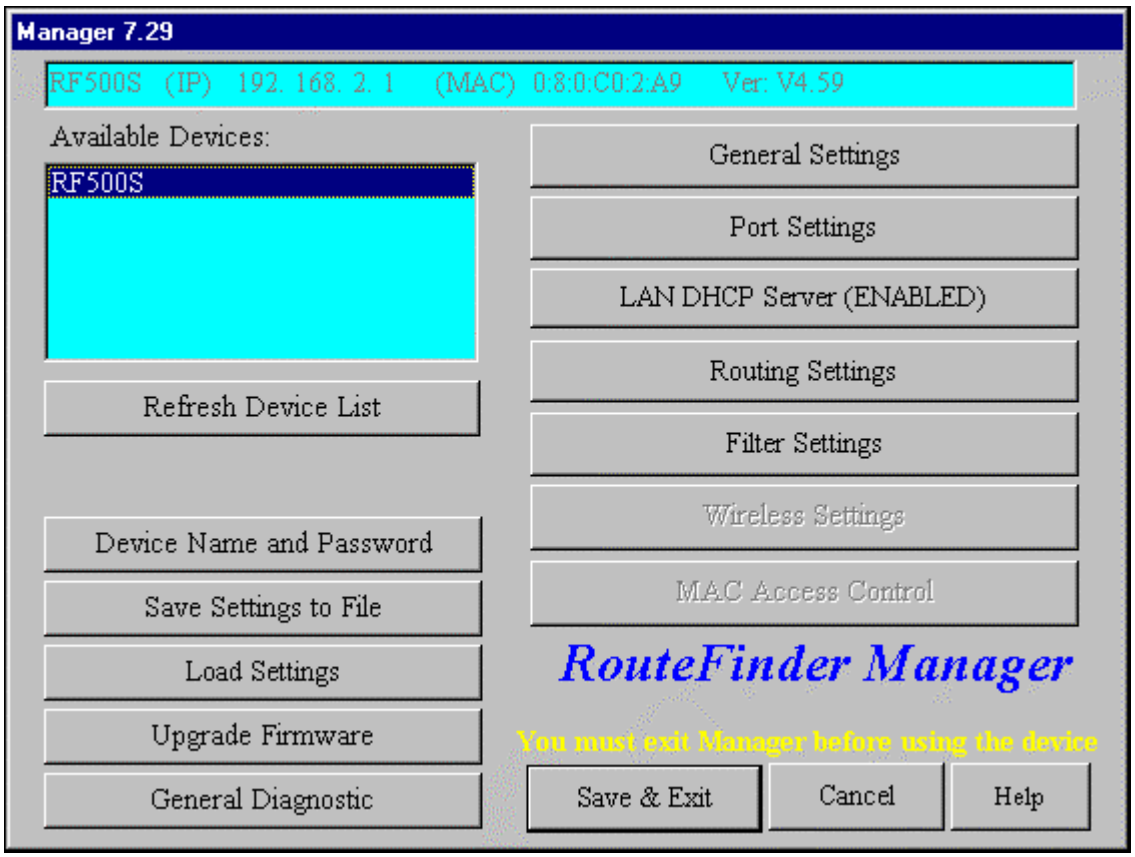
Chapter 5

RouteFinder Manager

Chapter 5 - RouteFinder Manager

RouteFinder Manager is a software program for configuring your RF500S.

1. To run RouteFinder Manager, click on the **RouteFinder Manager icon** on your desktop, or click **Start** | **Programs** | **RouteFinder Manager** | **RouteFinder Manager**.
2. The **Manager** screen displays.



3. The RF500S automatically searches your network for devices available for configuration and displays them in the **Available Devices** list box.

Note: Before using any of the Manager options, you must **select** the device you are attempting to configure from the **Available Devices** list. If you need to update the list, click **Refresh Device List**. Once the RF500S is configured, you must exit RouteFinder Manager before using it.

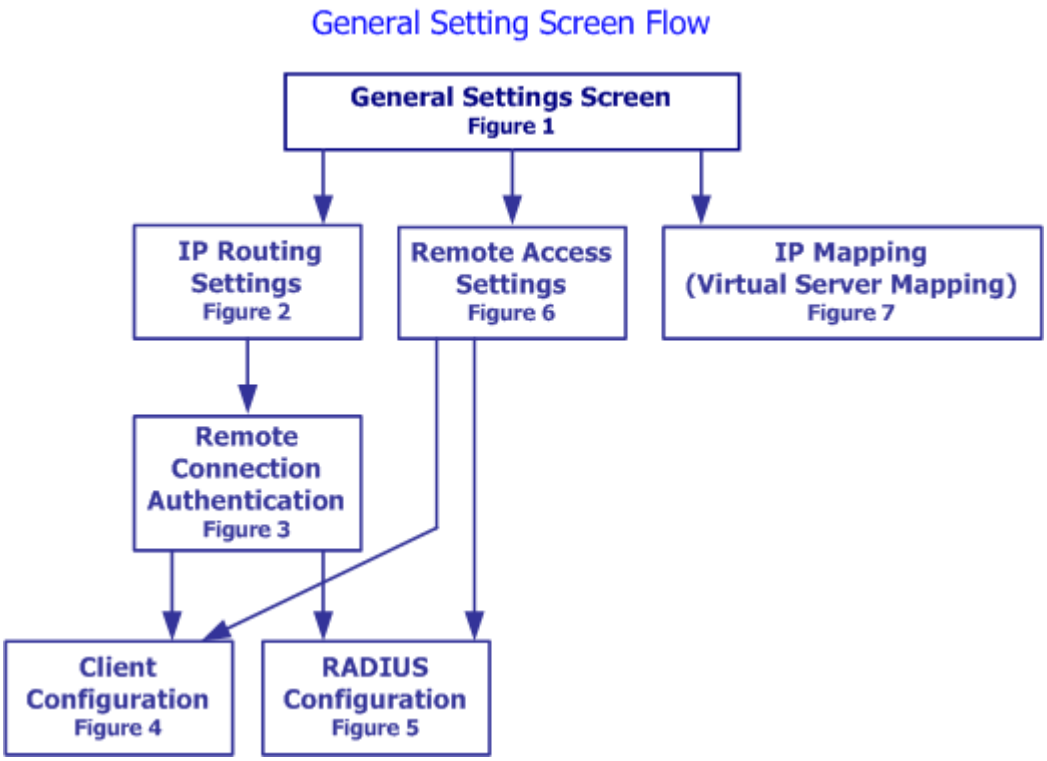
Status - After you have selected a device from the **Available Devices** list, the **Status** field provides the name, IP address, MAC address and Firmware version of your RouteFinder.

Buttons - The buttons in the left column can change the device's name and password, save and load settings, upgrade the firmware or run general diagnostics on the device. The buttons in the right column provide access to advanced configuration options for General Settings, Port Settings, LAN DHCP Server Options, Router Settings and Filter Settings. Additional information about all of these options is included in this chapter.

General Settings Screen

After selecting your device from the **Available Devices** list, click the **General Settings** button to view or change all of the network settings for the RF500S including LAN and WAN Ethernet segment settings, DNS information, IP Routing and Remote Access settings. Most of the settings were entered in the Setup Wizard; however, some important settings can be entered only in RouteFinder Manager.

The following diagram will help you visualize how the various screens of the **General Settings** functions are accessed.



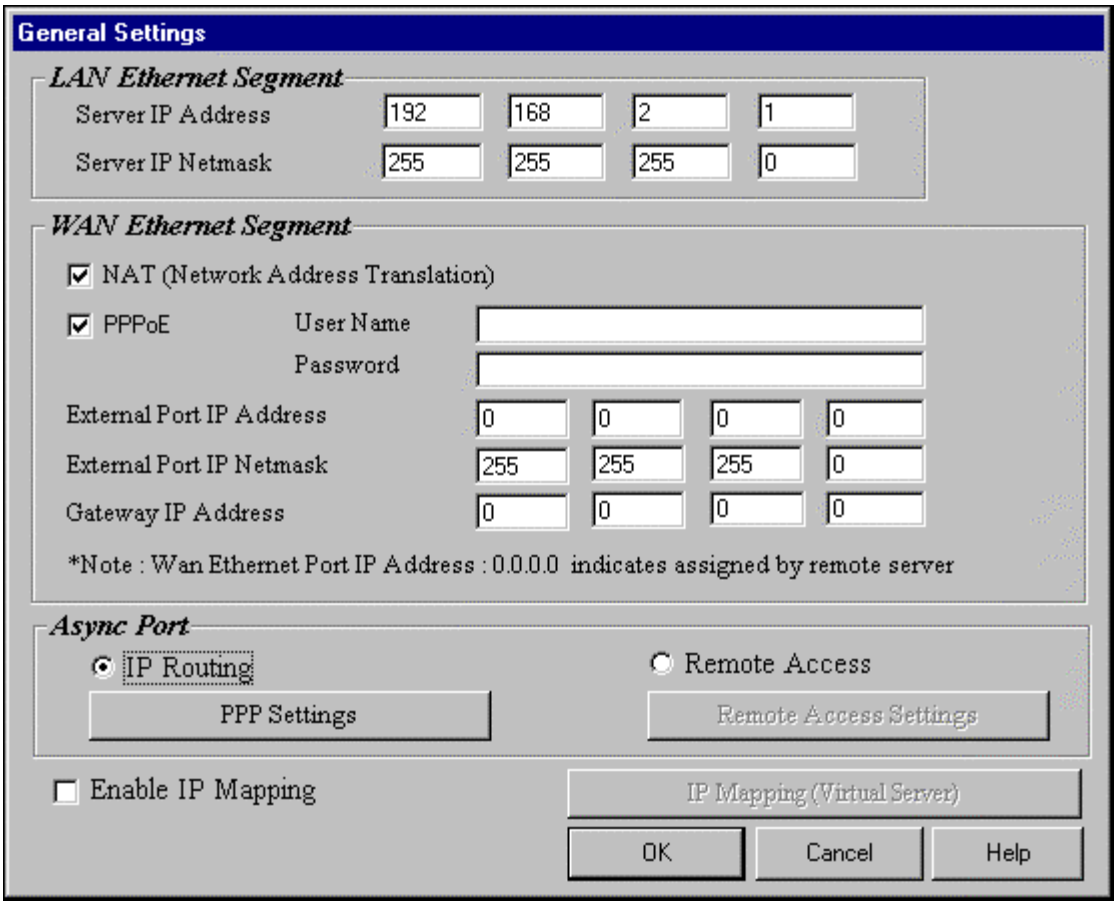


Figure 1 – General Settings Screen

LAN Ethernet Segment

Server IP Address - This is the RouteFinder's internal LAN IP address. The address entered into the Setup Wizard is displayed here (e.g., 192.168.2.1).

Server IP Netmask – This can generally can be left at the default 255.255.255.0.

WAN Ethernet Segment

Select **NAT (Network Address Translation)** to provide firewall protection and enable all local LAN users to share one IP address to access the Internet. If the NAT box is **not** checked, the WAN Ethernet is configured as a router to route network traffic between the LAN Ethernet segment and the WAN Ethernet segment.

PPPoE - If your ISP uses Point-to-Point Protocol over Ethernet for authentication purposes, select the PPPoE box and enter your ISP account User Name and Password in the fields provided.

External Port IP Address - Enter the IP address provided by your ISP or remote system administrator.

External Port IP Netmask - Enter the subnet mask of the port as provided by your ISP or remote system administrator.

Gateway IP Address - Enter your ISP or remote network's Gateway IP address.

Note: If your ISP uses a DHCP server to automatically assign a login IP address, subnet mask, gateway IP address or DNS IP address, enter 0.0.0.0 as your External Port IP Address and the Gateway IP Address.

IP Routing Settings

How to Access This Screen

1. On the RouteFinder Manager main screen, click the **General Settings** button
2. On the General Settings screen, check the **IP Routing** radio button.
3. Click the **PPP Settings** button. The IP Routing Settings screen displays.

The Async Port can be configured to provide either **IP Routing** and/or **Remote Access**. IP Routing connects your network to another router through the Serial async port. Remote Access allows remote users to dial-in to the device to access and share network resources as if they were logged on to the network locally.

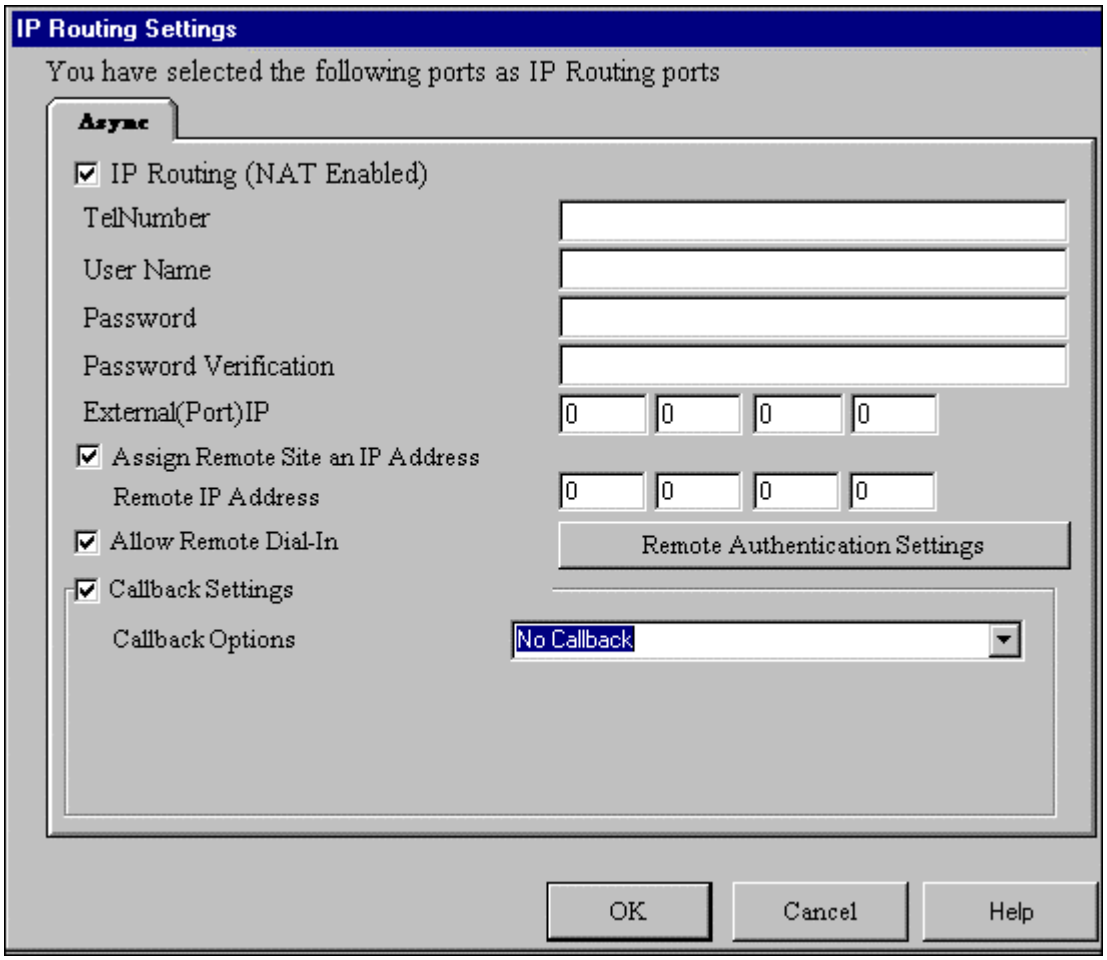


Figure 2 – IP Routing Settings

IP Routing (NAT Enabled)

If NAT is enabled, all local users will be firewall protected and will share one IP address through the Async port. Enter values in the fields as described:

Tel Number: Enter the phone number required to access your ISP.

User Name: Enter the account user name to be authenticated by your ISP.

Password: Enter the user account password to be authenticated by your ISP.

Password Verification: Re-enter the user account password for verification.

External (Port) IP: Enter the fixed IP address provided by the remote site System Administrator. If it is automatically assigned by the remote site DHCP server, enter 0.0.0.0

Assign Remote Site an IP Address

Check the **Remote IP Address** box to active the field, and enter the **Remote IP Address** the remote site will use.

Allow Remote Dial-In

Check the **Allow Remote Dial-in** box if you want to allow a remote site to dial-in to this network. When you click the **Remote Authentication Settings** button, the **Remote Authentication Settings** screen displays (see below).

Callback Settings

Callback Settings allow you to establish a connection with your ISP from a remote site.

Check the **Callback Settings** box to select one of three callback options:

1. **No Callback**
2. **Trigger (ISP) Server Connection -** The RouteFinder will establish a connection with the ISP server after a remote user dials into the asynchronous port. The device can be triggered to automatically establish a connection with the ISP in one of two ways:
   - The ISP server is dialed after the RF500S receives a PPP (modem) connection from a remote user.
   - The RF500S makes the connection to the ISP server after receiving a regular telephone call. The remote user calls the RF500S async port to trigger the connection to the ISP server.
3. **Remote Callback** - After dialing, the RF500S hangs up and waits for the remote site to callback. You must enter the callback telephone number (the telephone number the device should call) in the **Tel Number** field.

Remote Authentication Settings

How to Access This Screen

1. On the RouteFinder Manager main screen, click the **General Settings** button.
2. On the General Settings screen, check the **IP Routing** radio button.
3. Click the **PPP Settings** button. The IP Routing Settings screen displays.
4. From the **IP Routing Settings** screen, select check **Allow Remote Dial-In**.
5. Click the **Remote Authentication Settings** button. The **Remote Connection Authentication** screen displays.

Choose the desired authentication protocol and select/setup users' profiles.

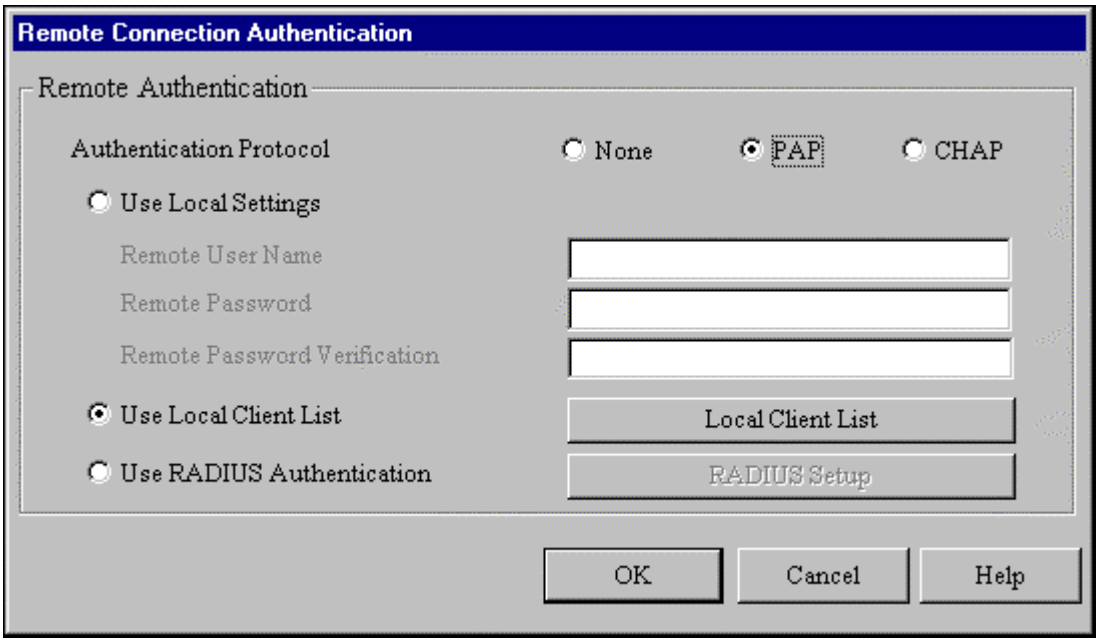


Figure 3 – Remote Connection Authentication

Authentication Protocol

Select one of three methods to define the authentication protocol to be used when a remote site is dialing into your site:

- **None** - No authentication needed.
- **PAP** - User Name and unencrypted Password are transmitted over the network.
- **CHAP** - DHCP sends a key which is used to encrypt the user name and password.

Note: If you select PAP or CHAP, you must indicate where the authentication process should occur, by selecting **Use Local Settings**, **Use Local Client List** or **Use RADIUS Authentication**.

Use Local Settings

If you check this option, the fields under this option become active for you to create a **Remote User Name** and **Remote Password**. All users will login to the system with this common user name and password.

Use Local Client List

This list consists of User Names and Passwords that can access your network from a remote site. When a remote user dials in to the RF500S, the user's Access Profile (user name, password, callback status, etc.) is validated against this list. The list can include up to 64 users. Click the **Local Client List** button to displays the Client Configuration screen.

Important: The RouteFinder's default user is **guest;** it requires no password. For security reasons, either delete the **guest** user or provide it with a password.

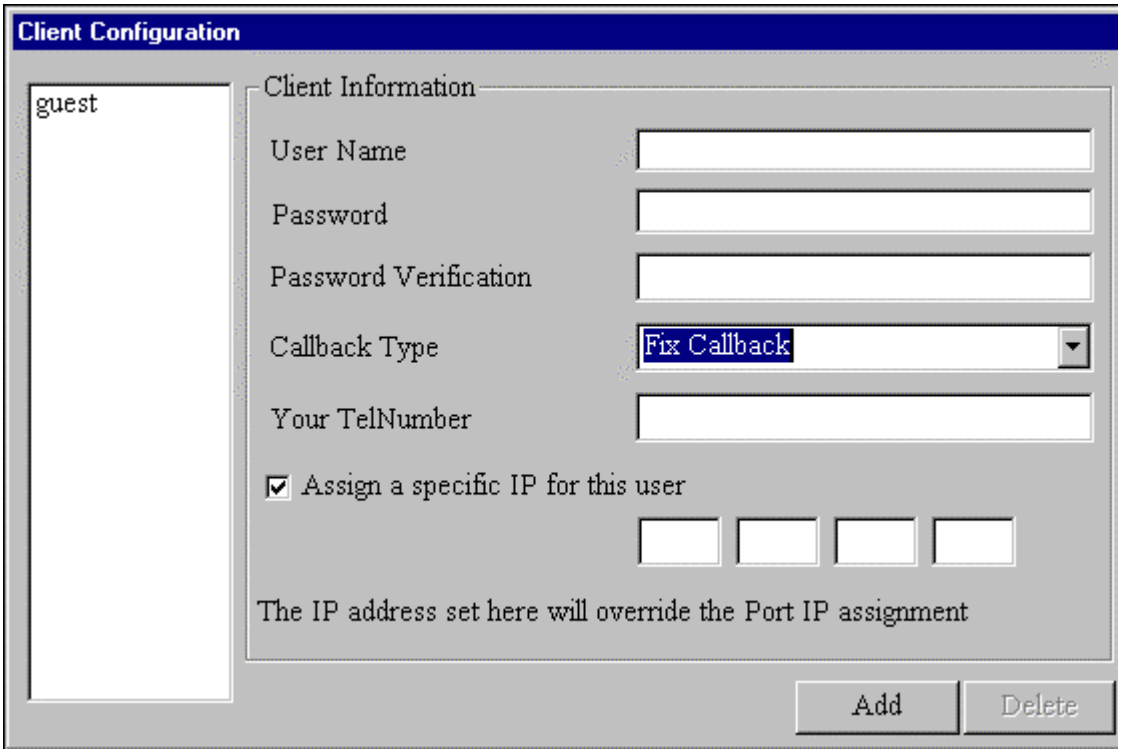


Figure 4 – Client Configuration (Shown without the OK, Cancel, and Help buttons)

Client Information for Each New Remote User

User Name – Enter a user name with a maximum of 16 characters.

Password – Enter a password for each user name with a maximum of 16 characters.

Password Verification – Verify the password by re-entering it.

Callback Type – When a remote client dials into the network, it disconnects. Then the RF500S calls the client back. There are three Callback Types:

No Callback – (Default) No callback function.

Fixed Callback – The RouteFinder connects to the client by dialing the number specified in the **Your TelNumber** field.

Variable Callback – The remote client specifies the phone number the RouteFinder should callback each time a dial-up connection is established.

Assign a Specific IP Address for This User - Check this option to specify an IP address for this user. This IP address will be used each time the client logs in and will override the **Assign Remote Site an IP Address** option as shown on the **IP Router Setting** screen, **Async** tab. Click **Add** to complete adding this client to the Local Client List.

Use RADIUS Authentication

Checking the **Use RADIUS Authentication** box allows you to use the user information (user name, password, IP address, etc.) stored on a separate RADIUS server on the network.

Note: A RADIUS Server (Remote Authentication Dial-In Service) is an accounting and authentication system used by many large companies and Internet Service Providers (ISPs). After a client dials in to the network and enters their user name and password, the information is passed to a RADIUS server. The RADIUS server checks the accuracy of the information, and then allows access to the system.

1. Check the **Use RADIUS Authentication** box and then click the **RADIUS Setup** button. The RADIUS Configuration screen displays.
2. Select the **Main RADIUS Server** or **Backup RADIUS Server** from the drop-down list box.
3. Enter the RADIUS Server IP Address. In most cases, the RADIUS Access Server and the RADIUS Accounting Server are the same device. If this is true for your configuration, enter the same IP address in both fields.
4. Enter your **Secret** RADIUS code or password and then re-enter it to confirm.
5. Click **OK** when complete.

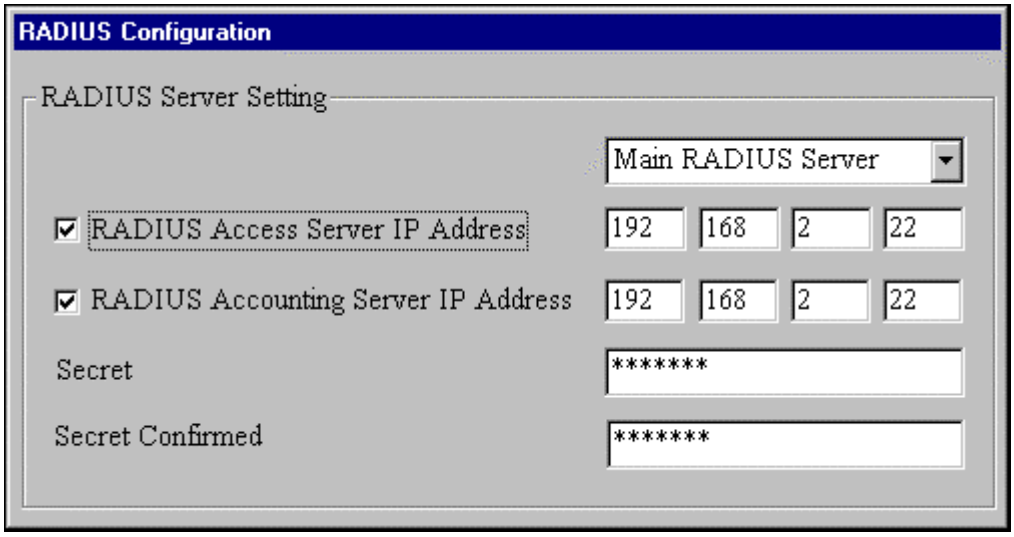


Figure 5 – RADIUS Configuration (Shown without the OK, Cancel, and Help buttons)

Remote Access Settings

How to Access This Screen

1. On the RouteFinder Manager main screen, click the **General Settings** button
2. On the General Settings screen, check the **Remote Access** radio button.
3. Click the **Remote Access Settings** button. The Remote Access Settings screen displays.

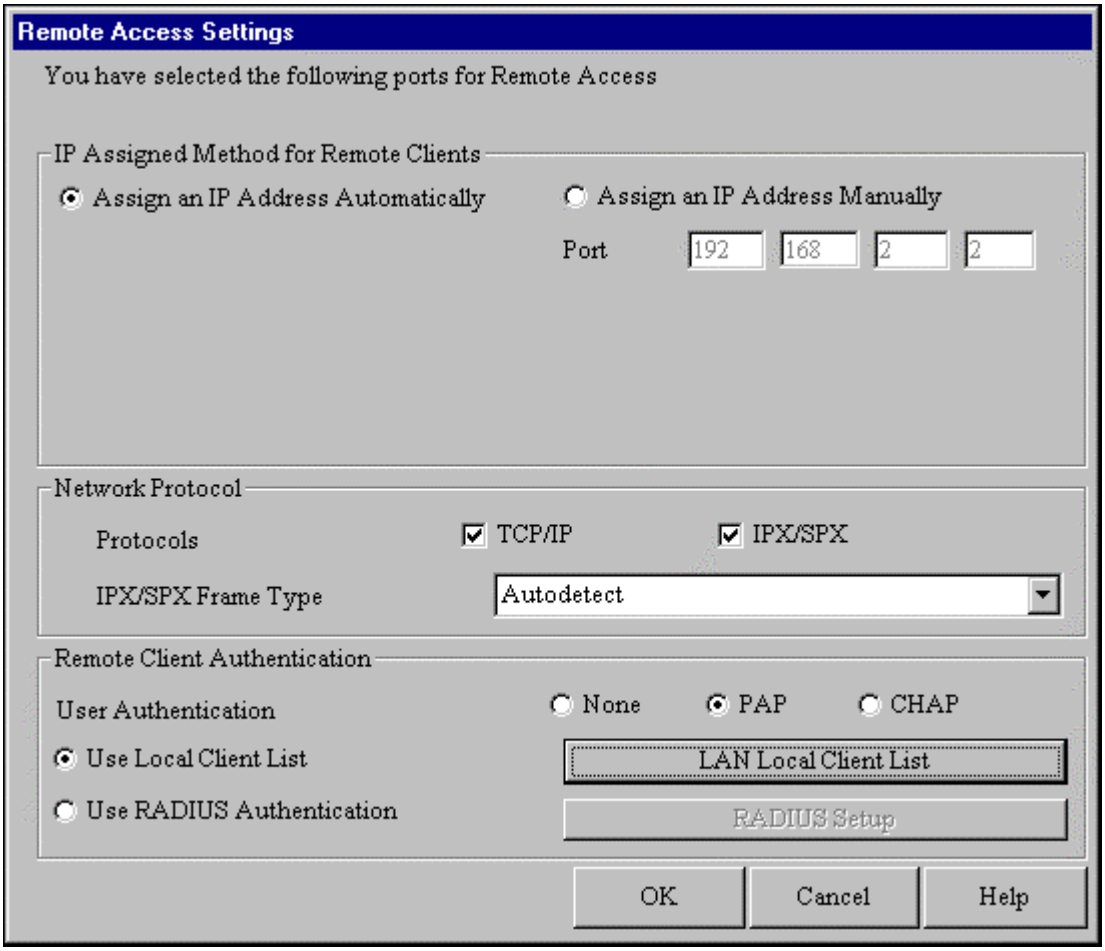


Figure 6 – Remote Access Settings

IP Assigned Method for Remote Clients

A remote client must have an IP address to connect to the network. IP addresses may be assigned automatically from a designated IP address pool using DHCP or assigned manually.

Assign an IP Address Automatically – DHCP will issue the remote site user an IP address automatically (if DHCP is enabled). If DHCP is disabled, the device will automatically search for a DHCP server and, if found, request an IP address for the remote client.

Assign an IP Address Manually – Enter an IP address for the remote client.

Network Protocols

You must have at least one network protocol enabled for the dial-in service. The default enables both TCP/IP and IPS/SPX. If you do not need both protocols, you may disable one of them. If you are connecting to a Netware Server, IPX/SPX must be enabled.

IPX/SPX Frame Type – The RF500S can automatically detect what kind of IPX/SPX frame type you are using. You may manually select a frame type by using the list box.

Remote Client Authentication

Remote authentication settings allow you to specify how you would like to authenticate remote users. You may select **Use Local Client List** or **Use RADIUS Authentication** (refer to Remote Connection Authentication Settings in this chapter for more information). Choosing RADIUS configuration allows you to use the user information (user name, password, IP address, etc.) stored on a separate RADIUS server on the network.

Click **OK** when complete.

IP Mapping - Virtual Server Mapping

How to Access This Screen

1. On the RouteFinder Manager main screen, click the **General Settings** button.
2. On the General Settings screen, check the **Enable IP Mapping** box.
3. Then click the **Enable Mapping (Virtual Server)** button. The screen displays.

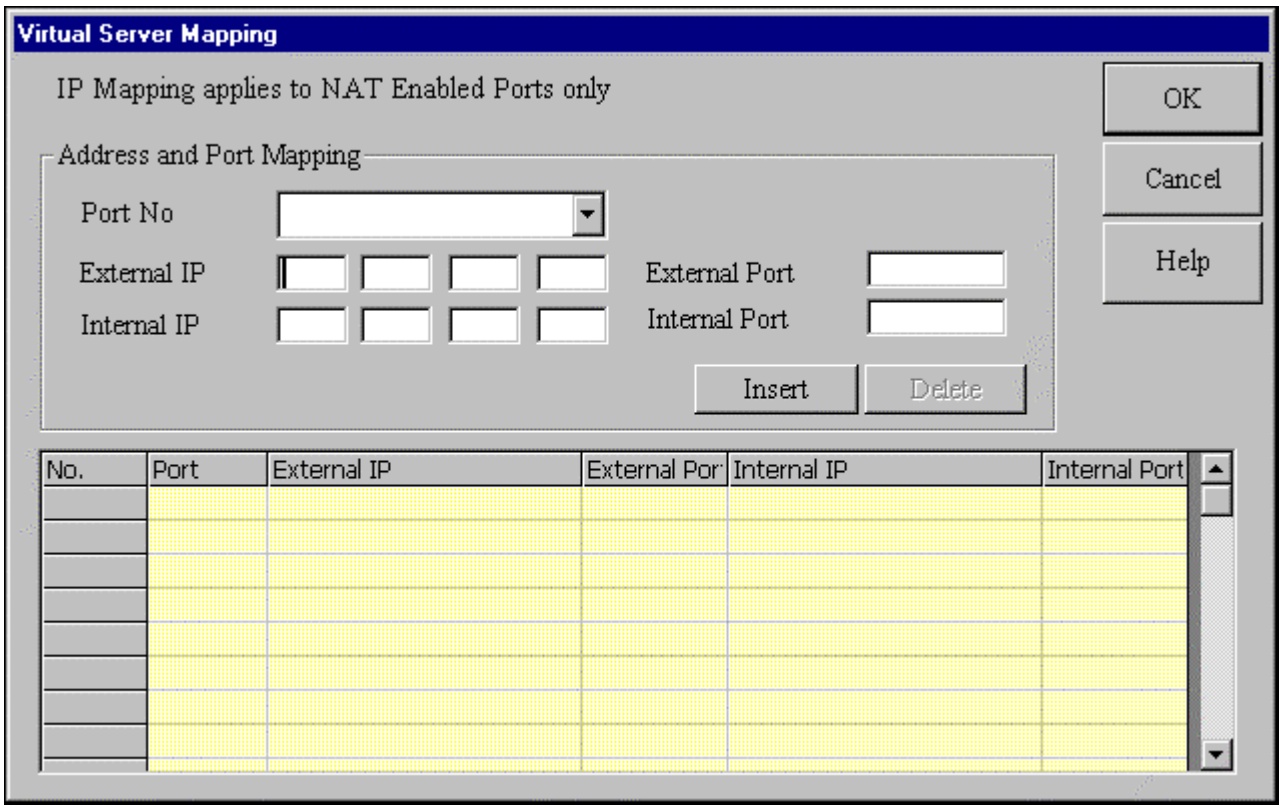


Figure 7 – IP Mapping (Virtual Server Mapping)

IP Mapping is available only when NAT is enabled on the General Settings screen. If NAT is enabled for a particular port, that port is firewall protected. The **Enable IP Mapping** function allows you to open a "hole" in your firewall to allow access to your LAN via the Internet. For example, you can use the IP mapping function to access an FTP server on your LAN via the Internet. IP Mapping is most suitable to fixed or static IP addressing.

For each service you'd like to set up, enter:

1. **Port No:** Select either the WAN or Async (Serial) port.
2. **External IP:** Enter the IP address supplied by your ISP in the External IP field. If your ISP uses dynamic IP addressing, set this field to 0.0.0.0. Your device will use the dynamically assigned address when connecting to your ISP.
3. **External Port:** Enter the TCP/IP port number for the service that you will be using for IP mapping. Common TCP/IP port numbers are:
   WWW Port 80
   FTP Port 20 or 21
   SMTP Port 25
   POP3 Port 110

If you would like to map all services for this external IP address to a computer on your LAN, you can enter port number 0. This means that whenever anyone accesses your external IP address, they will automatically be "mapped" to the internal computer that you specify, regardless of what port number they are using.

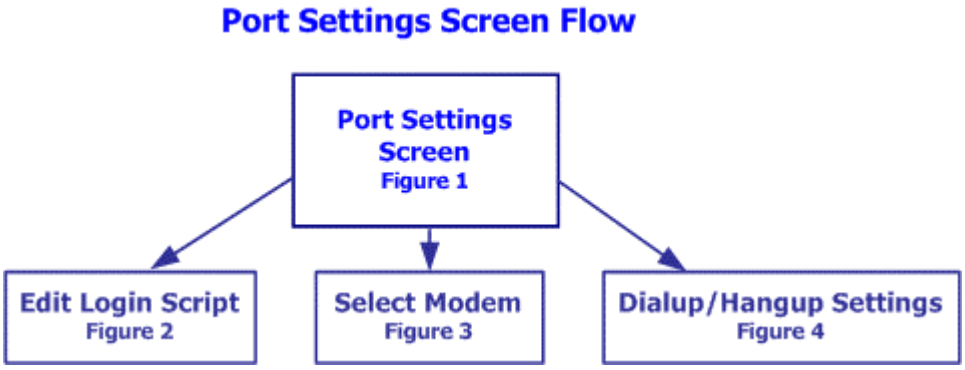
4. **Internal IP:** Enter the Internal IP address of the server to which you want to map the External IP address.
5. **Internal Port:** Enter the port number for the service that you will be using for this IP mapping.
6. Click Insert to include the mapping.
7. Click **OK** when you have completed mapping addresses.

Note: IP Mapping function allows you to have only one port service on your LAN. For example, if you map an external IP (16.895.1.3) to an internal IP address (192.168.2.22 - a www server), only the internal IP address in your local network can serve as the www.server for the external IP address.

Port Settings

The Modem Settings options are used to configure the communication between your modem or ISDN TA and your RouteFinder serial port. You must specify the baud rate, modem, and modem string settings for your device.

The following diagram will help you visualize how the various screens of the **Port Settings** functions are accessed.



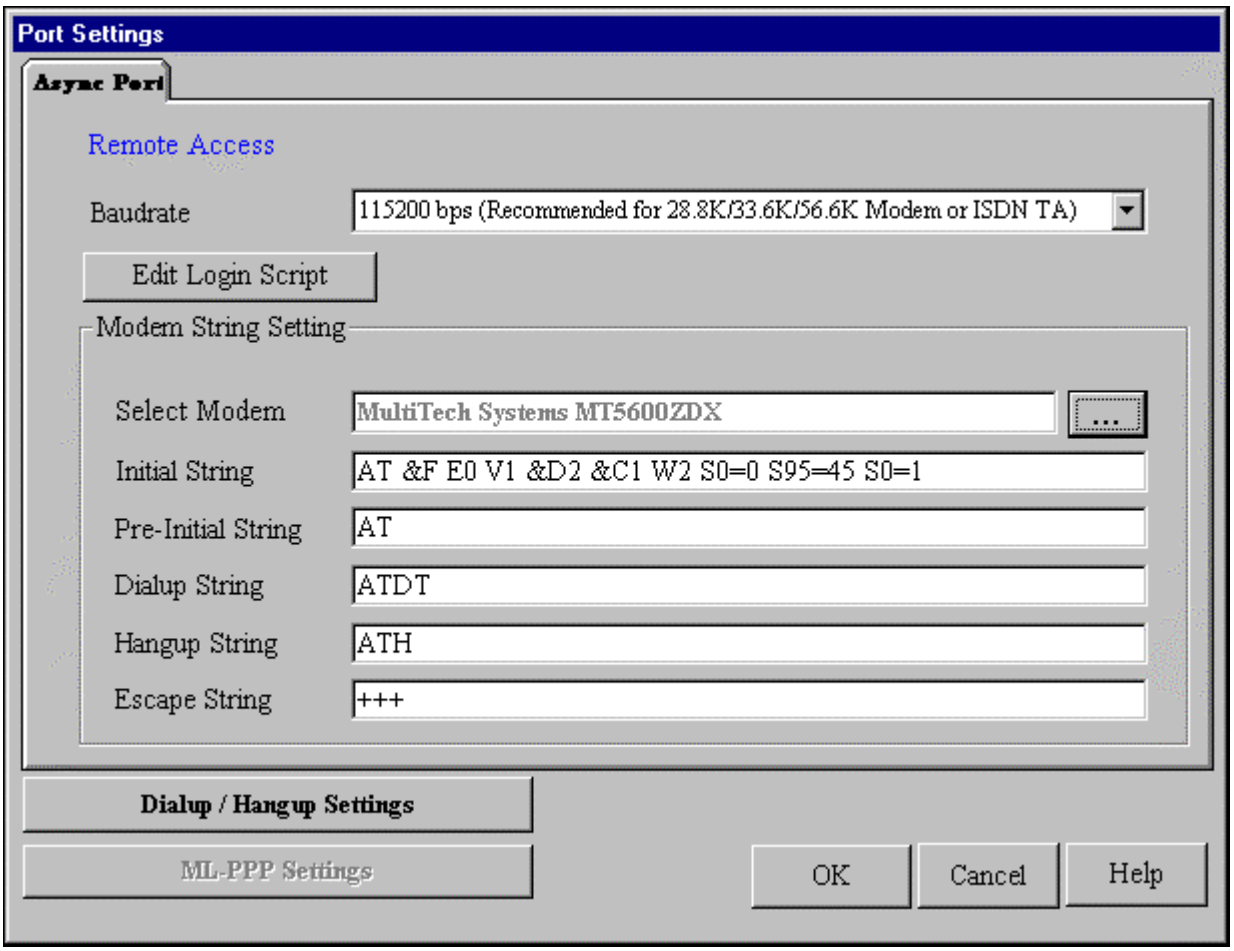


Figure 1 – Port Settings Screen

Baud Rate

Select the Remote Access DTE speed for your device from the drop-down list box.

The absolute maximum setting for a given port on the network device is 4 x the speed of your modem. If the baud rate is set too high, your network device may fail to establish a dial-up connection. For example, if you have a 14.4Kbps modem, the highest speed selected is 57.6Kbs.

If your modem does not appear in the list provided, the Standard Modem selection will work in most cases.

Important: If you are using an ISDN Terminal Adapter, refer to the Async to Sync PPP string in the User Manual provided with the device to determine the correct initialization, dialup and hang up strings.

Note: Due to variations in ISP connections and phone line quality, this theoretical maximum speed is not attainable. You may need to set the baud rate at a lower speed.

Edit Login Script

Click the **Edit Login Script** button to open a screen onto which you can type a login script.

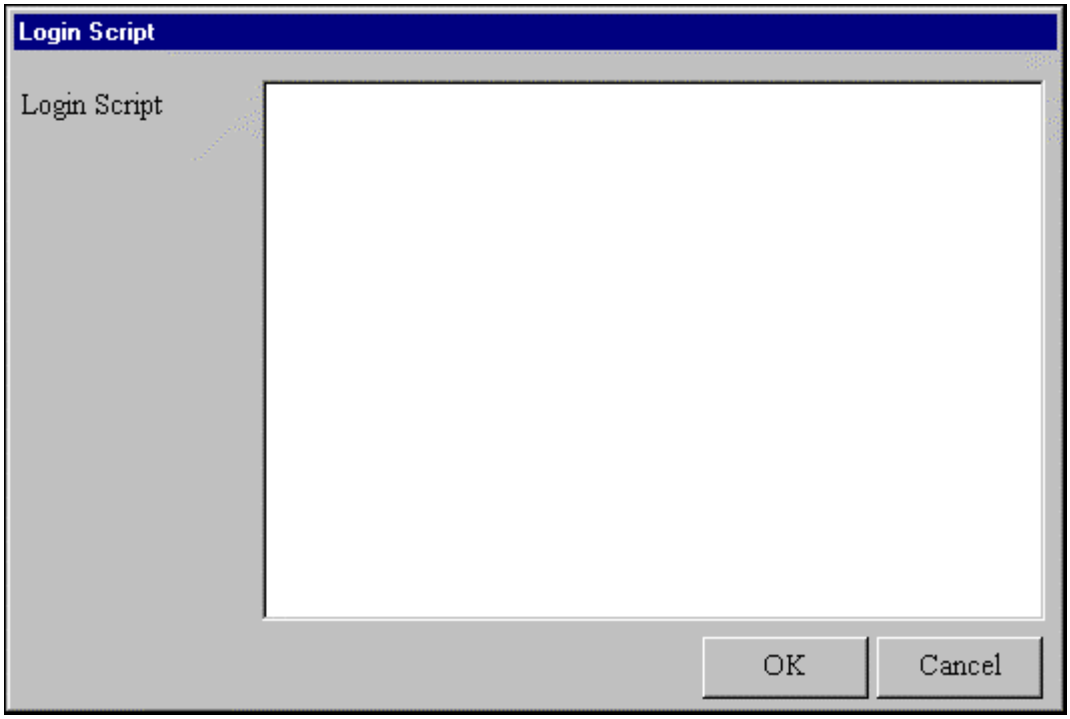


Figure 2 – Edit Login Script Screen

If a remote access client is configured to "bring up a terminal window after dialing", this remote access login script initiates. A sample remote access login script terminology is shown below.

For Remote Access, the device will act as the server side.

Send "**Welcome**" displays "**Welcome**" to remote site.

Send sends an Enter (Carriage return + line feed) to the remote site.

"**Send Username**" prompts the remote site for a user name.

"**Retrieve 1**" will wait for the remote site to enter the user name to be used for PPP authentication.

"**Send Password**" prompts the user for a password.

"**Retrieve 2**" will wait for the remote site to enter a password.

"**Verify 3**" instructs the device move to login script line 3 if PPP authentication fails.

"**Go**" means start PPP protocol.

Note: See Appendix E for Examples of Login Scripts

Select Modem

Click the button to access the drop-down list box, and select your modem manufacturer and modem model.

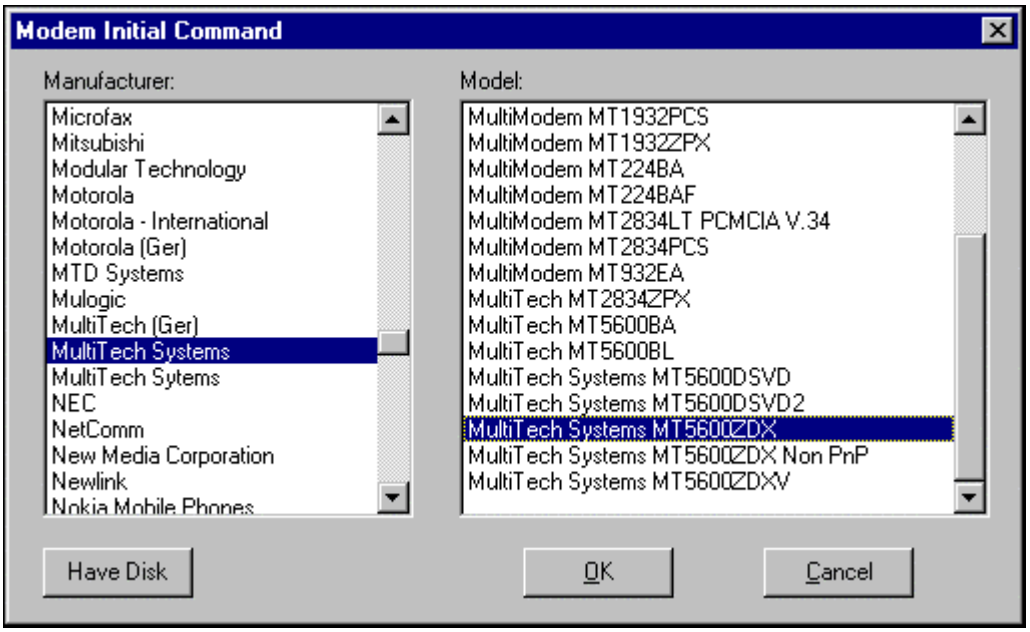


Figure 3 – Select Modem

Modem String Settings

Select Modem

For most analog modems, the Standard Modem selection will work. However, you can click the button at the end of the field for a list of modems and their manufactures from which to select your modem. For additional information, refer to the Modem Settings information presented in the Software Installation and Configuration chapter of this User Guide.

Initial String

The most important modem string is the initialization string because your network device uses it to establish communications with your modem or ISDN TA. The modem initialization string displayed is the modem or ISDN TA initialization string entered in the Setup Wizard.

Important: There is no standard ISDN TA initialization string. If your ISDN TA is not included in the modem list, check your ISDN TA User's Guide for information for the initialization string for an Asynchronous to Synchronous PPP connection. If you are using only one channel of your ISDN connection, you can enter the Async to Sync PPP initialization string. If you are bundling your connection channels, you'll need to use a Multilink-PPP initialization string. You must also enter the two phone numbers in the Telephone Number field of the **General Settings** screen. Also, verify that your ISDN TA supports the dial-up string ATDT. Most ISDN TAs support ATDT, but some support ATD or ATDI.

Every ISP has a unique login interface screen. Check with your ISP to determine how your ISP requests information from you when using a PPP connection.

Note: You can create a simple dial-up connection to view your ISP interface log-in screen using Dial-Up Networking in Windows 95, 98, Me, NT or 2000.

Some Common Commands Are:

Send and SH	Function
Send "ATZ"	Resets the Modem
Send "ATDT 888-1234"	Dials the phone number "888-1234"
Send "JaneDoe"	Types "JaneDoe" at the ISP interface
SH "1234"	Types "1234" at the ISP interface but displays **** on the RouteFinder monitor to hide the password.
Send "	Sends Enter (carriage return plus line feed) to the ISP

Wait	Function
Wait 5	The Modem will wait for 5 seconds before moving the next line in the login script.
Wait "CONNECT"	The Modem will wait for CONNECT to display before moving to the next command.
Wait "CONNECT 6"	Modem will wait for "CONNECT" to display before moving to the next command. If CONNECT does not display, the modem will go to line 6 of the login script.

Other	Function
Go	Begins PPP
Jump4	Goes back to line 4 of the login script.
Hangup	Hangs up the modem.

Dialup/Hangup Settings

How to Access This Screen

1. On the RouteFinder Manager main screen, click the **Port Settings** button.
2. On the Port Settings screen, click the **Dialup/Hangup** button displays. The Dialup/Hangup Settings screen displays.

The Dialup/Hangup settings allow you to specify your connection time (idle timeout or auto reconnect) and the number of times to attempt to connect (if connection cannot be established).

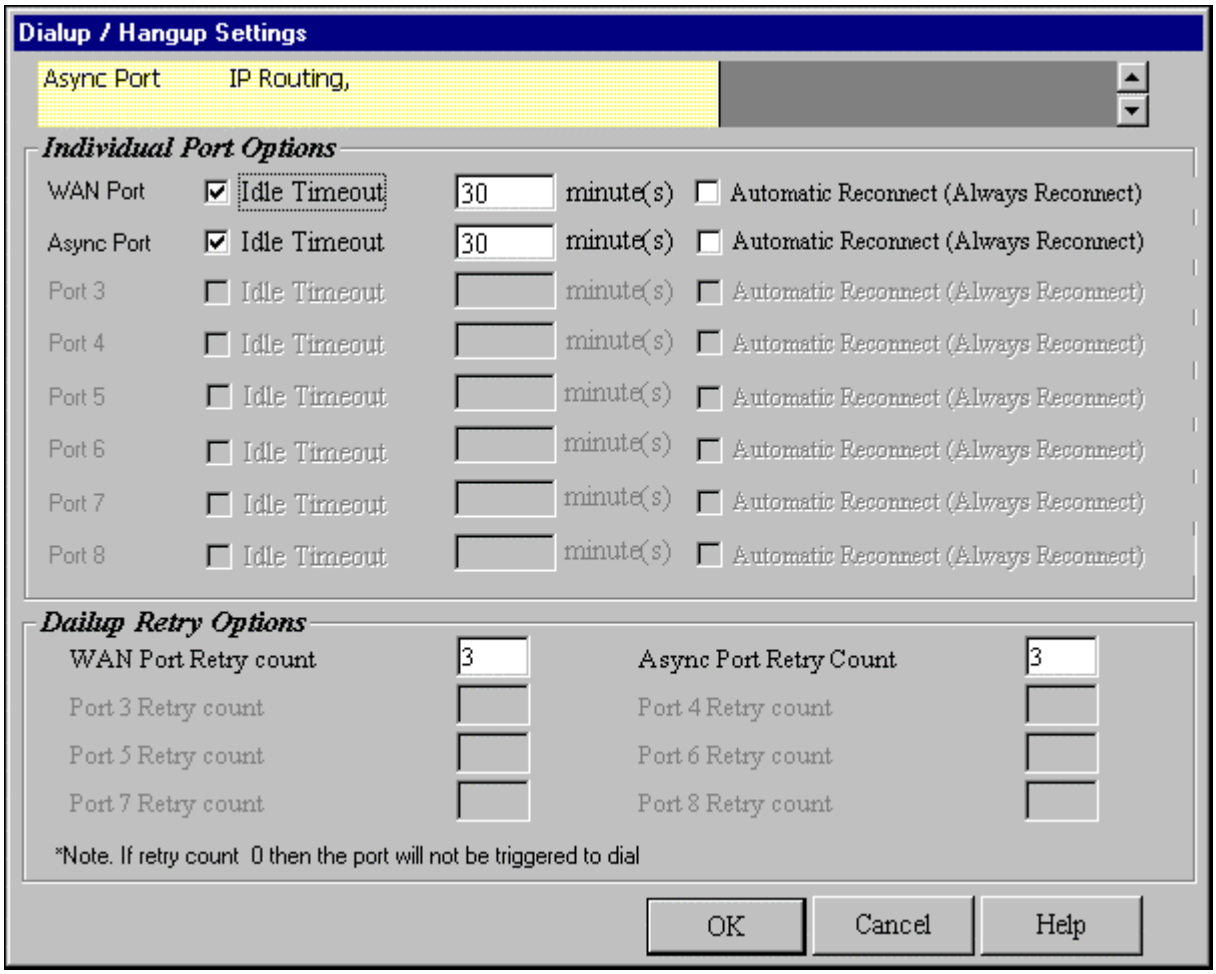


Figure 4 – Dialup/Hangup Settings Screen

Individual Port Options

This option lets you set the idle-timeout function for each serial port of the RouteFinder. You can set the number of minutes you wish to allow a connection to stay idle before disconnection.

Note: Default idle timeout for IP Routing is 5 minutes. Default idle timeout for Remote Access is 30 minutes.

If you un-check the idle-timeout, once a client establishes a connection, the connection will be maintained until you turn off your modem, unplug your network device or use the **Terminate Connection** function in the RouteFinder monitor program.

The Automatic Reconnect (Always connect) essentially maintains your connection (e.g., idle time out = infinite). If the connection is disconnected for any reason, it will automatically attempt to reconnect.

Dialup Retry Options

The Dial-Up Retry option allows you to specify the number of times the RouteFinder should attempt to establish a connection.

If the retry count is 0, the device will not dial-out to connect to the remote site.

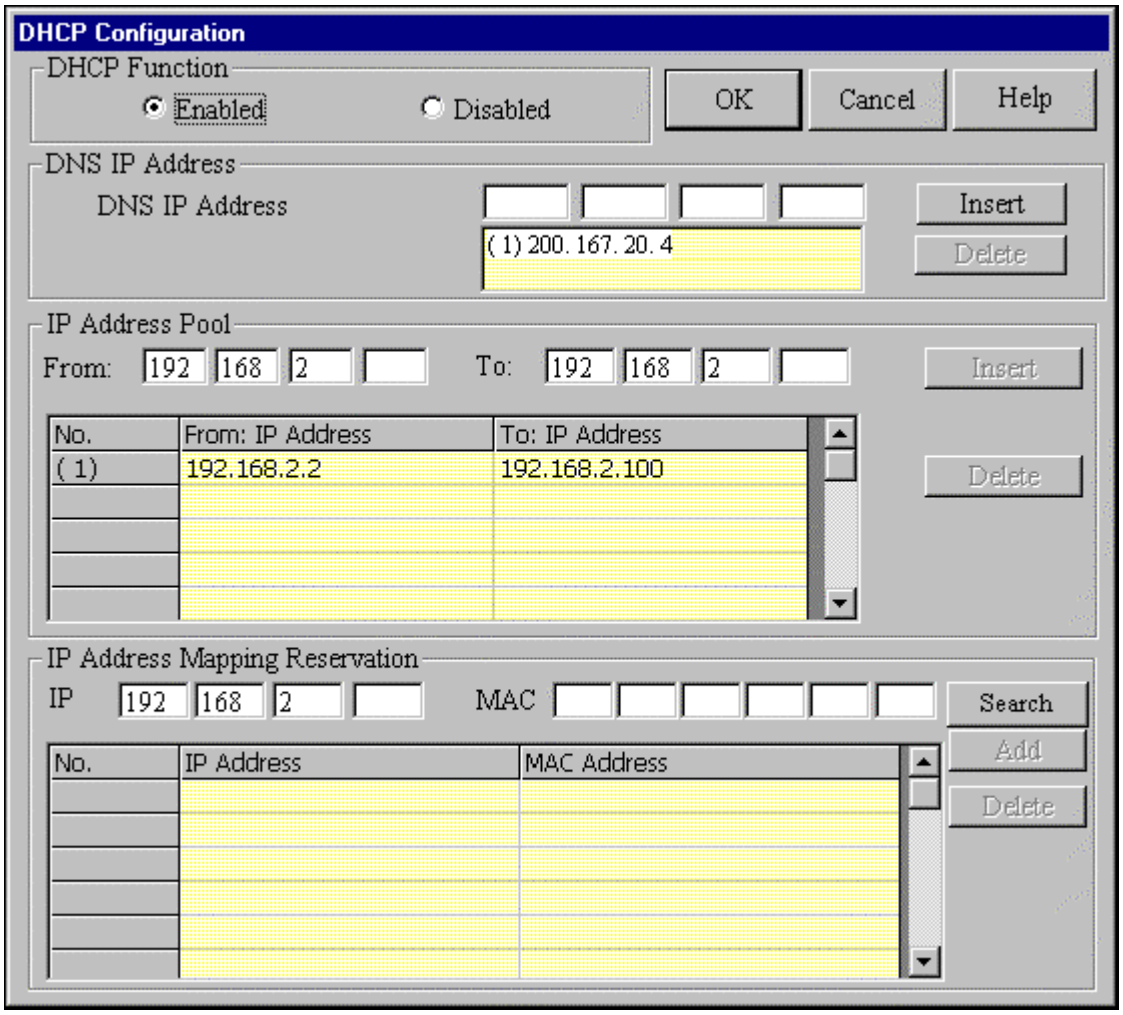
Note: Automatic Reconnect will override the Retry count setting if the retry count is set to 0.

LAN DHCP Server

How to Access This Screen

1. From the RouteFinder Manager main menu, click the **LAN DHCP Server** button.
2. The DHCP Configuration screen displays.

This is the only screen for the DHCP function.



DHCP Enabled

The LAN DHCP Server option indicates if DHCP is Enabled or Disabled. By default the function is Enabled. To disable, click the **Disabled** radio button and click **OK**.

DNS IP Address

Enter the ISP's DNS IP address. You may enter up to 4. Click **Insert**.

IP Address Pool

The IP Address Pool contains the range of IP addresses that will be automatically assigned to the clients of your network as they connect to the network.

Note: By default, the IP address pool range is from 100 to 200. Ranges are listed in the IP Address Pool table.

To **change** the range:
1. Select the existing range of addresses.
2. Enter a new range.
3. Press **Insert**.

To **delete** an IP Address range:
1. Select the range of addresses.
2. Press **Delete**.

IP Address Mapping Reservation

You can use the IP Address Mapping Reservation option to give a *static* IP address to particular computers on your network. Each time a computer is powered on and connects to the network, it will receive the same IP address. Static IP addresses are frequently assigned to network resources such as printers, servers, hubs and routers that are consistently shared by network clients.

To assign a static IP Address:
Enter the MAC address manually or use the MAC address search tool.

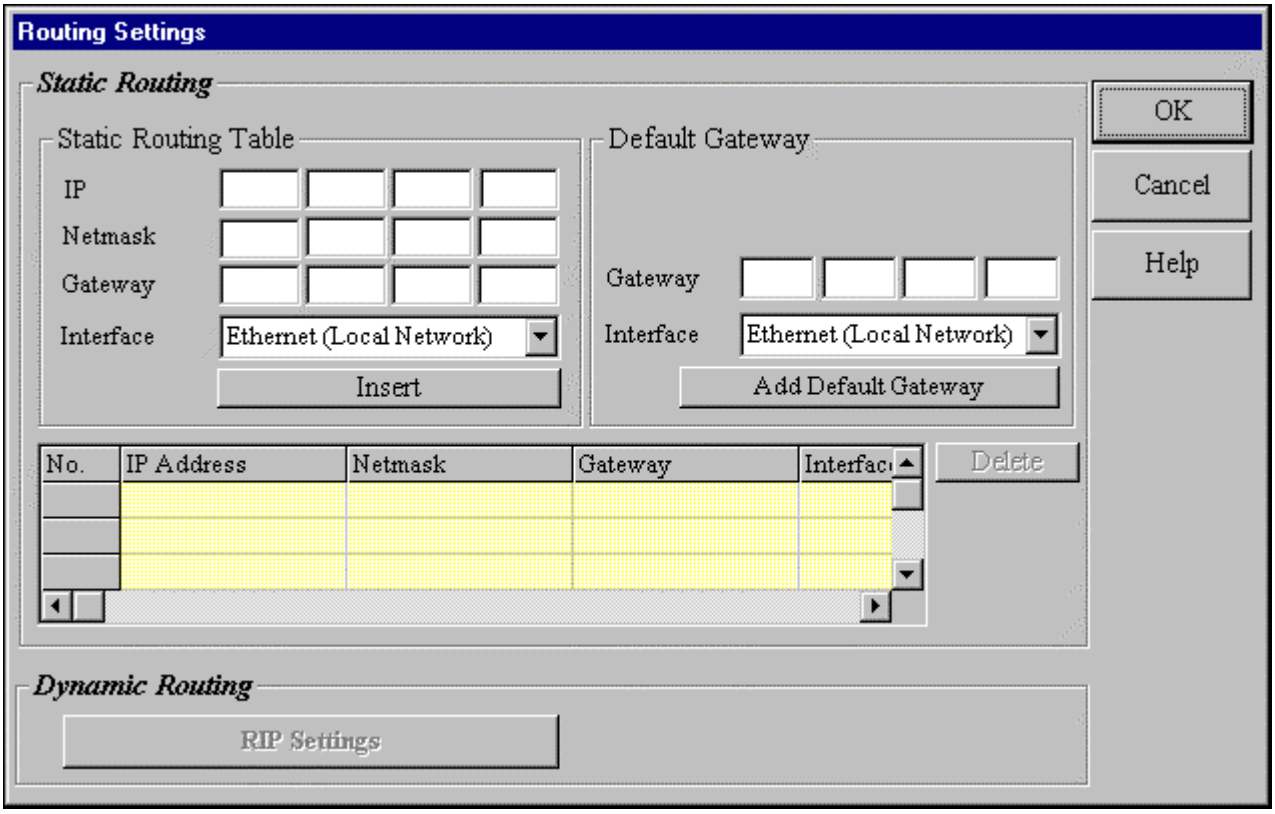
To use the MAC address search tool:
1. Enter the IP address of the computer.
2. Click **Search** to find the MAC address.
3. Once the address has been located, click **Add** to reserve the address.

To **delete** a static IP Address:
1. Select the static address you would like to delete.
2. Click **Delete**.

Routing Settings

How to Access This Screen

1. From the RouteFinder Manager main screen, click the **Routing Settings** button.
2. The **Routing Settings** screen displays. This is the only screen for the Routing Settings function.



Routing is the process of moving a packet of data from source to destination. The RF500S acts as a router to enable messages to pass from one computer to another and eventually reach the target machine. Part of this process involves analyzing a routing table to determine the best path. Use the information below to create a routing table to connect your network to another network, or to connect subnets within your network.

Note: This table is required to use the LAN-to-LAN routing function of the RF500S.

Static Routing

For each different subnet on your LAN, enter:

IP: The (network/subnet) IP address to which you want to route.

Netmask: The subnet mask of your Network IP address.

Gateway: The IP address of the gateway device linking your network to the other network/subnet. The IP address should be in the same subnet as your RF500S. If you are using this device with the LAN-to-LAN function, the gateway IP should be set as the IP address of the RouteFinder.

Interface: Select the port (LAN or WAN, etc.) that the routed packet should pass through. Select **Local Network** if you are using a separate router. If you are using the RF500S with the LAN-to-LAN function, the Interface should be set as the WAN port that connects you to the other subnet.

Click **Insert** to save the information to the routing table. To delete this information, select it from the routing table and click the **Delete** button.

Default Gateway

Gateway: The Default Gateway is an IP address that all packets are routed to, when the device is unable to find a route match (the destination IP address of the packet in the routing table). Click the **Add Default Gateway** button to save the IP address of the default gateway.

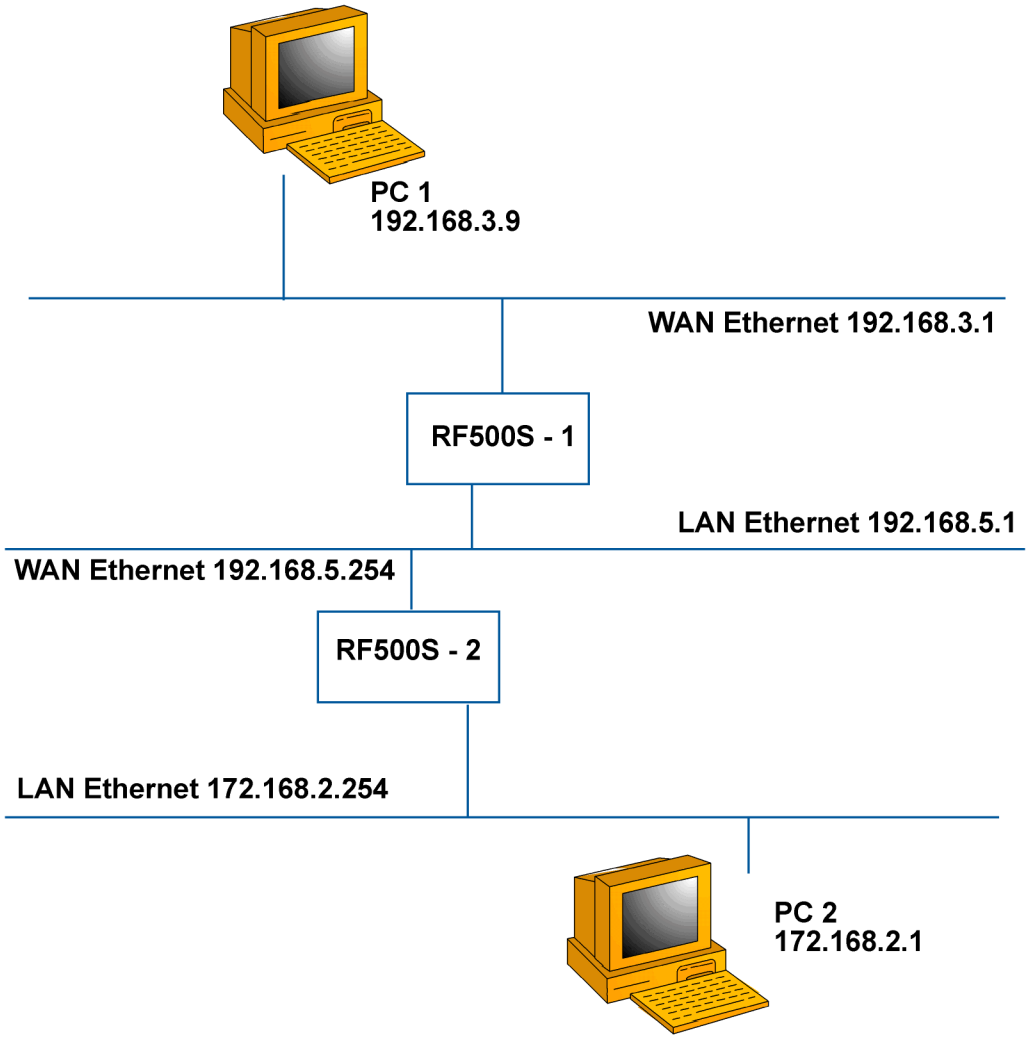
Interface: Select the port (LAN or WAN, etc.) interface where the gateway is located.

Dynamic Routing

This feature is not available.

Example of a Routing Table

The routing table stores the routing information so that the RF500S knows how to route the IP packets to the proper network.



What Is the Purpose of the Routing Table?

In the diagram above, the RF500S-1 has the routing information to route between 192.168.3.x and 192.168.5.x. The device does not have the information about how to route to the 172.168.2.x network.

If you want the RF500S-1 to route to 172.168.2.x, you must add the following information to the routing table:

IP:172.168.2.0
Network:255.255.255.0
Gateway IP:192.168.5.254
Interface: Ethernet (Local Network)

If you would like the RF500S-2. to route to 192.168.3.x, enter the following routing table information into the RF500S Routing settings:

IP: 192.168.3.0
Network:255.255.255.0
Gateway IP: 192.168.5.1
Interface: WAN Ethernet

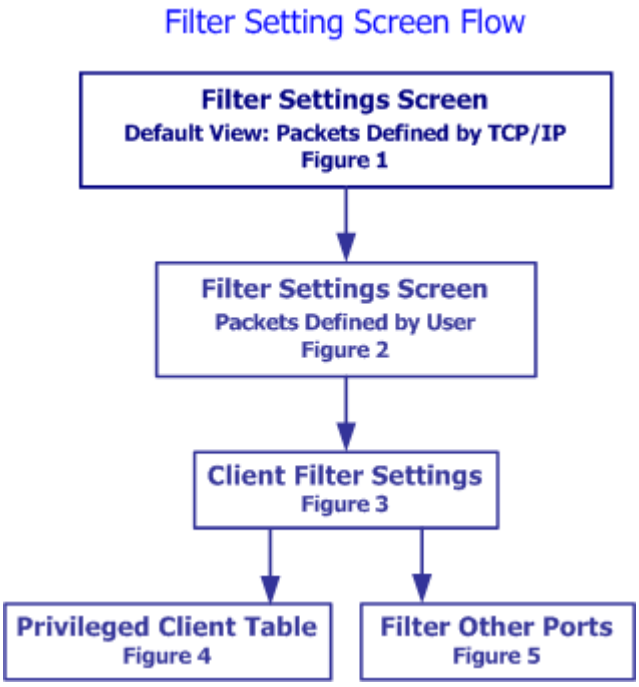
Filter Settings

You can use Filter Settings to choose which packets are allowed to enter the network and which packets will be blocked. Filter Settings can be used to filter network services such as Mail, WWW, FTP, Telnet and News.

How to Access the Screen

1. From the RouteFinder Manager main screen, select your RF500S from the **Available Devices** list, then click the **Filter Settings** button.
2. The **Filter Settings** screen displays.
3. Select the **Block** tab or the **Pass** tab to define your filtering.

The following diagram will help you visualize how the various screens of the **Filter Settings** functions are accessed.



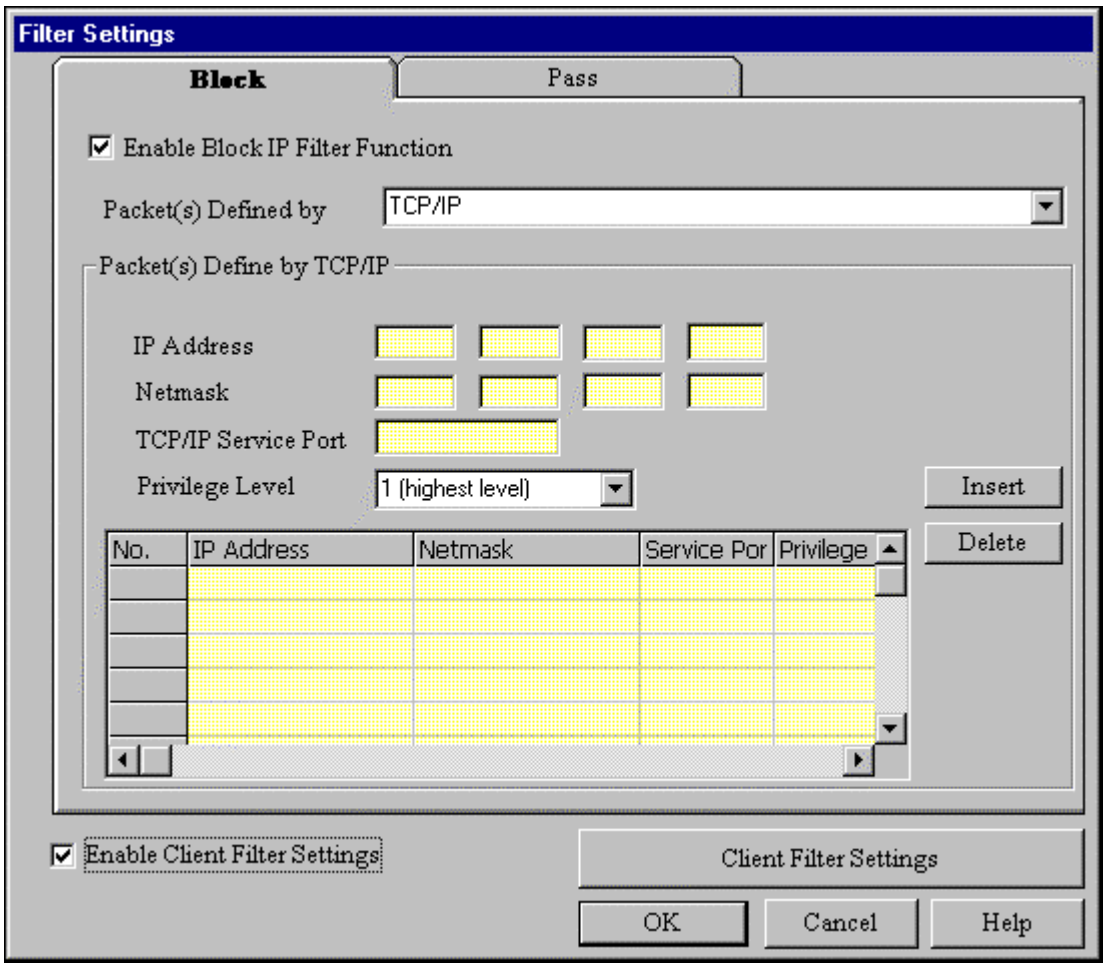


Figure 1 – Filter Settings (Packets Defined by TCP/IP)

Note: The Block and Pass screens displays the same fields, except that one enables the Block IP Filter Function and the other enables the Pass IP Filter Function. Both of them change when you select **User** from the **Packets Defined by** drop-down list box (the default is **Packets Defined by TCP/IP).**

The Block and Pass screens allow you to define whether or not users have permission to access the Internet. Choose Block or Pass by deciding which one will be more efficient in terms of the amount of input. For example, if most users will have access to the Internet, then use the Block screen to list the users who do not have access to the Internet (there will be fewer users to block).

Block Tab

The Block function filters by blocking packets from going **out** through the WAN port or coming **in** through the LAN port. To enable the Block IP filter function, select **Enable Block IP Filter Function**.

Pass Tab

The Pass function filters by defining which packets can go **into** your WAN port or come on to your LAN. To enable the Pass IP filter function, click the Pass tab and select **Enable Pass IP Filter Function**.

Packets Defined by …

TCP/IP – see Figure 1

IP Address – Enter the IP address of the packet to be Blocked or allowed to Pass.

Netmask – Enter the subnet mask for the packet.

TCP/IP Service Port – Enter the Port you would like to block or allow to pass (HTTP=80)

Privilege Level – It is already to leave this setting at the default. Level one is the highest level; level sixteen is the lowest privilege level.

User

User - Define the byte pattern of the packet(s). The RF500S uses the defined byte patterns to block or pass packets from the WAN or from the LAN.

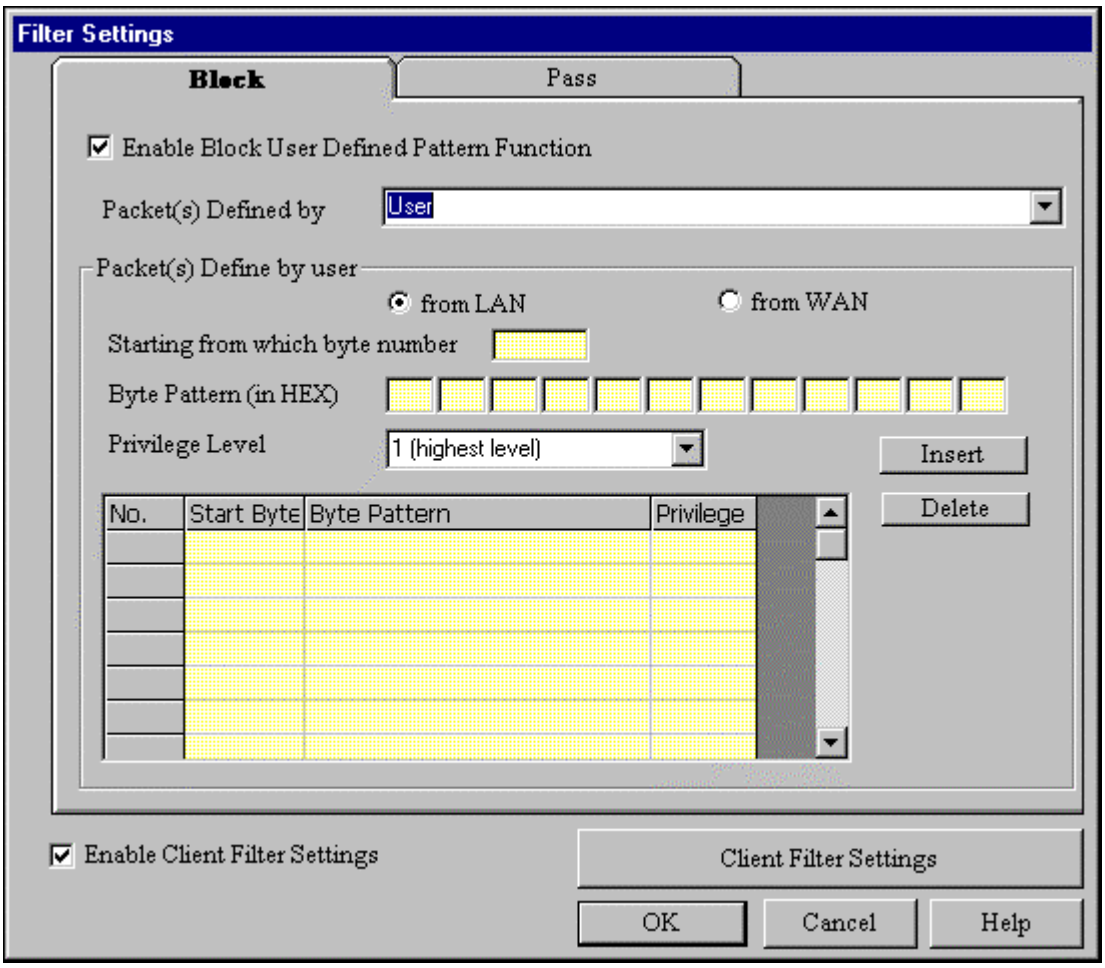


Figure 2 – Filter Settings (Packets Defined by User)

Select either **From LAN** or **From WAN**.

Starting from which byte number - Indicate the first byte in the packet the RF500S should read to determine if the byte pattern (in Hex) is one that should be filtered. Exclude the PPP header. Start from byte 0 of the network protocol.

Byte Pattern (in Hex) - Enter the packet byte pattern that the RF500S is to recognize as a filtered packet. (Block/Pass from the WAN to the LAN). Maximum pattern = 12 bytes.

Click **Insert** to add each IP address/byte pattern to the table.

To **Delete** a defined packet/byte pattern, select the entry in the table and click the **Delete** button.

Enable Client Filter Settings Button

The **Client Filter** allows you to decide which services are allowed into your network and which clients are authorized to access them. Check the radio buttons that apply to each filter.

How to Access this Screen

1. From the **Filter Settings** screen, check the **Enable Client Filter Settings** box.
2. Click **Client Filter Settings** button. The client **Filter Settings** screen displays.

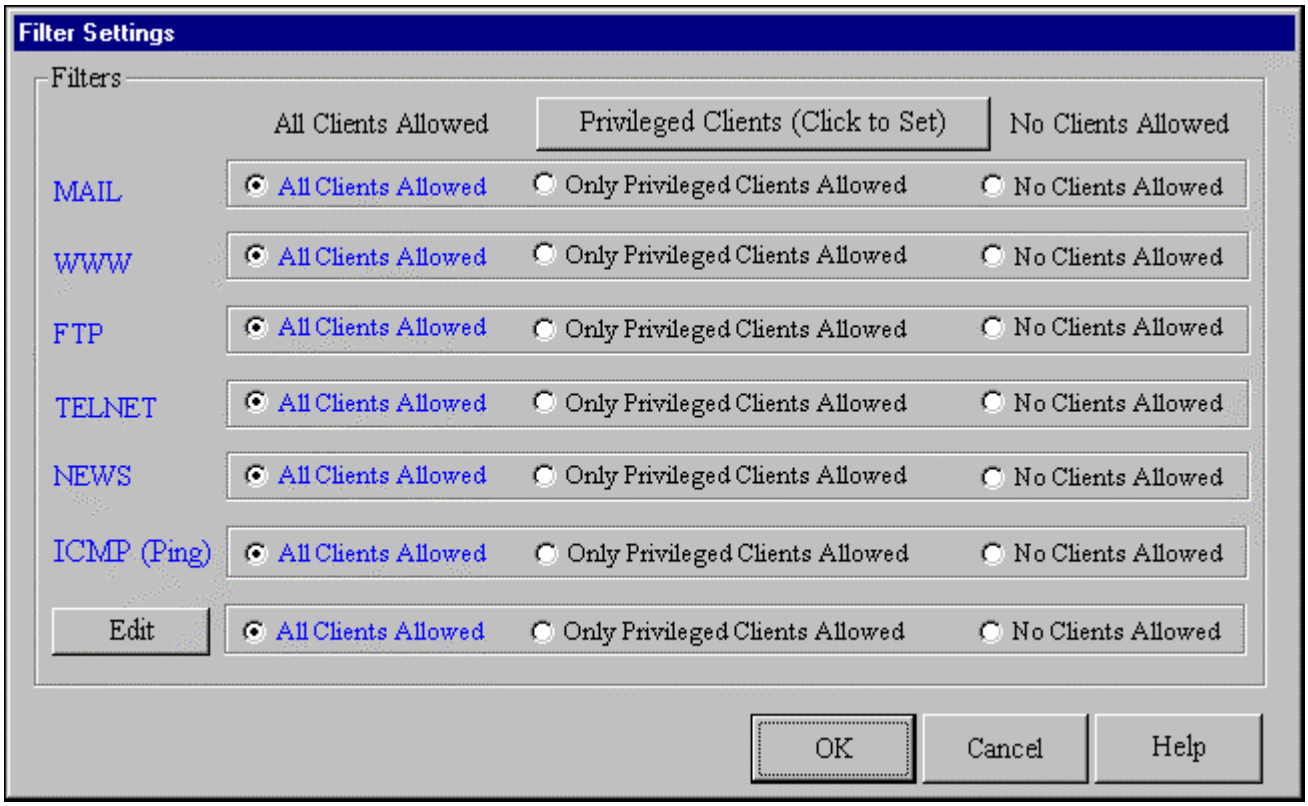


Figure 3 – Client Filter Settings

Privileged Clients

If you checked some **Only Privileged Clients Allowed** radio buttons in the client Filter Settings screen, you will have to enter the clients into the Privileged Client Table. Do this, by clicking the **Privileged Clients** button in the client Filter Settings screen. The Privileged Client Table displays.

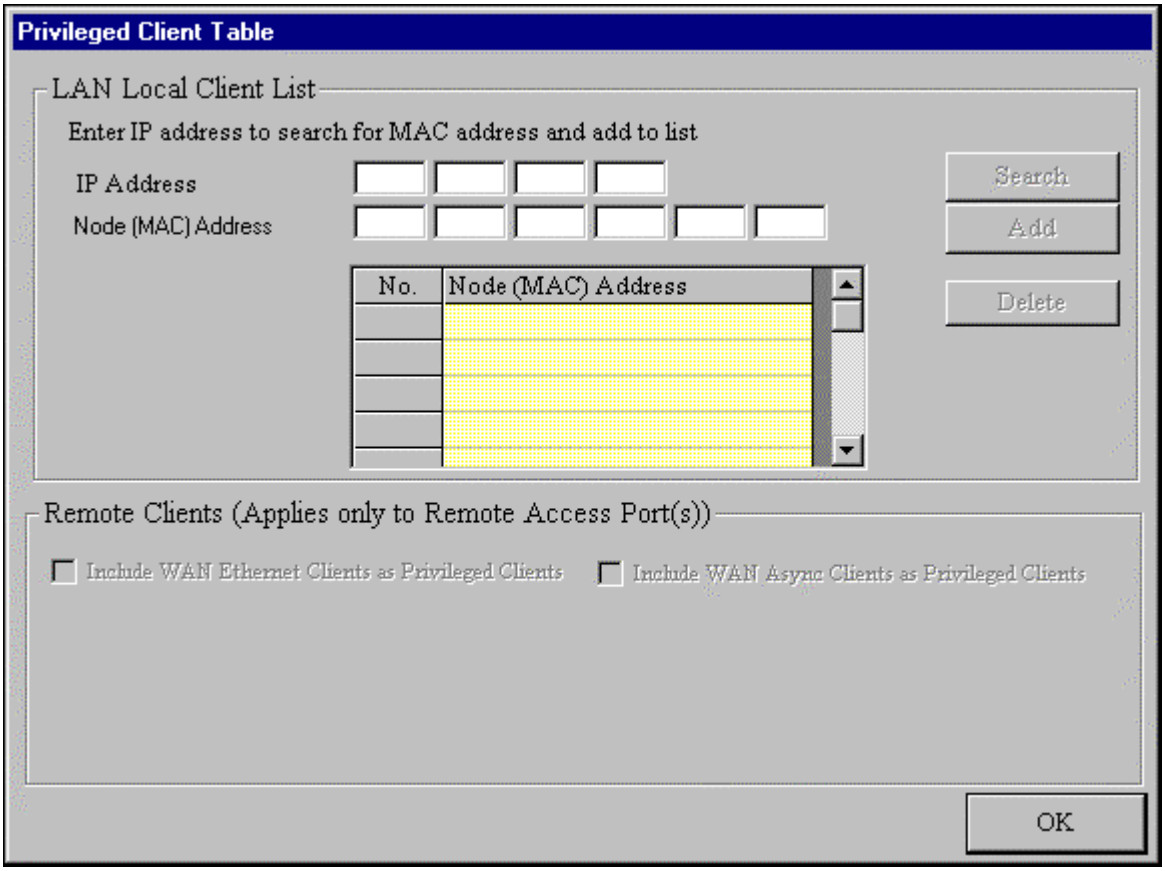


Figure 4 – Privileged Client Table

LAN Local Client List

In the Privileged Client Table, enter the clients you wish to have privileged access to the services that you have selected in the **Client Filter Settings** screen. The filter uses MAC addresses to identify the privileged clients. You can enter the MAC address directly or you can use the MAC address search tool by entering the IP address of the computer, then using the Search button to find the MAC address.

After completing the IP Address and MAC (Node) address, click the **Add** button to include the information in the Node (MAC) address list.

Remote Clients (Applies to Remote Access Ports)

Select **Include WAN Async Clients as Privileged Clients** or **Include WAN Ethernet Clients as Privileged Clients** to filter Remote Clients by the port they are coming in through.

Click **OK** when complete.

Edit Button Adds Filtering Port

The filter works by filtering TCP/IP ports numbers. The five most commonly used ports are listed for you. They include Mail, WWW, FTP, Telnet and News. If you would like to filter other services, you must know the port number for the service.

Click the **Edit** button to enter new service port numbers.

Enter the **TCP/UDP Port Number** and click the **Add** button.

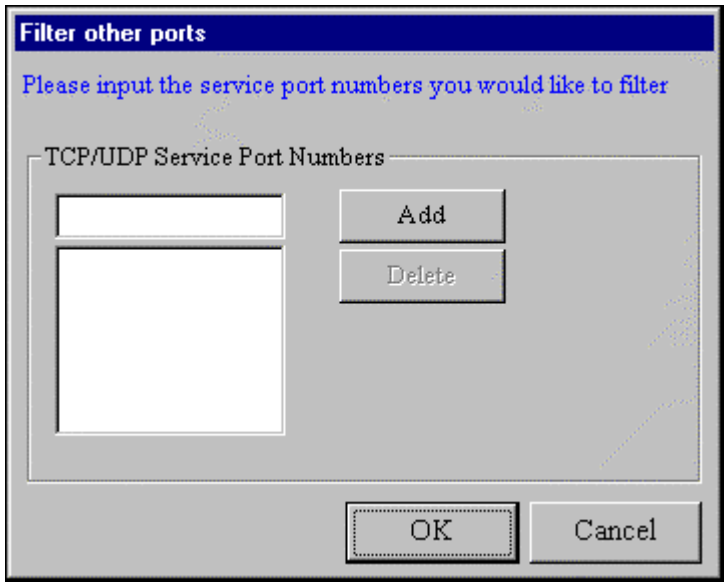


Figure 5 – Filter Other Ports

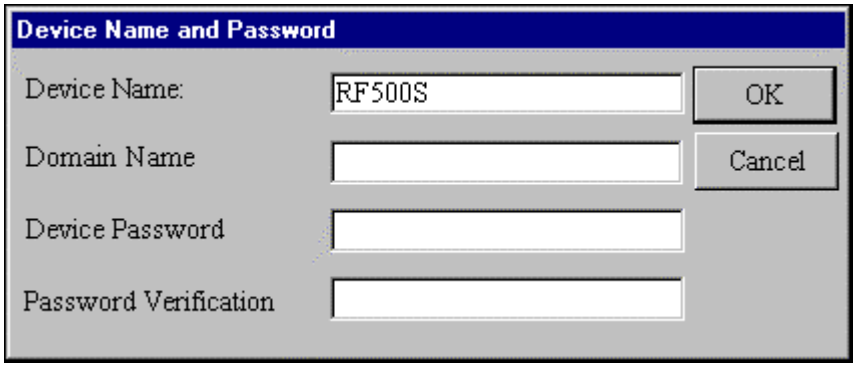
Refresh Device List

From the RouteFinder Manager main menu, click **Refresh Device List** to search the LAN for available network devices and display them in the **Available Devices** list. You will have to select your device from this before you can configure it.

Note: If a device does not appear in the list, click **Refresh Device List** again to determine if the device will appear on the list. If the device still does not appear, ensure that all cables are correctly connected and that the RF500S is powered on. If the device still does not appear in the list, refer to the Troubleshooting chapter of this User Guide.

Device Name and Password

From the RouteFinder Manager main menu, click the **Device Name and Password** button. You may use the default device name or use this screen to change the device name and/or add a password for your device.



Device Name

This field displays the name of your network device. To change the name, simply enter a new name in the field. If you are connecting to an ISP via cable modem or DSL, and your ISP requires you to enter a computer name, you may use the device name that you've entered on this screen.

Device Password

The RouteFinder manager does not come with a password enabled. If you choose to provide the device with a password, you will be prompted to enter the password each time you want to configure your network device. To enter a Password, type your password in the Device Password field, then re-enter your password in the Password Verification field.

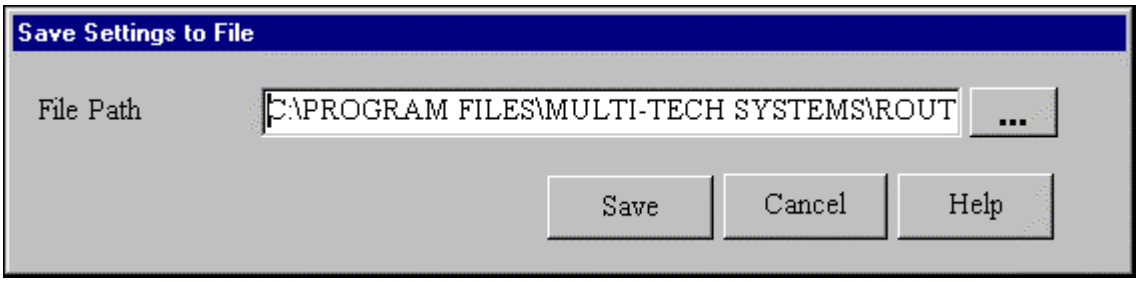
Note: If you choose to use a password, ensure you have selected something that will be easy to remember or write it down and store it in a safe location. If you have completely forgotten your password, contact the Multi-Tech Technical Support group for assistance. Refer to Chapter 10 in this User Guide for more information about our Technical Support services.

Save Settings to File

The **Save Settings to File** option allows you to save your configuration settings to a file. This option provides a method for backing up your system configuration so that it can be used in the event your settings become accidentally deleted. It can also be used if you would like to have more than one set of settings for your RouteFinder.

How to Access This Screen

1. From the RouteFinder Manager main screen, click the **Save Settings to File** button.
2. The Save Settings to File screen displays.



In the **File Path** field, enter a name for your file.

Note: Do not change the file type extension. If you try to use the Load Settings function, the Manager program will look for the specific file extension compatible with your device. For example, *.co1 is used only for 1 WAN port units, *.co2 is used only for 2 WAN port units.

The File Directory field displays the default path to the configuration files. You may save a copy of the file to a different location by changing the path in the File Directory field.

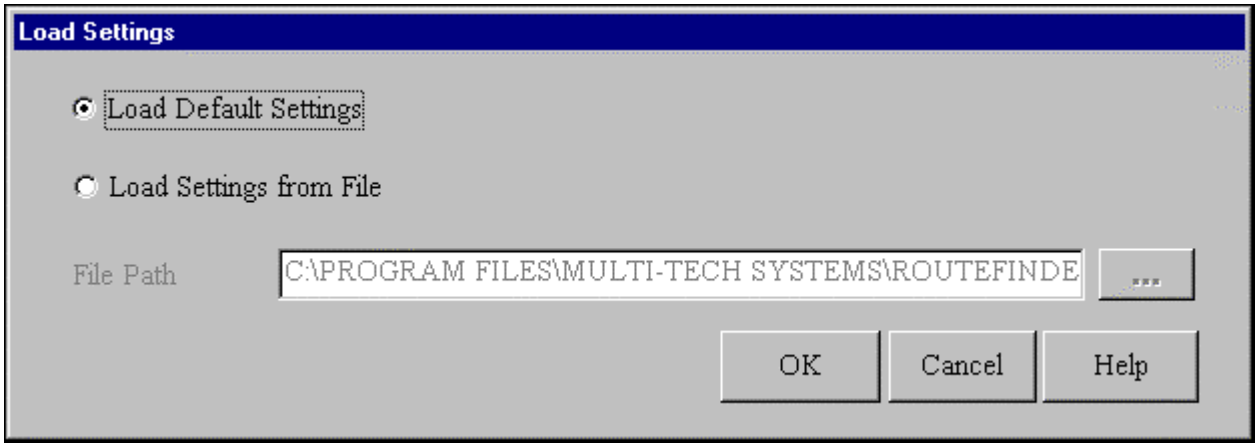
Click the **OK** button to save the settings to the specified file.

Load Settings

The **Load Settings** option allows you to load either the default settings of your network device or to load settings previously saved to a file.

How to Access This Screen

1. From the RouteFinder Manager main screen, click the **Load Settings** button.
2. The Load Settings screen displays.



Load Setting

To return the RouteFinder to factory default settings, select **Load Default Setting**.

To load a configuration from a file, select **Load Settings From File**.

Navigate to the file directory, and then click the **OK** button.

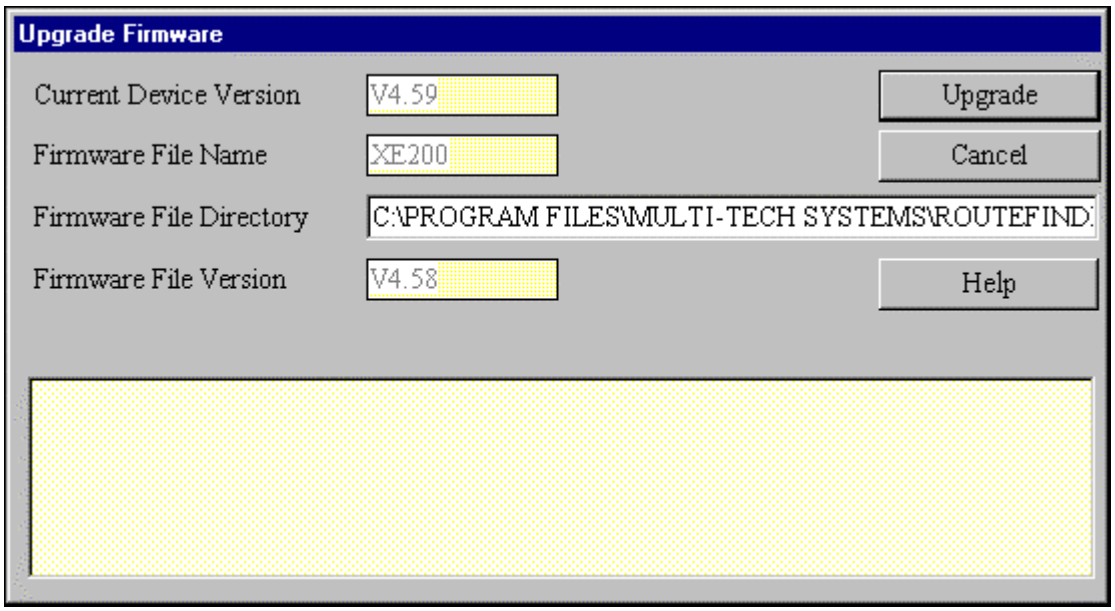
Upgrade Firmware

Warning: Upgrade the firmware of your RouteFinder RF500S only under the advice and direction of the Multi-Tech Technical Support Group. Improperly upgrading the RF500S may disable the device!

The Upgrade Firmware options allow you to upgrade your RF500S firmware. It upgrades the **firmware** of your RF500S, not the RouteFinder Manager or Monitor **software**.

How to Access This Screen

1. From the RouteFinder Manager main screen, click the **Upgrade Firmware** button.
2. The Upgrade Firmware screen displays.



To Upgrade Your Firmware

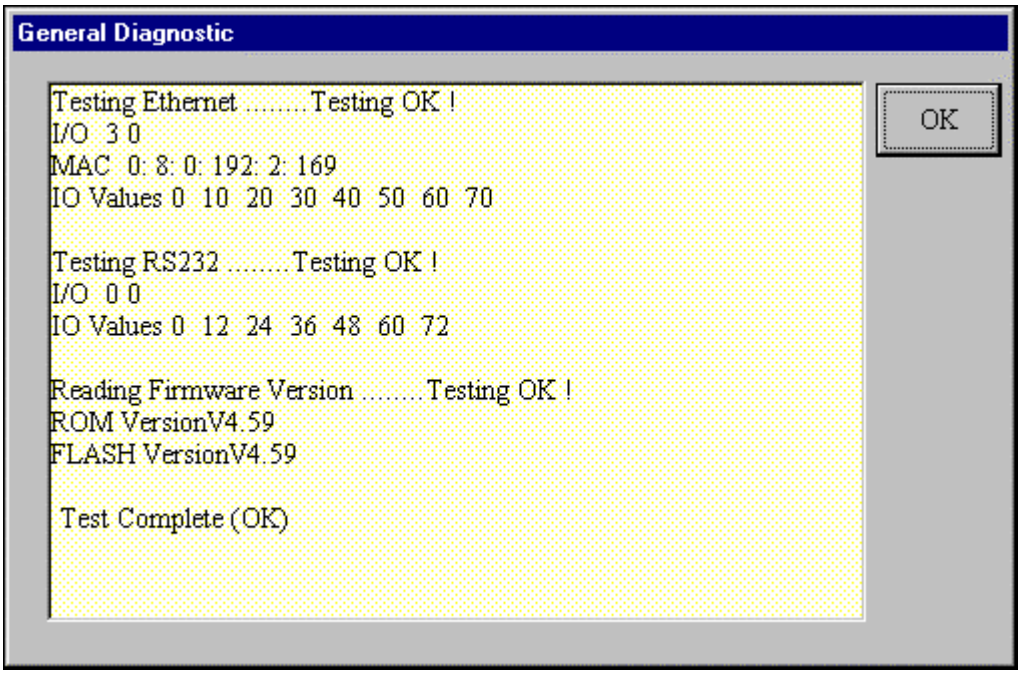
1. Download the latest firmware from the Multi-Tech System's web site at www.multitech.com.
2. Copy the firmware to the directory containing the RouteFinder Manager program files. Refer to the default Firmware File Directory field to determine the location of the files.
3. Enter the location of the new firmware file in the **Firmware File Directory** field. The RouteFinder Manager will automatically detect the new firmware file name and display it in the **Firmware File Name** field. The version number of your firmware will display in the **Firmware File Version** field.
4. Click the **Upgrade** button. A message appears stating the upgrade has started.
5. After several minutes, a message displays indicating the upgrade was successful.
7. Click **OK**.
8. From the RouteFinder Manager main screen, click **Save and Exit**.
9. Click **Yes** to restart the RouteFinder using the new firmware version.

General Diagnostic

When selected, the General Diagnostic option performs a check-up on your RF500S to make sure that everything is functioning properly.

How to Access This Screen

1. From the RouteFinder Manager main screen, click the **General Diagnostic** button.
2. The **General Diagnostic** screen displays information about the RF500S.



Chapter 6

RouteFinder Monitor

Chapter 6 - RouteFinder Monitor

RouteFinder Monitor is a software utility that provides both monitoring and troubleshooting functions for the RF500S.

How to Start the RouteFinder Monitor program.

1. Click on the RouteFinder Monitor icon on your desktop, or select **Start | Programs | RouteFinder Utilities | RouteFinder Monitor.**
2. The RouteFinder Monitor main screen displays. It opens on the TCP/IP Tab.

Note: If you receive a message stating "Device is not found", refer to the Troubleshooting chapter in this User Guide.

Event Messages are displayed in the lower half of the screen. Event Messages provide information about the communication occurring between your network device, ISDN TA/modem and the remote server (ISP).

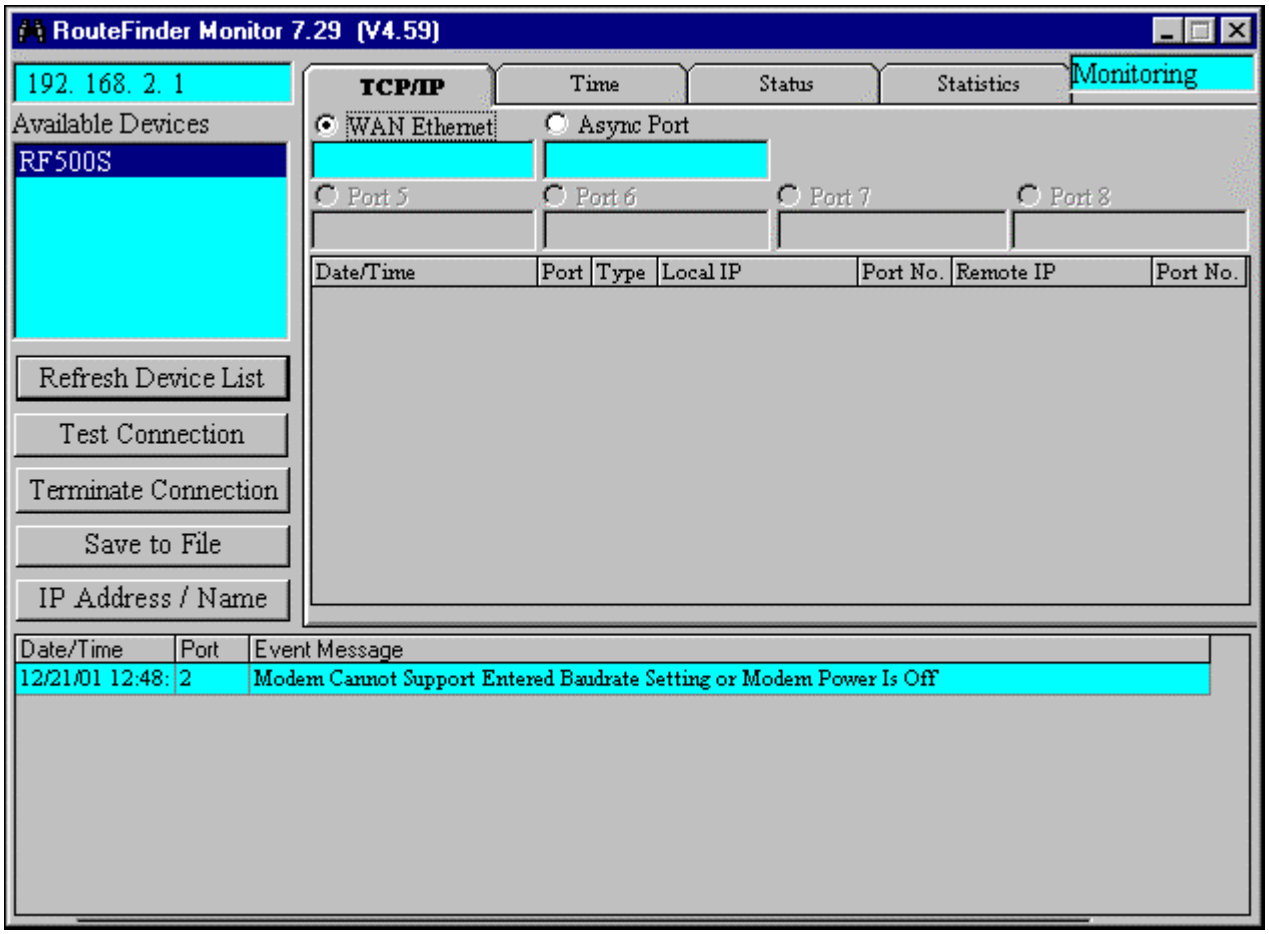
To assist you in troubleshooting, you may point and click on any event message to bring up a help screen.

RouteFinder Monitor TCP/IP Tab

The TCP/IP tab displays all TCP/IP requests made by your network device. You may select to view TCP/IP sessions for the **WAN Ethernet** or the **Async Port**.

The TCP/IP tab is the default tab displayed in the **RouteFinder Monitor** screen. If it is not displayed, click the TCP/IP tab.

Note: The TCP/IP sessions displays the history of the TCP/IP session through the selected port. The TCP/IP information presented does **not** represent the current status of the TCP/IP session.



TCP/IP Tab Information

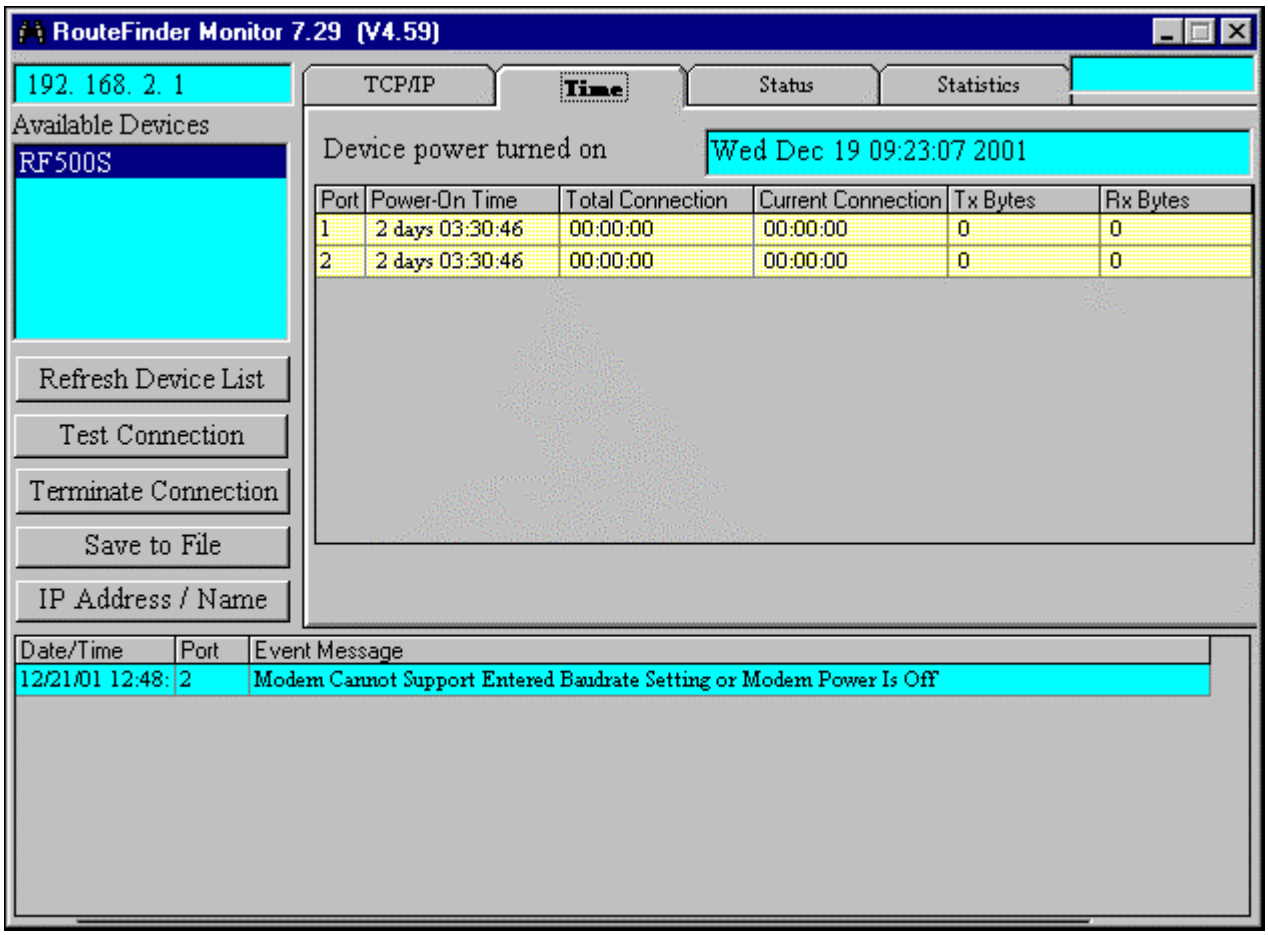
Date/Time: Indicates the date the request was made.
Port: Indicates the port you are viewing.
Type: Displays the type of request being made.
Local IP: Indicates which IP address you have requested information from.
Remote IP: Indicates which IP address was requested.
Port Number: Indicates which TCP/IP port was requested.

RouteFinder Monitor Time Tab

The Time Tab displays information about the device since it was last powered on.

How to Access This Screen

1. From the RouteFinder Monitor main screen, click the **Time** tab.
2. The **Time** tab displays information for each port.



Device Power Turned On – The time/date that your RF500S was powered on.

Power-On Time – The total time elapsed since the RF500S was powered on.

Total Connection Time – The total connection time for each port that has been logged on since the RF500S was powered on.

Current Connection – The time elapsed since the current connection was established.

TX Bytes – The total number of bytes transmitted for each port since the RF500S was last powered on.

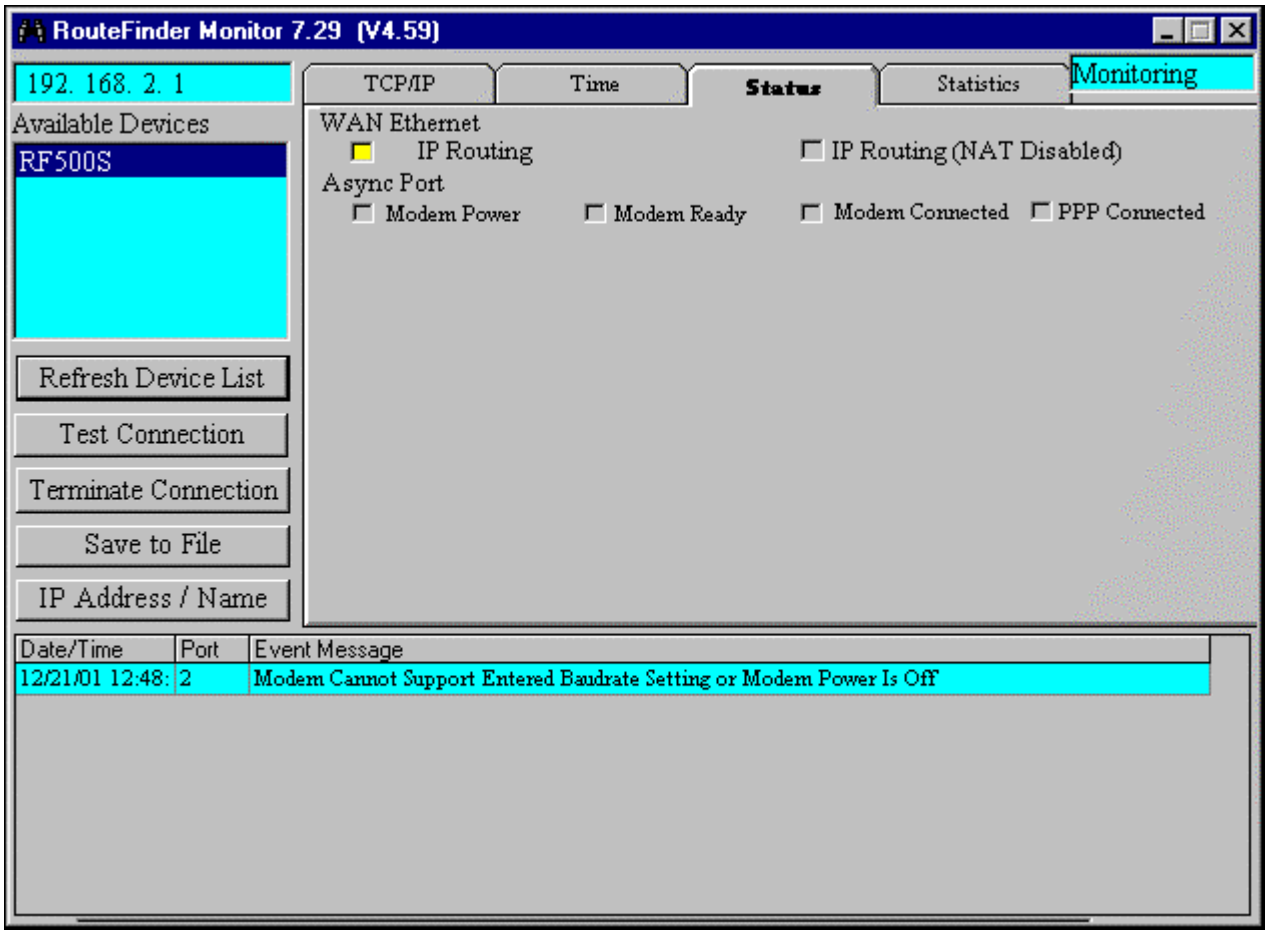
RX Bytes – The total number of bytes received for each port since the RF500S was last powered on.

RouteFinder Monitor Status Tab

The **Status tab** provides status information about of the **WAN Ethernet** and **Async** ports.

How to Access This Screen

1. From the RouteFinder Monitor main screen, click the **Status** tab.
2. The **Status** tab displays the status for each port.



WAN Ethernet

This indicator light shows which function is in use: **IP Routing** or **Remote Access.**

Async Port

Modem Power - The indicator light is lit when the modem power is turned on.

Modem Ready - The Network Device sends a pre-initialization and initialization command to the modem or ISDN TA. If this communication is successful, the indicator light will be lit, indicating your modem is ready to make a connection.

Modem Connected - If the Network Device has detected that your modem has successfully dialed up a connection to a remote site, the indicator light will be lit.

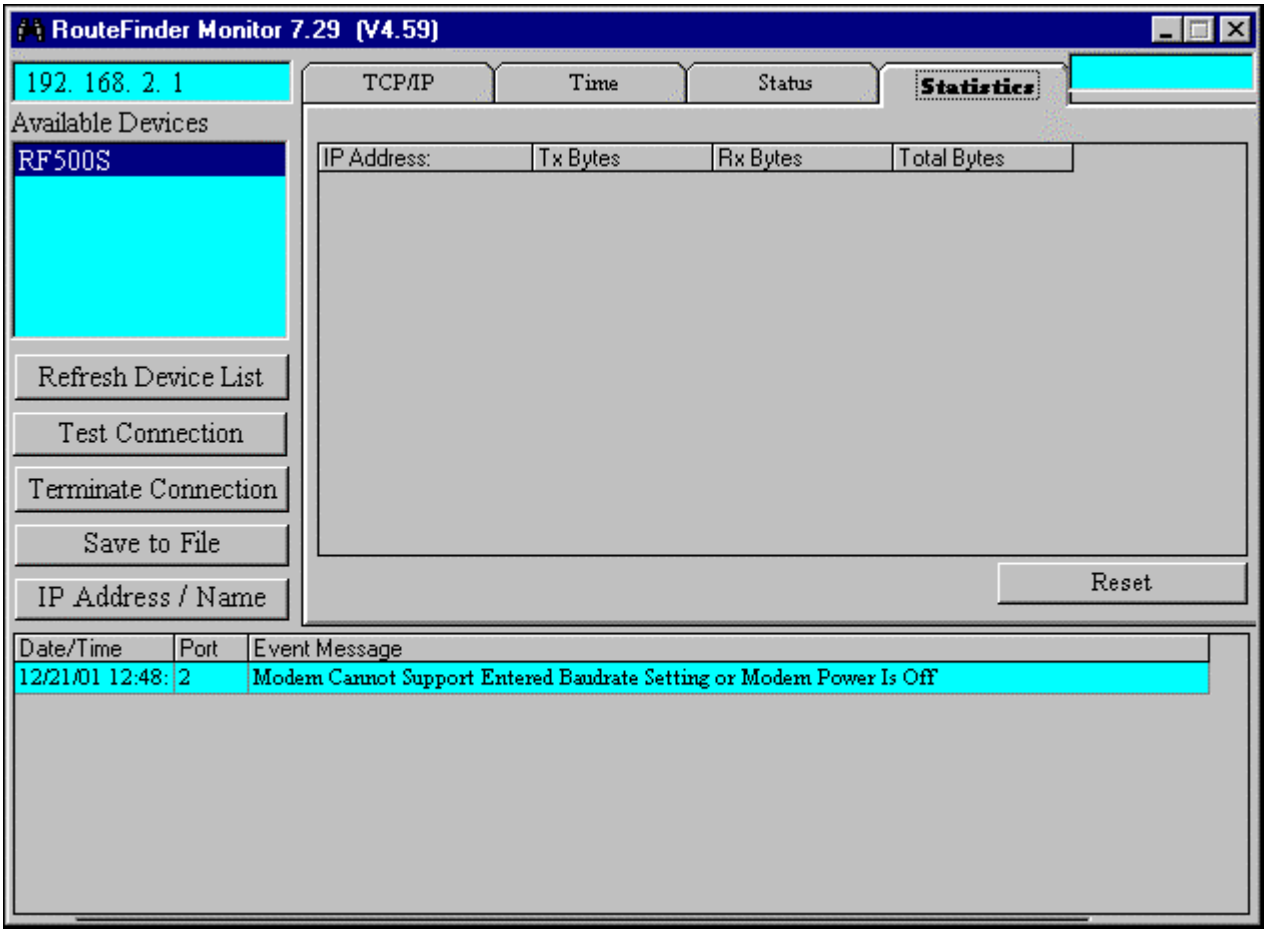
PPP Connected - After a connection is established, if the RouteFinder has detected that the PPP connection is successful, this indicator light will be lit.

RouteFinder Monitor Statistics Tab

The Statistics tab indicates, by port, how many bytes of data have come in and out through the RouteFinder.

How to Access This Screen

1. From the RouteFinder Monitor main screen, click the **Statistics** tab.
2. The **Statistics** tab displays the information for each IP Address.



IP Address Information

IP Address - The IP address of the network device.

Tx Bytes - The number of bytes transmitted from the PC with this IP address.

Rx Bytes - The number of bytes received from the PC with this IP address.

Total Bytes - The total number of bytes received and transmitted from the PC with this IP address.

Reset Button

Use the Reset button to set the IP statistics to zero.

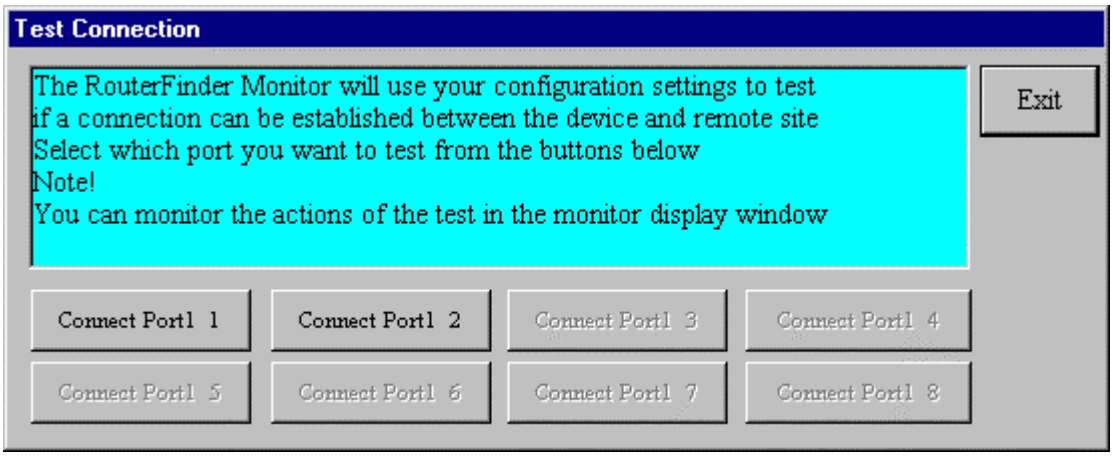
RouteFinder Monitor Main Screen Buttons

Refresh Device List Button

Click **Refresh Device List** button from the RouteFinder Monitor main screen to re-display a list of network devices in the **Available Devices** window.

Test Connection Button

Click the **Test Connection** button to run a test of your connection settings. This test can assist you in determining if problems are due to the modem, the RouteFinder, or an incorrect setting. **Test Connection** uses the attached modem(s) to dial-up the remote server (ISP) and establish a connection.

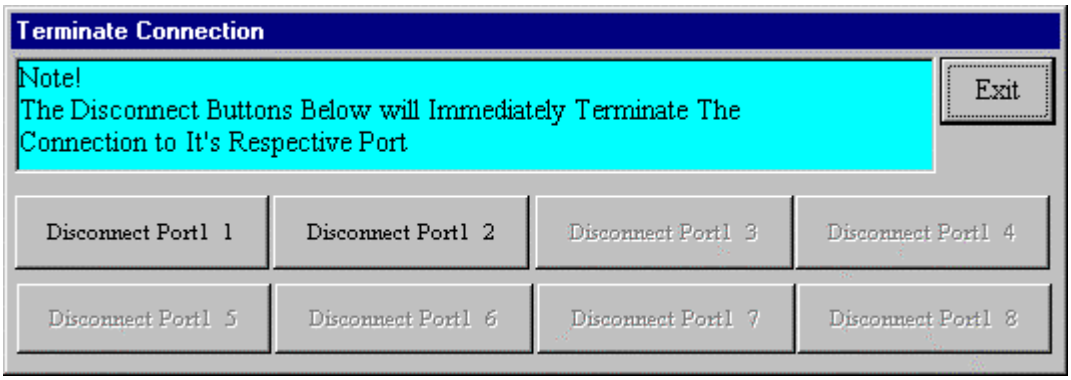


Select **Connect Port 1** to test the WAN connection, or select **Connect Port 2** to test the Async connection. The results of the test are displayed in the text box of this screen.

Click **Exit** to close the Test Connection screen.

Terminate Connection Button

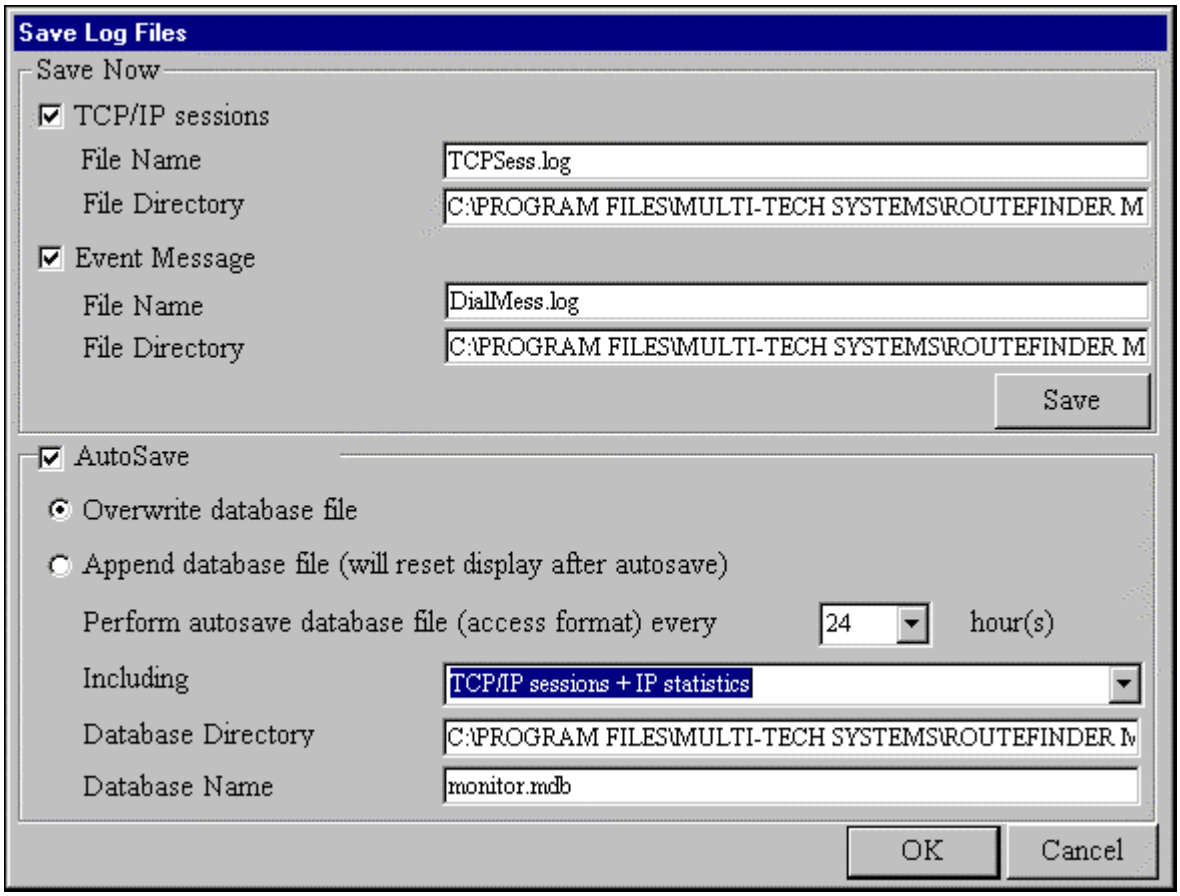
The **Terminate Connection** option is designed to allow the Network Administrator to terminate an RF500S connection instantly.



Select **Disconnect Port 1** or **Disconnect Port 2**, and then click the **Exit** button.

Save to File Button

Click **Save to File** button to save a monitoring session to a file. This feature can be used to create an event log to send to our Technical Support group for evaluation.



Save Now - If you want to save the monitor display at any point in time, select the monitor you'd like to save to a file (TCP/IP, Event Message, etc.) Select the **File Name** and **File Directory** to which you'd like to save the file and click **Save**.

Autosave - If you wish to automatically save the information displayed on the monitor to a database file, enable the AutoSave function. Options for this function include:

Overwrite database file - Saves the information collected by the monitor to a database file based on the time interval that you specify, overwriting the last saved database file.

Append Database file - Saves the information collected by the monitor to a database file based on the time interval that you specify, updating and appending to the file.

Note: The Append Database file option will reset the monitor and clear the screens after the autosave has appended the information to the file.

Warning: The database size limit is equal to the amount of available disk space. Use this option with caution!

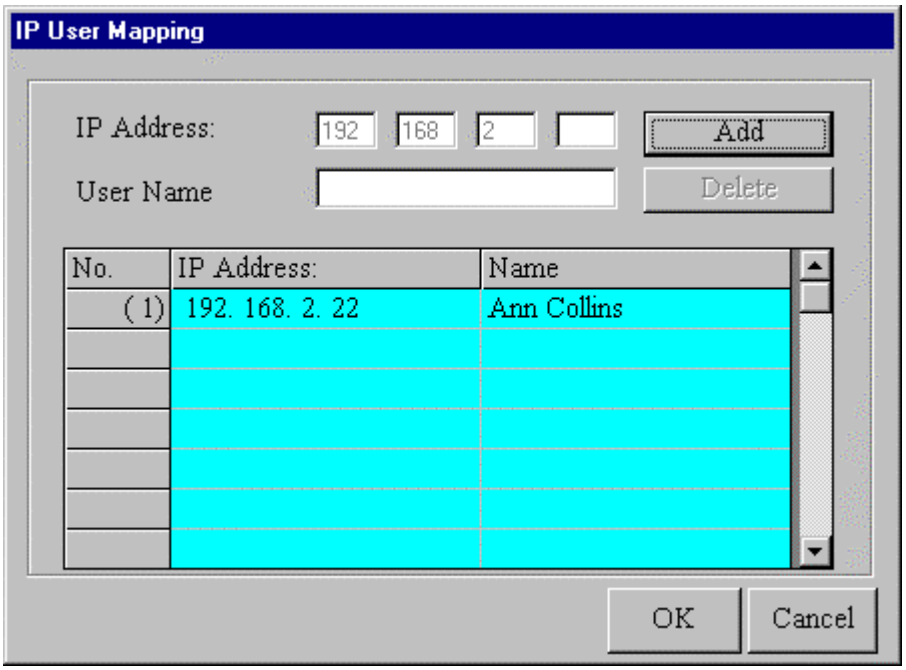
Click **OK** when complete.

IP Address/Name

The IP Address/Name function allows you to associate a name with a particular IP address and name on your network. his information will appear in the relevant monitor displays. The IP Address/Name option is used to assist the Network Administrator in determining which users are transmitting and receiving data without having to remember their specific IP addresses.

Each computer listed must have a fixed IP address for your network. You may configure a fixed IP address on the individual computer or use the RF500S's DHCP server IP reservation system (refer to the LAN DHCP section of RouteFinder Manager chapter of this User Guide).

When you click the **IP Address/Name** button, the **IP User Mapping** screen displays.



Enter each computer's IP Address and associated User Name in the provided fields.

Click **Add** after each IP address and name have been added to the list.

When all addresses have been added, the click **OK** button.

RouteFinder™

Chapter 7

Troubleshooting

MultiTech® Systems

Chapter 7 - Troubleshooting

This chapter provides a list of common problems encountered while installing, configuring or administering the RF500S. In the event you are unable to resolve your problem, refer to the Service, Warranty and Technical Support chapter of this User Guide for information about contacting our Technical Support representatives.

Problem #1

My computer can't detect my RouteFinder on the LAN when I start one of the RouteFinder Utilities (i.e. Device Not Found).

- Try pressing the Refresh Device List button.
- Unplug your network device and plug it back in, then press Refresh Device List.
- Ensure your computer has TCP/IP properly configured. You can check this by trying to "ping" the computer you are using. If you can successfully ping the computer from itself, the computer has TCP/IP correctly installed. Once you determine that you are able to ping the computer, try to ping another computer in the same segment of your network. If this ping is successful, your computer is properly connected to the network.
- Remove the TCP/IP Dial-up Adapter from your computer. For instructions, see Problem #2 in this section.
- Ensure your network device is properly connected to your Ethernet hub by pressing Refresh Device List in either RouteFinder Manager or RouteFinder Monitor. If your RouteFinder is correctly connected, the *WAN* indicator light on your RouteFinder will flash. If no flash occurs, it is not properly connected to the network. Reconnect your network device to the hub and try again. If there is still no flash, it is possible the Ethernet cable or hub has a problem.

Problem #2

Other computers can connect to the network device, but my computer can't.

Whenever I click on Internet Explorer or Netscape, I see the Windows Dial-up utility popping up on my screen asking for my phone number and password to dial-up my ISP.

- Remove the TCP/IP dial-up adapter from all computers that will be using your RouteFinder to access the Internet. TCP/IP dial-up adapter is not needed to use the RF500S to connect to the Internet.
  1. To remove the Dial-up Adapter, click Start | Settings | Control Panel.
  2. Double-click the Network icon.
  3. Click the Dial-up Adapter and press Remove. Restart the computer and try again.
- Ensure you have a correct IP address. From a DOS window in Windows 95/98, type winipcfg. From Windows NT, type ipconfig. If the address field is listed as 0.0.0.0, the computer does not have an IP address and you must ensure the automatic DHCP configuration has been correctly set up for this computer.
- Ensure that the Web browser is properly configured to connect to the Internet via the LAN.

Problem #3

The RouteFinder is connected to the Cable/DSL, but has problems accessing the Internet.

- Ensure the workstation has TCP/IP properly configured.
- Attempt to ping the IP address of the RF500S.
- Use RouteFinder Monitor to see if the WAN Ethernet port has successfully acquired a dynamic IP address from the ISP, or if the static IP address is valid.
- Use Winipcfg (Windows 95/98) or ipconfig (Windows NT/ 2000) to check to see if the computer's IP settings are correct.
- Ensure the DNS settings are correct.
- Ensure the Gateway IP address is the device's LAN Ethernet IP address (Server IP address).
- Ensure the IP address Netmask is correct.

Problem #4

When I install the RouteFinder Utilities, I get the error message "missed export file oleaut32.dll"

If you are using Windows 95/98, your computer has an old version of oleaut32.dll.

- Download the newest version of oleaut32.dll from the Microsoft web site (http://www.microsoft.com).
- Create a backup of the file c:\windows\system\oleaut32.dll.
- Copy the new file to c:\windows\system\oleaut32.dll.
- After you have successfully copied the file, reinstall the RouteFinder Utilities.
- If you have problems with the new oleaut.dll file, use the backup file.

Problem #5

I configured my RouteFinder but I can't get it to communicate with my modem.

- Check your initialization string. If you are using an ISDN TA and your ISDN TA was not listed as a choice in Setup Wizard, refer to the ISDN TA User Guide for the appropriate initialization string.
- After ensuring that the initialization string is correct, use the on-line help in RouteFinder Monitor.

Problem #6

My RouteFinder dials-up a connection, but can't seem to communication with the ISP.

- Verify that your baud rate is not set too high for your modem or ISDN TA. The maximum baud rate that your modem or ISDN claims it can achieve may not be attainable due to poor line or connection quality. Use RouteFinder Manager's Modem settings menu to correct set the baud rate to a lower rate and retry the connection.
- After lowering the baud rate, you are still not able to establish a connection, use the RouteFinder Monitor's on-line help. If your connection still doesn't work, contact your ISP.

Problem #7

Sometimes when I try and use the Internet or get my mail, the application can't connect to the Internet immediately.

- The most common reason for this is not due to a problem or error. If you are the first person to make a connection to the Internet through the RF500S, there will be a delay when the Dial-On-Demand function automatically makes the connection and logs on to your ISP. Subsequent users will be able to use the connection you've established without a delay.
- If the scenario described above does not fit your situation, use RouteFinder monitor to view all events that are taking place between the modem and your ISP as you attempt to make a connection (e.g., a busy signal).

Problem #8

After installing my RF500S, my modem connection seems to be slower.

- The RouteFinder device should have no effect on the modem speed. However, if more than one client is using the same modem through the RouteFinder, the speed will be reduced.
- Run RouteFinder Monitor to view the number of concurrent client connections to your ISP.

Problem #9

While the Serial async port is in use, my RF500S keeps dialing a connection to the Internet, but no one is using the Internet.

- The RF500S will only dial the connection if there is a request from one of the computers on the LAN for an IP address on the Internet. Keep in mind that certain applications can be configured to request information from the Internet. For example, Microsoft Outlook can be set up to "check for new mail every x minutes". If this feature is enabled, Outlook will send a request for your Internet POP3 server which will cause your RF500S to dial-up your ISP. To determine which computer on your network is processing a request for an Internet connection, use the RouteFinder Monitor. The event messages will provide information about which computer is causing the RF500S to dial and which service (port #) the computer is requesting.

Problem #10

The "Please set the Device IP" screen displays when configuring the RF500S.

- This system detects that the RouteFinder's LAN Ethernet IP address is not in the same subnet as the PCs. Use RouteFinder Manager to set the RouteFinders' IP address to the same network as your PC's.

Problem #11

A message appears indicating the IP address you have inputted is either not valid on your network or is in conflict with another IP address.

- The manager has detected the IP address of the RF500S you are configuring is in conflict with another device. Power off the conflicting device and configure the RF500S using a different Ethernet LAN IP address.

Chapter 8

Frequently Asked Questions

Chapter 8 – Frequently Asked Questions

1. Where is the Cable/DSL Router installed on the network?

In a typical environment, the Router is installed between the Cable/DSL Modem and the LAN. Plug the Cable/DSL Router into the Cable/DSL Modem's Ethernet port.

2. Does the Cable/DSL Router support IPX or AppleTalk?

No. TCP/IP is the only protocol standard for the Internet and has become the global standard for communications. IPX, a NetWare communications protocol used only to route messages from one node to another, and AppleTalk, a communications protocol used on Apple and Macintosh networks, can be used from LAN to LAN connections, but those protocols cannot connect from WAN to LAN.

3. Does the WAN connection of the Cable/DSL Router support 100Mbps Ethernet?

Because of the speed limitations of broadband Internet connections, the Cable/DSL Router's current hardware design supports 10Mb Ethernet on its WAN port. It does, of course, support 100Mbps over in the auto-sensing Fast Ethernet 10/100 switch on the LAN side of the router.

4. What is Network Address Translation and what is it used for?

Network Address Translation (NAT) translates multiple IP addresses on the private LAN to one public address that is sent out to the Internet. This adds a level of security since the address of a PC connected to the private LAN is never transmitted on the Internet. Furthermore, NAT allows the Cable/DSL Router to be used with low cost Internet accounts, such as DSL or cable modems, where only one TCP/IP address is provided by the ISP. The user may have many private addresses behind this single address provided by the ISP.

5. Does the Cable/DSL Router support any operating system other than Windows 95, Windows 98, Windows 2000, or Windows NT?

Yes, but Multi-Tech does not, at this time, provide technical support for setup, configuration or troubleshooting of any non-Windows operating systems.

6. What is DMZ?

Demilitarized Zone (DMZ) allows one IP Address (computer) to be exposed to the Internet. Some applications require multiple TCP/IP ports to be open. DMZ allows just one computer to be exposed for that purpose. It is recommended that you set your computer with a static IP if you want to use DMZ.

7. If DMZ is used, does the exposed user share the public IP with the Router?

No.

8. How can I play Internet games (i.e., Ages of Empire) with the router?

Enable DMZ in "Advanced Features" of the web configuration screen. For example, if your computer's IP address is 192.168.1.102, enter the last three digits, or "102", in the DMZ field. You may also try using the port forwarding option instead of using DMZ.

9. **Does the Router pass PPTP packets or actively route PPTP sessions?**
   The Router lets PPTP packets pass through.

10. **What is the maximum number of users supported by the Router?**
    The Router supports up to 253 users.

11. **Is the Router cross-platform compatible?**
    Any platform that supports Ethernet & TCP/IP is compatible with the router.

12. **Will the Router function in a Mac environment?**
    Yes, but Multi-Tech does not provide upgrade programs for the Macintosh. However, you may be able to find some software that uses TFTP for your Macs.

13. **Will the Router allow you to use your own public IPs and Domain, or do you have to use the IPs provided by the router?**
    The router mode allows for customization of your public IPs and Domain.

14. **How many ports can be simultaneously forwarded?**
    Theoretically, the Router can establish 520 sessions at the same time, but you can only forward 10 ports.

15. **Can multiple gamers on the LAN get on one game server and play simultaneously with just one public IP address?**
    It depends on which network game or what kind of game server it is. For example, Unreal Games support multi-login with one public IP.

16. **Does the Router replace a modem? That is, is there a cable or DSL modem in the router?**
    No. The Router must work in conjunction with a cable or DSL modem.

17. **Which modems are compatible with the router?**
    The Router is compatible with any cable or DSL modem that supports Ethernet.

18. **What are the advanced features of the Router?**
    The Router's advanced features include asynchronous port dial-up backup, VPN pass through, Hacker attack logging, Virtual server

19. **What is the maximum number of VPN sessions allowed by the router?**
    Only one VPN session at a time.

20. **How do I access the Router's setup pages with a Mac?**
    The router's setup pages are accessible to the Mac through a Telnet Session. Use the default address 192.168.2.1.

21. **Can I choose whether to use UDP or TCP on the Router's ports?**
    No, the Router does not have this feature. UDP and TCP are both automatically activated at the same time when the Router's service ports are specified to be opened.

22. Does Multi-Tech provide syslog support?

At this time, Multi-Tech does not support syslog.

23. How can I check whether I have static or DHCP (dynamic) IP addresses?

Consult your ISP to confirm this data.

24. Does the Router support PPP over Ethernet (PPPoE)?

Yes, the router does support PPPoE.

25. Why does the Router not obtain the IP address assigned by my ISP?

- Make sure that your cable or DSL modem is connected properly.
- Try resetting your cable or DSL modem by powering the modem off and on.
- If you are using dynamic IP addressing, make sure that your cable or DSL modem is DHCP- capable.
- Some ISPs require a MAC address to be registered with them.

26. If all else fails in the installation, what can I do?

- Reset your cable modem or DSL modem by powering the unit off and on.
- Obtain the latest release of firmware on the RF500S at www.multitech.com
- Reset the Router's factory default by holding down the reset button for at least 3 seconds.
- Flash the firmware again to the Router, to ensure that it was successfully written to the unit.

27. How will I be notified of new router firmware upgrades?

All Multi-Tech firmware upgrades are posted on the Multi-Tech Web site at www.multitech.com, where they can be downloaded for free.

Your Router does NOT need the latest firmware upgrade if your Internet connection is already successful, as firmware upgrades will not increase your connection speed or enhance your Router's performance.

28. Does the Router support IPsec?

The RF500S supports IPsec Pass Through.

29. What type of firewall is the router equipped with?

The Router uses NAT.

30. I am not able to get my e-mails or my ISP web page (e.g., http://www.isp.com/). What can I do?

Contact the ISP to get the full URL, or you can do the following:

1. Connect one of the computers directly to the cable modem or DSL modem.
2. Open a command prompt and ping the ISP web server or mail server name given. For example, at the command prompt, type in ping www and press Enter. You should be able to get an IP address when it responds.
3. After you get the IP address, enter the IP address on the mail server option.

Appendixes

Appendix A – Warranty, Service, and Technical Support

This chapter is divided into three parts covering the Multi-Tech product warrant, Multi-Tech's Service, and Multi-Tech's Technical Support.

Multi-Tech Systems, Inc. Warranty & Repairs Policies

Warranty

Multi-Tech Systems, Inc., (hereafter "MTS") warrants that its products will be free from defects in material or workmanship for a period of two, five, or ten years (depending on model) from date of purchase, or if proof of purchase is not provided, two, five, or ten years (depending on model) from date of shipment.

MTS MAKES NO OTHER WARRANTY, EXPRESS OR IMPLIED, AND ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE HEREBY DISCLAIMED.

This warranty does not apply to any products which have been damaged by lightning storms, water, or power surges or which have been neglected, altered, abused, used for a purpose other than the one for which they were manufactured, repaired by Customer or any party without MTS's written authorization, or used in any manner inconsistent with MTS's instructions.

MTS's entire obligation under this warranty shall be limited (at MTS's option) to repair or replacement of any products which prove to be defective within the warranty period or, at MTS's option, issuance of a refund of the purchase price. Defective products must be returned by Customer to MTS's factory – transportation prepaid.

MTS WILL NOT BE LIABLE FOR CONSEQUENTIAL DAMAGES, AND UNDER NO CIRCUMSTANCES WILL ITS LIABILITY EXCEED THE PRICE FOR DEFECTIVE PRODUCTS.

Repair Procedures for U.S. and Canadian Customers

In the event that service is required, products may be shipped, freight prepaid, to our Mounds View, Minnesota factory:

Multi-Tech Systems, Inc.
2205 Woodale Drive
Mounds View, MN 55112
Attn: Repairs, Serial # _____

A Returned Materials Authorization (RMA) is not required. Return shipping charges (surface) will be paid by MTS.

Please include, inside the shipping box, a description of the problem, a return shipping address (must have street address, not P.O. Box), your telephone number, and if the product is out of warranty, a check or purchase order for repair charges.

For out of warranty repair charges, go to www.multitech.com/documents/warranties

Extended two-year overnight replacement service agreements are available for selected products. Please call MTS at (888) 288-5470, extension 5308 or visit our web site at http://www.multitech.com/programs/orc/ for details on rates and coverage's.

Please direct your questions regarding technical matters, product configuration, verification that the product is defective, etc., to our Technical Support department at (800) 972-2439 or email tsupport@multitech.com. Please direct your questions regarding repair expediting, receiving, shipping, billing, etc., to our Repair Accounting department at (800) 328-9717 or (763) 717-5631, or email mtsrepair@multitech.com.

Repairs for damages caused by lightning storms, water, power surges, incorrect installation, physical abuse, or user-caused damages are billed on a time-plus-materials basis.

Repair Procedures for International Customers (Outside U.S.A. and Canada)

Your original point of purchase Reseller may offer the quickest and most economical repair option for your Multi-Tech product. You may also contact any Multi-Tech sales office for information about the nearest distributor or other repair service for your Multi-Tech product.

http://www.multitech.com/COMPANY/offices/DEFAULT.ASP

In the event that factory service is required, products may be shipped, freight prepaid to our Mounds View, Minnesota factory. Recommended international shipment methods are via Federal Express, UPS or DHL courier services, or by airmail parcel post; shipments made by any other method will be refused. A Returned Materials Authorization (RMA) is required for products shipped from outside the U.S.A. and Canada. Please contact us for return authorization and shipping instructions on any International shipments to the U.S.A. Please include, inside the shipping box, a description of the problem, a return shipping address (must have street address, not P.O. Box), your telephone number, and if the product is out of warranty, a check drawn on a U.S. bank or your company's purchase order for repair charges. Repaired units shall be shipped freight collect, unless other arrangements are made in advance.

Please direct your questions regarding technical matters, product configuration, verification that the product is defective, etc., to our Technical Support department nearest you or email tsupport@multitech.com. When calling the U.S., please direct your questions regarding repair expediting, receiving, shipping, billing, etc., to our Repair Accounting department at

+(763) 717-5631 in the U.S.A., or email mtsrepair@multitech.com.

Repairs for damages caused by lightning storms, water, power surges, incorrect installation, physical abuse, or user-caused damages are billed on a time-plus-materials basis.

Repair Procedures for International Distributors

Procedures for International Distributors of Multi-Tech products are on the distributor web site.

http://www.multitech.com/PARTNERS/login/

10-Sep-01

Technical Support

Multi-Tech provides free technical support for as long as your product remains in service. Before calling Technical Support, please read through the Troubleshooting chapter of this User Guide. Fill out the **Recording RouteFinder Information** section below.

Contact our Technical Support group using one of the following contact options.

Contacting Technical Support

Country	Using Email	By Phone
France	support@multitech.fr	+(33) 1-64 61 09 81
India	support@multitechindia.com	+(91) 124-340778
U.K.	support@multitech.co.uk	+(44) 118 959 7774
Rest of World	support@multitech.com	800-972-2439 (U.S. & Canada) or +763-785-3500

Recording RouteFinder Information

Before placing a call to our Technical Support staff, record the following information about your Multi-Tech RouteFinder.

Model no.: _____

Serial no.: _____

Firmware version:_____

Software version: _____

Note the status of your RouteFinder in the space provided before calling tech support. Make certain to include screen messages, diagnostic test results, problems with a specific application, etc.

_____

_____

_____

On-line Warranty Registration

If you have access to the World Wide Web, you can register your Multi-Tech product online at the following URL: http://www.multitech.com/register

Multi-Tech on the Internet

Multi-Tech System, Inc. maintains a Web and an FTP site at: http://www.multitech.com and ftp://ftp.multitech.com

Ordering Accessories

SupplyNet, Inc. can provide you with replacement transformers, cables and connectors for select Multi-Tech products. Contact SupplyNet via mail, phone, fax or the Internet at:

Mail: SupplyNet, Inc.
614 Corporate Way
Valley Cottage, NY 10989

Fax: (914) 267-2420

Email: info@thesupplynet.com

Phone: (800) 826-0279

Internet: http://www.thesupplynet.com

Appendix B – Software User License Agreement

IMPORTANT - READ BEFORE OPENING THE SOFTWARE PACKAGE

This license agreement is a legal agreement between you (either an individual or a single entity) and Multi-Tech Systems, Inc. for the Multi-Tech software product enclosed, which includes computer software and may include associated media, printed materials, and "online" or electronic documentation ("SOFTWARE PRODUCT"). The SOFTWARE PRODUCT also includes any updates and supplements to the original SOFTWARE PRODUCT provided to you by Microsoft. Any software provided along with the SOFTWARE PRODUCT that is associated with a separate end-user license agreement is licensed to you under the terms of that license agreement.

By installing, copying, downloading, accessing, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this End User License Agreement (EULA). If you do not agree to the terms of this EULA, do not install or use the SOFTWARE PRODUCT; you may, however, return it to your place of purchase for a full refund.

SINGLE-USER SOFTWARE LICENSE AGREEMENT

This copy of Multi-Tech software is provided only on the condition that you, Customer, agree to the following license. READ THIS LICENSE CAREFULLY. If you do not agree to the terms contained in this license, return the packaged program UNOPENED to the place you obtained it. If you agree to the terms contained in this license, fill out the enclosed Software Registration Card, date, sign and return the card by mail. Opening the packaged program constitutes agreement to be bound by the terms and conditions of this Software License Agreement. Your right to use the software terminates automatically if you violate any part of this software license agreement.

MULTI-TECH SOFTWARE LICENSE AGREEMENT

Multi-Tech Systems, Inc. (MTS) agrees to grant and Customer agrees to accept on the following terms and conditions, a non-transferable and non-exclusive license to use the software program(s) delivered with this Agreement.

1. GRANT OF LICENSE. MTS grants Customer the right to use one copy of the software on a single computer (the Licensed System). You may not network the software or otherwise use it on more than one computer or computer terminal at the same time.
2. COPYRIGHT. The software is owned by MTS and is protected by United States copyright laws and international treaty provisions. Therefore, Customer must treat the software like any copyrighted material. Customer may install the software to a single hard disk and keep the original for backup or archival purposes. Customer shall NOT copy, or translate into any language, in whole or in part, any documentation which is provided by MTS in printed form under this Agreement.
3. OTHER RESTRICTIONS. The software may not be assigned, sublicensed, translated or otherwise transferred by Customer without prior written consent from MTS. Customer may not reverse engineer, decompile, or disassemble the software. Any updates shall be used only on the Licensed System, and shall remain subject to all other terms of this Agreement. Customer agrees not to provide or otherwise make available the software including, but not limited to documentation, programs listings, object code, or source code, in any form, to any person other than Customer and his employees and /or agents, without prior written consent from

MTS. Customer acknowledges that the techniques, algorithms, and processes contained in the software are proprietary to MTS and Customer agrees not to use or disclose such information except as necessary to use the software.

Customer shall take reasonable steps consistent with steps taken to protect its own proprietary information to prevent the unauthorized copying or use by third parties of the software or any of the other materials provided under this Agreement. Any previous version of the software must be destroyed or returned to Multi-Tech Systems, Inc. within 90 days of receipt of the software upgrade or update.

4. WARRANTY. MTS warrants that the software will perform substantially in accordance to the product specifications in effect at the time of receipt by Customer. If it fails to perform accordingly, MTS will optionally repair any defect, or replace it. This warranty is void if the failure has resulted from accident, abuse, or misapplication. A signed Software Registration Card must be on file at MTS for this warranty to be in effect.

   THE FOREGOING WARRANTY IS IN LIEU ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT WILL MTS BE LIABLE FOR CONSEQUENTIAL DAMAGES RESULTING FROM USE OF THE LICENSED PROGRAM, WHETHER AS A RESULT OF MTS NEGLIGENCE OR NOT, EVEN IF MTS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

5. INDEMNIFICATION. MTS will indemnify and defend Customer from any claim that the software infringes on any copyright, trademark, or patent. Customer will indemnify and defend MTS against all other proceedings arising out of Customers use of the software.

6. GENERAL. If any of the provisions, or portions thereof, of this Agreement are invalid under any applicable statute or rule of law, they are to that extent deemed to be omitted.

   This is the complete and exclusive statement of the Agreement between the parties, which supersedes all proposals, oral, written and all other communications between the parties relating to the subject matter of this Agreement. This Agreement may only be amended or modified in writing, signed by authorized representatives of both parties.

   This Agreement shall be governed by the laws of the State of Minnesota.

   The waiver of one breach or default hereunder shall not constitute the waiver of any subsequent breach or default.

Appendix C – Regulatory Compliance Information

Class B Statement
FCC Part 15

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference. (2) This device must accept any interference that may cause undesired operation.

Warning: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Industry Canada

This Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe B respecte toutes les exigences du Reglement Canadien sur le matériel brouilleur.

CE

EMC, Safety, and R&TTE Directive Compliance

The CE mark is affixed to this Multi-Tech product to confirm compliance with the following European Community Directives:

Council Directive 89 / 336 / EEC of 3 May 1989 on the approximation of the laws of Member States relating to electromagnetic compatibility.

and

Council Directive 73 /23 / EEC of 19 February 1973 on the harmonization of the laws of Member States relating to electrical equipment designed for use within certain voltage limits:

and

Council Directive 1999 / 5 / EC of March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity.

Appendix D – Tools for Your RF500S

RouteFinder Monitor

If you are having problems, the RouteFinder Monitor can be a valuable tool to assist in troubleshooting. Additional troubleshooting information is available through the on-line help screens. Refer to Chapter 6 for more information about using the RouteFinder monitor.

PING

Ping is an acronym for **P**acket **I**nter**n**et **G**roper. The PING utility is used as a diagnostic tool to determine if a communication path exists between two devices on the network. The utility sends a packet to the specified address and then waits for a reply. PING is used primarily to troubleshoot Internet connections, but it can be used to test the connection between any devices using the TCP/IP protocol.

WINIPCFG and IPCONFIG

There are two tools which are helpful in finding a computer's IP configuration, MAC address and default gateway.

WINIPCFG (for Windows 95/98)

1. Select **Start** | **Run** and type **WINIPCFG**.
2. The IP address, default gateway (the RF500S IP address), and the MAC (adapter address) display.

IPCONFIG (for Window NT/2000)

1. From a DOS Prompt, type **IPCONFIG** and press **Enter**.
2. The IP address, default gateway (the RF500S IP address), and the MAC (adapter address) display.

TRACERT

TRACERT is an extensive PING utility that allows you to trace the route of an IP address. The utility reports the number of router hops, the time for each hop, and any failed attempts to cross a hop. The information provided by this utility assists you to locate the specific site of a failed PING. You can run TRACERT at the DOS prompt (e.g., c:\tracert www.yahoo.com). The utility will provide information about the route and number of hops required to reach the destination IP address associated with the network address or URL.

H.323 Compatible Firmware Available

Until now, most firewall products have had problems passing H.323 traffic because of the dynamic nature of the H.323 protocol. Multi-Tech has solved this problem and can now provide customers with the ability to pass H.323 voice over IP traffic through its line of RouteFinder routers. A customer can now make outbound VoIP calls over their existing Internet connection using either a MultiVOIP gateway or Microsoft NetMeeting without any special configuration. The RouteFinder will simply recognize the H.323 packets and pass

them through to a distant H.323 VoIP gateway or NetMeeting client. If the need is for both outbound and inbound calls, the user must configure the MultiVOIP or the PC running NetMeeting to work in the demilitarized zone (DMZ) of the RouteFinder. This configuration is done by mapping internal and external port 0 to the IP address of the MultiVOIP or to the PC running NetMeeting.

To set up the DMZ, go to the IP Mapping (Virtual Server) screen under the General Settings tab in the RouteFinder configuration software. Keep in mind that a static IP address is going to be necessary when inbound calls are required to NetMeeting and is always required when running the MultiVOIP in H.323 mode.

Other significant features in the new firmware release for the RF500S are as follows:

- Support for outbound IPSec pass through
- Support for multiple Dialpad users
- Support for multiple WOWcall user

NetMeeting Note: There is no special configuration needed for NetMeeting. However, NetMeeting requires opening the correct ports. You will have to contact Microsoft to get these. Also, you cannot setup simultaneous NetMeeting sessions because you can only map the ports once.

Appendix E – Writing a Login Script

Writing a Login Script for IP Routing

To write an effective login script, you must obtain the correct login script information from your ISP and become familiar with using the login script commands.

Example 1: Script for Normal Reliable ISP

#	Login Script	Meaning of Each Login Script Command
1	Send"ATZ"	Rests Modem
2	Send"ATS0 =1"	Sends initial string 'ATS0 =1' to modem
3	Send"ATDT888-1234"	Dial phone number 888-1234
4	Wait"CONNECT"	Waits for ISP to send reply 'CONNECT'
5	Wait"username:"	Waits for ISP to send reply 'username'
6	Send"JaneDoe"	Sends the user name 'JaneDoe' to the ISP
7	Wait"password"	Waits for ISP to send reply 'password'
8	SH"1234"	Sends password '1234' to the ISP
9	Wait"===>"	Waits for ISP to send reply '===>'
10	Send"1"	Selects option 1(PPP) for this ISP
11	Go	Starts PPP mode

Example 2 : Script for Unreliable ISP (Redial until connected)

#	Login Script	Meaning of Each Login Script Command
1	Send"ATZ"	Resets modem
2	Send"ATS0 =1"	Sends initial string 'ATS0 =1' to modem
3	Send"ATDT8881234"	Dials phone number 888-1234
4	Wait"CONNECT"2	Wait for ISP to send reply 'CONNECT'. If no CONNECT, returns to line 2 to re-dial
5	Wait"username:"12	Waits for ISP to send reply 'username'. If no response, goes to line 12.
6	Send"JaneDoe"	Sends the username 'JaneDoe' to the ISP
7	Wait"password"	Waits for ISP to send reply' password'
8	SH"1234"	Sends password '1234' to ISP
9	Wait"====>"	Waits for ISP to send reply '===>'
10	Send"1"	Selects option 1 (PPP) for this ISP
11	Go	Starts PPP mode
12	Hangup	Hangs up Modem

Example 3 : Script for Unreliable ISP (2nd ISP backup)

#	Login Script	Meaning of Each Login Script Command
1	Send"ATZ"	Resets modem
2	Send"ATS0 =1"	Sends initial string 'ATS0 =1' to modem
3	Send"ATDT8881234"	Dials phone number 888-1234
4	Wait"CONNECT" 12	Waits for ISP to send reply 'CONNECT'. If no reply, goes to line 12 for ISP #2.
5	Wait "username:" 12	Waits for ISP to send reply 'username'. If no response, goes to line 12 for ISP #2.
6	Send"JaneDoe"	Sends the username 'JaneDoe' to ISP
7	Wait"password"	Waits for ISP to send reply' password'
8	SH"1234"	Sends password '1234' to ISP
9	Wait"====>"	Waits for ISP to send reply '===>'
10	Send"1"	Selects option 1 (PPP) for this ISP
11	Go	Starts PPP mode (Rest of script ignored)
12	Hangup	Hangs up Modem
13	Send "AT S0=1"	Sends initial string 'AT SO=1' to modem
14	Send 'ATDT 8885678'	Dials phone number 888-5678 (ISP #2)
15	Wait 'Connect' 23	Waits for ISP to send reply 'CONNECT'. If no CONNECT, goes to line 23.
16	Wait "username:" 23	Waits for ISP to send reply 'username'. If no response, goes to line 23.
17	Send "Stephen"	Sends the username 'Stephen' to ISP
18	Wait "password:"	Waits for the ISP to send 'password:'
19	SH "5678"	Sends password '5678' to ISP
20	Wait"====>"	Waits for ISP to send reply '===>'
21	Send"1"	Selects option 1 (PPP) for this ISP
22	Go	Starts PPP mode
23	Hangup	Hangs up Modem
24	Jump 2	Goes back to line 2 to re-dial ISP#1

RouteFinder™

Glossary

MultiTech® Systems

Glossary

B

Baud Rate
Baud rate refers to the number of bits per second (Bps) that are transmitted between your network device and modem or ISDN TA.

D

DHCP (Dynamic Host Configuration Protocol)
A protocol that was made to lessen the administrative burden of having to manually configure TCP/IP Hosts on a network. DHCP makes it possible for every computer on a network to extract its IP information from a DHCP server instead of having to be manually configured on each network computer. The DHCP server built-in to your RouteFinder allows every computer on your network to automatically extract IP information from the RouteFinder.

Why is it called Dynamic?
Each time a network client turns on their computer your RouteFinder DHCP server will automatically give them an IP address from the IP address pool configured in the DHCP Configuration screen in RouteFinder Manager. It is called Dynamic because the address that is issued could be different each time a computer connects to the network.

DNS (Domain Name System)
A DNS Server can be thought of as the computer at your ISP whose job is to take all the URLs that you type into your web browser and translate them to their corresponding IP address. To use this the DNS translator, you need to know the IP address of your ISP's DNS Server.

E

Ethernet
A LAN (Local Area Network) protocol developed by Xerox and DEC. It is a very commonly used type of LAN.

F

Firewall
A system designed to prevent unauthorized access to or from a private network. Firewalls are typically installed to give users access to the Internet while protecting their Internal Information. Your RouteFinder uses a firewall technology known as NAT (see NAT). Each message entering or leaving the intranet passes through the firewall. The firewall examines each message and blocks those that do not meet the specified security criteria.

Firmware
Software that has been has been permanently or semi-permanently written to the RouteFinder's memory. Your RouteFinder supports flash ROM which means you can upgrade the firmware in your network device very easily by downloading a copy of the new firmware from the Multi-Tech web site and using the RouteFinder Manager Upgrade Firmware function.

FTP (File Transfer Protocol)
A protocol which allows a user on one host to access, and transfer files to and from another host over a network.

I

IP (Internet Protocol)
The Internet Protocol is the network layer for the TCP/IP Protocol Suite. It is a connectionless, best-effort packet switching protocol.

Intranet
An Intranet is the use of Internet technologies within a company. Intranets are private networks that exist only within organizations, while the Internet is a global network open to all.

IP Addresses
A computer on the Internet is identified by an IP Address. A computer's IP address is like a telephone number. It identifies one address or in this case one computing device. Every computer or device on the network must have a different IP address.

An IP address consists of four groups of numbers called **octets**, which are separated by periods. For example, 213 .0.0.1 is an IP address. An IP address consists of a **network portion** and a **host portion**. The network portion identifies the subnet that the computer belongs to. The host portion identifies the particular computer or node on that network.

IP addresses can either be dynamic (temporary) or static (permanent or fixed). A dynamic IP address is a temporary IP address that is assigned to you by a server (usually a DHCP server) when the computer is powered on. A static IP address is a permanent IP address that is set up on each individual computer. When your RouteFinder dials-up your ISP, your ISP can give it a fixed or dynamic IP address. Likewise when you power on your computer, the RF500S can give your computer a dynamic or fixed IP address.

ISDN TA
(Integrated Services Digital Network Terminal Adapter) ISDN is a high speed digital telephone connection involving the digitization of the telephone network using existing wiring. An ISDN Terminal Adapter can be thought of as an ISDN Modem.

ISP (Internet Service Provider)
An organization that provides Internet services. An ISP is the company that provides the connection from your computer to the Internet. An ISP can offer a range of services, such as dial-up accounts, e-mail, web hosting or News.

L

LAN (Local Area Network)
A data network intended to serve an area of only a few square kilometers or less. This often means a small private network in companies.

M

ML-PPP (Also called MP or MPPP)
Stands for Multilink Point to Point Protocol and is an advancement of the PPP protocol that allows for the bridging or bundling of two ISDN or analog channels for faster connections.

MAC Address
The hardware address of a Device connected to a shared media. To find out the MAC address of your computer please see **Troubleshooting.**

N

NAT Technology

NAT is short for Network Address Translation. NAT is an Internet standard that enables a local-area network to use one set of IP addresses for internal traffic and a second set of IP addresses for external traffic. The RF500S provides the necessary IP address translations. NAT is sometimes referred to as "IP Address Masquerading". This technology provides a type of firewall by hiding the internal IP addresses.

How does it work?
Every IP address on the Internet is a Registered or legal IP address. Therefore, no two IP addresses on the Internet are the same. For you to use your network device to access the Internet you need a registered IP address from your ISP (Internet Service Provider). Using a registered IP address on your Intranet or LAN is not necessary. When clients on your network start surfing the Internet, your RouteFinder will receive all the requests for information. The RouteFinder will dial-up your ISP and your ISP will give your RouteFinder a registered legal IP address. Your RouteFinder uses this IP address to request information saying ,"send all information back to me at this IP address". In essence it appears as though all your clients requests are coming from that one IP address (hence the name IP masquerading). When all the information comes back through the RouteFinder, it sorts the data using an Address Translation Table and returns the data to the computer on your network that requested it.

If someone on the Internet tries to access your network, the RouteFinder's firewall function stops the request. The device will not reverse translate network addresses unless you have specifically allowed this feature using the Virtual Server function (IP Mapping).

Network Address

The network portion of an IP address. For a class A network, the network address is the first byte of the IP address. For a class B network, the network address is the first two bytes of the IP address. For a class C network, the network address is the first three bytes of the IP address. In each case, the remainder is the host address. In the Internet, assigned network addresses are globally unique.

P

Packet

A packet is a piece of a message transmitted over a packet-switching network. A packet contains the destination address of the message as well as the data. In IP networks, packets are often called datagrams.

Port Number

The term *port* can mean the connector on your computer or it can be thought of as a server number. Every service that travels over phone lines and modems has a standard port number. For example, the World Wide Web service uses the standard port number, **80** and the standard telnet port is **23**.

Port numbers are controlled and assigned by the IANA (Internet Assigned Numbers Authority). Most computers have a table in their systems containing a list of ports that have been assigned to specific services. You can also find lists of standard port numbers on the World Wide Web.

Protocol

A formal description of message formats and the rules two computers must follow to exchange those messages. You can think of protocols like languages. If two computers or devices aren't speaking the same language to each other, they won't be able to communicate.

PPP (Point -to- Point Protocol)

PPP enables dial-up connections to the Internet and is the method that your network device connects to the Internet. PPP is more stable than the older SLIP protocol and provides error checking features.

R

Router

A device which forwards traffic between networks. If you request information from a location on your network or the Internet, the router will route the request to the appropriate destination. The router's job is to listen for requests for IP addresses that are not part of your LAN and then route them to the appropriate network which may either be the Internet or another sub-network on your LAN.

S

Server

A provider of resources (e.g., file servers and name servers). For example your RouteFinder provides Internet Access and can be thought of as an Internet Access Server.

Subnet

A portion of a network that shares a common address component. On TCP/IP networks, subnets are defined as all devices whose IP Addresses have the same prefix. For example, all devices with IP addresses that start with 213 .0 .0 .would be part of the same subnet.

Subnet Mask /IP Address Mask

Subnet mask is what is used to determine what subnet an IP address belongs to. Subnetting enables the network administrator to further divide the host part of the address into two or more subnets.

T

TCP/IP (Transmission Control Protocol/Internet Protocol)

A suite of communication protocols used to connect hosts on the Internet. Every computer that wants to communicate with another computer on the Internet must use the TCP/IP protocol to transmit and route data packets. The format of an IP address is a 32-bit numeric address written as four octets separated by periods. Each number can be zero to 255. Within an isolated network, you can assign IP addresses at random as long as each one is unique. However, connecting a private network to the Internet requires using registered IP addresses to avoid duplication.

The four groups of numbers (octets) are used to identify a particular network and host on that network. The InterNIC assigns Internet addresses as Class A, Class B, or Class C. Class A supports 16 million hosts on each of 127 networks. Class B supports 65,000 hosts on each of 16,000 networks. Class C supports 254 hosts on each of 2 million networks. Due to the large increase in access to the Internet, new classless schemes are gradually replacing the system based on classes.

U

UDP (User Datagram Protocol)

An Internet Standard transport layer protocol. It is a connectionless protocol that adds a level of reliability and multiplexing to IP.

Index

M

N

O

P

R

S

T

U

V

W