RouteFinder® SOHO

SOHO Security Appliance

RF820 & RF820-AP
RF830 & RF830-AP

User Guide

MultiTech® Systems

User Guide

RouteFinder SOHO Security Appliance

Models: RF820 & RF820-AP
RF830 & RF830-AP

Document Product Number S000399E, Revision E

Revision	Date	Description
A	04/24/06	Initial release. Software version 1.00
B	06/01/06	Added explanation of Load Balancing on the Network Setup screen.
C	01/03/07	Software version 1.30. Added wireless builds: RF820-AP and RF830-AP. Added Table of Commonly Supported Subnet Addresses.
D	04/05/07	Updated the Technical Support contact list. Updated the Multi-Tech Warranty policy.
E	10/23/07	Software version 1.40. *Save and Restart* functionality changed.
	05/04/09	Added a link to the Multi-Tech Web site for the Warranty statement.

Patents

This device is covered by one or more of the following U.S. Patent Numbers: 6,219,708; 5,301,274; 5,309,562; 5,355,365; 5,355,653; 5,452,289; 5,453.986.

Warranty

For Warranty information, see the Multi-Tech Web site at http://www.multitech.com

Trademarks

The Multi-Tech logo and *RouteFinder* are registered trademarks of Multi-Tech Systems, Inc.

World Headquarters

Multi-Tech Systems, Inc.
2205 Woodale Drive
Mounds View, Minnesota 55112
Phone: 763-785-3500 or 800-328-9717
Fax: 763-785-9874
Internet Address: http://www.multitech.com

Country	By Email	By Phone
Europe, Middle East, Africa	support@multitech.co.uk	+(44) 118 959 7774
U.S., Canada, all others	support@multitech.com	(800) 972-2439 or +763-717-5863

Contents

Chapter 1 – Introduction and Description

Welcome to the world of Internet security. Your Multi-Tech RouteFinder SOHO security appliances, models RF820 and RF830, and RouteFinder wireless security appliances, models RF820-AP and RF830-AP, are ideal for the small office or home office (SOHO) that needs secure access to a corporate LAN.

In addition to providing a WAN Ethernet port for DSL or cable broadband Internet access, these security appliances also offer both client-to-LAN and LAN-to-LAN VPN connectivity based on the IPSec or PPTP protocols. The RouteFinder SOHO supports up to 15 VPN tunnels and provides 168-bit 3DES and AES encryption to ensure that your information remains private. In addition, these security appliances offer secure Internet firewall services.

Key Features

- One (RF820/RF820-AP) and two (RF830/RF830-AP) WAN Ethernet ports connect to a DSL or cable modem for shared Internet access.
- Models RF820-AP and RF830-AP allow wireless access.
- Supports IPSec VPN tunnels and PPTP tunnels for secure LAN-to-LAN and Client-to-LAN access over the Internet.
- 3DES and AES encryption.
- Dual WAN load balancing (RF830/RF830-AP).
- Internet and VPN failover (RF830/RF830-AP).
- Shared Internet access via PPPoE, DHCP or static IP.
- Serial port for automatic dial-backup if your broadband connection goes down (RF820/RF820-AP).
- Built-in 4-port 10/100M bps switch.
- Stateful Packet Inspection firewall with packet filter rules, DNAT, SNAT and IP MASQUERADE.
- Built-in dynamic DNS client.
- Supports VPN tunneling using FQDN.
- Protects your LAN against Denial of Service (DoS) attacks.
- Network monitoring via Syslog allows network administrator to view all incoming and outgoing packets, status of connections and specific connection events.
- Configuration and management using any Web browser.
- Internet access control tools provide client and site filtering.
- Traffic monitoring and reporting.
- Flash memory of easy updates.
- IP address mapping/port forwarding.
- Two-year warranty.

Feature Details

- **Secure VPN Connections.** The RouteFinder SOHO security appliance uses the IPSec or PPTP industry standard protocol, data encryption, and the Internet to provide high-performance, secure VPN connections. For LAN connectivity, the RouteFinder SOHO security appliance utilizes the IPSec protocol to provide up to 15 tunnels with strong 3DES or AES encryption using IKE and PSK key management. For Client-to-LAN connectivity, Multi-Tech provides optional IPSec client software allowing road warriors secure access to the company's internal network.
  This RouteFinder also supports remote users who want to use the PPTP VPN client built into the Windows operating system. This provides 40-bit or 128-bit encryption, user name and password authentication.
- **Connect Multiple Users to the Internet with Broadband Speed.** With the RouteFinder SOHO security appliance, multiple users can share access to the Internet with only one IP account. The WAN Ethernet port(s) support DSL or cable speeds of up to 20M bps.
- **Built-in 10/100 Switch.** The integrated 4-port 10/100M bps 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 SOHO appliance provides network layer security utilizing Stateful Packet Inspection, the sophisticated firewall technology found in large enterprise firewalls, to protect the network against intruders and Denial of Service (DoS) attacks. It also uses Network Address Translation (NAT) to hide internal, non-routable IP addresses and allows internal hosts with unregistered IP addresses to function as Internet-reachable servers.
- **Dual WAN Load Balancing, Internet and VPN Failover.** The RouteFinder SOHO security appliance model RF830/RF830-AP has a second WAN port for Internet access. This allows for two separate ISP connections giving administrators the ability to balance traffic by distributing it over the two links. In addition, if one port were to go down, the RouteFinder appliance would automatically re-route all Internet and VPN traffic to the other connection. The second WAN port greatly enhances performance and system uptime.
- **Automatic Dial Backup.** The RouteFinder SOHO (RF820/RF820-AP) security appliance also provides an additional serial port that, when connected to a dial-up modem or ISDN terminal adaptor, can serve as a backup resource for Internet access if your cable or DSL service goes down. It can also serve as the primary connection if you do not have broadband connectivity yet in your area.
- **Virtual Server Support.** In addition to providing shared Internet access, the RouteFinder SOHO security appliance can support a Web, FTP or other Internet servers. Once configured, it accepts only unsolicited IP packets addressed to the Web, FTP or other specified servers.
- **Dynamic DNS Client.** The RouteFinder SOHO security appliance has a built-in Dynamic DNS client that is compatible with *DynDNS.org*. It automatically sends an update to the *DynDNS.org* update server if the WAN IP address changes. A registered Dynamic DNS account allows you to host your own Web site, mail server, or other services on the Internet without having to obtain a static IP address or keep track of a dynamic IP address. It also aids in creating static-to-dynamic or dynamic-to-dynamic IPSec VPN tunnels. In addition, with a Dynamic DNS account, you can establish a PPTP VPN tunnel behind the RouteFinder SOHO security appliance by configuring your PPTP client to connect to *yourhostname.dydns.org* instead of a dynamic IP address.
- **Fully Qualified Domain Name (FQDN) Feature.** The FQDN featured on the RouteFinder SOHO security appliance allows you to utilize a static name in the IPSec VPN setup, like *"branchof.ce.dyndns.org"*, instead of a dynamic IP address, to create static-to-dynamic or dynamic-to-dynamic VPN IPSec tunnels. This allows all of the IPSec VPN connections to act like static-to-static connections. The RouteFinder SOHO security appliance checks the FQDN IPSec configuration every two minutes for IP address changes. If the IP address is different than the last time it checked, it drops the current tunnel and creates a new one. This helps to keep IPSec VPN tunnels readily available with minimal interruptions in data communication.
- **Optional VPN Client Software.** Multi-Tech provides easy-to-use IPSec VPN client software that transparently secures Internet communications anytime, anywhere. VPN client software is ideal for business users who travel frequently or work from home providing secure remote access through the RouteFinder security appliance for applications such as remote access, file transfer, e-mail, Web browsing, messaging or IP telephony. Encryption and authentication operations are completely transparent to the end user. In general, IPSec provides stronger encryption than PPTP resulting in better overall security. A 30-day free trial CD is included with the RouteFinder SOHO security appliance.

RouteFinder Ship Kit Contents

The RouteFinder shipping box contains the following items:

- One SOHO RouteFinder
- Power Supply
- 2.4 GHz 5dBi SWI-Reverse-F Swivel Access Point Antenna (Included with the wireless models only)
- Ethernet cable (included with the RF830 model)
- This Quick Start Guide
- IPSec VPN Client 30-day evaluation software on CD (not the full working version)
- One RouteFinder CD which contains RouteFinder documentation and Adobe Acrobat Reader.

If any of the items is missing or damaged, please contact Multi-Tech Systems, Inc.

RouteFinder Documentation

Quick Start Guide

The Quick Start Guide is a shorter version of this User Guide. The Quick Start is included in printed form with your RouteFinder. The guide provides the necessary information for a qualified person to unpack, cable, and configure the device for proper operation.

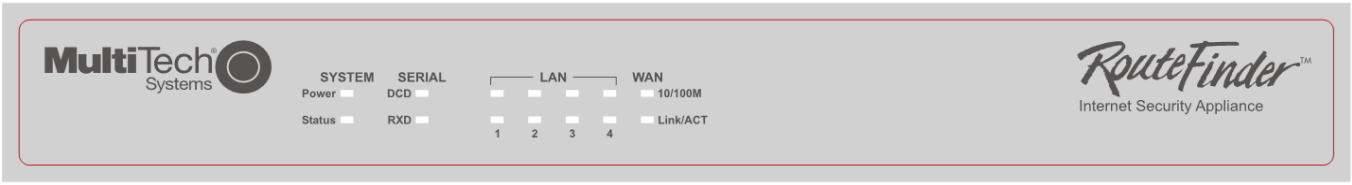
User Guide

The User Guide can be installed from the RouteFinder CD by clicking Install Manuals on the Installation screen or downloading the file from our Web site at: http://www.multitech.com

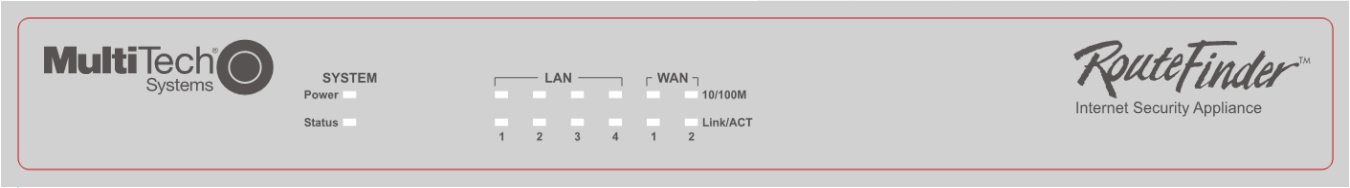
Telecom Warnings for the Modem

1. Never install telephone wiring during a lightning storm.
2. This product must be disconnected from the telephone network interface when servicing.
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. Use caution when installing or modifying telephone lines.
6. 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. Never install telephone jacks in a wet location unless the jack is specifically designed for wet locations.

RF820/RF820-AP Front Panel



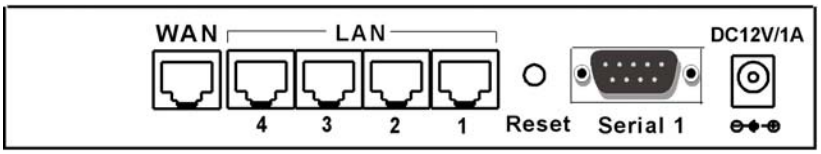
RF830/RF830-AP Front Panel



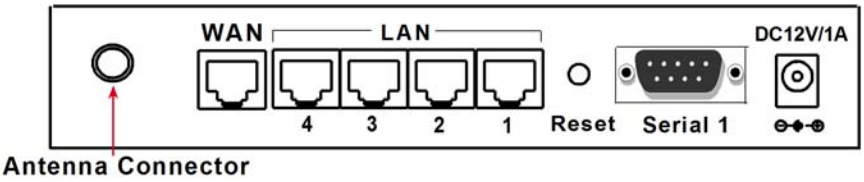
LEDs	Description
Power	Lights when power is being supplied to the RouteFinder.
Status	When functioning normally, the LED blinks. The LED is a solid light when the RouteFinder is booting up, saving the configuration, restarting, or updating the firmware.
Serial DCD	(RF820/RF820-AP only) Lights when Serial port is connected to a remote site.
Serial RXD	(RF820/RF820-AP only) Blinks when Serial port is receiving or transmitting data.
LAN10/100M	Lights when a successful connection to the 100BaseT LAN is established. Off when connected to the 10BaseT.
LAN Link / ACT	Lights when the LAN port has a valid Ethernet connection. Blinks when it is receiving or transmitting data.
WAN 10/100M	Lights when a successful connection to the 100BaseT WAN is established. Off when connected to the 10BaseT.
WAN Link / ACT	Lights when the WAN port has a valid Internet connection. Blinks when it is receiving or transmitting data.

Back Panels

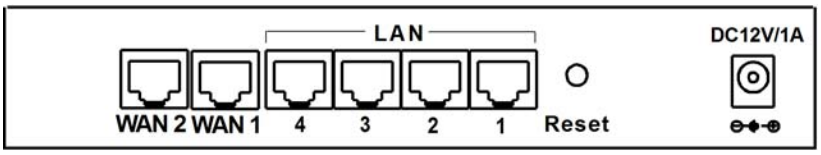
RF820



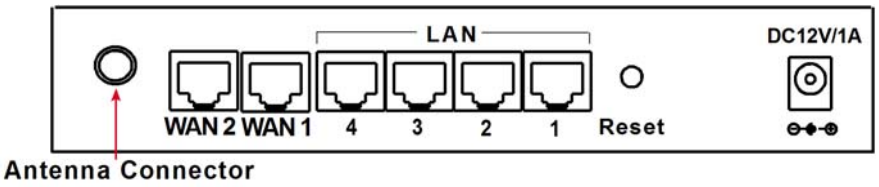
RF820-AP



RF830

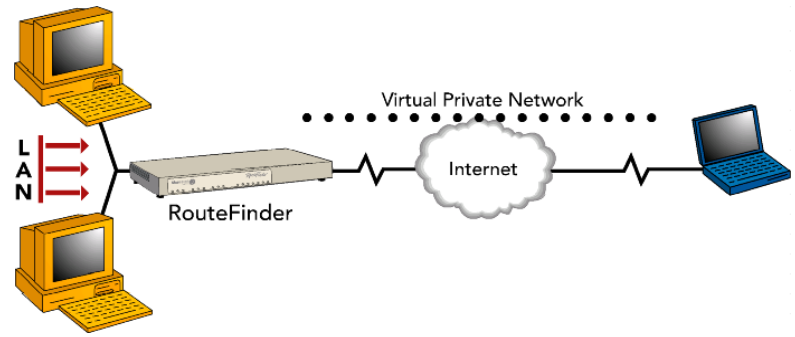
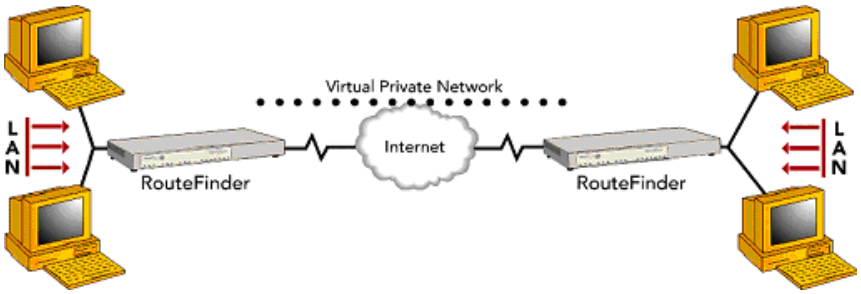
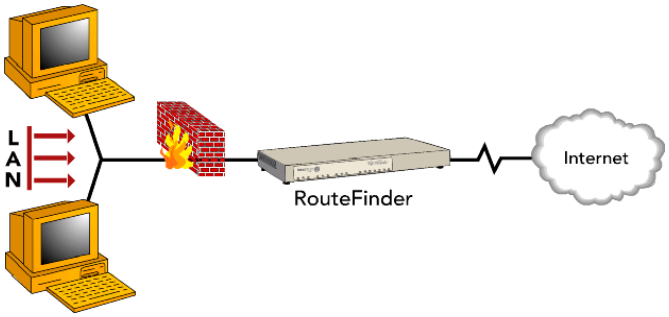
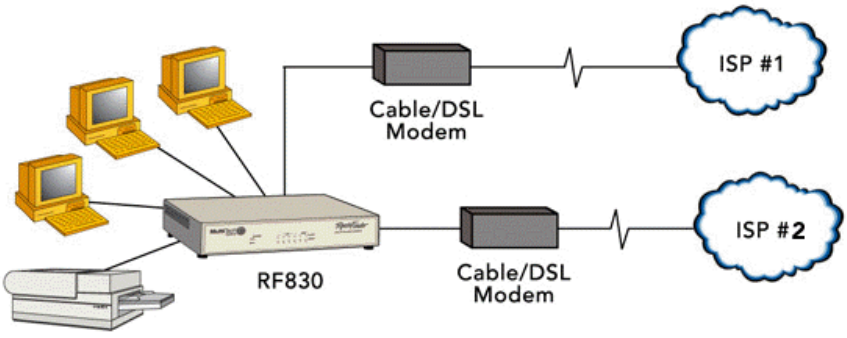


RF830-AP



Connector	Description
Antenna Connector	Connector for the 2.4 GHz 5dBi SWI-Reverse-F antenna. **Note:** The antenna must be attached in order for the RouteFinder to be operational.
WAN	The WAN (10/100BaseT) port connects the DSL modem or cable modem. The RF820 and 820-AP have one WAN port and the RF830 and RF830-AP have two WAN ports.
LAN Ports	There are 4 LAN ports. You can connect to PCs, FTP servers, printers, or other devices you want to put on your network.
Reset	The Reset button resets the RouteFinder to its factory defaults. Press and hold the Reset button until the Status LED blinks, and then release it. Do not press this button unless you want to restore all settings to the factory defaults.
Serial	(RF820 and RF820-AP only) The Serial port connects to a standard modem.
12VDC Power	The power port connects the AC power adapter.

Typical Applications

Remote User. The client-to-LAN application replaces traditional dial-in remote access by allowing a remote user to connect to the corporate LAN through a secure tunnel over the Internet. The advantage is that a remote user can make a local call to an Internet Service Provider, without sacrificing the company's security, as opposed to a long distance call to the corporate remote access server.	
Branch Office. The LAN-to-LAN application sends network traffic over the branch office Internet connection instead of relying on dedicated leased line connections. This can save thousands of dollars in line costs and reduce overall hardware and management expenses.	
Firewall Security. As businesses shift from dial-up or leased line connections to always-on broadband Internet connections, the network becomes more vulnerable to Internet hackers. The RouteFinder provides a full-featured firewall based on Stateful Packet Inspection technology and NAT protocol to provide security from intruders attempting to access the office LAN.	
Load-Balancing. Load Balancing distributes LAN-to-LAN traffic over two WAN links. This allows for the amount of traffic on each line to be based on a specified weighed value so that communication can be made faster and more reliable. **Failover.** If one port were to go down, the RouteFinder appliance would automatically re-route all Internet and VPN traffic to the other connection. The second WAN port greatly enhances performance and system uptime.	

Specifications

These specifications are for the RF820/820-AP and RF830/830-AP.
See the next page for the 802.11b/g specifications.

Specifications	RF820 and RF820-AP	RF830 and RF830-AP
Standards	10/100BaseT	10/100BaseT
Ethernet Ports	**LAN:** 4 Ports 10/100BaseT **WAN:** 1 Port 10/100BaseT	**LAN:** 4 Ports 10/100BaseT **WAN:** 2 Ports 10/100BaseT
Recommended Network Users	25	25
Firewall	Stateful Packet Inspection Network Address Translation (NAT) Filtering (Port Number & IP Address) Virtual Server Denial of Service Protection (DoS) Firewall Throughput (20M bps) H.323 Pass Through	Stateful Packet Inspection Network Address Translation (NAT) Filtering (Port Number & IP Address) Virtual Server Denial of Service Protection (DoS) Firewall Throughput (20M bps) H.323 Pass Through
VPN	Remote User (Client-to-LAN) IPSec, PPTP Branch Office (LAN-to-LAN) IPSec 3DES/AES Encryption IPSEC/PPTP VPN Encryption Throughput (3M bps) IKE VPN Using FQDN Recommended VPN Tunnels: up to 15	Remote User (Client-to-LAN) IPSec, PPTP Branch Office (LAN-to-LAN) IPSec 3DES/AES Encryption IPSEC/PPTP VPN Encryption Throughput (3M bps) IKE VPN Using FQDN Recommended VPN Tunnels: up to 15
Management	Web-Based (HTTP) Email Alerts Local and Remote Management Syslog Intrusion Logging	Web-Based (HTTP) Email Alerts Local and Remote Management Syslog Intrusion Logging
Dimensions	9.75" w x 1.5" h x 6.5" d (24.8 cm x 3.8 cm x 16.5 cm)	9.75" w x 1.5" h x 6.5" d (24.8 cm x 3.8 cm x 16.5 cm)
Weight	2.4 lbs. (1.0 kg.)	2.4 lbs. (1.0 kg.)
Operating Temperature	+32° to +120° F (0° to 50° C)	+32° to +120° F (0° to 50° C)
Humidity	25–85% non-condensing	25–85% non-condensing
Power Requirements	**Input:** 100 ~240V, 0.6A 50-60- Hz **Output:** 12VDC, 1A	**Input:** 100 ~240V, 0.6A 50-60- Hz **Output:** 12VDC, 1A
Certifications and Approvals	CE Mark FCC Part 15 (Class B) UL 60950	CE Mark FCC Part 15 (Class B) UL 60950
Warranty	2 years	2 years

Specifications for 802.11b/g Interface

Specifications	RF8230AP and RF830AP
Network Standards	IEEE 802.11b IEEE 802.11g
Frequency Band	2.400-2.4835GHz
Data Rate	**IEEE 802.11b (auto-fallback):** • CCK: 11, 5.5 Mbps • QPSK: 2 Mbps • BPSK: 1 Mbps **IEEE 802.11g (auto-fallback):** • OFDM: 54, 48, 36, 24, 18, 12, 9 and 6 Mbps
Media Access Control	CSMA/CA with ACK
Channel	**IEEE 802.11b** Ch. 1 to 11 – North America Ch. 1 to 14 – Japan Ch. 1 to 13 – Europe ETSI Ch. 10 to 11 – Spain Ch. 10 to 13 – France **IEEE 802.11g** Ch. 1 to 11 – North America Ch. 1 to 13 – Japan Ch. 1 to 13 – Europe ETSI Ch. 10 to 11 – Spain Ch. 10 to 13– France
Transmission	IEEE 802.11b (DSSS) IEEE 802.11g (OFDM)
Modulation	**IEEE 802.11b (DSSS)** CCK @ 11.1.1 Mbps QPSK @ 2 Mbps BPSK @ 1 Mbps **IEEE 802.11g (OFDM)** BPSK @ 6, 9 Mbps QPSK @ 12, 18 Mbps 16-QAM @ 24, 36 Mbps 64-QAM @ 48, 54 Mbps
Network Architecture	Infrastructure Mode
Antenna	SMA antenna connector
Output Power	**IEEE 802.11b** 11Mbps; 17.5 +/- 2 dBm **IEEE 802.11g** 54Mbps; 14.0 +/- 1 dBm
Receiver Sensitivity	11 Mbps CCK @ 8% PER = -80 dBm 54 Mbps OFDM @ 10% PER = -65 dBm
Range	Up to 400m outdoor operating range
Security	64/128-bit WEP, WPA, TKIP, AES, WPA2

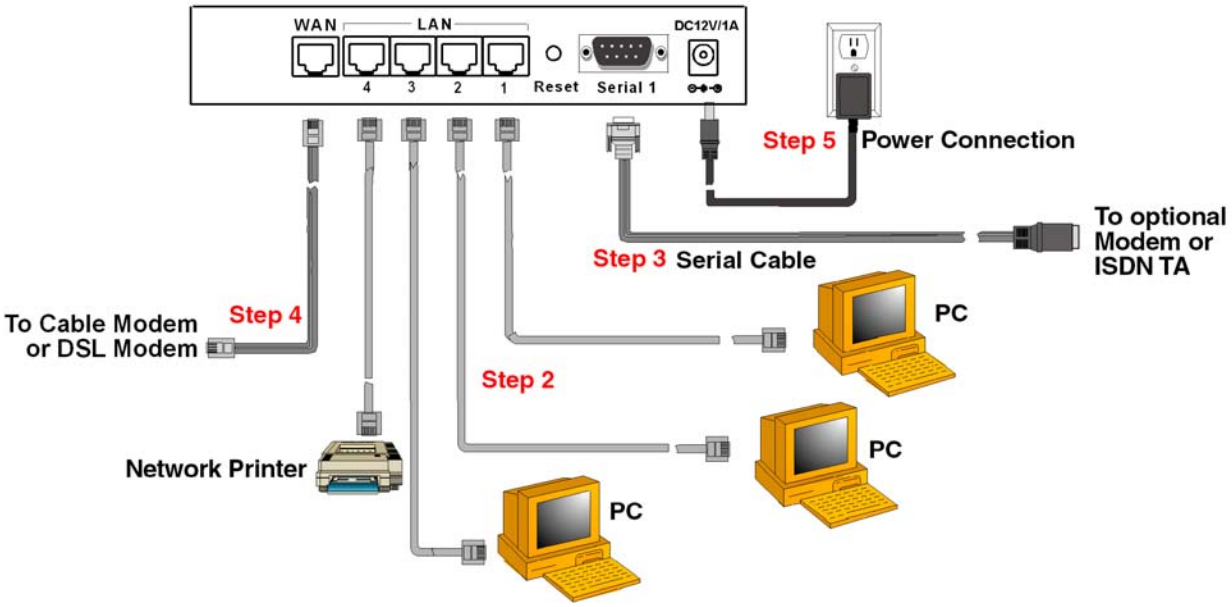
Chapter 2 – Installation

Cabling Your RouteFinder

Your RouteFinder requires making the appropriate connections to PCs, a cable or xDSL modem, an analog modem or ISDN TA, and AC power.

After your device is properly cabled, it must be configured. See Chapter 3 for basic directions. For advanced configurations, see the User Guide.

RF820



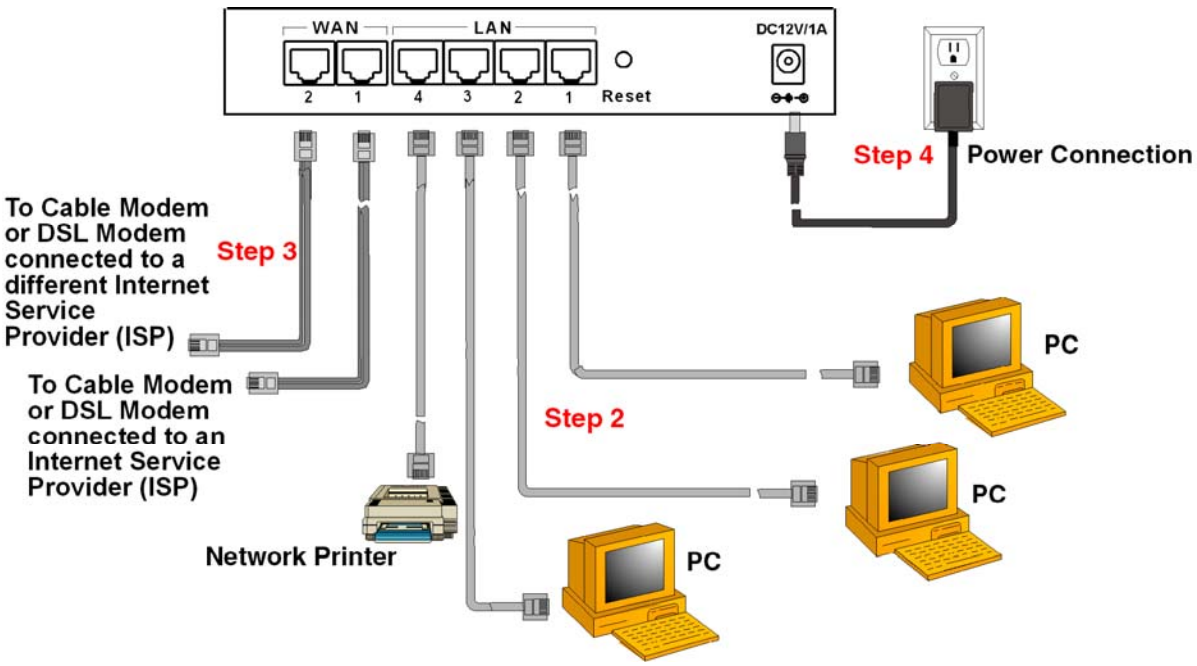
1. Turn the power off on all network devices (PCs, cable modems, DSL modems, analog modems, ISDN TAs, and the router).
2. Plug one end of a RJ-45 cable into the Ethernet port on the PC and other into one of the LAN port on the RouteFinder. (If you have more than one PC, connect the others in the same way to the other LAN ports).
3. If using an analog modem, connect it to the RF820's serial port.
4. Connect a network cable from the DSL modem or cable modem to the WAN port on the RouteFinder.
5. Connect the provided power supply cable to the 12VDC power port on the back of the RouteFinder, and plug the other end of the power supply into an AC power outlet as shown.

RF820-AP

Use the cabling procedures above and attach the wireless antenna. See the Back Panel section earlier in this chapter for the location of the antenna connector.

Note: The antenna must be attached in order for the RouteFinder to be operational.

RF830



1. Turn the power off on all network devices (PCs, cable modems, DSL modems, analog modems, ISDN TAs, and the router).
2. Plug one end of a RJ-45 cable into the Ethernet port on the PC and other into one of the LAN port on the RouteFinder. (If you have more than one PC, connect the others in the same way to the other LAN ports).
3. Connect a network cable from the DSL modem or cable modem to the WAN port on the RouteFinder. A second WAN port is provided for connecting a second DSL modem or cable modem that uses a different Internet Service Provider (ISP). This gives you the option to switch from one ISP to another in case one provider is not available.
4. Connect the provided power supply cable to the 12VDC power port on the back of the RouteFinder, and plug the other end of the power supply into an AC power outlet as shown.

RF830-AP

Use the cabling procedures above and attach the wireless antenna. See the Back Panel section earlier in this chapter for the location of the antenna connector.

Note: The antenna must be attached in order for the RouteFinder to be operational.

Chapter 3 – Setting up a Workstation and Starting the RouteFinder

This section of the User Guide covers the steps for setting up TCP/IP communication on the PC(s) connected to the RouteFinder, starting up the RouteFinder, and opening the RouteFinder Web Management program.

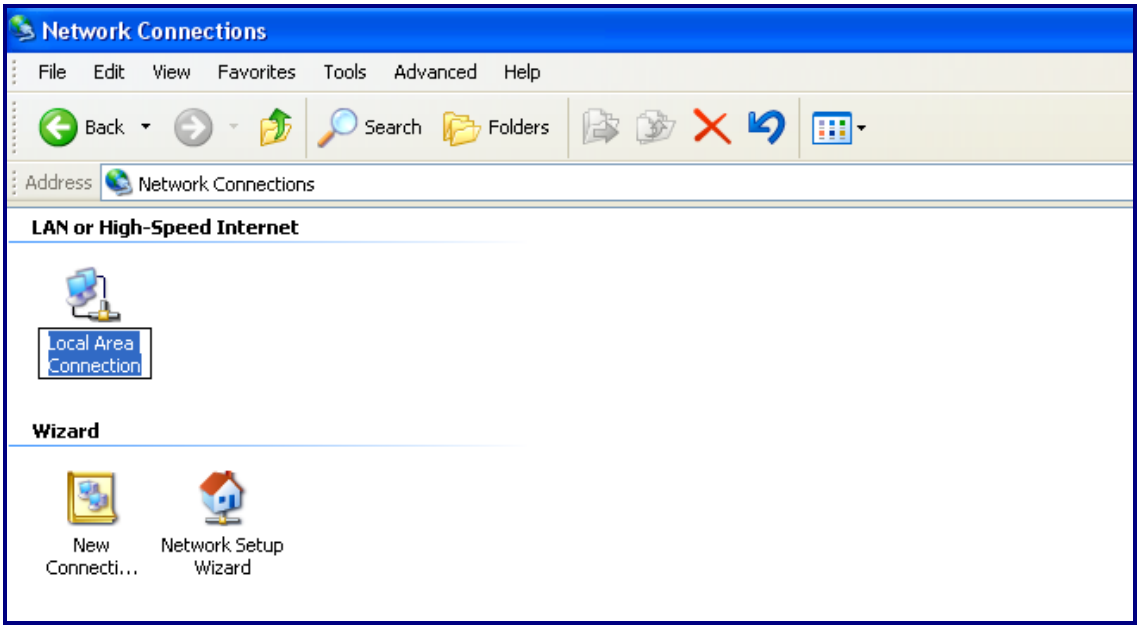
Establish TCP/IP Communication

Notes:
- The RouteFinders have built-in DHCP server functionality, so you can set the PC to obtain a dynamic IP address.
- The following directions are for Windows 2000+/XP operating systems.

Obtain a Dynamic IP Address

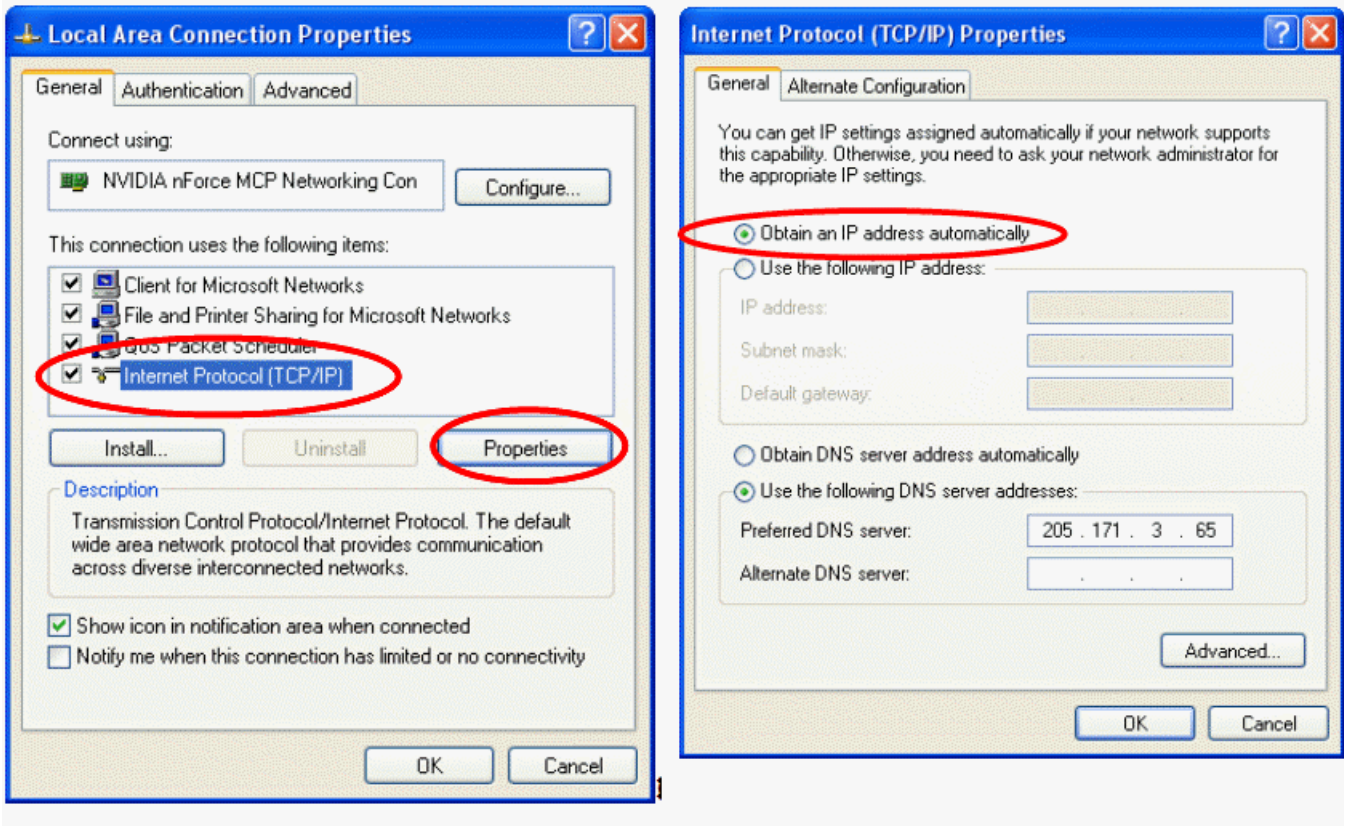
To obtain a dynamic IP address so it can be assigned to the Ethernet port:

1. Make the RouteFinder connections as described on the previous two pages.
2. Click **Start | Settings | Control Panel**. Double-click the **Network Connections** icon.
3. The **Network Connections** screen displays. Right-click the **Local Area Connection** icon and choose **Properties** from the drop down list.



4. **The** Local Area Connection Properties **dialog box displays.**
   - **Select** Internet Protocol [TCP/IP]**.**
   - **Click the Properties button.**

5. Once you click the **Properties** button, the following screen displays (below) . To have your DCHP client obtain a dynamic IP address, click the button for Obtain an IP address automatically**.**



6. Close out of the Control Panel.
7. Repeat these steps for each PC on your network.

To Set a Fixed IP Address

To set a Fixed IP Address, check **Specify an IP address** instead of **Obtain an IP address automatically**. Then click **OK**.

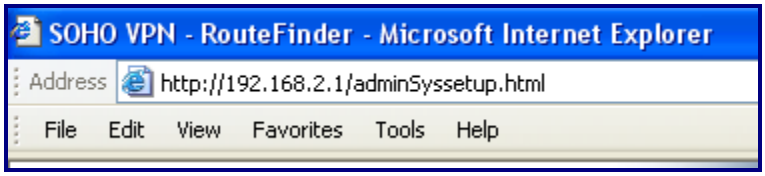
1. Enter the workstation IP address as **192.168.2.x**. Note that the **x** in the address stands for numbers 101 and up.
2. Enter the Subnet mask as 255.255.255.0
3. Enter the Default gateway as 192.168.2.1
4. Close out of the Control Panel.
5. Repeat these steps for each PC on your network.

Open a Web Browser

Note: Be sure that the RouteFinder is cabled and that the power is connected as shown in Chapter 2.

Bring up a Web browser on the PC.

1. Type the default gateway address line:
   http://192.168.2.1
2. Press Enter.



Note: Make sure your PC's address is on the same network as the router's address. **IPCONFIG** is a tool for finding out a PC's IP configuration (the default gateway and the MAC address).

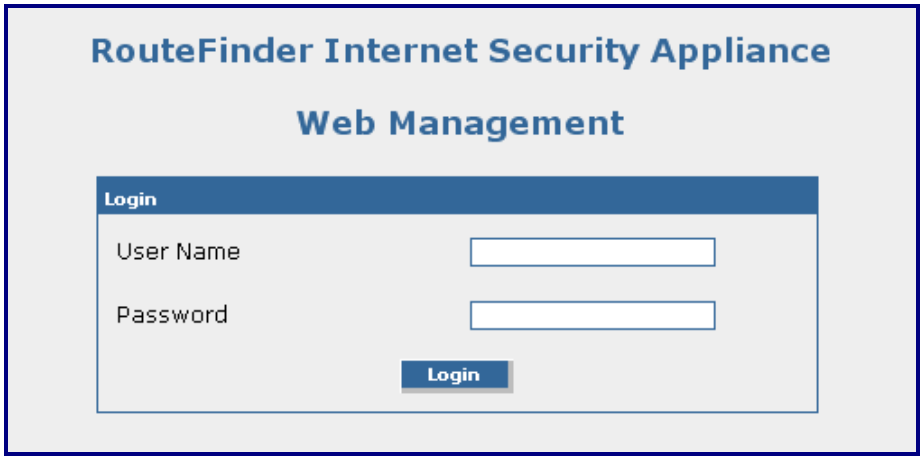
Login

The Login screen for the RouteFinder software displays.

- Type **admin** (*admin* is the default user name) in the user name box.
- Type **admin** in the password box.
- Click **Login**.

  Note: The **User name** and **Password** entries are case-sensitive (both must be typed in lower-case). The password can be up to 12 characters. Later, you will want to change the password from the default (**admin**) to something else (see the User Guide). If Windows displays the **AutoComplete** screen, you may want to click **No** to tell Windows OS to **not** remember the password for security reasons.

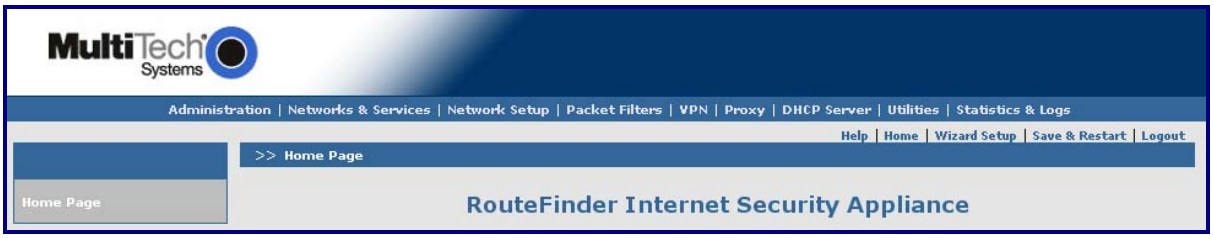
  Password Caution: Use a safe password! Your first name spelled backwards is not a sufficiently safe password; a password such as xfT35$4 is better. It is recommended that you change the default password. Create your own password.



Web Management Software Opens

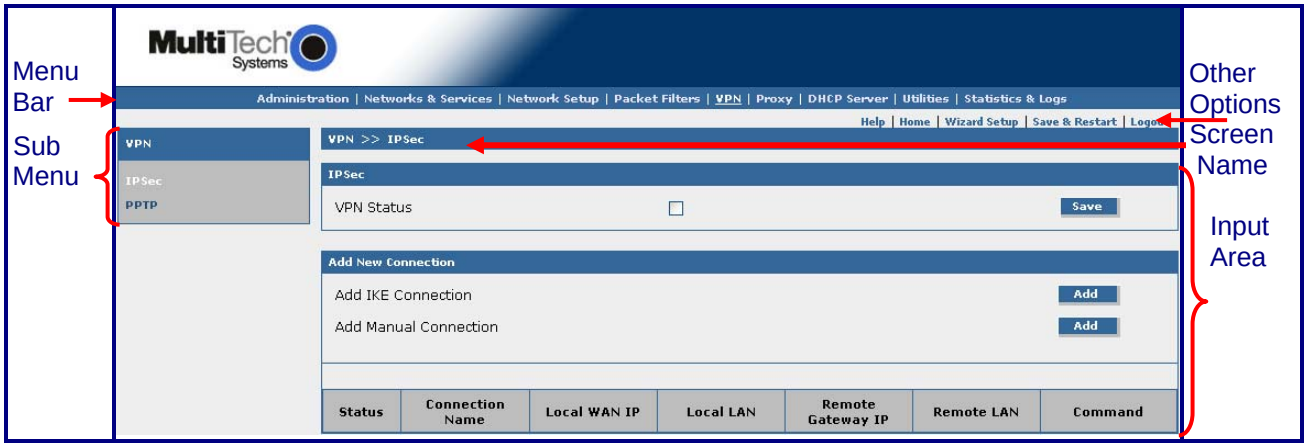
This is the Home screen from which you can access all setup functions.

Note: Only the top portion of the Home screen is shown here**.**



Navigating the Screens

Before using the software, you may find the following information about navigating through the screens and the structuring of the menus helpful.



Menu Bar

See menu categories and their submenus below.

Sub-Menus

Each Menu Bar selection has its own sub-menu, which displays on the left side of the screen.

When you click one of the Main Menu choices, the first screen listed in the sub-menu displays. You can choose other sub-menu options/screens by clicking on your sub-menu choice.

This is an example of the **Administration** sub-menu. It displays when you click **Administration**.

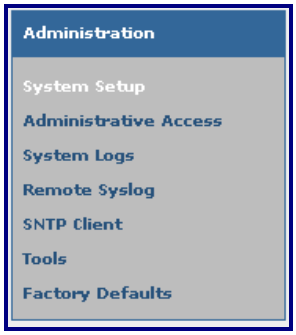


Table of Menus and Sub-Menus

Administration	Networks & Services	Network Setup	Packet Filters	VPN
System Setup Administrative Access System Logs Remote Syslog SNTP Client Tools Factory Defaults	Network Configuration Service Configuration	IP Settings Wireless LAN WLAN Security WLAN Client Filter Advanced IP Settings PPP Cellular/Analog Backup (RF820/RF820-AP only) Load Balancing (RF830/RF830-AP only) Dynamic DNS Static Routes IP Masquerading SNAT DNAT	Packet Filter Rules Advanced Filters ICMP Packet Filter Log	IPSec PPTP
Proxy	**DHCP Server**	**Utilities**	**Statistics & Logs**	
HTTP Proxy Custom Filters DNS Proxy	LAN LAN Subnet Settings LAN Fixed Addresses *These menu options:* Wireless LAN: WLAN Subnet Settings WLAN Fixed Addresses *display when you go to* ***Network Setup > Wireless LAN*** *and select* ***Independent Subnet***	Backup Firmware Upgrade	System Information Network Interface Details Packet Filter Log IPSec Live Log PPTP Live Log DHCP Server Live Log PPP Cellular/Analog Log (RF820/RF820-AP only) WLAN Client Live Log Log Traces	

Chapter 4 – Configuring the RouteFinder

Now that the cabling is completed and each PC on the network is configured to accept the IP addresses that the RouteFinder will provide, you are ready to configure your RouteFinder.

Note: The antenna must be attached in order for the RouteFinder to be operational.

About the Browser Interface

Initial configuration is required in order for you to begin operation. The browser-based interface eases configuration and management.

About IPSec

The VPN functionality is based on the IPSec protocol and uses 168-bit Triple DES (3DES) encryption to ensure that your information remains private.

Start the RouteFinder Configuration

1. **Connect your workstation.**

   Be sure your workstation is connected to one of the RouteFinder's LAN ports and that the antenna is attached to the RouteFinder.

2. **Apply power.**

   Apply power to the RouteFinder and wait for the Status LED to blink indicating that the unit is ready.

3. **Set the workstation IP address.**

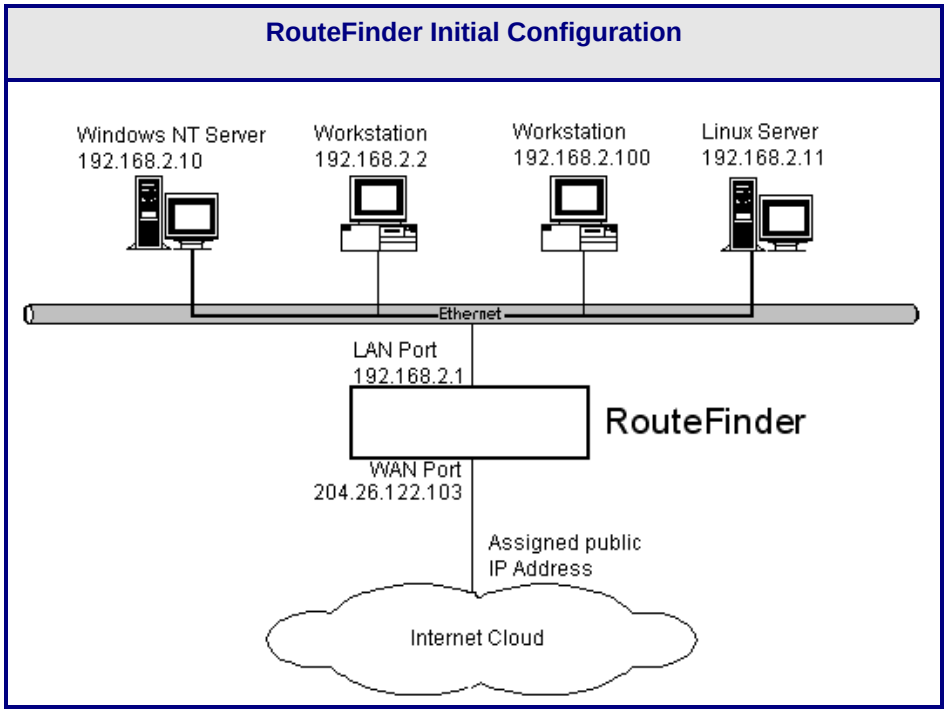
   The directions for setting your workstation IP address are covered in Chapter 3.

Using the Wizard Setup Screen to Configure Your RouteFinder

Using the Wizard Setup is a quick way to enter the basic configuration parameters to allow communication between the LAN workstation(s) and the Internet as shown in the example below.

Important Note: An initial configuration must be completed for each type of RouteFinder functions: firewall configuration, LAN-to-LAN configuration, a LAN-to-Remote Client configuration.

RouteFinder Initial Configuration



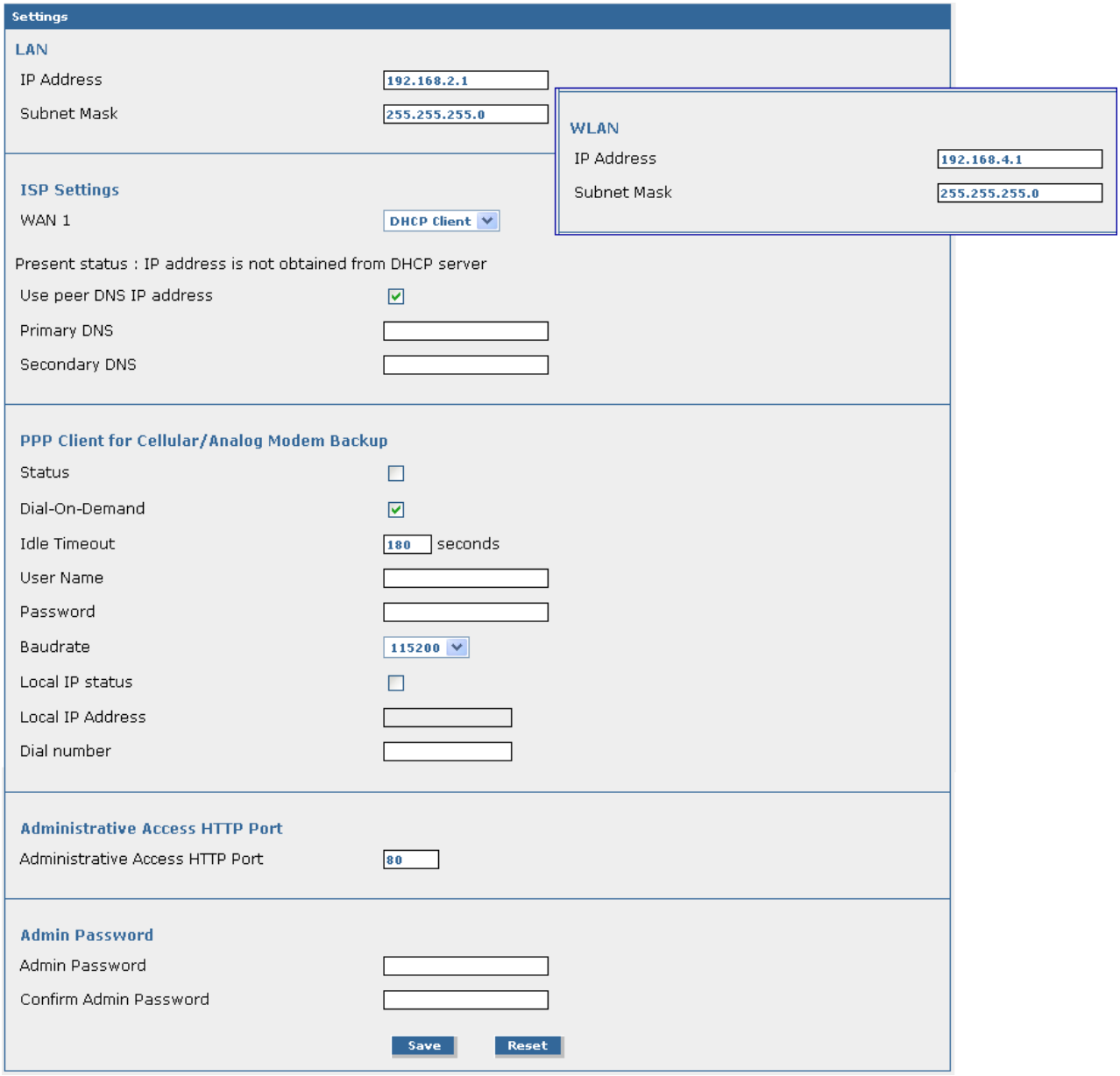
RF820/RF820-AP and RF830/RF830-AP Wizard Setup

Click the **Wizard Setup** button located under the Menu Bar. The following screen displays.

Use the same directions for the RF820/RF820-AP and RF830/RF830-AP.

Screen Notes:

- ***PPP Client for Cellular/Analog Modem Backup* is available on the RF820/RF820-AP only.**
- **The RF830/RF830-AP has two WAN ports; the RF820/RF820-AP only one. A WAN 2 section displays on the RF830/RF830-AP Wizard Setup screen for configuring this second port.**
- **If you are using the AP build, a section labeled *WLAN* (inset shown on the right of the screen shot) displays after you select *Independent Subnet* on the *Network Setup > Wireless LAN* screen.**



LAN

IP Address – 192.168.2.1 defaults into this field.

Subnet Mask – 255.255.255.0 defaults into this field. These should be acceptable for your site.

ISP Settings

WAN 1

Select the way the IP Address should be assigned for the WAN link. The default is **DHCP Client**. When you select **Static IP** or **PPPoE**, the input fields change.

- **WAN 1 DHCP Client Choice**

  DHCP (Dynamic Host Configuration Protocol) is a protocol that allows individual devices on an IP network to get their own network configuration information (IP address, subnet mask, broadcast address, etc.) from a DHCP server.

  Present Status: If the DHCP client is **not** enabled, the following message displays: *Present Status: IP address is not obtained from DHCP server.* If DHCP client is enabled, and if the IP address has been assigned by the DHCP server, then the following values will display:

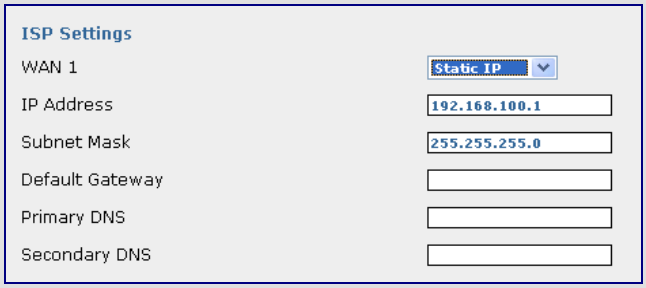
  Assigned IP Address
  Mask
  DHCP Server Address
  DNS Address
  Gateway Address
  Renew Time
  The time that the DHCP client should begin to contact its server to renew the lease it has obtained.
  Expiry Time
  Expiry time is the time that the DHCP client must stop using the lease if it has not been able to contact a server in order to renew.

  Use Peer DNS IP Address
  Check this box if you want the DNS server addresses from the peer (DHCP server) is to be obtained.
  Note: The DNS address obtained from the DHCP server will be displayed on the *Network Setup* > *Interface* screen.

  Primary DNS
  In this field, enter a primary domain server name (DNS). DNS (Domain Naming System) allows you to enter a name (i.e., mydomain.com) to be used in place of the computer's numeric IP address.

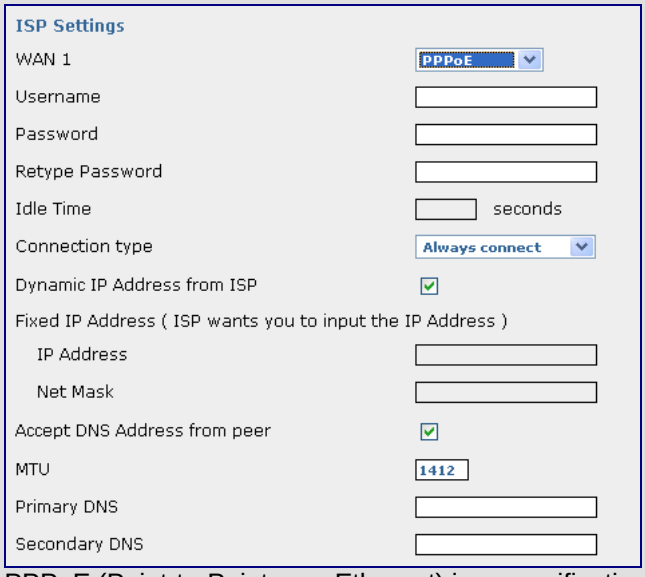
  Secondary DNS
  In this field, enter a secondary domain server name

- **WAN 1 Static IP Choice**



  If you choose Static IP for WAN 1, the IP Address (default is 192.168.100.1) and the Subnet Mask (default is 255.255.255.0) fields displays.
  Enter the *Default Gateway*, the *Primary DNS* address and the *Secondary DNS* address for the IP address provided.

- **WAN 1 PPPoE Choice**



PPPoE (Point-to-Point over Ethernet) is a specification for connecting multiple computer users on an Ethernet local area network to a remote site through DSL or cable modems or wireless connection to the Internet. The following fields display when you select PPPoE:

User Name

Enter the user name give by the ISP.
Example: user1@xyz.com or user 1

Password

Enter the user's password.
These characters are not allowed: <, >.
The maximum number of allowed is 18.

Retype Password

Retype the password to confirm the one entered above. Passwords must match in order to continue. If you receive an error, enter password in both fields again.

Idle Time

This option is available only when the Connection Type is *Trigger on Demand.* Specify the inactivity time (in seconds) after which the PPPoE link should be brought down.

Connection Type

Specify the type of connection for the link. Options are:
Always Connect: The link will always be established. It is not dependent on whether or not there is data or a traffic flow through the RouteFinder. **Default.**
Trigger on Demand: The link will be established only when there is data or a traffic flow through the RouteFinder.

Dynamic IP Address from ISP

Check the box to Enable the Dynamic IP address to be provided by the ISP. If enabled, the IP address obtained from the ISP is dynamic. If disabled, enter the IP address and subnet mask from the ISP in the following *Fixed Address* fields:
IP Address
Net Mask
Note: If the ISP does not support the Fixed Address option, then the RouteFinder will accept the dynamic IP address provided by the ISP.

Accept DNS Address from Peer

Check this box if you want the DNS server address to be obtained from the peer (the ISP). The DNS address obtained from the ISP will be displayed on the *Network Setup > Interface* screen. The details of the address/subnet mask obtained from the ISP are displayed as the *Present Status* on this screen.

(Continued on next page)

- **WAN 1 PPPoE Choice (Continued)**

  MTU

  A Maximum Transmission Unit (MTU) is the size (in bytes) of the largest packet that can be passed onwards. To read more about MTU, see the following Web site:
  The default for this field is 1412, which should be acceptable for most applications.
  http://en.wikipedia.org/wiki/Maximum_transmission_unit
  Also see the hyperlinked references listed on this Web site.

  Primary DNS

  In this field, enter a primary domain server name (DNS). DNS (Domain Naming System) allows you to enter a name (i.e., mydomain.com) to be used in place of the computer's numeric IP address.

  Secondary DNS

  If a secondary domain server name is configured, enter its name here. The servers are consulted in the order in which they are configured.

PPP Client for Cellular/Analog Modem Backup (For RF820/RF820-AP Only)

The PPP link is used as a backup link to the WAN interface. If the **Internet Keep-alive URLs** (see below) are not reachable through the WAN Ethernet interface, the PPP backup link automatically comes up and the system regains its connection to the ISP. The PPP dial backup settings are:

Status
Check this box to enable PPP Dial Backup on WAN interface.
User Name
Enter the user name to authenticate the RouteFinder with the ISP.
Password
Enter the user password. The password is optional. These special characters cannot be used: <, >.
Baud Rate
Select the serial baud rate from the drop down box.
Local IP Status
Check this box to enable support for negotiating an IP address with the ISP (this address will be enter in the next field).
Local IP Address
Enter the IP address from which the RouteFinder can negotiate for an IP address from the ISP.
Dial Number
Enter the PSTN number to be dialed.
Note
When the backup link comes up or goes down, an email alert is sent to the administrator.

Administrative Access HTTP Port (for RF820/RF820-AP & RF830/RF830-AP)

Select the HTTP port for administrative access. The default is port 80. The port number should be between 1 and 65535. Well known ports and ports used by the firewall are not allowed.

Admin Password (for RF820/RF820-AP & RF830/RF830-AP)

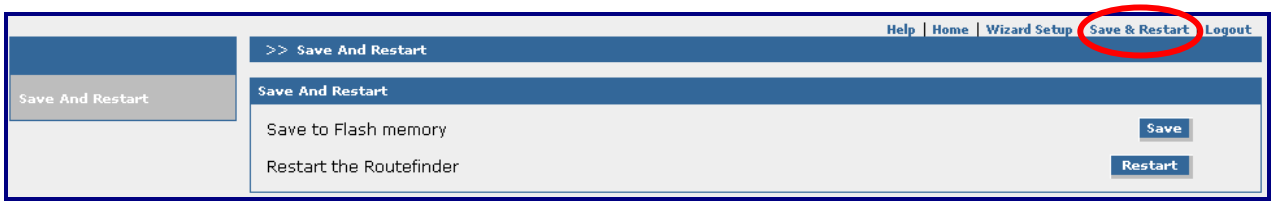
Change administrator's *Password*. Enter the password and a confirmation of the password. These characters are not allowed: <, >. Also, spaces are not allowed.

Save, Reset (for RF820/RF820-AP & RF830/RF830-AP)

Click **Save** located at the bottom of the screen to save these entries. Use **Reset** if you want to change the entries you have just made.

Save & Restart Button Under Menu Bar

Select the **Save and Restart** button located just under the menu bar. The *Save and Restart* screen displays.



Save to Flash Memory

If a connection is established, then the settings have been entered correctly and your basic configuration is now complete. Now, you must save your settings to the Flash Memory; this saves the current settings in the flash prom and prevents settings from getting lost at the next power up.

Restart

This is optional. You do not have to restart the RouteFinder after saving to the flash memory.

Your Basic Configuration Using the Setup Wizard is now Complete.

Important Note About *Save and Restart*

After you have completed and saved the settings for other settings within the Web management software, you must save your settings to the Flash Memory. This is a final step after you have saved the settings on each individual screen.

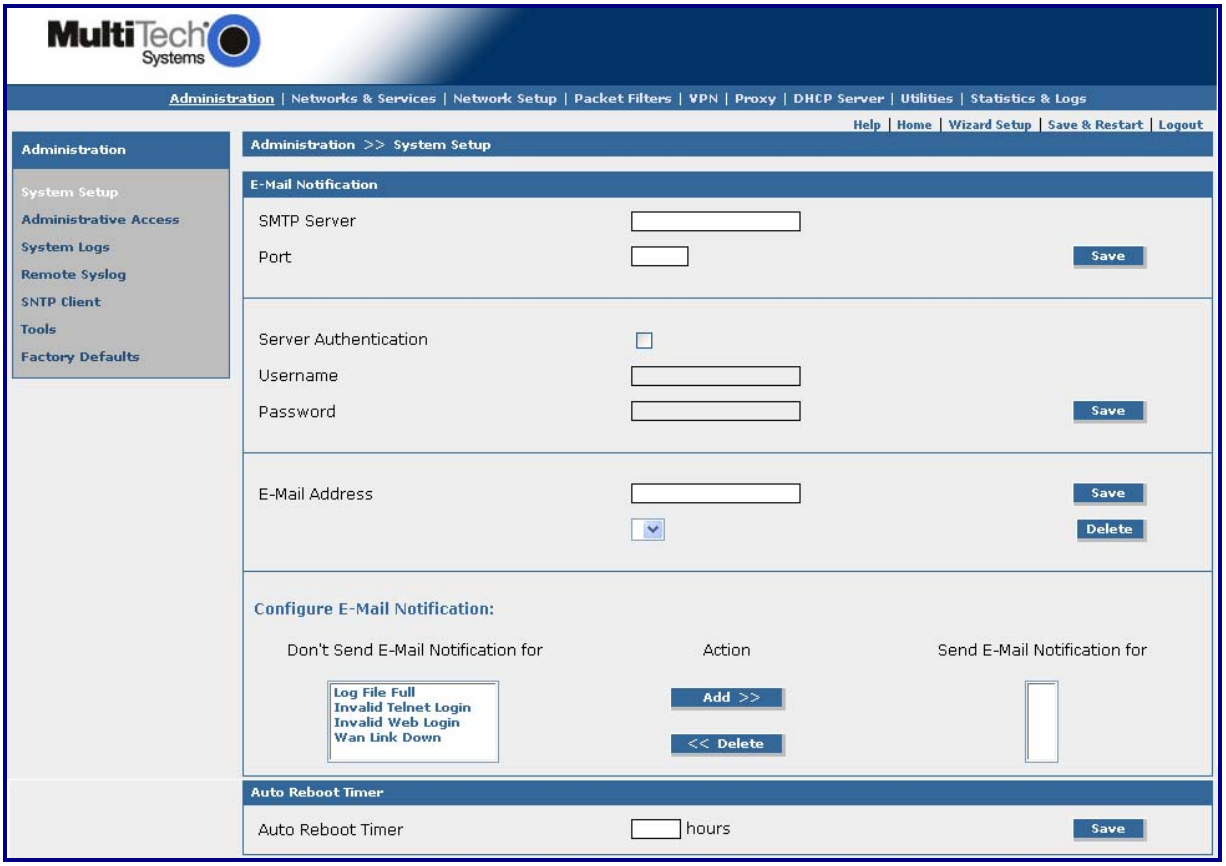
Chapter 5 – Configuration Using Web Management Software

This chapter takes you screen-by-screen through the software.

Administration

Administration › System Setup

In the *Administration* part of the software, you can set the RouteFinder general system-based parameters. *System Setup* includes the setting the Administrator's email address and the types of email notifications that will be sent to the System Administrator.



Email Notification

SMTP Server

Enter the IP address of the mail server.

SMTP Server

Enter the port number on which the mail server listens.

Server Authentication

Some mail servers accept connection only after a user name and password are authenticated.

User Name
If your mail server accepts connection only after a user name and password are authenticated, enter your user name.

Password
If your mail server accepts connection only after a user name and password are authenticated, enter your password.

Email Address
Enter the email address of the administrator who will receive the email notifications. Enter it in proper user@domain format. Click **Save**. You can delete the entry and change it at any time, if desired. At least one email address must be entered in this field.

Configure Email Notification
Select the types of notifications that you want sent (Invalid Telnet Login, Export File Backup, Log File Full, etc). Click the **Add** button. The name will then display in the *Send Email Notification For* box. You can remove a type by highlighting the type and clicking the **Delete** button. The name will then move back to the *Don't Send Email Notification For* box.

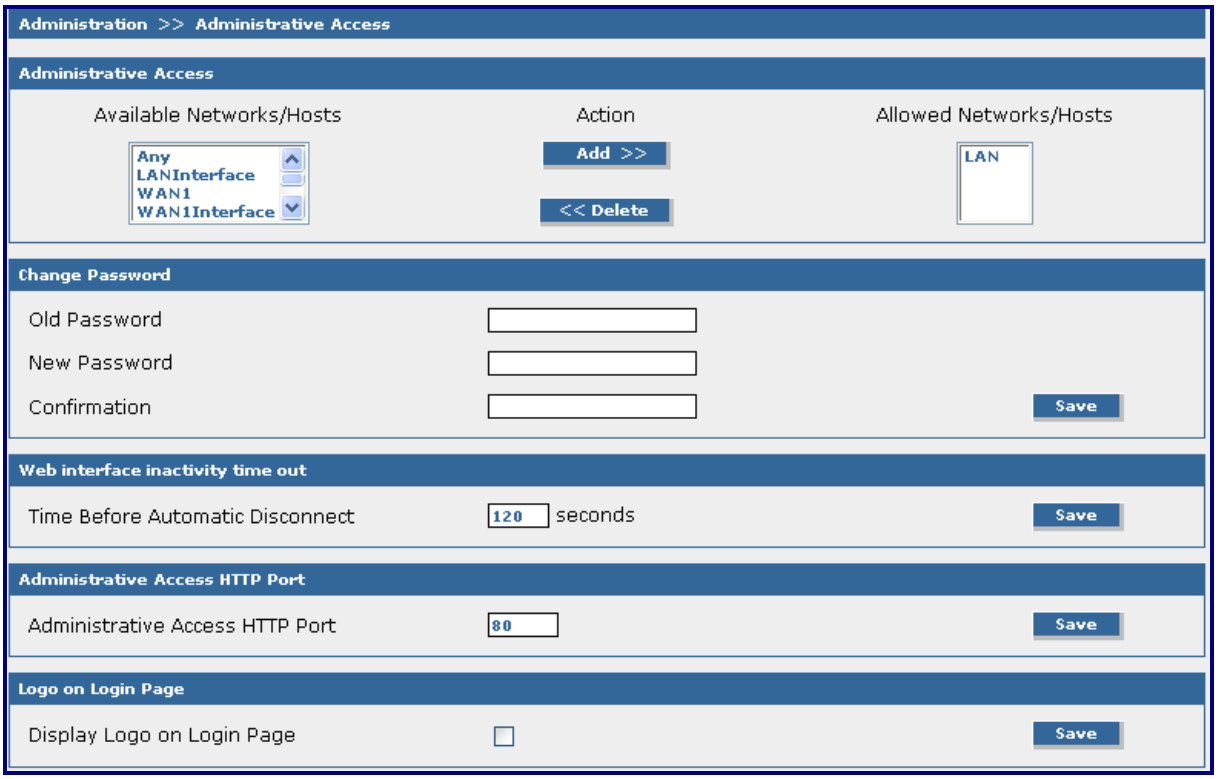
Auto Reboot Timer
Enter the number of hours you want the RouteFinder to automatically reboot. Then click **Save**.
Note: Setting the value to zero, disables the feature.

Administration › Administrative Access

The networks and hosts that are allowed to have administrative access are selected on this screen. This is a good way to regulate access to the configuration tools.

Screen Note:

If you are using the AP build and you select *Independent Subnet* on the *Network Setup > Wireless LAN* screen, *WLAN Interface* is available in the drop down list box of *Available Networks/Hosts*.



Administrative Access

Available Networks/Hosts and Allowed Networks/Hosts

Select the networks/hosts that will be allowed administrative access. Note that the selection box list will include those networks you enter under *Networks & Services > Network Configuration.*

You can change access by moving network/hosts names from the *Available* list to/from the *Allowed* list. The RouteFinder will display an ERROR message if you try to delete access to a network that would cause you to lock yourself out.

Note: Any defaults here for ease of installation. ANY allows administrative access from everywhere once a valid password is provided.

Caution: As soon as you can limit the location from which the RouteFinder is to be administered (e.g., your IP address in the internal network), replace the entry *ANY* in the selection menu with a smaller network. The safest approach is to have only one administrative PC given access to the RouteFinder. You can do this by defining a network with the address of a single computer from the *Networks and Services > Network Configuration* screen.

Change Password

You should change the password immediately after initial installation and configuration, and also change it regularly thereafter.

Old Password, New Password, Confirmation

To change the password, enter the existing password in the *Old Password* field, enter the new password into the *New Password* field, and confirm your new password by re-entering it into the *Confirmation* entry field.

Caution: Use secure passwords! For example, your name spelled backwards is not secure enough; something like **xfT35$4** is better.

Web Interface Inactivity Time Out

An automatic inactivity disconnection interval is implemented for security purposes. In the *Time Before Automatic Disconnect* entry field**,** enter the desired time span (in seconds) after which you will be automatically disconnected from the software program if no operations take place.

After the initial installation, the default setting is 120 seconds.

The smallest possible setting is 60 seconds.

The maximum setting is 3000 seconds.

If you close the browser in the middle of an open configuration session without closing via Exit, the last session stays active until the end of the time-out and no new administrator can log in.

Administrative Access HTTP Port

This field is used for setting the HTTP port for Web administration. After changing the HTTP port, the connection is terminated. The browser settings have to be changed for the new port number before starting the next session.

By default, port 80 is configured for HTTP sessions. The value of the port number should lie between 1 and 65535. Well known ports and ports already used by the firewall are not allowed.

If you want to use the HTTP service for other purposes (e.g., a diversion with **DNAT**), you must enter a different TCP port for the interface here. Possible values are 1-65535, but remember that certain ports are reserved for other services. We suggest you use ports 440-450. To have Administrative Access after the change, you must append the port to the IP address of the ROUTEFINDER separated by a colon (e.g., http://192.168.0.1:445).

Logo and Version on Logon Page

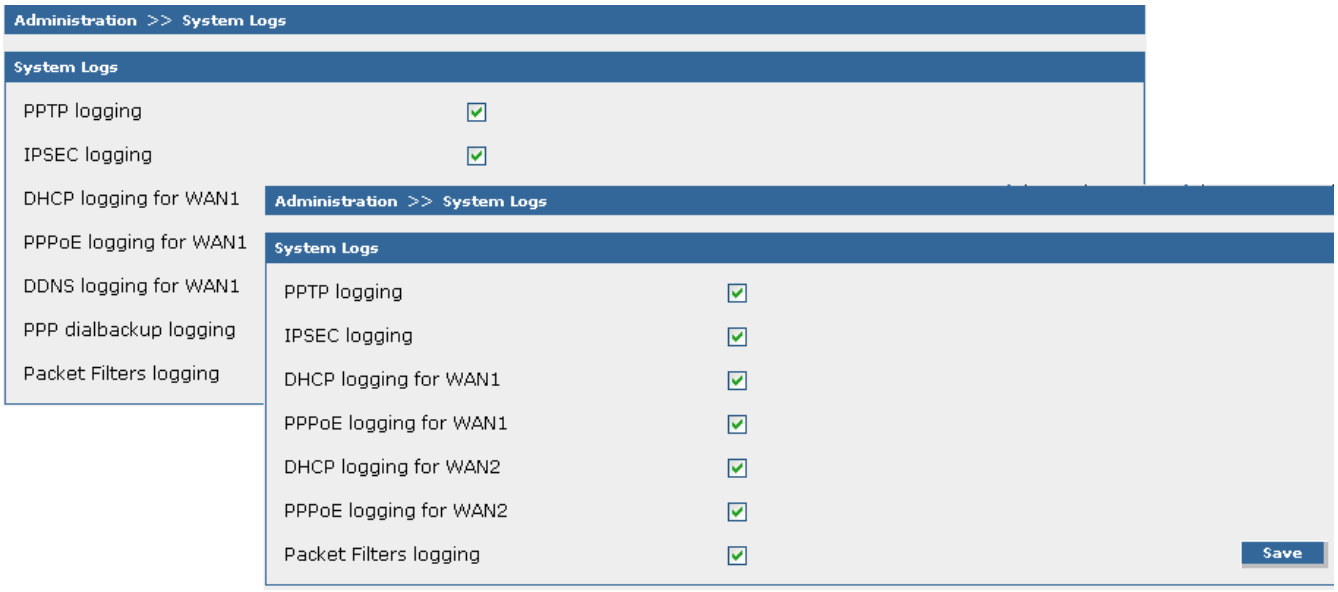
Check this box if you want the logo and version number to display on the logon page. Click **Save**.

Administration › System Logs

Screen Notes:

- ***PPP Dial Backup Logging* is available on the RF820/RF820-AP only.**
- **The RF830/RF830-AP has two WAN ports; the RF820/RF820-AP only one.**

RF820 Screen

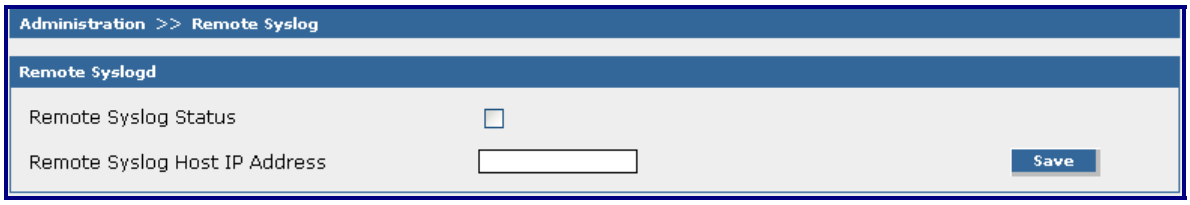


RF830 Screen

Enable System Logs

To enable the RouteFinder System Logs, place a checkmark across from the log you want enabled. Then click the **Save** button.

Administration › Remote Syslog



Note: Enabling Remote Syslog logging will slow down the performance of the RouteFinder. It should be used strictly for debugging purposes only.

Remote Syslog

Remote Syslog Status

Check the Remote Syslog Status box to enable the remote syslog function.

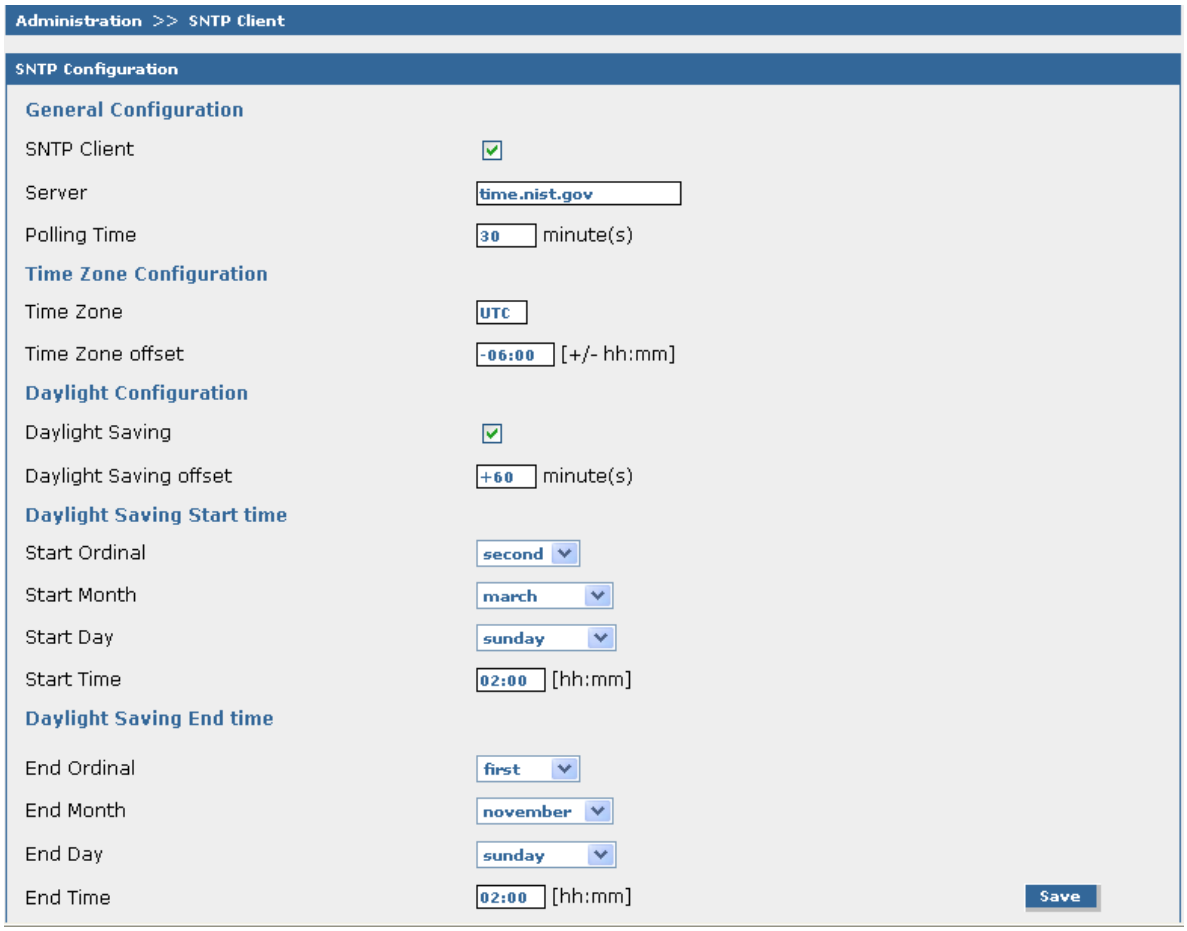
Remote Syslog Host IP Address

If Remote Syslog is enabled, then you must specify the Host IP Address. All log messages from the RouteFinder will be forwarded to this address.

On the remote host, syslog should be invoked with the “-r” option to enable the host to receive log messages from the other machines.

Administration › SNTP Client

SNTP (Simple Network Time Protocol) is an internet protocol used to synchronize the clocks of computers on the network. Clicking the SNTP Client check box enables the firewall to act as a SNTP client.



SNTP Configuration

General Configuration

SNTP Client

Enable or disable the SNTP Client to contact the configured server on the UDP port 123 and set the local time. Default is *Disable*.

Server

Enter the SNTP server name or IP address to which the SNTP Client must contact in order to update the time. No default.

Polling Time

Enter the polling time at which the SNTP client requests the server to update the time. Default is 300 minutes. Time must be entered in minutes.

Time Zone Configuration

Time Zone
Enter your time zone. Default = UTC (Universal Coordination).
See the following Web site for Time Zone information:
http://wwp.greenwichmeantime.com/info/timezone.htm

Time Zone Offset
Enter +/- hh:mm. Default = +00:00. Offset is the amount of time varying from the standard time of a Time Zone.

Daylight Configuration

Daylight Saving
Enables/disables Daylight Saving mode. Default is *Enable*.

Daylight Saving Offset
Set the offset to use during Daylight Saving mode. Default is *+60 minutes*. Enter the time in + / - minutes.

Daylight Saving Start Time

Start Ordinal
Set the start ordinal to use during Daylight Saving mode. Options are first/second/third/fourth/last. Default is *second*.

Daylight Saving time usually starts at the same time on the same day of the week in the same month every year. Each day of the week occurs four or five times a month. Therefore, you will be selecting the week in which daylight saving time starts: the first, second, third, fourth or the last of the month. In the U.S.A., daylight saving time starts at 2:00 a.m. on the second Sunday in March.

Start Month
Set the start month to use during Daylight Saving mode. Default is *March*.

Start Day
Set the start weekday to use during Daylight Saving mode. Default is *Sunday*.

Start Time
Set the start time to use during Daylight Saving mode. Default is 02:00 (hh:mm).

Daylight Saving End Time

End Ordinal
Set the end ordinal to use during Daylight Saving mode. Select the week in which daylight saving time ends. Options are first/second/third/fourth/last. Default is *first*.

End Month
Set the end month to use during Daylight Saving mode. Default is *November*.

End Day
Set the end weekday to use during Daylight Saving mode. Default is *Sunday*.

End Time
Set the end time to use during Daylight Saving mode. Default is 02:00 (hh:mm).

Submit Button

Click the **Submit** button to save these settings.

Administration › Tools

There are three tools that can help you test and maintain network connections and RouteFinder functionality.

Ping and **Trace Route** test the network connections on the IP level.

The **DDNS** Client is used to update the IP address of the modem/router in a DDNS server for the configured domain name whenever the IP Address changes, thus, leaving the domain name to be pointing to the current IP Address of the modem/router all the time.

Screen Notes:

1. For these tools to function, the ICMP on firewall function in **Packet Filter > ICMP** must be enabled.
2. For the Name Resolution function, enable the DNS proxy function in **Proxy > DNS Proxy**. To use the Name Resolution function, enable a name server in the menu (item) **Proxy > DNS Proxy**. When the Name Server is enabled, the IP addresses of the reply packets will be converted into valid names.
3. The screen for the RF830/RF830-AP has an additional section for *DDNS WAN 2*.

PING

Ping is an acronym for Packet Internet Groper. 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.

If you PING an IP address, the PING utility will send four packets and stop.

If you add a -t to the end of the command, the PING utility will send packets continuously.

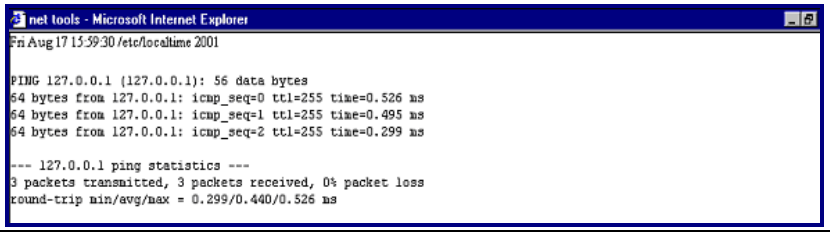
Host — Specify the IP address/name of the other PC for which connectivity is to be checked.

No. of Pings — Select the number of pings. You can choose 3 (the default), 10 or 100 pings. Enter the IP address or the name into the Host entry field (e.g., port **25** for SMTP).

Timeout — Specify the time that packets can exist.

Packet Size — Specify the number of data bytes to be sent.

Start Button — After clicking **Start**, a new window opens with the PING statistics accumulating.



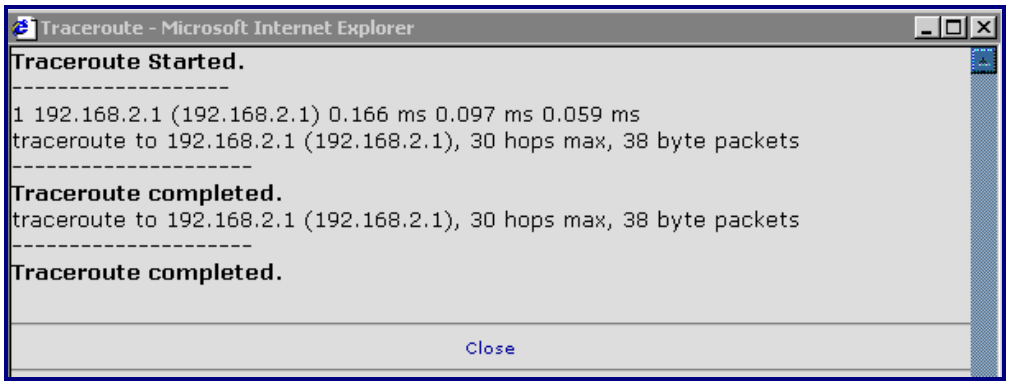
Trace Route

Trace Route is a tool for finding errors in the network routing. It lists each router's addresses on the way to remote systems. If the path for the data packets is temporarily unavailable, the interruption is indicated by asterisks (*****). After a number of tries, the attempt is aborted. The interrupted connection can have many causes, including the packet filter on the RouteFinder not allowing the operation of Trace Route.

Trace Route lists the path of the data packets all the way to the desired IP address. The path ends when the destination address has been reached. Should the data packets' path momentarily not be traceable, stars (*****) appear to indicate a time-out. After a fixed number of time-outs, the attempt is aborted. This can have various reasons (e.g., a packet filter doesn't allow Trace Route). If it is not possible to locate a name despite activated name resolution, the IP address is shown after several attempts instead.

Host Specify the **IP address** or the name of the other computer to test this tool.

Start Click the **Start** button to start the test.



A Sample Trace Route Log

DDNS – WAN 1

DDNS Force Update

Click the **Update** button to force the DDNS to update condition. Note that the RF830/RF830-AP screen has an input section for setting up DDNS – WAN 2

DDNS Status

Click the **Refresh** button to display the DDNS Status after a forced update.

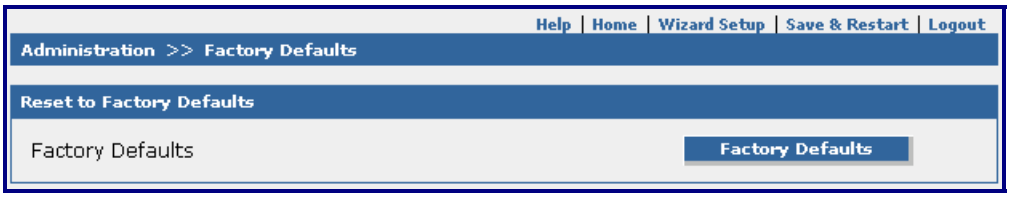
Reset Modem

Reset the Modem

Click the **Reset** button to reset the modem.

Administration › Factory Defaults

Use this screen to load the original RF820/RF820-AP or RF830/RF830-AP factory defaults.



Reset to Factory Defaults

Factory Defaults

Click the **Factory Defaults** button to load the default settings.

Networks & Services

Networks & Services › Network Configuration

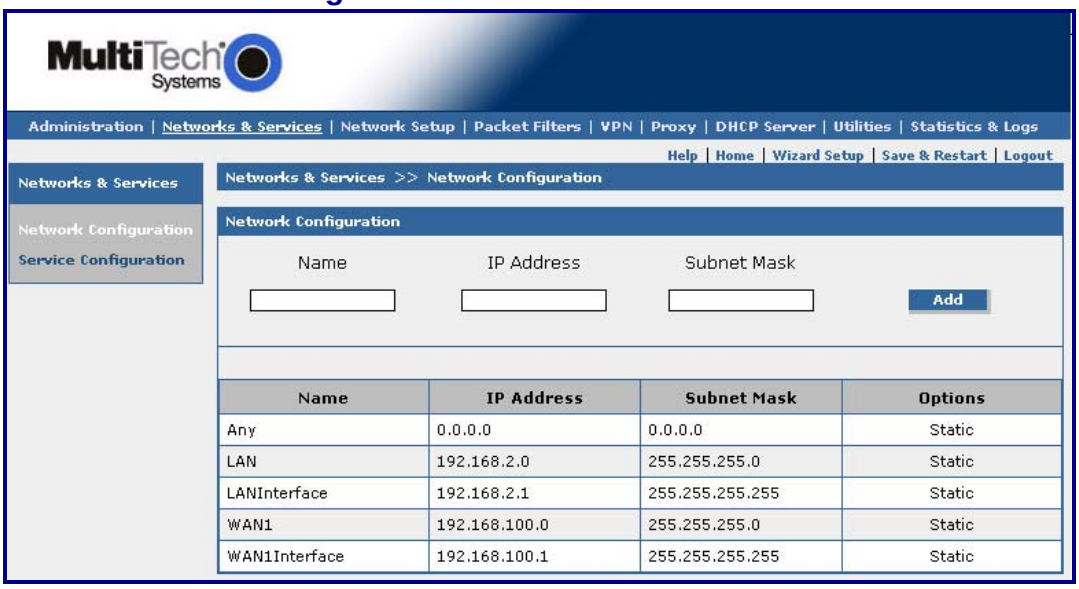
The names, addresses, and network masks or hosts are defined here. **Edit** and **Delete** options are used for editing or deleting the networks/hosts. However, the name of the network/host cannot be edited. The Edit link has to be clicked in order to change the address or mask entries. When you click **Edit**, the corresponding address and mask displays. The changed entries can be saved by clicking the **Save** button. For all other screens where that particular network/host is being used, the corresponding change in the IP address or mask will be made automatically. The networks/hosts can be deleted only if is not used for any route or by any other module.

If a network is being used by the routing screen, that network cannot be edited. Similarly, if a host address is edited and changed to a network address, and if that host was used by SNAT or DNAT, the change will not be performed.

Network Entries on the Network Configuration Screen Will Display on the Following Screens

Administration > Administration Access
Network Setup > Static Routes
Network Setup > IP Masquerading
Network Setup > SNAT, DNAT
Packet Filters > Packet Filter Rules
Network Intrusion Detection
VPN > IPSec
VPN > PPTP
VPN > HTTP Proxy

RF820 Network Configuration Screen



RF820-AP Network Configuration Screen

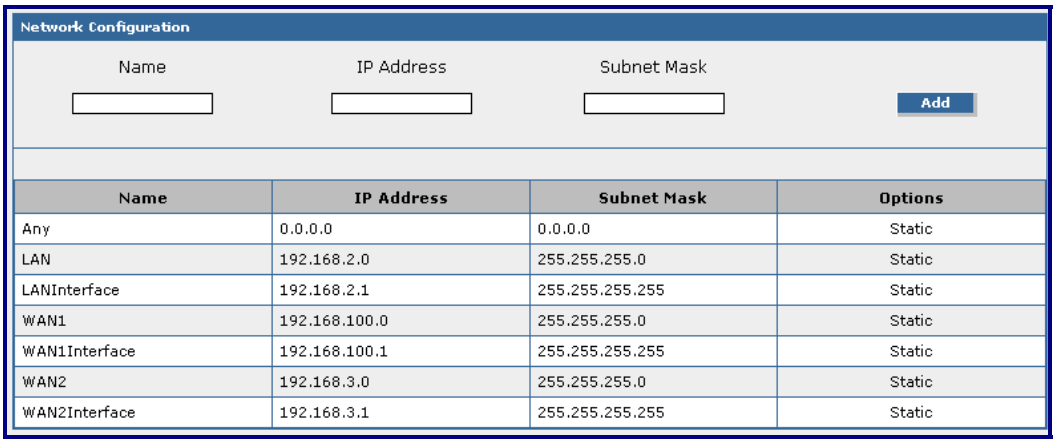
Note that the AP build will show the additional networks: WLAN and WLANInterface.

Name	IP Address	Subnet Mask	Options
Any	0.0.0.0	0.0.0.0	Static
LAN	192.168.2.0	255.255.255.0	Static
LANInterface	192.168.2.1	255.255.255.255	Static
WLAN	192.168.4.0	255.255.255.0	Static
WLANInterface	192.168.4.1	255.255.255.255	Static
WAN1	192.168.100.0	255.255.255.0	Static
WAN1Interface	192.168.100.1	255.255.255.255	Static

RF830/RF830-AP Network Configuration Screen

Screen Note:

If the AP build is used, it will display the additional networks: WLAN and WLANInterface.



Name	IP Address	Subnet Mask	Options
Any	0.0.0.0	0.0.0.0	Static
LAN	192.168.2.0	255.255.255.0	Static
LANInterface	192.168.2.1	255.255.255.255	Static
WAN1	192.168.100.0	255.255.255.0	Static
WAN1Interface	192.168.100.1	255.255.255.255	Static
WAN2	192.168.3.0	255.255.255.0	Static
WAN2Interface	192.168.3.1	255.255.255.255	Static

Network Configuration Fields

Name

Enter the name of network or host you want added to the list. This name has to unique; in other words, it should not be present in the displayed list. A space cannot be used in the name; it is considered an invalid character.

IP Address

Enter the IP address of the new network or host. The same address-mask pair should not be present in the displayed list.

Subnet Mask

Enter the network mask for the network/host. For host addresses, the mask is entered 255.255.255.255

How to Confirm Your Entries

Confirm your entries by clicking the **Add** button.

After a successful definition, the new network is entered into the network table. This network will now be referenced in other menus under this name. You can edit and delete networks by clicking **Edit** or **Delete** in the **Options** column for the network you want to change. The **Edit Network Publications** (in this example) is displayed. The name of the network cannot be changed, but the IP Address and Subnet Mask can be edited. You can delete a newly created network by clicking on **Delete** in the Options column for a desired network.

Example 1: IP address 192.168.2.1 – Subnet mask 255.255.255.0 – Define a private Class-C net.

Example 2: IP address 216.200.241.66 – Subnet mask 255.255.255.255 – Define a host in the Internet.

Note About Entries: Entries can be made in the dot notation style (e.g. 255.255.255.0 for a class C network).

Important Network Notes:

- LAN and WAN interfaces will change if changes are made to LAN/WAN IP addresses in Network Setup.
- To define a single host, enter its IP address and use a netmask of 255.255.255.255. Technically, single hosts are treated in the same way as networks.
- You can also use the bit "spelling" for the Subnet mask (e.g., write 30 instead of 255.255.255.252).
- A network or host can be deleted only if it is not used for any route or by any other module.
- If a network is being used by a routing section, that network cannot be edited. Similarly, if a host address is edited and changed to a network address, and if that host was used by SNAT or DNAT, the changed will not be performed.

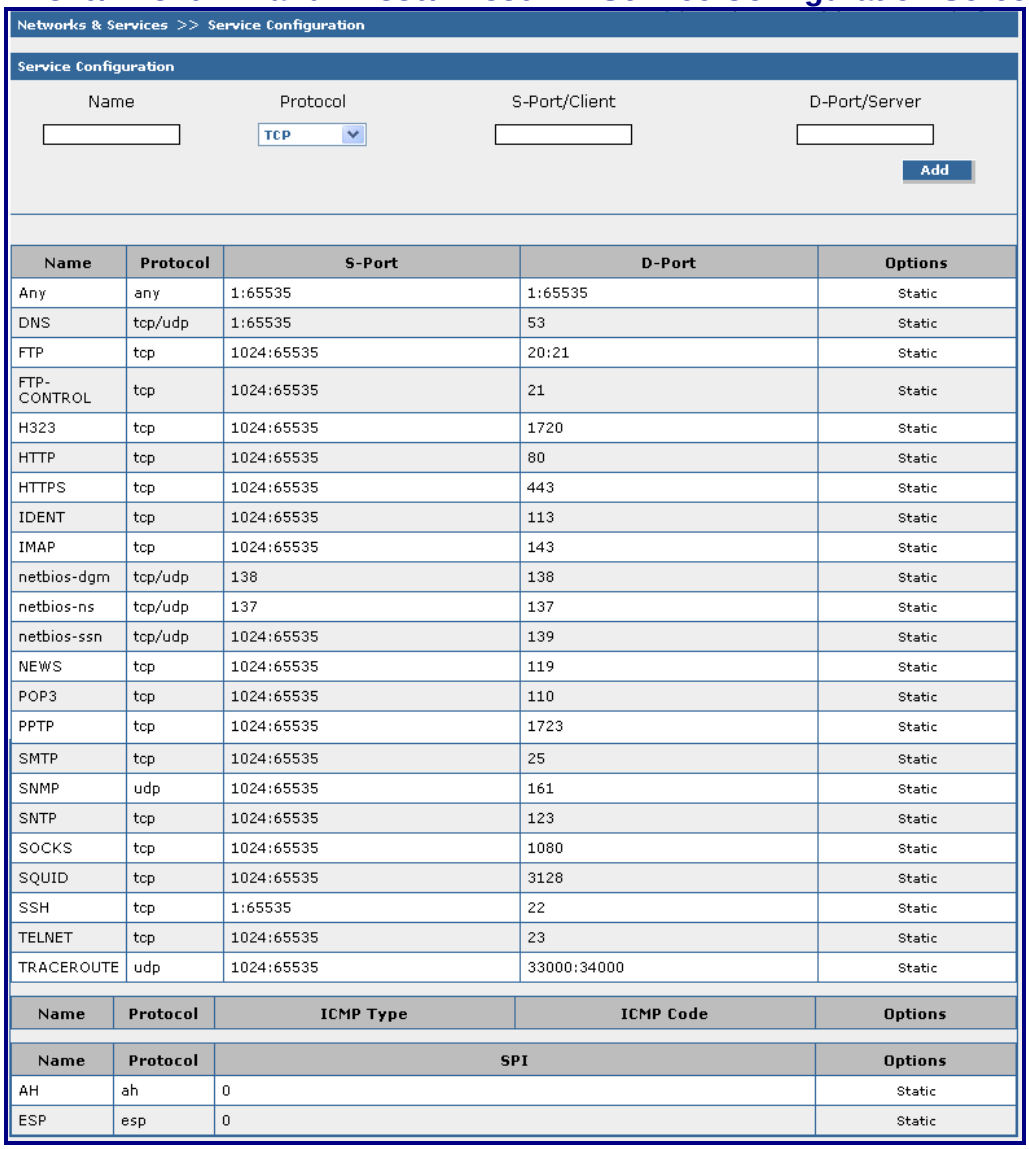
Networks & Services › Services

On this screen you can specify the standard set of well known services available on the system. These services enable the configuration of the user defined services. The options to Delete or Edit a service after it has been defined and added are available by using the table at the bottom of the screen. However, standard sets of well known services cannot be edited or deleted.

Service Entries on This Service Configuration Screen Will Display on the Following Screens

Packet Filters > Packet Filter Rules
Packet Filters > Advanced Filters > MAC Address Based Filtering
Network Setup > SNAT, DNAT

RF820/RF820-AP and RF830/RF830-AP Service Configuration Screen



Networks & Services >> Service Configuration

Service Configuration

Name | Protocol (TCP) | S-Port/Client | D-Port/Server | Add

Name	Protocol	S-Port	D-Port	Options
Any	any	1:65535	1:65535	Static
DNS	tcp/udp	1:65535	53	Static
FTP	tcp	1024:65535	20:21	Static
FTP-CONTROL	tcp	1024:65535	21	Static
H323	tcp	1024:65535	1720	Static
HTTP	tcp	1024:65535	80	Static
HTTPS	tcp	1024:65535	443	Static
IDENT	tcp	1024:65535	113	Static
IMAP	tcp	1024:65535	143	Static
netbios-dgm	tcp/udp	138	138	Static
netbios-ns	tcp/udp	137	137	Static
netbios-ssn	tcp/udp	1024:65535	139	Static
NEWS	tcp	1024:65535	119	Static
POP3	tcp	1024:65535	110	Static
PPTP	tcp	1024:65535	1723	Static
SMTP	tcp	1024:65535	25	Static
SNMP	udp	1024:65535	161	Static
SNTP	tcp	1024:65535	123	Static
SOCKS	tcp	1024:65535	1080	Static
SQUID	tcp	1024:65535	3128	Static
SSH	tcp	1:65535	22	Static
TELNET	tcp	1024:65535	23	Static
TRACEROUTE	udp	1024:65535	33000:34000	Static

Name	Protocol	ICMP Type	ICMP Code	Options

Name	Protocol	SPI	Options
AH	ah	0	Static
ESP	esp	0	Static

This is an example of screen with the TCP protocol selected.

Service Configuration

Name

Enter the name of network or host you want added to the list. This name has to unique; in other words, it should not be present in the displayed list. A space cannot be used in the name; it is considered an invalid character. After you have entered the name, click the **Add** button.

Protocol

Select from the following protocols: **TCP, UDP, TCP & UDP, ICMP, AH,** and **ESP**. When you select one of the protocols, the fields to the right will change according to the protocol selected.

TCP, UDP, and TCP& UDP

S-Port/Client

Enter the source port for the service. The entry options are a single port (e.g. 80), a list of port numbers separated by commas (e.g. 25, 80, 110), or a port range (e.g. 1024:64000) separated by a colon (**:**).

D-Port/Server

Enter the Destination port.

ICMP

ICMP Type

Choose the Type from the drop down box.

ICMP Code

Choose the Code from the drop down box.

AH and ESP

SPI Value

Enter the SPI value.

Editing and Deleting User-Added Services

There are options for editing or deleting the user added services. However, there are some standard services which cannot be edited or deleted. If the service is used by the Packet Filter rules, SNAT, or DNAT, it cannot be deleted.

For editing any user-defined service, the **Edit** button has to be clicked to get the fields corresponding to the service entry.

Edit By clicking **Edit** in the Options column, the information is loaded into the entry menu of the **Edit Service** screen. You can then edit the entry. You can edit user-added services only. The entries can be saved using the **Save** button.

Delete By clicking **Delete** in the Options column, the service is deleted from the Services table. Changes can be saved using the **Save** button.

Notes About Protocols

- **TCP & UDP** allow both protocols to be active at the same time.
- The **ICMP** protocol is necessary to test network connections and RouteFinder functionality, as well as for diagnostic purposes. In the *Packet Filter* > *ICMP* menu you can enable *ICMP Forwarding* between networks, as well as RouteFinder ICMP reception (e.g., to allow **ping** support).
- The **ESP** protocol is required for Virtual Private Network (VPN).
- The **AH** protocol is required for Virtual Private Network (VPN).
- For **AH** and **ESP**, the **SPI** is a whole number between 256 and 65536, which has been mutually agreed upon by the communication partners. Values below 256 are reserved by the Internet Assigned Numbers Authority (IANA).

Network Setup

Network Setup › IP Settings

Screen Notes:

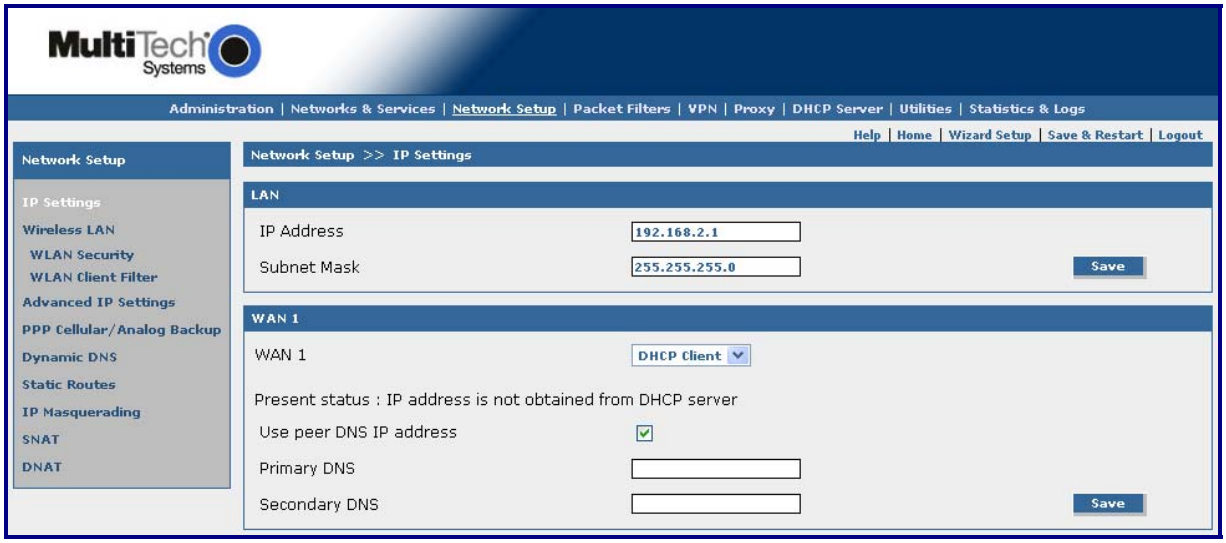
Submenu Differences Between the RF820/RF820-AP and RF830/RF830-AP

- The RF820/RF820-AP submenu lists a screen for *PPP Cellular/Analog Modem Backup*.
- The RF830/RF830-AP submenu lists a screen for *Load Balancing.*

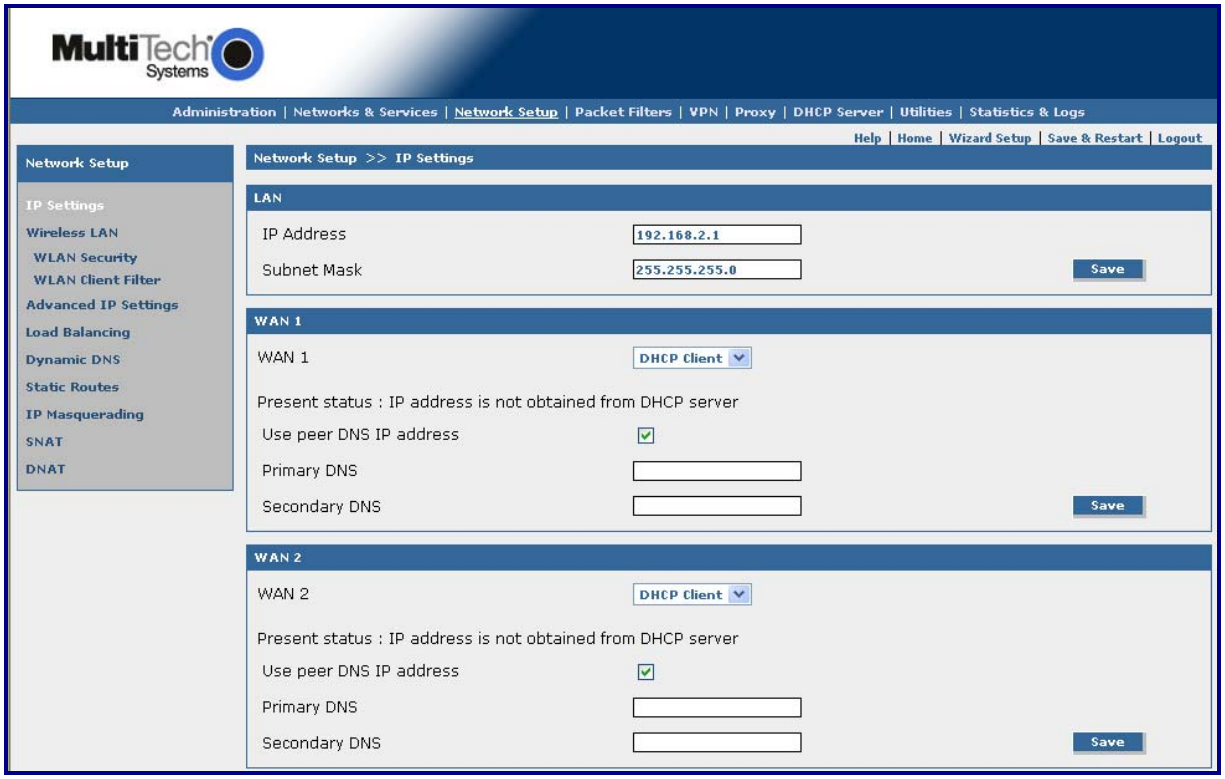
Screen Differences Between the RF820/RF820-AP and RF830/RF830-AP

- The RF830/RF830-AP includes an additional input section for *WAN 2*.

RF820/RF820-AP Network > IP Settings Screen



RF830/RF830-AP Network > IP Settings Screen



LAN

IP Address
192.168.2.1 defaults into this field.

Subnet Mask
255.255.255.0 defaults into this field.
These should be acceptable for your site.

WAN 1 & WAN 2 (WAN 2 is for the RF830/RF830-AP only)

Select they way the IP Address should be assigned for the WAN link. The default is **DHCP Client**. When you select **Static IP** or **PPPoE**, the input fields change.

WAN Choice: DHCP Client (Default)

DHCP (Dynamic Host Configuration Protocol) is a protocol that allows individual devices on an IP network to get their own network configuration information (IP address, subnet mask, broadcast address, etc.) from a DHCP server.

Present Status
If the DHCP client is not enabled, the following message displays: *Present Status: IP address is not obtained from DHCP server.* If DHCP client is enabled, and if the IP address has been assigned by the DHCP server, then the following values will be displayed on the page:

Assigned IP Address
Mask
DHCP Server Address
DNS Address
Gateway Address
Lease to be Renewed on (the time that the DHCP client should begin to contact its server to renew the lease it has obtained)
Lease Expires on (time at which the DHCP client must stop using the lease if it has not been able *to contact a server in order to renew it)*

Use Peer DNS IP Address
Check this box if you want the DNS server addresses from the peer (DHCP server) is to be obtained; otherwise, it should be unchecked. The DNS address obtained from the DHCP Server will display on this screen.

WAN Choice: Static IP

If you choose Static IP for WAN 1, the IP Address (default is 192.168.100.1) and the Subnet Mask (default is 255.255.255.0) fields displays.
Enter the *Default Gateway*, the *Primary DNS* address and the *Secondary DNS* address for the IP address provided.

Default Gateway
Enter the default gateway address. Default: 192.168.100.1

Primary DNS
In this field, enter a primary domain server name (DNS). DNS (Domain Naming System) allows you to enter a name (i.e., mydomain.com) to be used in place of the computer's numeric IP address.

Secondary DNS
In this field, enter a secondary domain server name.

WAN Choice: PPPoE

PPPoE (Point-to-Point Protocol over Ethernet) is a specification for connecting multiple users on an Ethernet local area network to a remote site through DSL or cable modems or wireless connection to the Internet. The following fields display when you select PPPoE:

User Name

Enter the ADSL user name give by the ISP.
Example: user1@xyz.com or user 1

Password

Enter the user's password.
These characters are not allowed: <, >.
Maximum characters allowed are 18.

Retype Password

Retype the password to confirm the one entered above. Passwords must match in order to continue. If you receive an error, enter password in both fields again.

Idle Time

This option is available only when the Connection Type is *Trigger on Demand*. Specify the inactivity time (in seconds) after which the PPPoE link should be brought down.

Connection Type

Specify the type of connection for the link. Options are:
Always Connect: The link will always be established. It is not dependent on whether or not there is data or a traffic flow through the RouteFinder. **Default.**
Trigger on Demand: The link will be established only when there is data or a traffic flow through the RouteFinder.

Dynamic IP Address from ISP

Check the box to enable the Dynamic IP address from the ISP. If enabled, the IP address obtained from the ISP is dynamic. If disabled, enter the IP address and subnet mask from the ISP in the following *Fixed Address* fields:

IP Address
Subnet Mask

Note: If the ISP does not support the Fixed Address option, then the RouteFinder will accept the dynamic IP address provided by the ISP.

Accept DNS Address from Peer

Check this box if you want the DNS server address to be obtained from the peer (the ISP). The DNS address obtained from the ISP will be displayed on the *Network Setup* > *Interface* screen. The details of the address/subnet mask obtained from the ISP are displayed as the Present Status on this screen.

MTU

A Maximum Transmission Unit (MTU) is the size (in bytes) of the largest packet that can be passed onwards. To read more about MTU, see the following Web site:
The default for this field is 1412, which should be acceptable for most applications.
http://en.wikipedia.org/wiki/Maximum_transmission_unit
Also see the hyperlinked references listed on this Web site.

Primary DNS

In this field, enter a primary domain server name (DNS). DNS (Domain Naming System) allows you to enter a name (i.e., mydomain.com) to be used in place of the computer's numeric IP address.

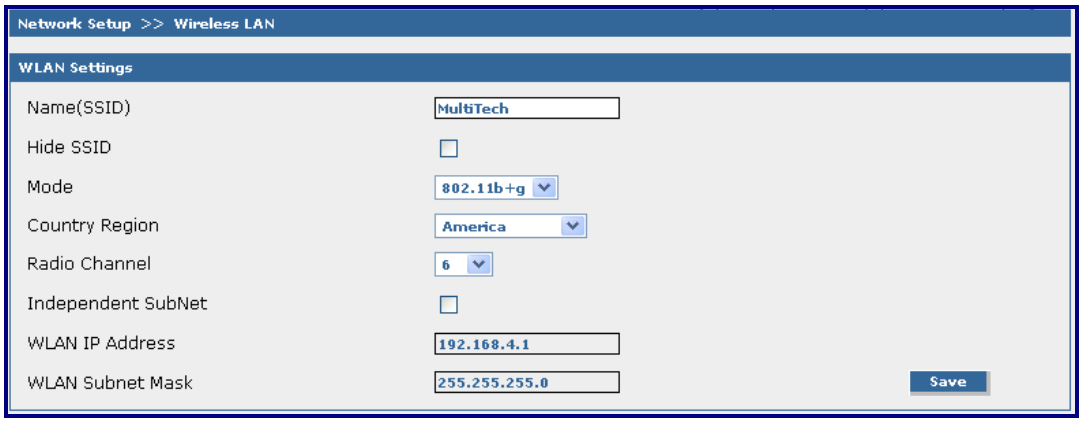
Secondary DNS

In this field, enter a secondary domain server name. The servers are consulted in the order in which they are configured.

Network Setup › Wireless LAN

Screen Note: This screen applies to the RF820-AP and RF830-AP only.

Use the following screen to setup the wireless LAN (WLAN) interfaces.



WLAN Settings

Name (SSID)

An SSID is the name of a wireless local area network (WLAN). All wireless devices on a WLAN must employ the same SSID in order to communicate with each other. SSIDs are case sensitive, consist of a sequence of alphanumeric characters (letters and numbers), and have a maximum length of 32 characters. Example: Multi-Tech.

Hide SSID

Check this box to hide the SSID.

Mode

Select the Wi-Fi mode. Mode ***g*** supports a maximum speed of 54M bps. Mode ***b*** supports a maximum speed of 11M bps. Mode ***b+g*** is compatible with both ***b Only Clients*** as well as ***g Clients***.

Country or Region

Choose the Country or Region in which this device will be used.

Radio Channel

Select the Radio Channel allowed in the selected country or region.

Independent Subnet

Check this box if you would like the Wireless LAN located on a different Network from the default LAN Network.

When you check this box and **Save** this screen, you will be able to set up a separate Network subnet address for the wireless LAN. You might want to use this to give a certain workstation access to the Internet and not to the your local network or *vice versa.*

Additionally, once the Independent Subnet box is checked, the following options become available on the *DHCP Server* sub-menu for setting up the separate subnet address:

Wireless LAN
WLAN Subnet Settings
WLAN Fixed Addresses

WLAN IP Address

Specify the IP Address of the WLAN Interface.

WLAN Subnet Mask

Specify the WLAN Subnet Mask.

Network Setup › Wireless LAN › WLAN Security

Screen Note: This screen applies to RF820-AP and RF830-AP only.

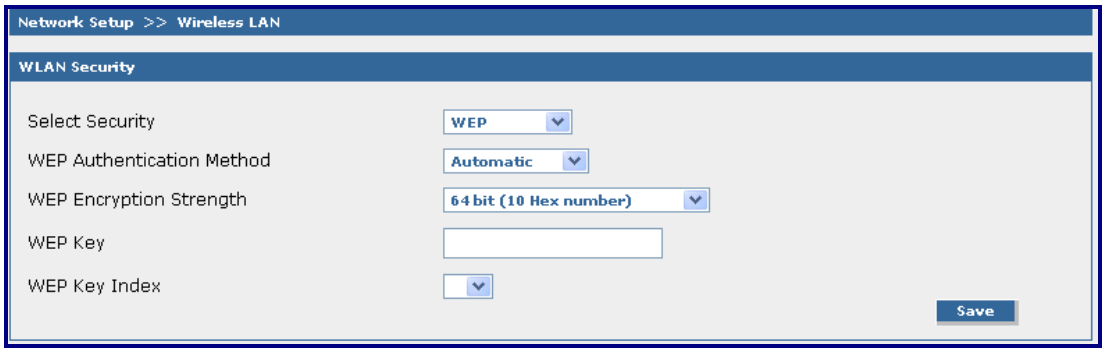
Select the Security option for the Wireless LAN network. The default is *Disable*.

WLAN Security

Select Security

Select the Security option from the drop down box for the Wireless LAN network. Each selection will display a separate set of input fields.

- **Security Selection – Disable**
  This option provides no security for the WLAN network.
- **Security Selection – WEP**



WEP (Wired Equivalency Privacy) offers the privacy equivalent to that of a wired LAN. If activated, data is encrypted before transmission, and then the receiving station, such as an access point or another radio, performs decryption upon arrival of the data. 802.11 WEP encrypts data only between 802.11 stations.

WEP Authentication Method

Automatic – Automatic authentication allows any wireless station configured with the Open System / Shared Key authentication method to associate with the AP.

Open System – Using Open Authentication, any wireless station can request authentication. Open Authentication allows any device access to the network.

Shared Key – Using Shared Authentication, each wireless station is assumed to have received a secret shared key over a secure channel that is independent from the 802.11 wireless network communications channel. Shared Key Authentication requires that the client configure a static WEP key. The client is granted only if it passed a challenge-based authentication.

WEP Encryption Strength

The choices are:
64 bit (10 Hex number)
64 bit (5 ASCII characters)
128 bit (26 Hex number)
128 bit (13 ASCII characters)

WEP Key

The WEP Key is used to encrypt/decrypt the data. Enter the Key value based on the WEP Encryption Strength.

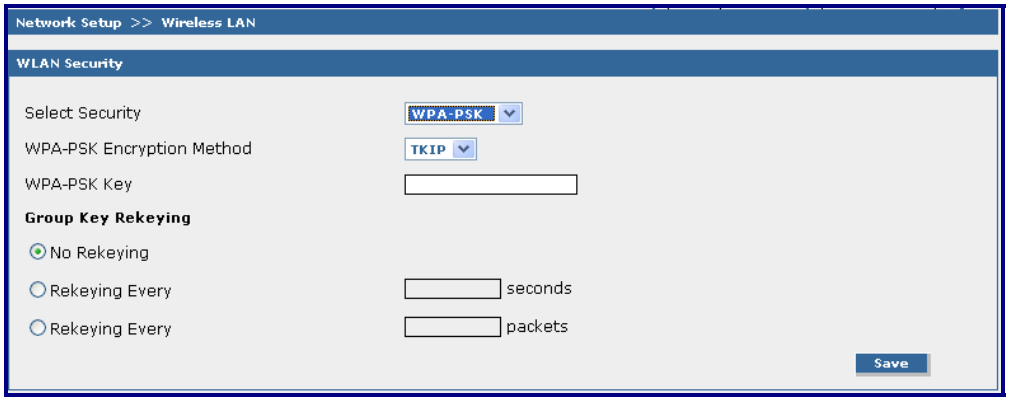
WEP Key to Index

The Key Index shows in which order the WEP Key values are stored.
Example: *WEP Key Index: 1*
This means that the WEP Key is stored as the first WEP Key in the configuration.

- **Security Selections – WPA-PSK and WPA2-PSK**

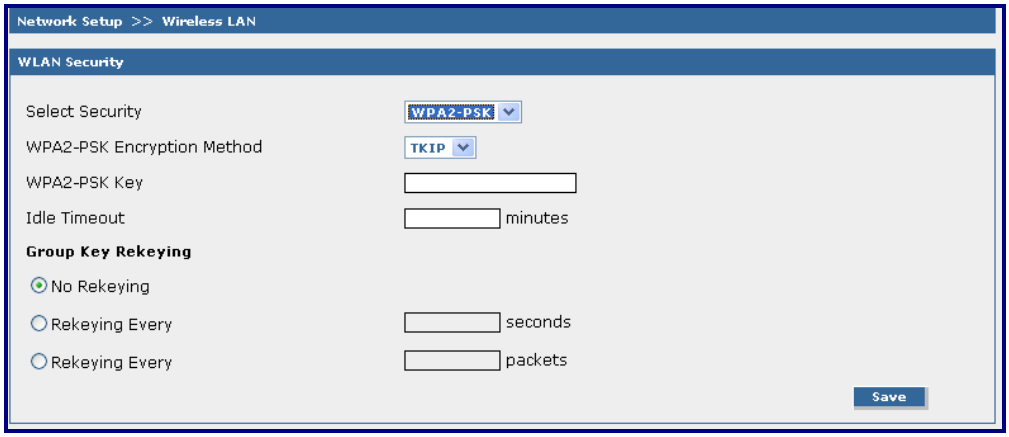
This is the WAP-PSK screen.

Screen Note: This screen applies to RF820-AP and RF830-AP only.



This is the WPA2-PSK screen.

Screen Note: This screen applies to RF820-AP and RF830-AP only.



Wi-Fi Protected Access (WPA) is a class of systems to secure wireless (Wi-Fi) computer networks. WPA is designed for use with an IEEE 802.1x authentication server, which distributes different keys to each user. However, it can also be used in a less secure "pre-shared key" (PSK) mode in which every user is given the same passphrase. Pre-Shared Key mode (PSK, also known as personal mode) is designed for home and small networks that cannot afford the cost and complexity of an 802.1x authentication server. Each user must enter a passphrase to access the network.

WPA-PSK/WPA2-PSK Encryption Method

Select an encryption method. The choices are:

TKIP – TKIP (Temporal Key Integrity Protocol) is a security protocol used in Wi-Fi Protected Access (WPA).

AES – AES (Advanced Encryption Standard), also known as Rijndael, is a block cipher adopted as an encryption standard.

WPA-PSK/WPA2-PSK Key

Enter a sequence of digits to be used for your preshared key. The WPA preshared key should be a random sequence of hexadecimal digits between 8 and 63 digits.

Idle Timeout (for WPA2-PSK only)

Enter the amount of idle time in minutes that will pass before the Key will timeout (for the WPA2-PSK Key only).

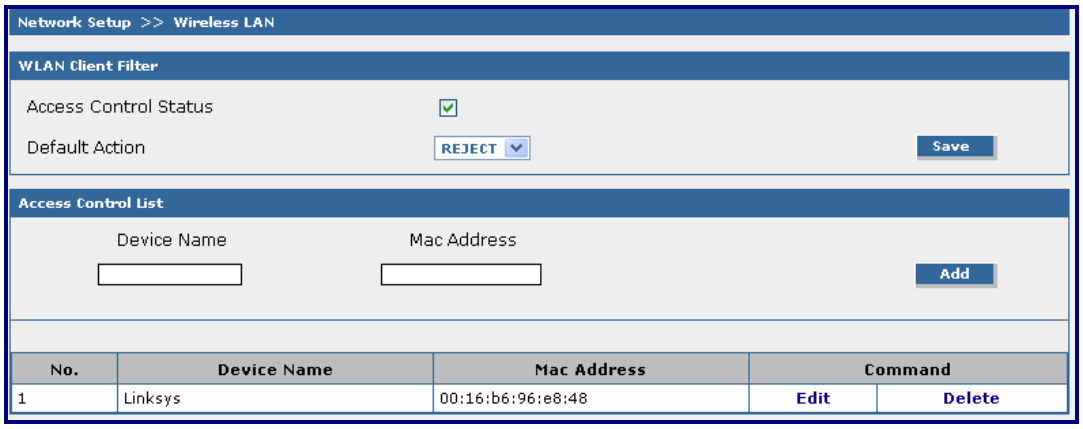
Group Key Rekeying

The encryption keys are automatically changed (called rekeying) and authenticated between devices after a specified period of time or after a specified number of packets has been transmitted. This is called the rekey interval.

Select either **No Rekeying**, **Rekeying Every** (number of seconds and enter the number of seconds desired), or **Rekeying Every** (number of packets and enter the number of packets desired).

Network Setup › Wireless LAN › WLAN Client Filter

Screen Note: This screen applies to the RF820-AP and RF830-AP only.



WLAN Client Filter

The WLAN Client Filter is used to Allow/Reject the wireless station's association with the Access Point.

Access Control Status

Check this box to enable Access Control on the WLAN.

Default Action

Choices are:

ALLOW – Select this to allow the WLAN Client based on the Access Control list.

REJECT – Select this to deny the WLAN Client based on the Access Control list.

Access Control List

Device Name

Enter the name of the device that will be allowed access to the WLAN.

Mac Address

Enter Mac Address of the device that will be allowed access to the WLAN.

Add Button

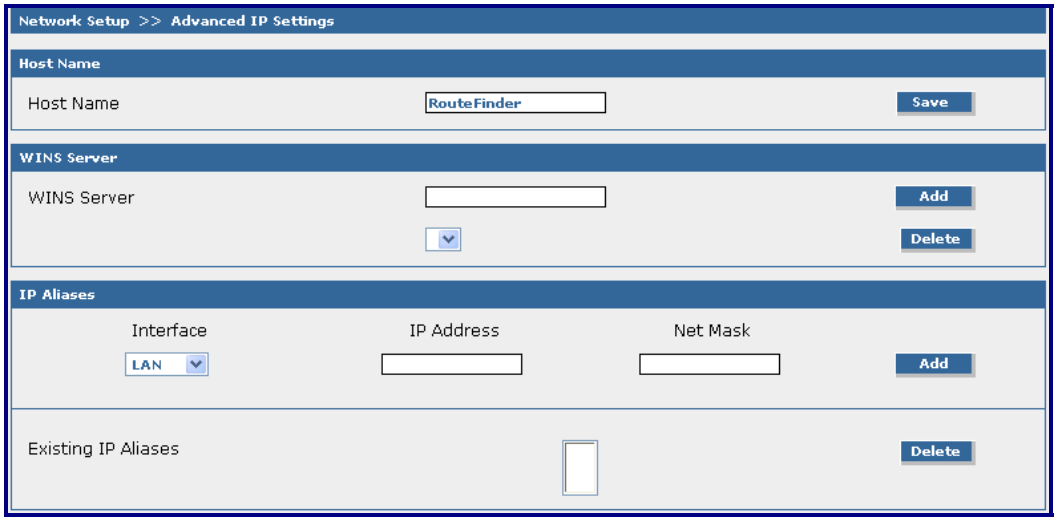
Click the **Add** button after the Device Name and Mac Address have been entered. They will then display at the bottom of the screen.

Add/Edit/Delete

The maximum number of devices allowed on the Access Control List is 20.
You can **Edit** and **Delete** clients from the list at the bottom of the screen.

Network Setup › Advanced IP Settings

Specify the Host Name, the External Server for the system and the IP Aliases for each of the interfaces.



Host Name

The Host Name must be defined for your RouteFinder. The name must be entered into this format: FIREWALL.mydomain.com. Click the **Save** button.
Example: Localhost.xscale.com

WINS Server

Enter a name for the WINS Server. Click the **Add** button.

IP Aliases

Multiple IP addresses can be assigned to a network interface using IP Aliases. The RouteFinder will treat the additional addresses as equals to the primary network card addresses. IP aliases are required to administer several logical networks on one network card. They can also be necessary in connection with the SNAT function to assign additional addresses to the firewall.
Note: The same IP Address cannot be configured many times for an interface. Similarly, the same IP Address cannot be entered as an IP Alias Address for two different interfaces.

Interface

From the drop down list box, select the network name to which you want to assign an alias.

IP Address

Enter the network IP address for the network named.

Netmask

Enter the Netmask to be used for this network.

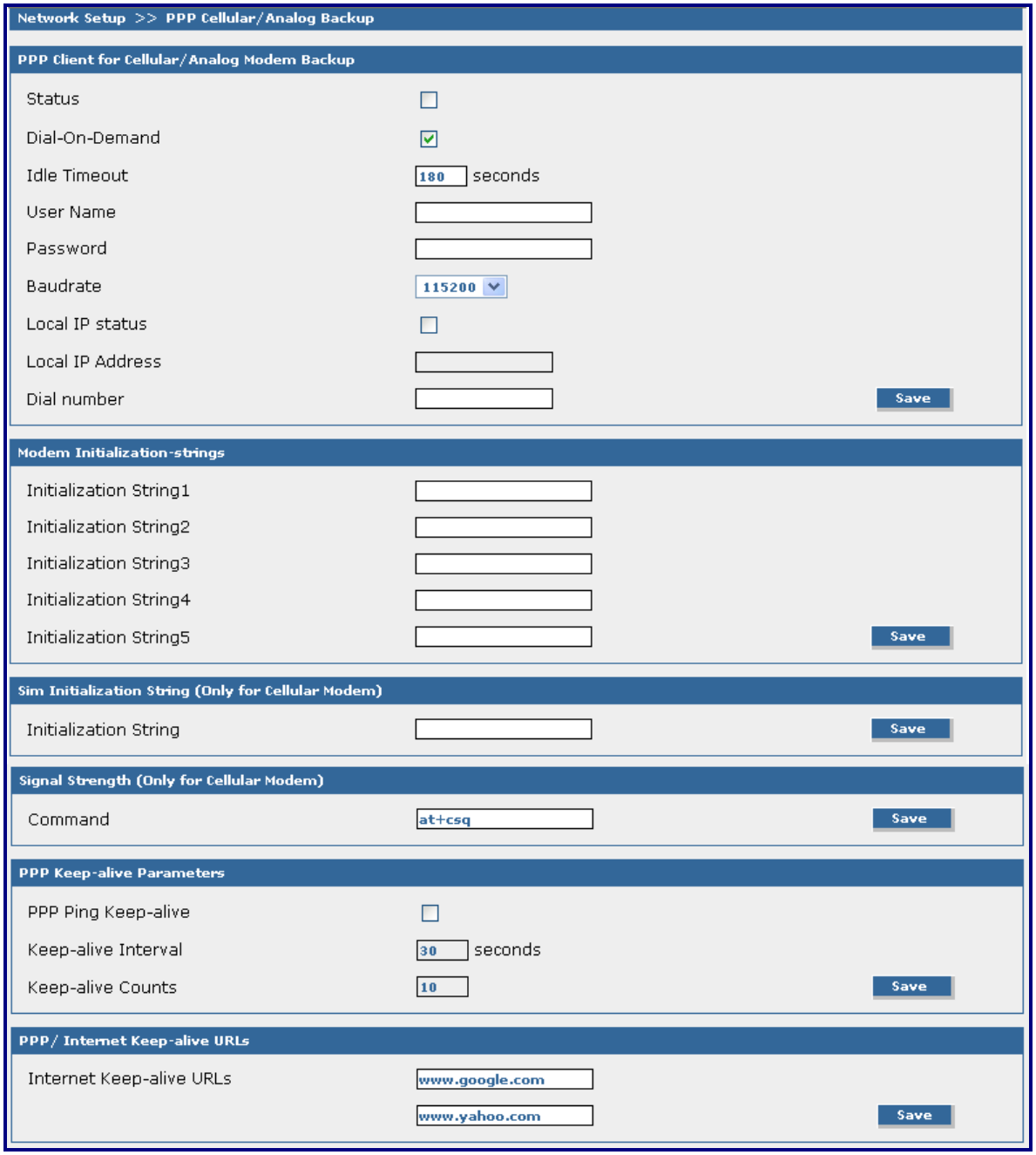
Save and Delete

Click the **Save** button when finished. An IP alias is deleted by highlighting it in the table and then clicking the **Delete** button.

Network Setup › PPP Cellular/Analog Backup

Screen Note: This screen applies to the RF820/RF820-AP only.

The PPP link is used as a backup link to the WAN interface. If the **Internet Keep-alive URLs** (see below) are not reachable through the WAN Ethernet interface, the PPP backup link automatically comes up and the system regains its connection to the ISP.



PPP Client for Cellular/Analog Modem Backup

Status

Check this box to enable PPP Dial Backup on WAN interface.

Dial-On-Demand

Check this box to initiate dial-on-demand, which automatically makes the connection when there is traffic.

Idle Timeout
Enter the amount of time in seconds that you want to elapse before the link will disconnect. The link will stay connected as long as there is traffic.

User Name
Enter the user name to authenticate the RouteFinder with the ISP. The *User Name* is optional.

Password
Enter the user password. These special characters cannot be used: <, >. The *Password* is optional.

Baud Rate
Select the serial baud rate from the drop down box.

Local IP Status
Check this box to enable support for negotiating an IP address with the ISP (this address will be enter in the next field).

Local IP Address
Enter the IP address from which the RouteFinder can negotiate for a certain IP address from the ISP.

Dial Number
Enter the PSTN number to be dialed.

Note: When the backup link comes up or goes down, an email is sent to the administrator.

Click the **Save** button after all the above information is entered.

Modem Initialization Strings
Initialization Strings
Enter the modem initialization string. An initialization (init) string is a list of commands sent to the modem to initialize and prepare it for a connection. The init string typically sets options such as speed, error correction, compression, various timeout values, and how to display results to the user. Click the **Save** button after the initialization strings are entered.

SIM Initialization String (only for Cellular Modems)
Initialization String
Enter the SIM initialization string. The SIM initialization string is sent to the cellular modem during boot up in order to initialize the Cellular SIM. This is not applicable for analog modems. Click the **Save** button after the initialization string is entered.

Signal Strength (only for Cellular Modems)
Command
Enter the command or use this default command to find out the cellular signal strength. This is not applicable for analog modems. Click the **Save** button.

PPP Keep-Alive Parameters
PPP Ping Keep-Alive
Check this box to enable the PPP Keep-Alive function on the dial backup link. Once the link is up, this option checks whether the PPP link is alive or not by periodically pinging to the Keep-Alive URLs at a specified interval. This will not occur when the link is down.

Keep-Alive Interval
Enter the amount of time in seconds that the pinging to the Keep-Alive URLs should occur.

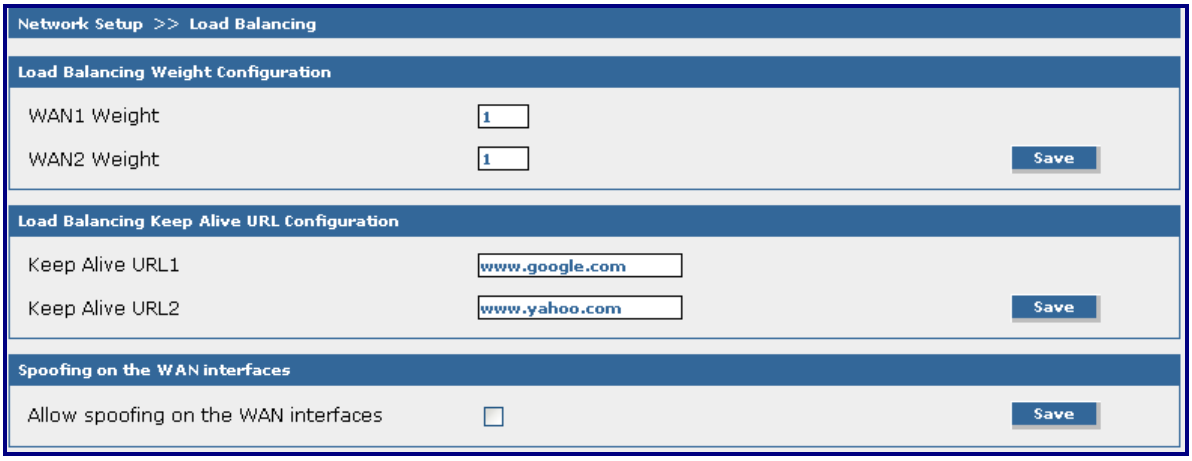
Keep-Alive Counts
Enter a number that specifies how many ping packets should be sent to each URL. The default is 10. Click the **Save** button.

PPP/Internet Keep-Alive URLs
Internet Keep-Alive URLS
The two URLs you enter here will be used to check to see if the Internet is reachable through the WAN/PPP links. If the Internet is not reachable through the WAN link, then the link is assumed to be down and all the traffic will be forwarded through the PPP link. The same URLs are used for the PPP Keep-Alive function. These URLs can either be a valid domain or a valid Public IP address. Example: www.google.com. Click the **Save** button.

Network Setup › Load Balancing

Screen Note: Load Balancing applies to the RF830/RF830-AP only.

Load Balancing distributes LAN-to-LAN traffic over two or more WAN links. This allows for the amount of traffic on each line to be based on a specified weighed value so that communication can be made faster and more reliable.



Load Balancing Weight Configuration

WAN1 & WAN2 Weight

Enter a numeric value from 1 to 10 in the *Weight* fields. This value sets the number of data packets to be sent/received by WAN1 before the communication process is transferred to WAN2.
A value of 3 for each WAN link seems to work well. However, if one WAN link is faster than the other, then you might want to enter a higher number for that link; e.g., use a 3:1 ratio.
After entering both weights, click *Save*.

Load Balancing Keep Alive URL Configuration

Keep Alive URL1 & URL2

Enter the *Keep Alive URL* address. Then click **Save**.
An ICMP echo request is sent to the configured URLs entered here. The request triggers the system to check the connectivity to the Internet through the WAN Ethernet interface(s). Supports a maximum of two URLs.

Spoofing on the WAN Interfaces

Allow Spoofing on the WAN Interface

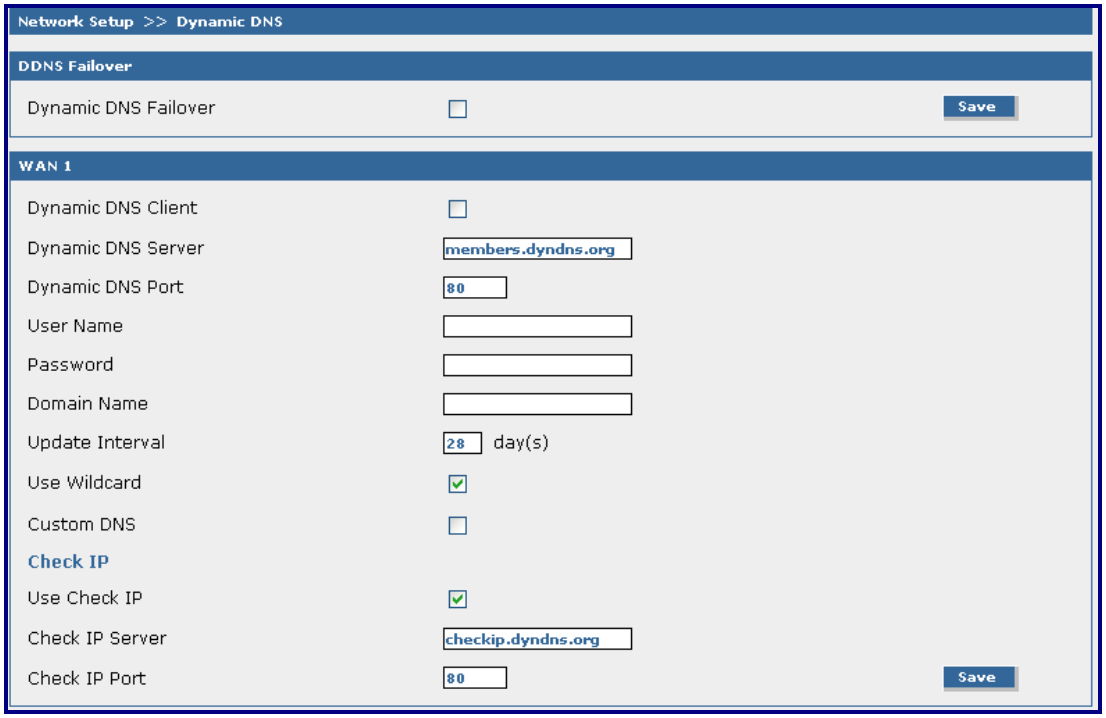
Check this box to allow spoofing on the WAN Interface. Then click **Save**.

Network Setup › Dynamic DNS

The DDNS Client is used to update the IP address of the modem/router in a DDNS server for the configured domain name whenever the IP Address changes, thus, leaving the domain name to be pointing to the current IP Address of the modem/router all the time.

Screen Notes:

- **This screen applies to the RF820/RF820-AP and the RF830/RF830-AP.**
- **The RF830/RF830-AP includes a WAN 2 section which is the same as the WAN 1 section.**
- ***Dynamic DNS Failover* is available only on the RF830/RF830-AP.**



DDNS Failover (for the RF830/RF830-AP only)

Dynamic DNS Failover

Check the box to enable DDNS failover. This is valid only if both the interfaces, WAN 1 and WAN 2, are configured with DDNS. When enabled, DDNS updates the IP Address of the failed link with that of the link that is up. So both the FQDNs (Fully Qualified Domain Name) will be pointing to the same IP Address.

WAN 1

Dynamic DNS Client

Check the box to enable DDNS Client. Default = Disable.

Dynamic DNS Server

Enter the name of the IP Server to which obtained IP addresses will be registered.

Dynamic DNS Port

Enter the port number through which the DDNS has to update the server. By default, port 80 is used. This port is configurable.

User Name

Enter the name of the user who will be allowed access the DDNS Server.

Password

Enter the Password the user will use to access the DDNS Server.

Domain Name

Enter the domain name registered with the DDNS server. The external world reaches the RouteFinder when the Domain Name is configured.

Update Interval

Enter the interval in days after which the IP Address will be updated by the DDNS server. Default: 28 days.

Use Wildcard
If this option is enabled, subdomains of the registered domain will also be resolved to the same IP address. For example, if test.dyndns.org has been registered and the IP address it is resolved to is a.b.c.d., all subdomains like dns.test.dyndns.org will also get resolved to a.b.c.d. However, this will work only if the dynamic DNS server supports this option.

Custom DNS
If enabled, this option specifies the domain name registered is of custom type. Also, its specified server belongs to custom type.

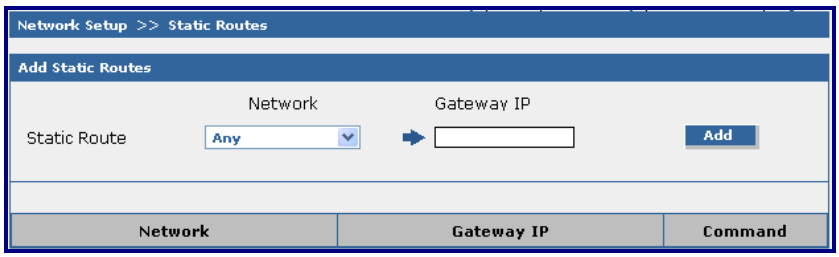
Check IP
If enabled, this option specifies the RouteFinder will use the *Check IP* utility to verify the IP addresses that are already registered for the domain name configured.

Check IP Server
Enter the name of the IP Address of the *Check IP* server.

Check IP Port
Enter the number of the port which the *Check IP* utility connects to the server.

Network Setup › Static Routes

Routing information is used by every computer connected to a network to identify whether it is sending a data packet directly to the firewall or passing it on to another network. This screen can be used to describe the networks to be reached through a configured gateway.



Add Static Routes

Static Route Network

Select a defined network from the drop down list.

Static Route Gateway IP

Enter the external IP address which will act as a gateway for this network. The entries are added by clicking the Add button. The entry will then display at the bottom of the screen.

The options to Delete or Edit a route after it has been defined and added are available will become available after the network and Gateway IP are added.

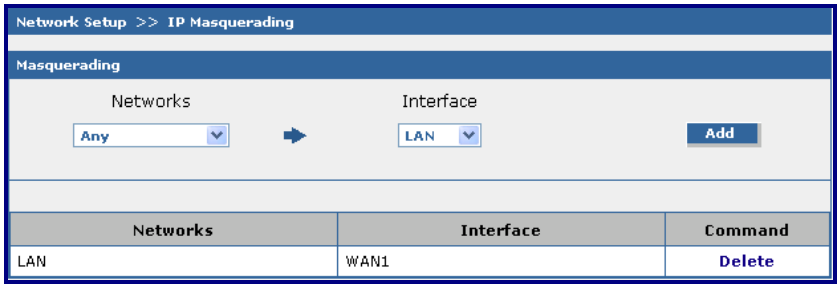
Important: The Static Route screen will not display until the network is defined in *Networks & Services.*

Network Setup › IP Masquerading

Masquerading is a process that allows attaching of private networks to public networks. Since private addresses are not routed to the Internet, a source NAT on the RouteFinder's external interface is required. Masquerading enables the user to enter only one source network. Also, if the external interface's IP address keeps changing (as in the case of a DHCP client or PPPoE connections) the user need not keep changing the masquerading rule.

On this screen you can select networks or network groups to be masked. Masquerading is especially useful for connecting private networks to the Internet. It allows you to hide internal IP addresses and network information from the outside network.

Screen Note: This screen applies to the RF820/RF820-AP and the RF-830/RF830-AP. However, the RF830/RF830-AP includes an additional line at the bottom of the screen for the WAN2 Interface.



Networks

Select a defined network from the drop down list.

Interface

The selected Network will be masqueraded with the interface selected from this drop down list. Example: network1 > WAN; Defaults: LAN > WAN1, LAN > WAN2

Add

Click the **Add** button. The Masqueraded network route will display on the bottom part of the screen.

Edit or Delete a Route

A Masqueraded network route can be edited or deleted. When deleting a Masqueraded network route, the interface adapts accordingly.

Network Setup › SNAT

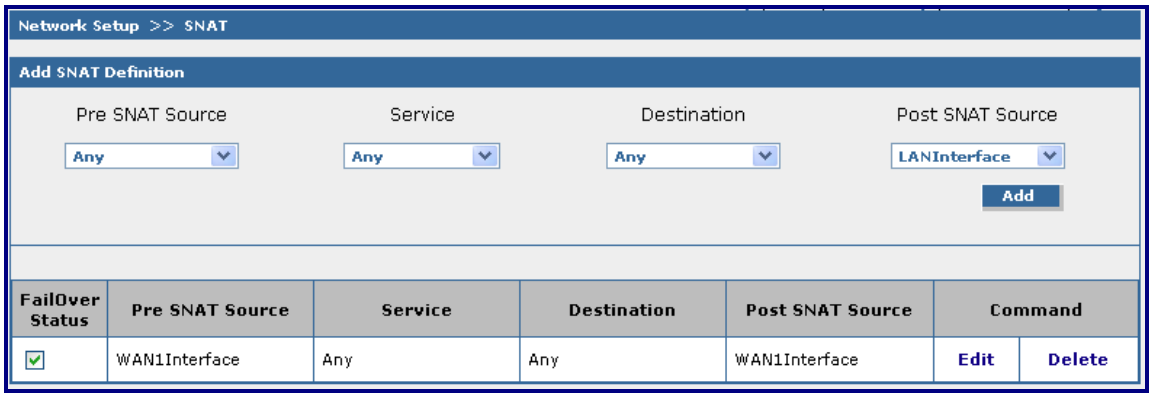
The SNAT (Source Network Address Translation) process allows attaching private networks to public networks. SNAT is used when you want to have a LAN using a private IP network to be connected to the internet via a firewall. Since the private IP addresses are not routed on the internet, you have to apply SNAT on the firewall's external interface.

The RouteFinder's internal interface serves as the default gateway for the LAN. Hence, a rule is added to the RouteFinder to replace the source address of all packets crossing its external interface from inside to outside with the RouteFinder's own interface IP address. Once the request gets answered from the Internet host, the RouteFinder will receive the reply packets and will forward them to the client on the LAN.

On this screen you can set up the RouteFinder's ability to rewrite the source address of in-transit data packages using SNAT. This functionality is equivalent to DNAT, except that the source addresses of the IP packets are converted instead of the target addresses being converted. This can be helpful in more complex situations (e.g., diverting reply packets of connections to other networks or hosts).

Important

- For SNAT support, the TCP and/or UDP settings must be enabled in the *Networks* menu.
- As the translation takes place after the filtering by packet filter rules, you must allow connections that concern your SNAT rules in *Packet Filters* > *Packet Filter Rules* with the original source address. Packet filter rules are covered later in this chapter.
- To create simple connections from private networks to the Internet, you should use the *Network Setup* > *Masquerading* function instead of SNAT. In contrast to Masquerading, SNAT is a static address conversion, and the rewritten source address does not have to be one of the RouteFinder's IP addresses.



Add SNAT Definition – From the drop down lists, select IP packet characteristics to be translated.

Pre SNAT Source

Select the original source network of the packet. The network must be predefined in the *Networks* menu. The entry is confirmed by clicking the **Add** button. Existing entries can be deleted or edited.

Service

Allows the corresponding service for the Pre SNAT Source entry field to be chosen from the select menus. The service must have already been defined in the *Services* menu.

Destination

Select the target network of the packet. The network must have been defined in the *Network* menu. The entry is confirmed by clicking the **Add** button. Existing entries can be deleted or edited by clicking the **Edit** or the **Delete** buttons.

Post SNAT Source

Selects the source addresses of all the packets after the translation. Only one host can be specified here. The entry is confirmed by clicking the **Add** button. Existing entries can be deleted or edited by clicking the **Edit** or the **Delete** buttons.

About Failover Status (For the RF830/RF830-AP Only):

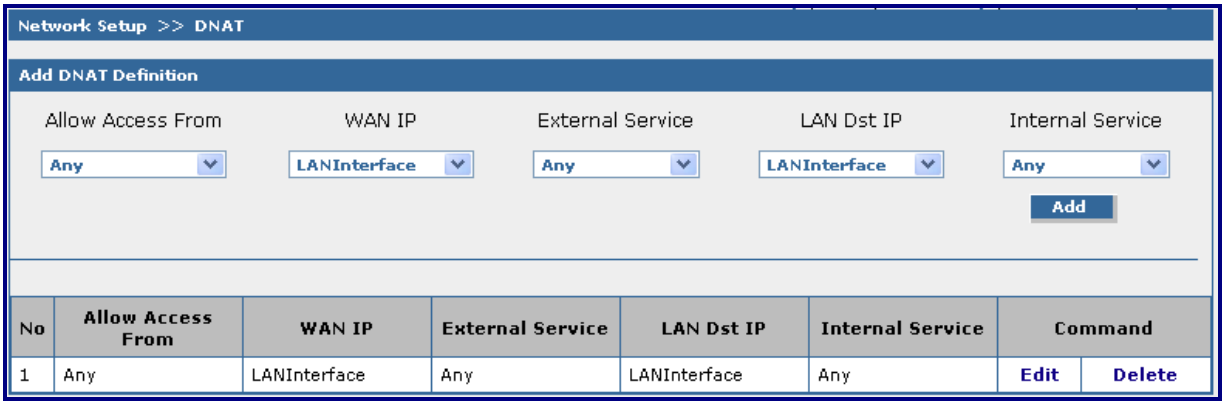
Failover is a transition that takes place when one individual computer fails and a backup unit automatically takes over its request load. Failover can be enabled on this device only if the Post SNAT Source is **WANLINK1 Interface** or **WANLINK2 Interface**. Additionally, Failover requires that Spoofing be disabled and that there are Masquerading rules between **LAN > WAN1** and **LAN > WAN2**.

Network Setup › DNAT

The DNAT (Destination Network Address Translation) process allows placing servers within the protected network and making available for a certain service to the outside world. Normally, the RouteFinder has a network server running in the LAN providing a network service with an address in the specified range, and wants this service accessible to the outside world. The DNAT process running on the RouteFinder translates the destination address of incoming packets to the address of the real network server on the LAN. The packets then get forwarded.

Important Notes:

- A DNAT rule with the Pre-DNAT Network as *ANY,* a Service as *ANY*, and a Destination Service as *ANY* cannot be added. This will cause all the packets to be routed to the system with Post DNAT network and services in the RouteFinder will not function properly.
- As the address conversion takes place BEFORE the filtering by the packet filter rules, you must set the appropriate rules in the *Packet Filter* > *Packet Filter Rules* menu to let the already-translated packets pass. You can find more about setting packet filter rules earlier in this chapter.



Add DNAT Definition

Allow Access From

Select the source network/host to which the DNAT rule will apply.

WAN IP

Select the original target host or network of the IP packets that are to be re-routed. This target host or network SHOULD BE reachable from the Internet. The network/host must have been defined in the *Networks* section of this software. Example: network1

External Service

Select the Pre DNAT service. The service must have been defined in the Services section of this software. Example: FTP, TELNET

LAN Dst IP

Select the designation to which IP packets are to be diverted. Only one host can be defined as the Post DNAT destination. Normally, this IP address is the service running on the private LAN segment. Example: host1

Internal Service

Select the service for the Post DNAT service. Example: FTP

Add

Click the **Add** button to save your choices.

Edit, Delete

After saving the settings, a table is created and displayed at the bottom of the screen. You can edit or delete entries by highlighting the desired entries and clicking either the **Edit** or **Delete** button listed under **Command**.

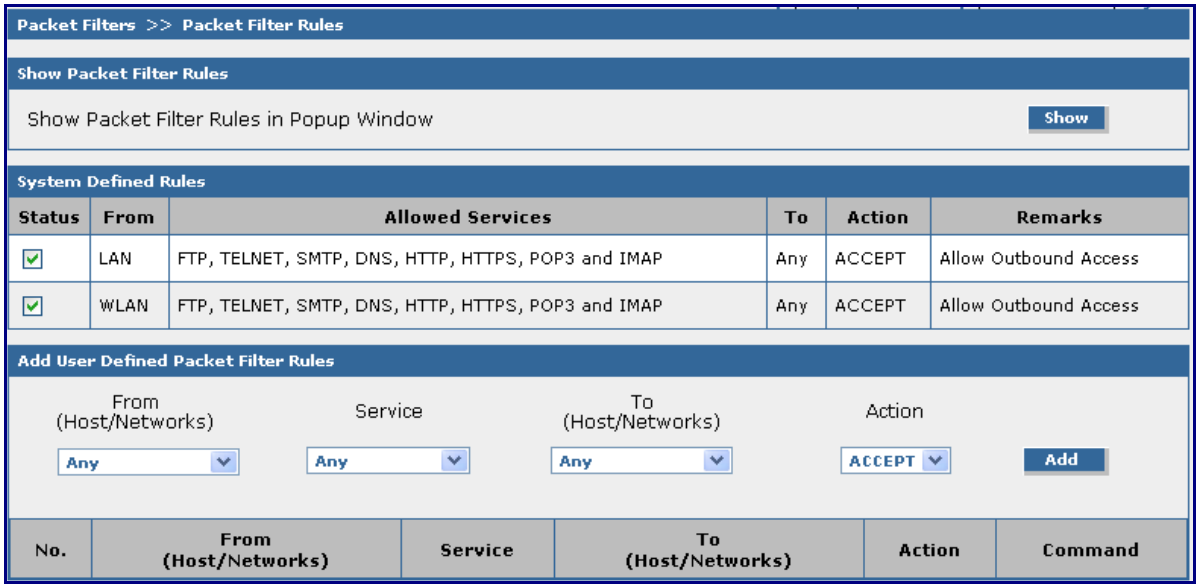
Packet Filters

Packet Filter › Packet Filter Rules

Packet filters are used to set firewall rules which define what type of data traffic is allowed across the RouteFinder's firewall. There are certain System Defined Rules that exist by default. In addition, you can specify whether particular packets are to be forwarded through the RouteFinder system or filtered. These rules are set with the help of network/host and service definitions that have already been set up in the **Networks** section.

Screen Notes:

- **This screen applies to the RF820/RF820-AP and RF830/RF830-AP.**
- **The RF830/RF830-AP screen includes an option for a *WAN2Interface*.**
- **If the AP build is used, *WLAN* displays in the System defined rules.**



Show Packet Filter Rules in Popup Window

Clicking this button opens up a new window that displays the RouteFinder's live packet filter rules.

System Defined Rules

These rules define a set of common application services that are allowed outbound access through the RouteFinder's WAN interface. The services that come under this definition FTP, TELNET, SMTP, DNS, HTTP, POP3, IMAP, and HTTPS; they form the ***Default Outbound Service Group***. The Default Outbound Service Group is enabled by default.

Add User Defined Packet Filter Rules

New packet filter rules are created by choosing from four drop-down lists. All services, networks, and groups previously defined in Networks and Services are available for selection.

Click **Add** to create the rule; it then displays at the bottom of the table. The new rule automatically receives the next available number in the table. The overall effectiveness of the rule is decided by its position in the table. You can move the new rule within the table with the **Move** function in the **Command** column. You can also **Edit** and **Delete** rules.

Important Note about the Order of Rules:

The order of the rules in the table is essential for the correct functioning of the firewall. By clicking the **Move** button, the order of execution can be changed. In front of rule to be moved, enter the line number that indicates where the rule should be placed. Confirm by clicking **OK**.
By default, new rules are created at the end of the table.

From (Host/Networks)

Select the host/network from which the information packet must originate for the filter rule to match. The *Any* option, which matches all IP addresses regardless of whether they are officially assigned or private addresses, may also be specified. The networks/host must be pre-defined in the Networks section. Example: *network1* or *host1* or *Any*

Services

Select the service that is to be matched with the filter rule. These services must be pre-defined in the Services section. The default entry Any selects all combinations of protocols and parameters (e.g., ports). Example: *SMTP, ANY*

To (Host/Networks)

Select the host/networks to which the packet is to be sent in order for the filter rule to match. The *Any* option, which matches all IP addresses regardless of whether they are officially assigned or private addresses, may also be specified. The networks/host must be pre-defined in the Networks section. Example: *network2*, or *host 2* or *Any*

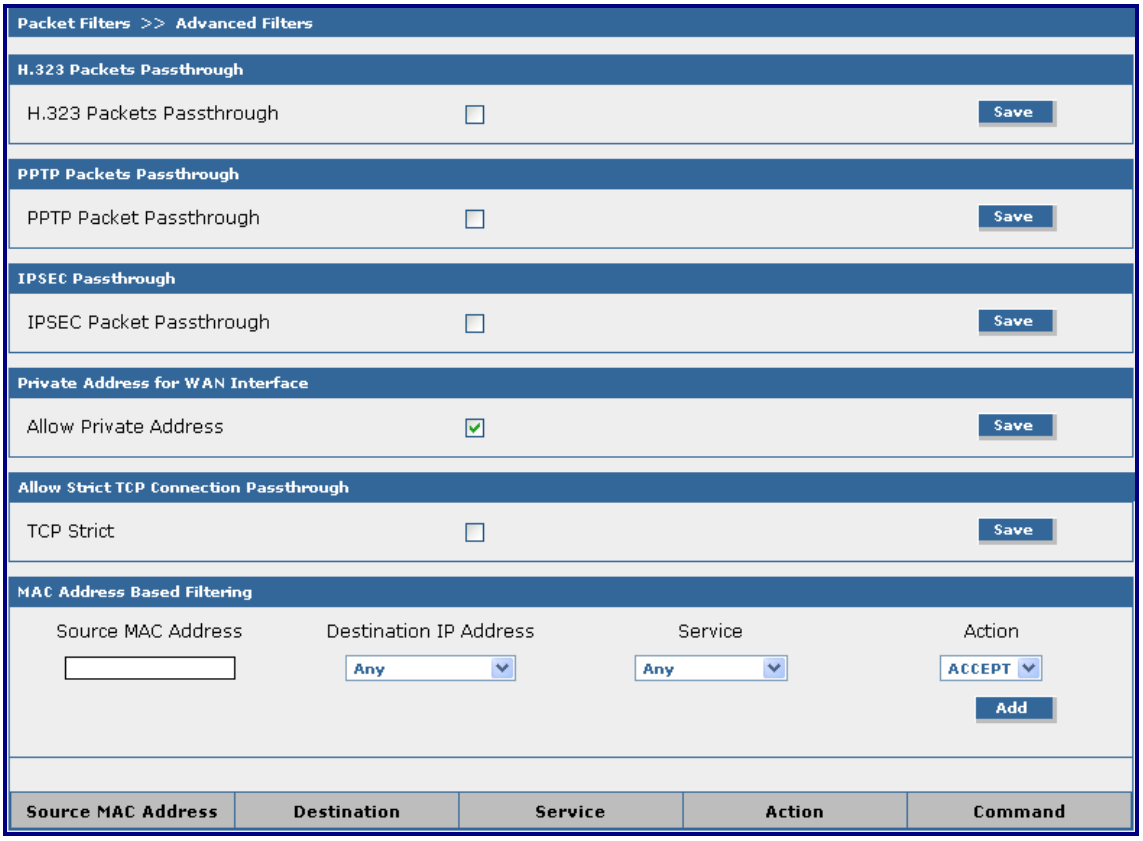
Action

Select the action that packet filter executes if the rule matches any traffic traversing the RouteFinder firewall. There are four types of actions:

- **Accept –** Allows/accepts all packets that match this rule.
- **Reject –** Blocks all packets that match this rule. The host sending the packet will be informed that the packet has been rejected.
- **Drop –** Drops all packets that match this rule, but the host is not informed. It will appear to the host that the destination address is not responding; in other words, it is a silent drop.
- **Log –** Packets matching the rule will be logged. Source address, destination address, and service will be logged. The logged messages are routed to the Remote Syslog Server if enabled in the Administration section.

Packet Filters › Advanced Filters

This section allows configuration of some advanced filter settings.



H323 Packets Passthrough

Check this box to enable the forwarding of H323 packets across the firewall.

PPTP Packets Passthrough

Check this box to enable PPTP Packets Passthrough (PPTP NAT support). This includes two features:

- Server behind the firewall and clients on the Internet – DNAT of PPTP packets.
- Client behind the firewall and server on the Internet – SNAT / masquerading of PPTP packets.

IPSec Packet Passthrough

Check this box to enable the forwarding of IPSec packets across the firewall.

Private Addresses on WAN Interface

Allow Private Addresses

By default, packets from the WAN interface of the RouteFinder destined to any private address will be dropped. Check this option to allow private addresses to pass through.

Allow Strict TCP Connection Passthrough

TCP Strict

By default, packets with invalid flag combinations or TCP Sequence numbers passing via the RouteFinder will be dropped. Check this option to allow these packets to pass through.

MAC Address Based Filtering

Use this section of the screen to allow filtering / forwarding of packets based on the source MAC address.
Note: MAC Address based rules will be applied to packets destined to the RouteFinder as well as packets forwarded by the RouteFinder.

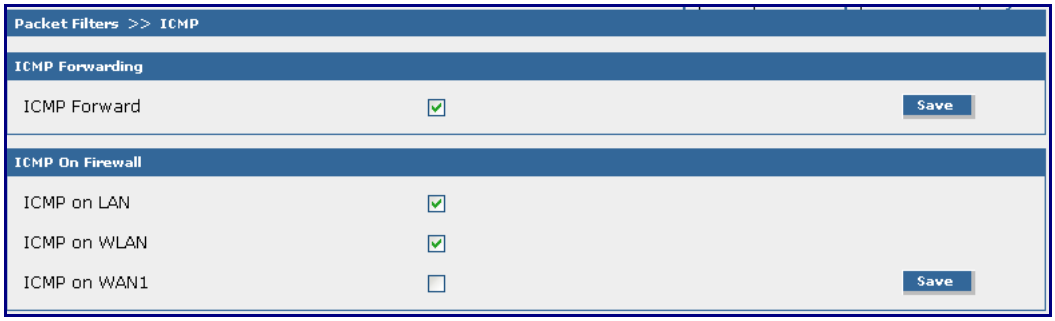
- Source MAC Address – Enter the MAC address of the source machine for this filter rule.
- Destination IP Address – Select the destination host/network this IP address will be sent.
- Service – Select the protocol-port pair for this filter rule.
- Action – Select the Action to be taken on this packet (Accept, Reject, Drop Log)

Packet Filter › ICMP

ICMP (Internet Control Message Protocol) is used to test the network connections and the functionality of the RouteFinder. It is also used for diagnostic purposes.

ICMP-on-Firewall and *ICMP Forwarding* always apply to all IP addresses (*Any*). When these are enabled, all IP hosts can PING the RouteFinder (ICMP-on-Firewall) or the network behind it (ICMP Forwarding). Unique IP addresses can then no longer be ruled out with packet filter rules. If the ICMP settings are disabled, separate IP hosts and networks can be allowed to send ICMP packets through the RouteFinder firewall by using appropriate *user defined packet filter rules*.

Screen Notes: The RF830/RF830-AP screen includes a field for *ICMP on WAN2.*
With the AP build, an additional screen option for *ICMP on WLAN* displays.



ICMP Forwarding

Check the *ICMP Forward* checkbox to enable the forwarding of ICMP packets through the firewall into the local network and all connected DMZs. The default is *Enabled*.

ICMP on Firewall

ICMP on LAN

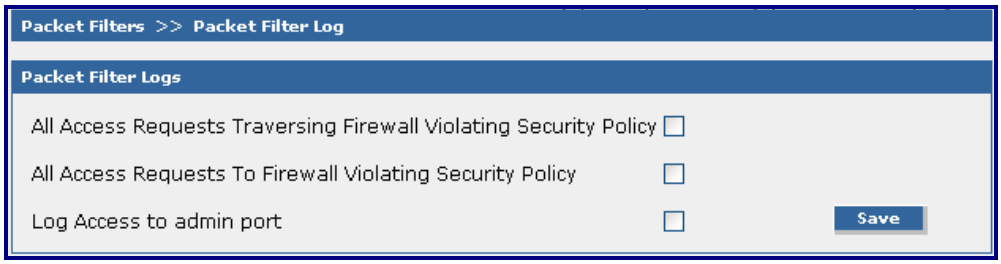
Check the *ICMP on LAN* checkbox to enable the forwarding of ICMP packets through the firewall into the local network and all connected DMZs. The default is *Enabled*.

ICMP on WAN1

Check the *ICMP on WAN1* checkbox to enable the transfer of ICMP packets on the WAN1 interface.

Packet Filter › Packet Filter Log

Use this section to enable or disable Packet Filter Logs.



All Access Requests Traversing Firewall Violating Security Policy

Check this box to enable the logging of all access requests from private (LAN) and public (WAN) network clients to traverse the RouteFinder that violate the configured security policy.

All Access Requests to Firewall Violating Security Policy

Check this box to enable the logging of all access requests from private (LAN) and public (WAN) network clients to send traffic to the RouteFinder itself that violate the configured security policy.

Log Access to Administrative Access Port

Check this box to enable the logging of all access requests from private (LAN) and public (WAN) network clients to send traffic to the RouteFinder itself on the administrative access port.

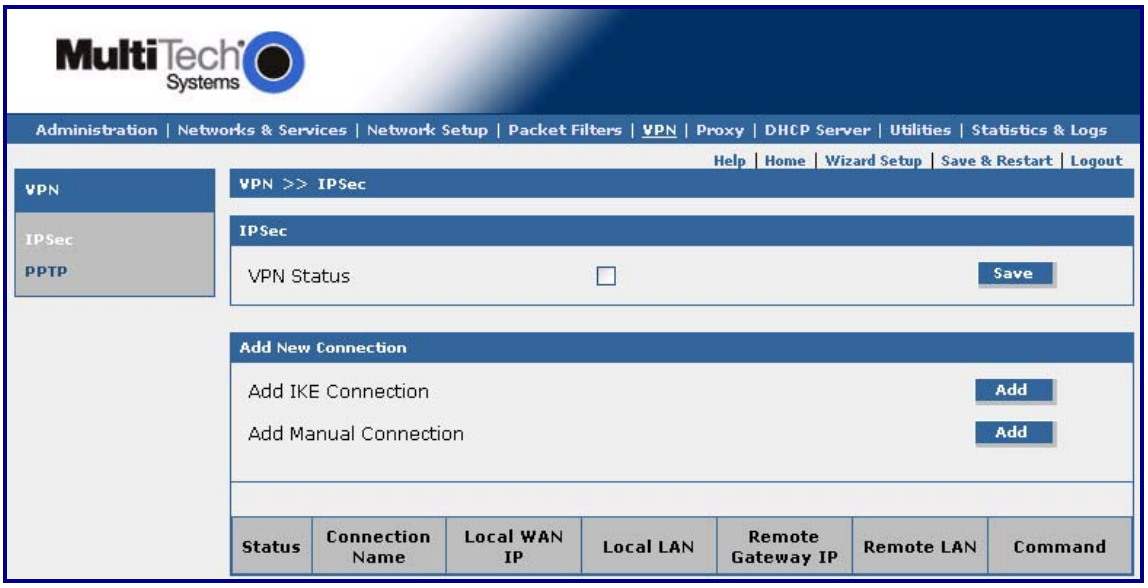
VPN (Virtual Private Network)

VPN › IPSec

Introduction to Virtual Private Networks

A Virtual Private Network (VPN) is a secure communication connection via an insecure medium – usually the Internet. A VPN is useful in situations where information is sent and received via the Internet and it is important that no third party can read or change that information. Such a connection is secured via VPN software that is installed at both ends of the connection. This software allows authentication, key exchange, and data encryption according to an open standard (IPSec).

The IPSec protocol suite, based on modern cryptographic technologies, provides security services like encryption and authentication at the IP network layer. It secures the whole network traffic providing guaranteed security for any application using the network. It can be used to create private secured tunnels between two hosts, two security gateways, or a host and a security gateway.



VPN IPSec

VPN Status

Check the VPN *Status* checkbox to enable IPSec. Click the **Save** button.

Add a New Connection

Add IKE Connection

Click the *Add IKE Connection* button. A screen displays for setting up an IKE connection.

Add Manual Connection

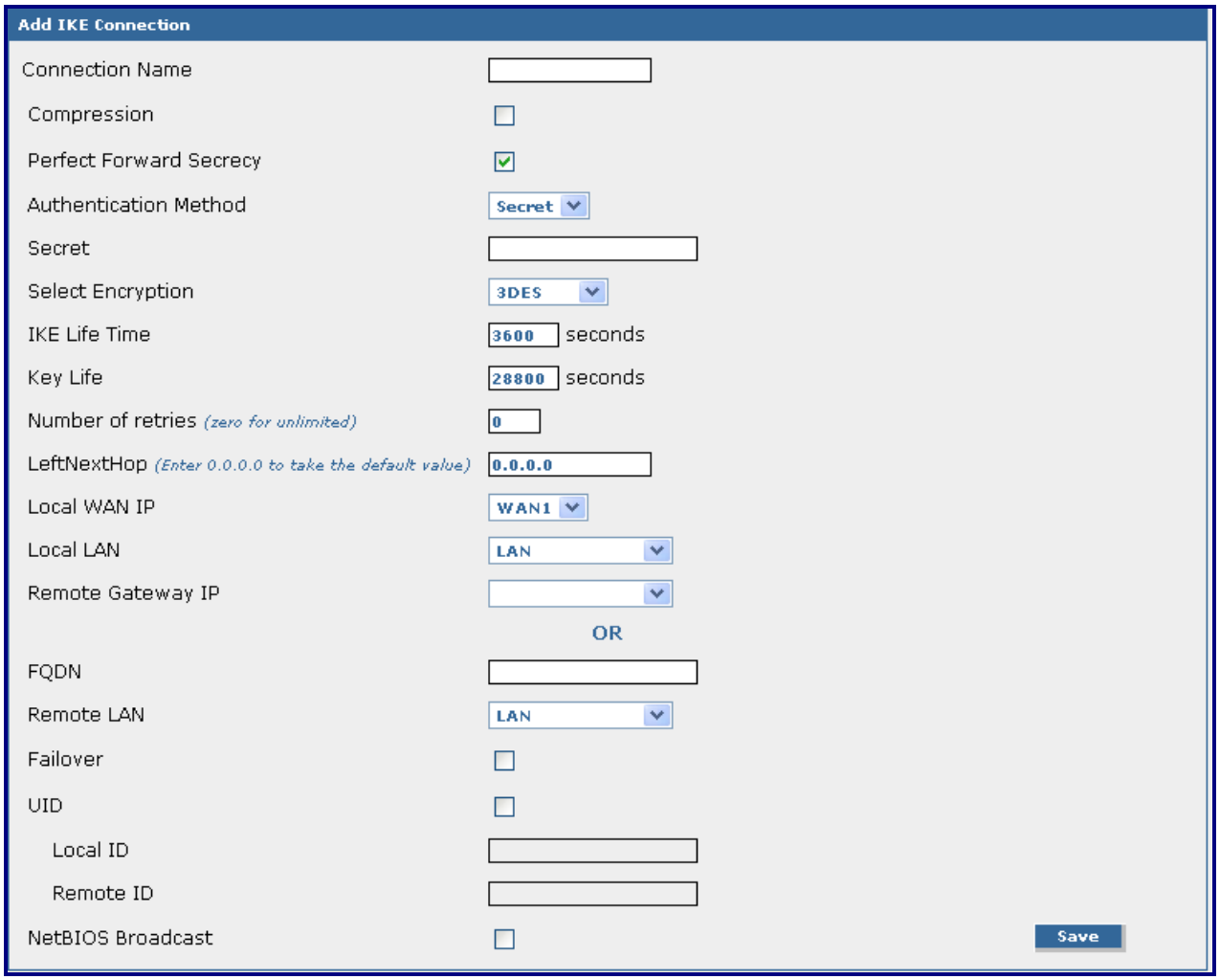
Click the *Add Manual Connection* button. A separate screen displays for setting up a manual connection.

Important Note About Activating a Connection: Once connection information is entered, it will display at the bottom of this screen. Be sure to the check the box in the **Status** column to activate the connection.

Add an IKE Connection

This section enables setting IPSec tunnels through an IKE connection.

Screen Note: *Failover* is available on the RF830/RF830-AP only.



Add IKE Connection

Connection Name

Enter a text name that will identify the connection for you.

Compression

Check the compression checkbox to enable IPCOMP, the compression algorithm.

Perfect Forward Secrecy (PFS)

Check the PFS checkbox to enable PFS, a concept in which the newly generated keys are unrelated to the older keys). This is enabled by default.

Authentication Method

Authentication can be done using Pre-Shared Secrets.

Secret

The Pre-Shared Secret must be agreed upon and shared by the VPN endpoints; it must be configured at both endpoints of the tunnel.

Select Encryption

Select the encryption method. 3DES is recommended. Options include: 3DES, DES, AES-128, AES-192, AES-256

IKE Life Time

The duration for which the ISAKMP SA should last is from successful negotiation to expiration. The default value is 3600 seconds and the maximum is 28800 seconds.

Key Life
The duration for which the IPSec SA should last is from successful negotiation to expiration. The default value is 28800 seconds and the maximum is 86400 seconds.

Number of Retries
Specify the number of retries for the IPSec tunnel. Enter zero for unlimited retries.

Left Next Hop
Next Hop is the address of the next device in a routing table's path that moves a packet to it's destination. This setting can be configured or left as a static value: 0.0.0.0. When not configured, the value is set to the Gateway of the Box/Gateway configured on the Interface/Right IP. The selection is based on the Left and Right IP.

Local WAN IP
This is the interface initiating the IPSec tunnel.

Local LAN
Internal subnet of the local security gateway for which the security services should be provided. If the RouteFinder acts as a host, this should be configured as None.

Remote Gateway IP
Interface where the IPSec tunnel ends. In the case of a Road Warrior with a Dynamic IP address, this should be configured to **ANY**.

FQDN
FQDN is a DNS resolvable fully qualified domain name with which identity the right peer can be identified. When FQDN is selected, the Remote Gateway IP should be blank.

Remote LAN
Internal subnet of the remote security gateway for which the security services should be provided. If the remote end is the host, this should be configured as None.

Failover (Note: Failover is available on the RF830/RF830-AP only.)
Check the box to enable VPN failover for the tunnel. When this field is enabled, the tunnel will failover onto the other interface if the local interface is down. For example, if the tunnel is configured on WAN 1 but the link goes down, the tunnel again comes up on the link that is up (i.e., LAN 2). Failover is possible only when the remote gateway is an FQDN (Fully Qualified Domain Name) and Dynamic DNS Failover is enabled (see the *Network > Dynamic DNS* screen).

UID (Unique Identifier String)
Check the UID box to enable the Local ID and Remote ID. Local ID and Remote ID are active only when UID is enabled.

Local ID
Enter a string identifier for the local security gateway.

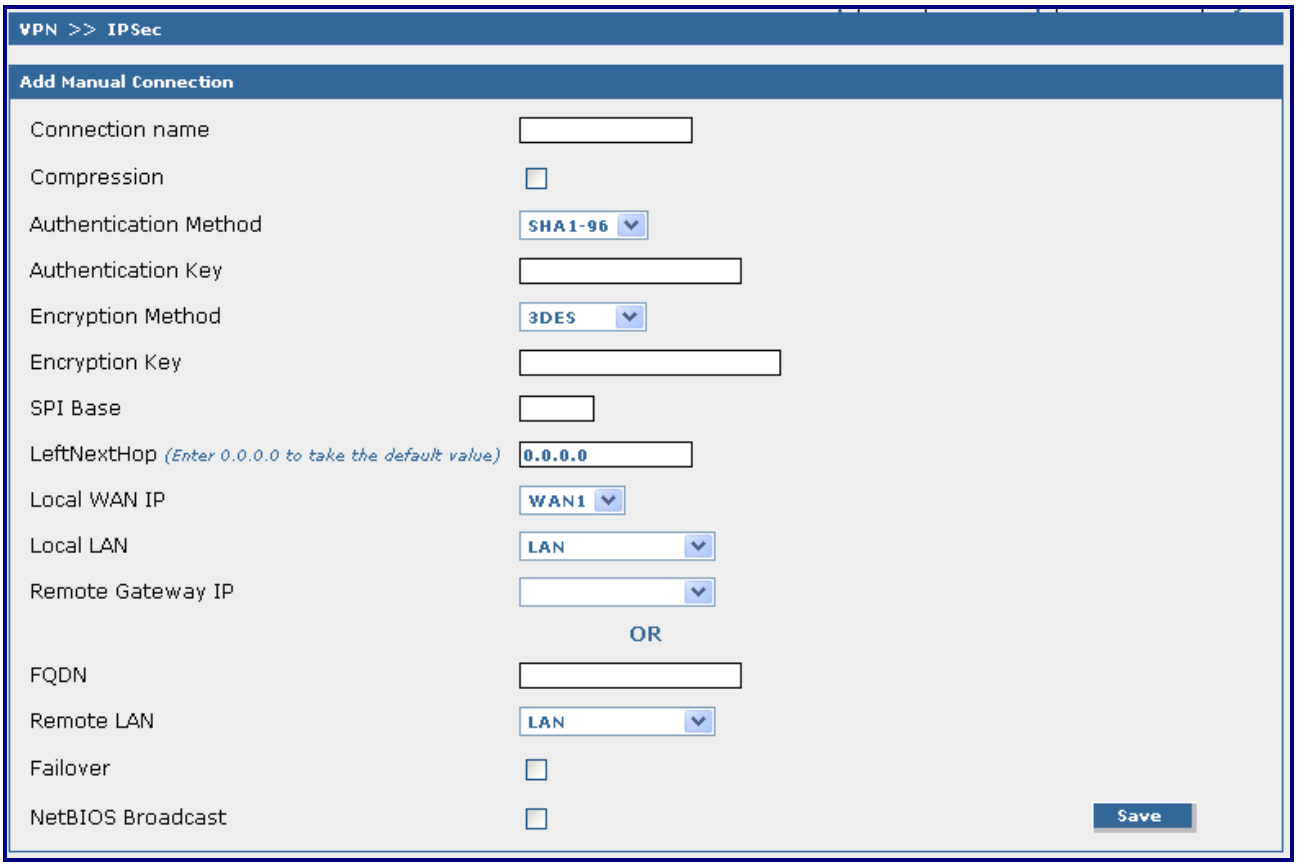
Remote ID
Enter a string identifier for the remote security gateway.

NetBIOS Broadcast
Check this option to enable broadcasts over the connection. It will allow computers on the network to share Microsoft file and printer sharing information.

Add a Manual Connection

This section enables setting IPSec tunnels through manual connection.

Screen Note: *Failover* is available only on the RF830/RF830-AP.



Add Manual Connection

Connection Name

Enter a text name that will identify the connection for you.

Compression

Check the compression checkbox to enable IPCOMP, the compression algorithm.

Authentication Method

Select the authentication algorithms to be used for the respective security services. Options are: MD5-96 and SHA1-96.

Authentication Key

The VPN firewall could use either MD5 or SHA1 for authentication
MD5-96 bit key example: 0x123456789012345678.
SHA1-96 bit key example: 0x123456789012345678

Encryption Method

Select the encryption method. Options include: 3DES, DES, AES-128, AES-192, AES-256, and NULL (no encryption).

Encryption Key

The RouteFinder can use any one of the methods listed above. See the online Help for examples.

SPI Base

The Security Parameter Index identifies a manual connection. The SPI is a unique identifier in the SA (Secure Association – a type of secure connection) that allows the receiving computer to select the SA under which a packet will be processed. The SPI Base is a number needed by the manual keying code. Enter any 3-digit hexadecimal number, which is unique for a security association. It should be in the form 0xhex (0x100 through 0xfff is recommended). If you have more than one manual connection, then the SPI Base must be different for each one.

Left Next Hop
Next Hop is the address of the next device in a routing table's path that moves a packet to it's destination. This setting can be configured or left as a static value: 0.0.0.0. When not configured, the value is set to the Gateway of the Box/Gateway configured on the Interface/Right IP. The selection is based on the Left and Right IP.

Local WAN IP
Select the Interface to initiate the IPSec tunnel (Left Security Gateway). Options are LAN, WAN1, and WAN 2 (for the RF830/RF830-AP only).

Local LAN
Select the internal subnet of the local security gateway for which the security services are to be provided. If the RouteFinder acts as a host, this should be configured as **None**. Other options are: Any, LAN, LAN Interface, WAN 1, WAN 1 Interface. (RF830/RF830-AP includes WAN 2 and WAN 2 Interface options).

Remote Gateway IP
Select the interface in which the IPSec tunnel ends. In the case of Road Warriors with a Dynamic IP addresses, this should be configured as **ANY**. Other options include: LAN, LAN Interface, WAN 1, WAN 1 Interface, and None. (RF830/RF830-AP includes WAN 2 and WAN 2 Interface options).

FQDN
FQDN is a DNS resolvable fully qualified domain name with which identity the right peer can be identified. When FQDN is entered, the Remote Gateway IP should be blank.

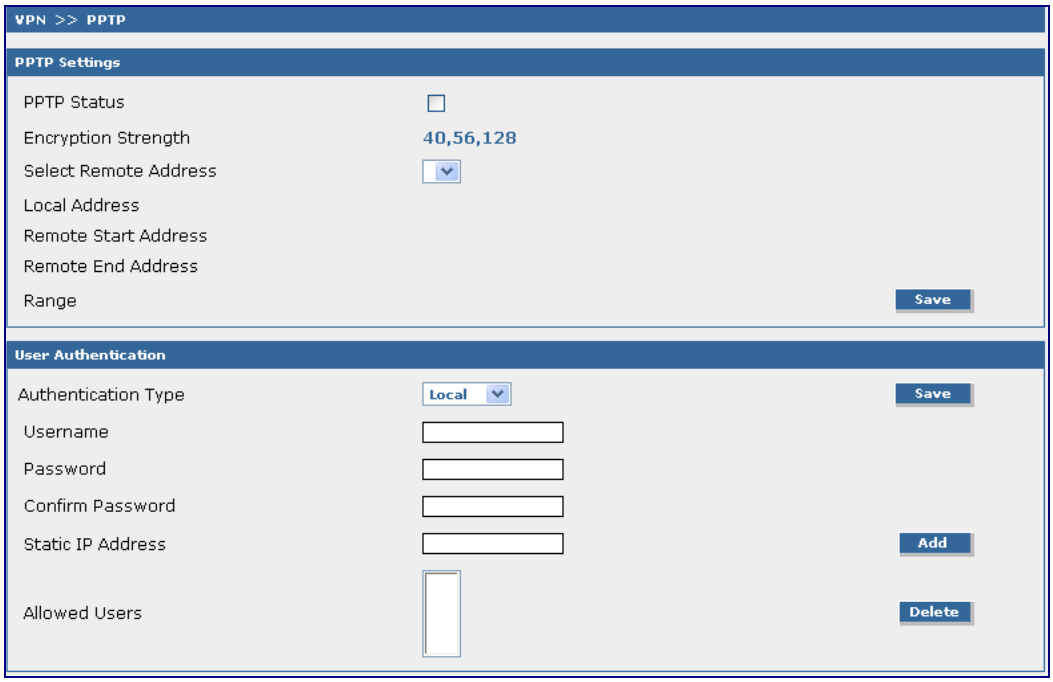
Remote LAN
This is the internal subnet of the remote security gateway for which the security services are to be provided. If the remote end is a host, this should be configured as **None**.

Failover (available on the RF830/RF830-AP only)
Check the box to enable VPN failover for the tunnel. When this field is enabled, the tunnel will failover on to the other interface if its local interface is down. For example, if the tunnel is configured on WAN 1 but the link goes down, the tunnel again comes up on the link that is up (i.e., LAN 2). Failover is possible only when the remote gateway is an FQDN (Fully Qualified Domain Name) and Dynamic DNS Failover is enabled (see the Network > Dynamic DNS screen).

NetBIOS Broadcast
Check this option to enable broadcasts over the connection. It will allow computers on the network to share Microsoft file and printer sharing information.

VPN › PPTP

PPTP (Point-to-Point Tunneling Protocol) is a tunneling protocol meant for tunneling IP packets and non-IP packets through the IP only network (the Internet). PPTP offers connections to PPTP clients so that they can become virtual members of the IP pool owned by the PPTP server. In effect, these clients become virtual members of the local subnet regardless of their real IP address.



PPTP Settings

PPTP Status

Check this PPTP Status box to enable PPTP.

Encryption Strength

Select the encryption strength for the remote access connection. Options are 40 bit, 56 bit, or 128 bit.

Select Remote Address

The local IP address for the PPTP link and the range of remote IP addresses can be selected with this option. The network has to be defined in the Network section. The Local Address, Remote Start Address, Remote End Address, and Range are displayed below as configured from the network.

Check *Select Remote Address*; click the **Save** button. Then the following information displays:

Local Address – Displays the private LAN IP Address, which is NOT modifiable.

Remote Start Address – Displays the first IP address in a range of IP addresses to be assigned to remote clients.

Remote End Address – Displays the last IP address in a range of IP addresses to be assigned to remote clients.

Range – Displays the range of IP addresses that can be assigned to remote clients.

User Authentication

Authentication Type

Select the desired user **Authentication Type** and click the **Save** button:

- **Local –** Authentication type used when local users have individual access rights.
- **RADIUS –** Authentication type used when access rights comes from a central server for user authentication.

Local or RADIUS

Local Authentication Input

User Name – Enter the user's name in lowercase.

Password – Enter the user's password (in lowercase).

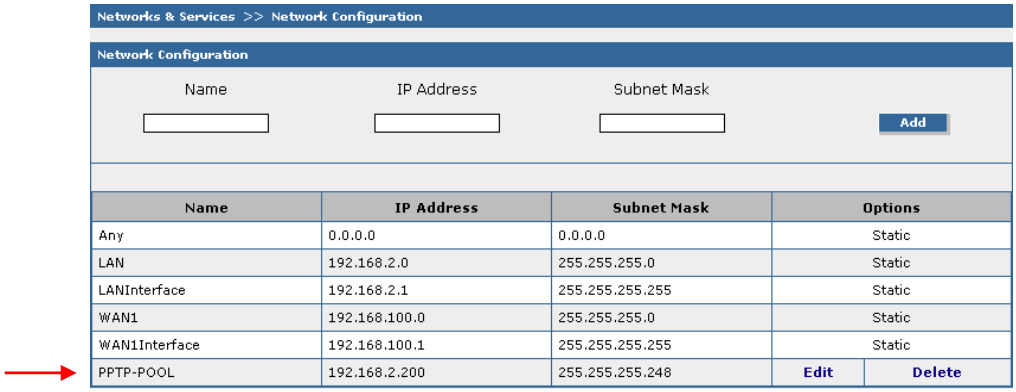
Confirm Password – Retype the password to confirm it.

Static IP Address – Enter the specific Static IP Address from the range so that the server will issue it to the client when it is connected.

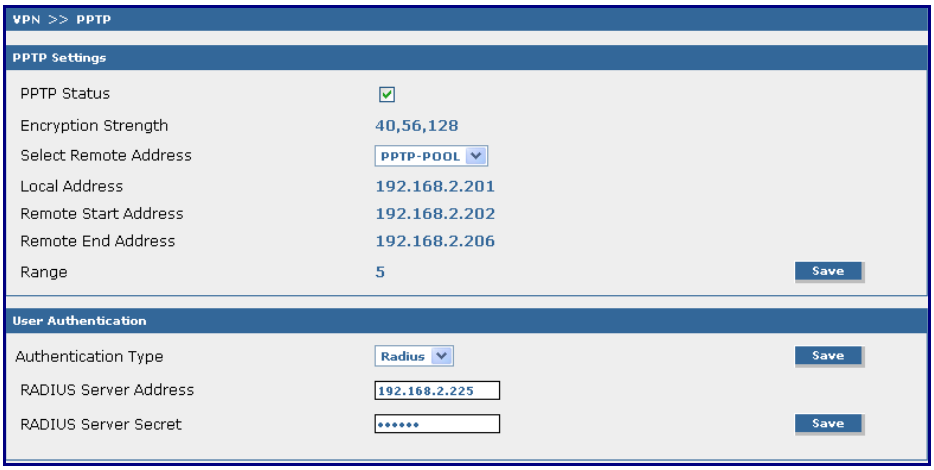
Allowed Users – The names of the users entered above display in this text box. If you wish to delete a name, click the *Delete* button.

RADIUS Authentication Input

Prerequisite Step – In order to select RADIUS as the authentication type, you must set up a PPTP network by going to the ***Network & Services > Network Configuration*** screen and enter a Network Name, IP Address and Subnet Mask as in this example:



Return to the VPN > PPTP Screen – Select PPTP-POOL as the Remote Address:



Authentication Type – Select RADIUS.

RADIUS Server Address – Enter the RADIUS server IP Address.

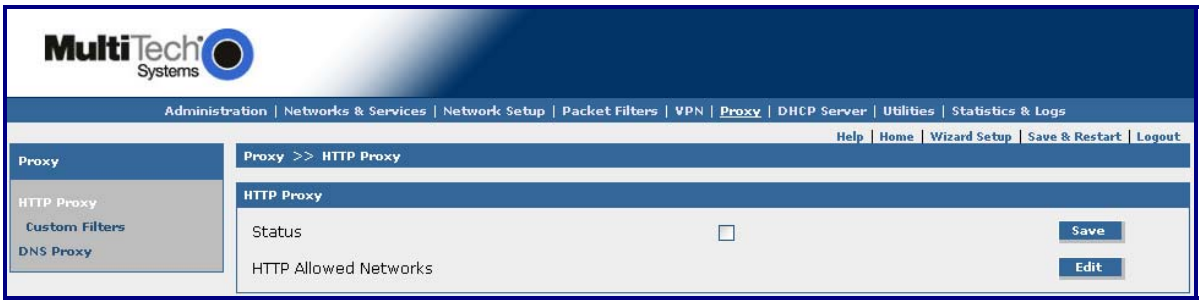
RADIUS Server Secret – Enter the secret which is configured in the RADIUS server.

Proxy

While the packet filter filters the data traffic on a network level, the use of a **Proxy** (also called an Application Gateway) increases the security of the RouteFinder on the application level, as there is no direct connection between client and server.

Proxy › HTTP Proxy

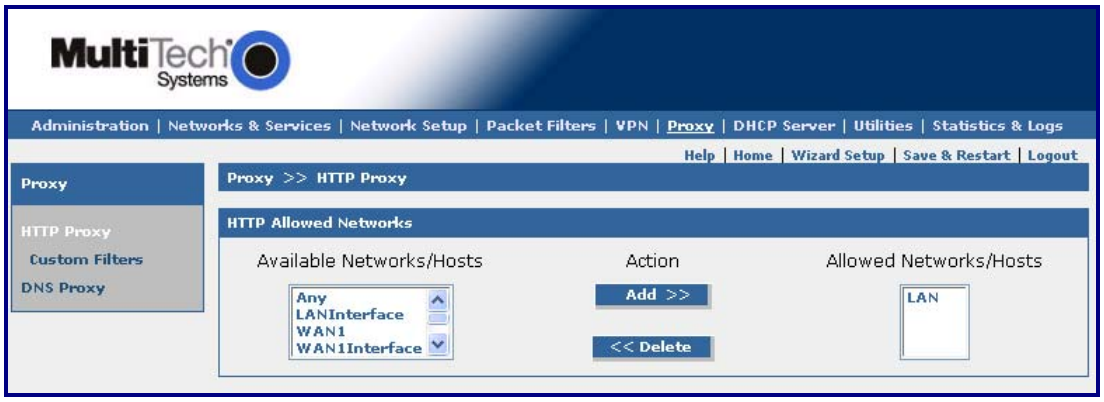
The HTTP Proxy is a module built into the RouteFinder to redirect HTTP requests from the clients in the LAN to the Internet.



HTTP Status

To enable HTTP, check the *Status* box and click **Save**. When you click **Edit**, the HTTP Allowed Networks part of the screen displays.

Screen Note: The RF830/RF830-AP includes two additional options in the *Available Networks/Hosts* drop-down box: *WAN2* and *WAN2 Interface*.



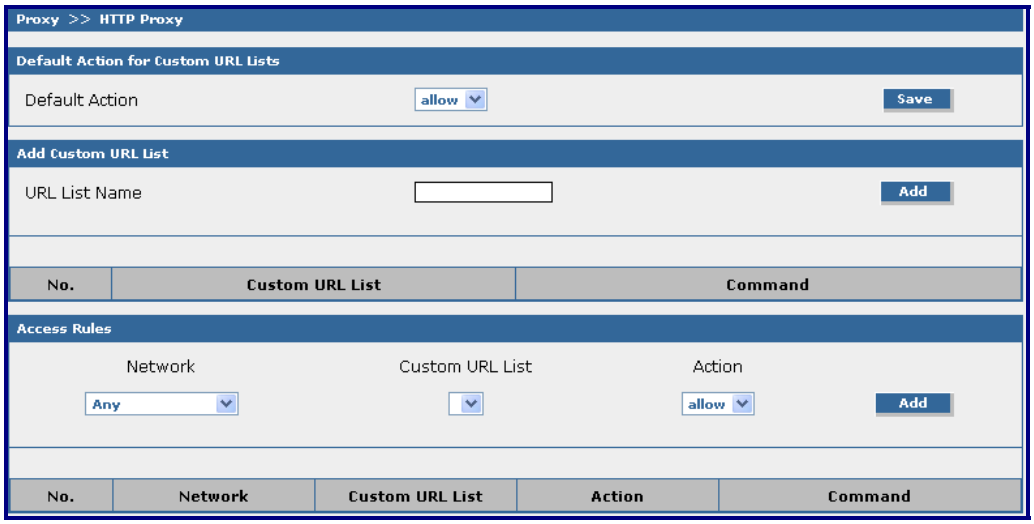
HTTP Allowed Networks

Available Networks/Hosts

This defines the allowed network/host for access to the HTTP. To select the networks you want to be available for the HTTP proxy, highlight the network name and click the **Add** button.

Proxy › Custom Filters

The custom URL list allows URLs to be filtered or forwarded by the RouteFinder. Custom URL lists are configured here. Sets of URLs to be forwarded/filtered for a particular network/host can also be configured.



Default Action for Custom URL Lists

Default Action

The default action can be set to either *Allow* or *Deny*. Click the **Save** button to set the default action.

Add Custom URL List

A custom URL list has to be defined before a rule is added. The name for the URL list is entered here. Click the **Add** button to save the name.

To enter URLs into the list, click the Edit button

Add Custom URL List

URL List Name

A Custom URL List has to be named before defining a rule. Enter a name for the URL to include in the list here. Click the **Add** button to save the name. The name will be added to the Custom URL List on this screen. Once the name is listed, you can edit it and delete it.

Access Rules

The **Access Rules** function enables you to define custom rules for the URL lists. With these custom rules, networks/hosts can be allowed or denied access to certain URLs.

An access rule consists of three parts:

1. Network or Host
2. URL List
3. Allow or Deny Access

Example

List Name: URL List named **list1** contains the URL www.google.com
Networks: There are two networks **net1** and **net2** defined.
Rules: Two rules have been configured:

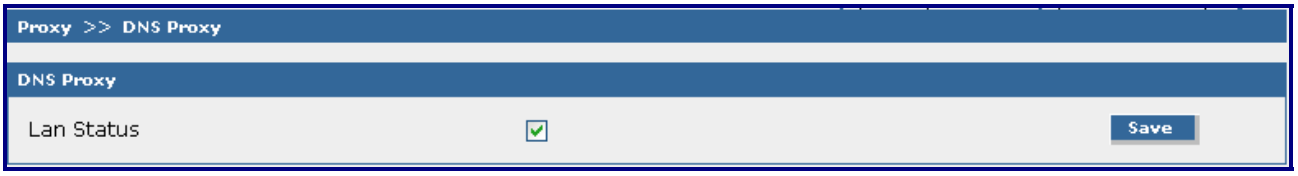
net1 – list1 – allow
and
net2 – list1 – deny

What Does This Mean:

- Users from **net1** trying to access google.com will be allowed to access the site.
- Users from **net2** trying to access google.com will not be allowed to access the site.
- Users from any other network will be allowed/denied access based on default action.

Proxy › DNS Proxy

DNS Proxy is a module used to redirect DNS requests to name servers. This module supports a caching-only name server which will store the DNS entries for a specified item. So, when there is a query next time, the values will be taken from the cache and the response will be sent from the module itself. This will shorten the waiting time significantly, especially if it is a slow connection.



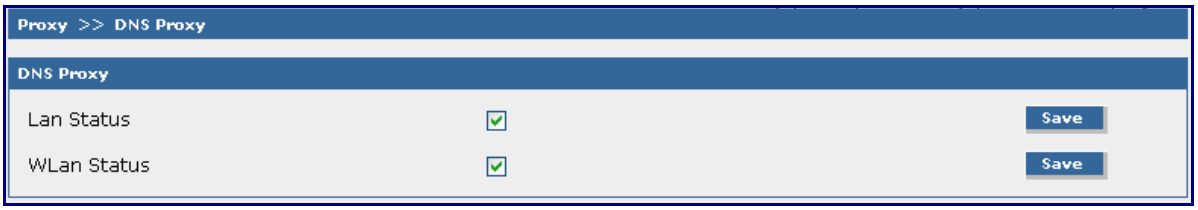
DNS Proxy

LAN Status

Click the *LAN Status* box to enable the DNS proxy. Click the **Save** button.
If enabled, the DNS Proxy will be listening on the LAN interface.

WLAN Status

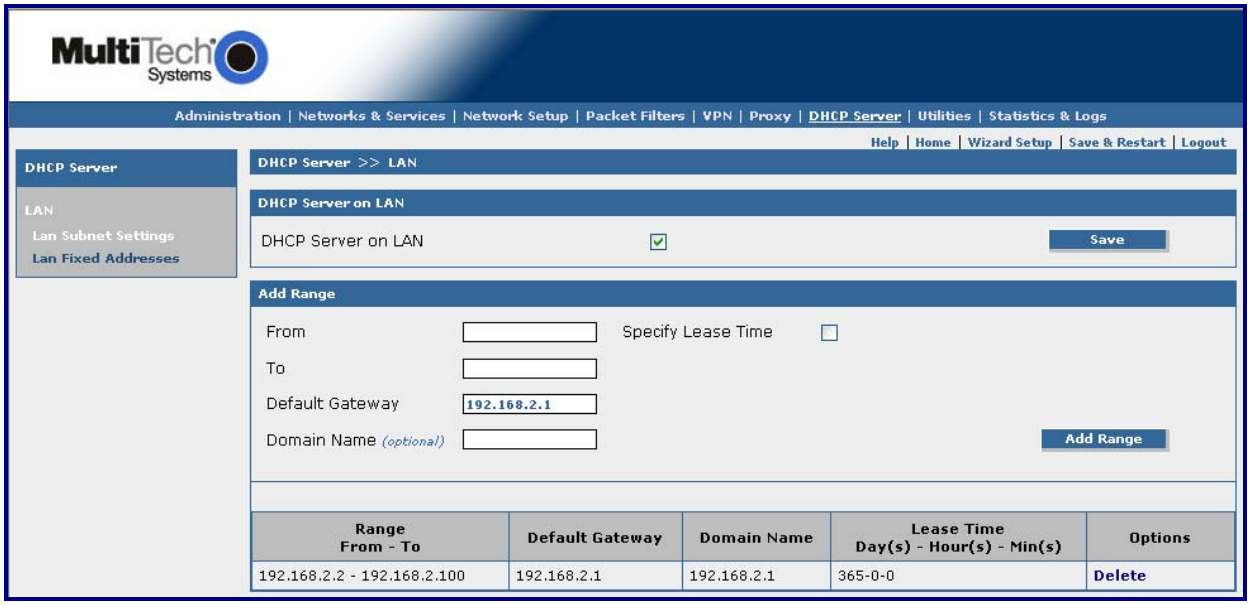
With AP build, you can select *WLAN Status* to enable DNS proxy. Click the **Save** button.



DHCP Server

DHCP Server › LAN Subnet Settings

DHCP (Dynamic Host Configuration Protocol) is a protocol that allows individual devices on an IP network to get their own network configuration information (IP address, subnet mask, broadcast address, etc.) from a DHCP server. The overall purpose of the DHCP is to make it easier to administer a large network.



DHCP Server on LAN

DHCP Server on LAN

The DHCP Server is enabled by default. If you would like to disable it, uncheck the *DHCP Server on LAN* checkbox. If you change the check mark, click the **Save** button to activate the change.

Add Range

From

To add a range of IP addresses, enter the beginning address of the range in this *From* field.

To

Enter the last IP address of the range in this *To* field.

Specify Lease Time

By default, infinite lease is assigned to the configured subnet. However, this is NOT mandatory and can be configured. If enabled by checking the box, the following lease time parameters can be configured:
Day, Hours, Mins

Default Gateway

Enter the RouteFinder's IP Address. This address will have to be assigned to the DHCP Client.

Domain Name (optional)

Enter the Domain Name Server's IP Address. This configured DNS IP address is passed on to the DHCP Client. This parameter is optional.

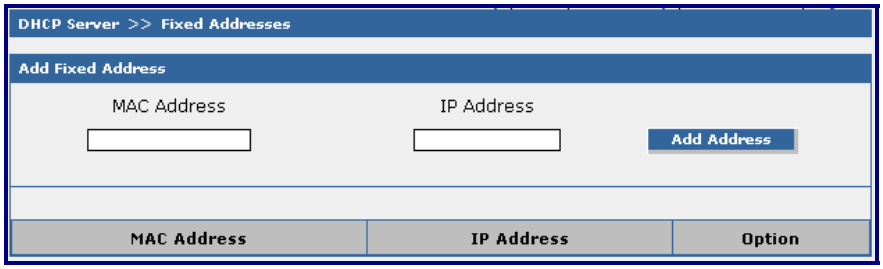
Click Add Range

Click the Add Range button when you have finished entering your parameters.

Delete

You can delete a range by selecting it and clicking **Delete**.

The DHCP server can be made to assign a fixed IP address for a particular system by identifying the MAC address. This binding can be made permanent by configuring it here. The same IP address will not be used for any DHCP client with a different MAC address, even if there is no active DHCP connection with that IP address.



Add Fixed Address

Enter both a MAC address and an IP address.

MAC Address

Enter the MAC address.

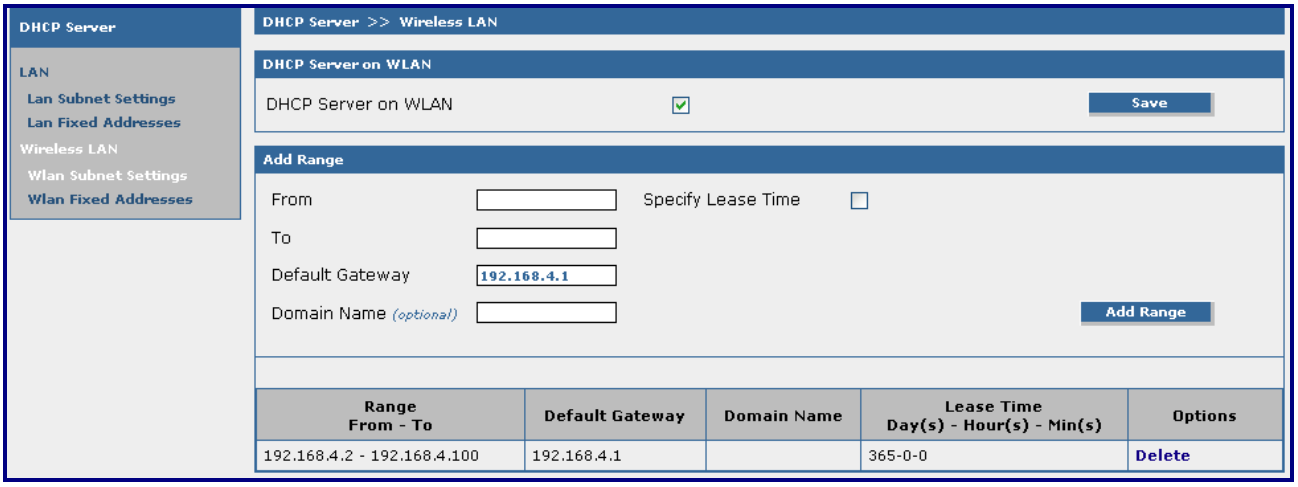
Add Fixed Address

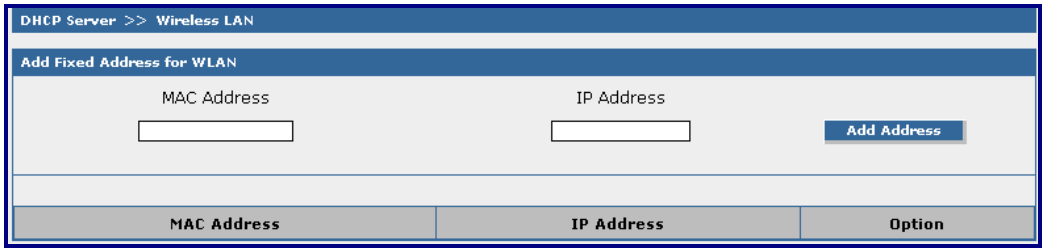
Enter the fixed IP address.

DHCP Server › WLAN Subnet Settings and WLAN Fixed Addresses

This screen becomes available after you have checked the *Independent Subnet* box on the *Network Setup* > *Wireless LAN* screen. On this DHCP screen, you will be able to set up a separate Network subnet address for the wireless LAN. You might want to use this to give a certain workstation access to the Internet and not to the your local network or *vice versa.*

Following the same directions for these screens as for the *LAN Subnet Settings* and *LAN Fixed Addresses*.

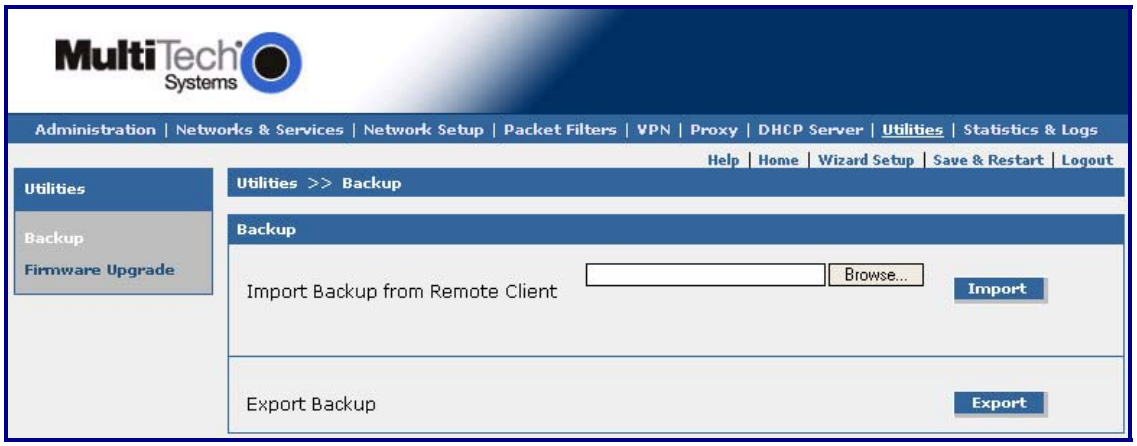




Utilities

Utilities › Backup

The Backup function lets you save the RouteFinder settings on a local hard disk or exported to a remote client. With a backup file, you can set a recently installed RouteFinder to the identical configuration level as an existing RouteFinder. This is also useful in case there is a problem with your new settings.



Backup

Import Backup from Remote Client

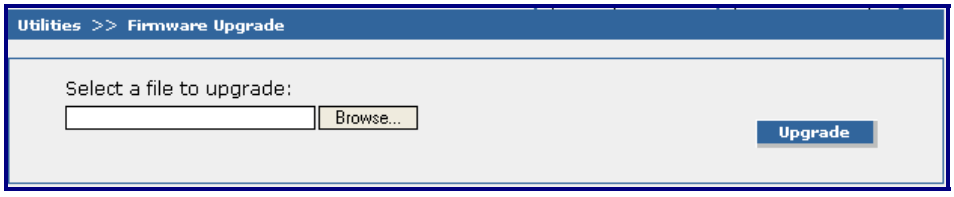
Use this section of the screen to import a saved configured. Click the **Browse** button to locate the file. Then click the **Impor**t button to restore the RouteFinder's configuration from this backup file. The configuration file is downloaded to the RouteFinder and the saved configuration restored.

Export Backup

Use this section of the screen to store the RouteFinder's configuration. Click the **Export** button to save the configuration file.

Utilities › Firmware Upgrade

The firmware on the RouteFinder can be upgraded to the latest version using this feature. All Multi-Tech firmware upgrades are posted on the Multi-Tech Web site from which they can be downloaded.



Select a File to Upgrade

Click the browse button to locate the latest firmware version.

Click the **Upgrade** button to start the download.

Note: The RouteFinder will reboot automatically after the firmware upgrade.

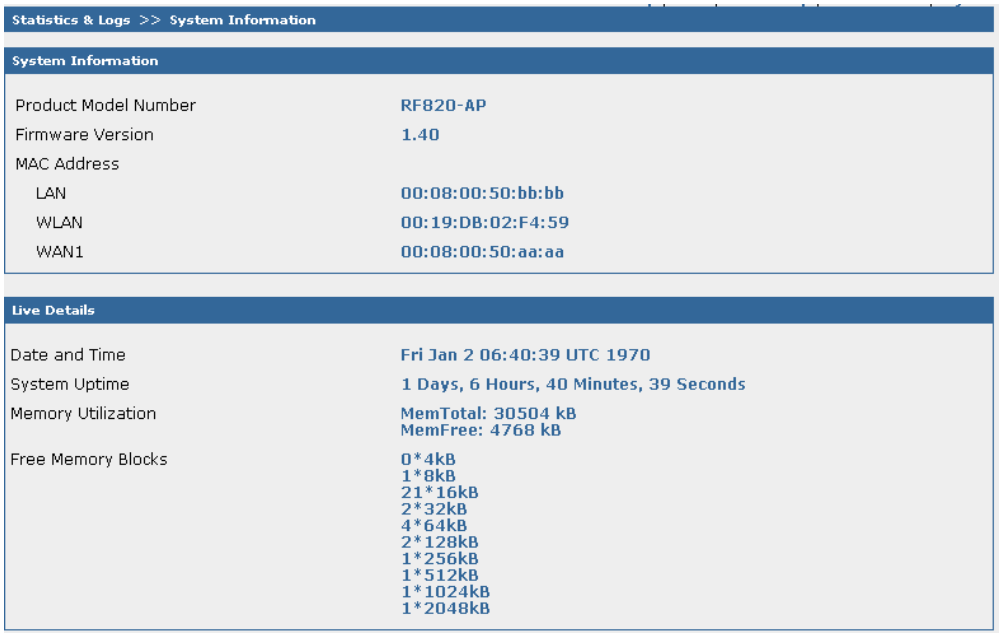
Statistics & Logs

Statistics & Logs › System Information

The System Information screen provides the following information:

1. System Information
   - Product Modem Number
   - Firmware Version
   - MAC Address
2. Live Details
   - Date and Time
   - System Uptime
   - Memory Utilization
   - Free Memory Blocks

RF820/RF820-AP Screen



RF830/RF830-AP Screen

The RF839/RF830-AP screen will displays system information for LAN, WLAN, WAN1, and WAN2.

Statistics & Logs › Network Interface Details

The screen provides information on the network traffic on all the interfaces.

Screen Note: The RF830/RF830-AP screen includes statistics for the WAN2 interface.

RF820/RF820-AP Screen

Statistics & Logs >> Network Interface Details

Network Statistics

Interface	Received Packets	Transmitted Packets	Received Bytes	Transmitted Bytes
LAN	5525	4760	659990	3209652
WLAN	356606	352	-	-
WAN1	0	123	0	72570

RF830/RF830-AP Screen

Statistics & Logs >> Network Interface Details

Network Statistics

Interface	Received Packets	Transmitted Packets	Received Bytes	Transmitted Bytes
LAN	13622	5077	1822363	2830243
WLAN	39567939	37531	-	-
WAN1	0	16267	0	9597530
WAN2	0	16267	0	9597530

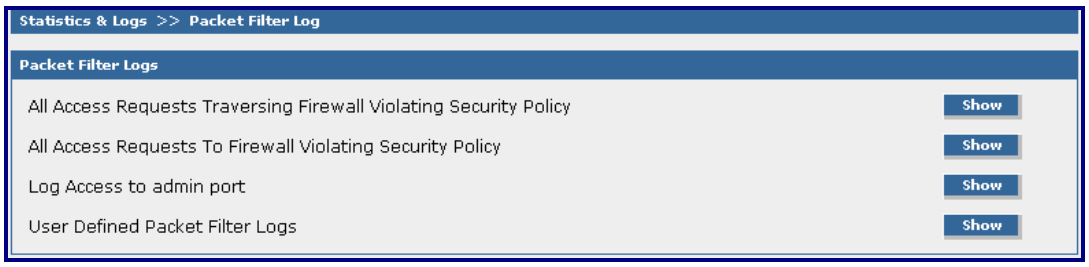
Statistics & Logs › Packet Filter Log

The screen displays the following Packet Filter Logs:

All Access Requests Traversing Firewall Violating Security Policy
All access requests from the private (LAN) and public (WAN 1 and WAN 2) network clients to traverse the RouteFinder that violate the configured security policy.

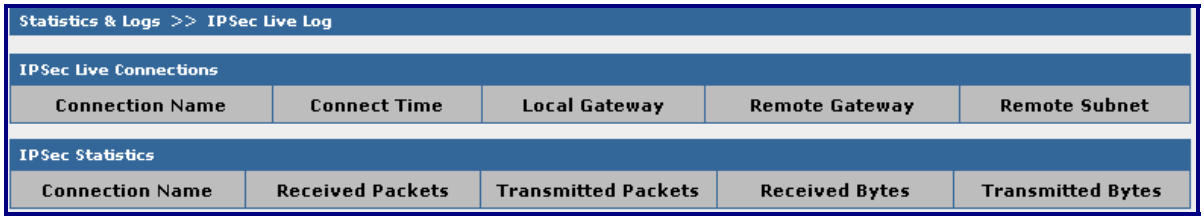
All Access Requests to Firewall Violating Security Policy
All access requests from the private (LAN) and public (WAN 1 and WAN 2) network clients to send traffic to the RouteFinder itself that violate the configured security policy.

Log Access to Administrative Access Port
All access requests from the private (LAN) and public (WAN 1 and WAN 2) network clients to send traffic to the RouteFinder on the administrative access port.



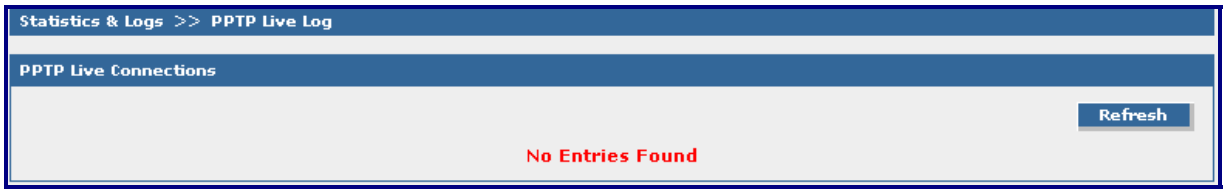
Statistics & Logs › IPSec Live Log

IPSec Live Log gives information on connections that are active.
IPSec Statistics gives statistics of transmitted and received packets/bytes.



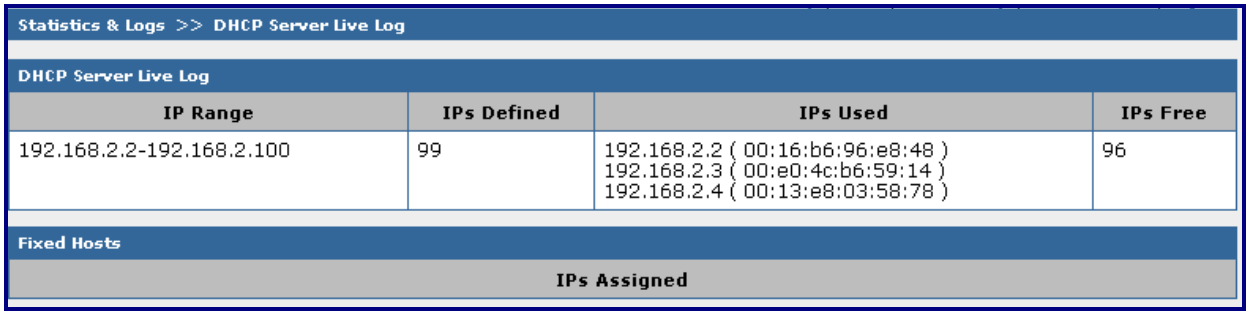
Statistics & Logs › PPTP Live Log

The PPTP Live Log gives information about users who are logged in into the PPTP server at any given point in time. It also gives the Connect Time (data and time), Interface Name (the link on which the user is connected), User Name, Local IP Address and Remote IP Address assigned, Bytes Received, and Bytes Sent.



Statistics & Logs › DHCP Server Live Log

The DHCP Server Live Log gives information for a sub network:



Statistics & Logs › PPP Cellular/Analog Log

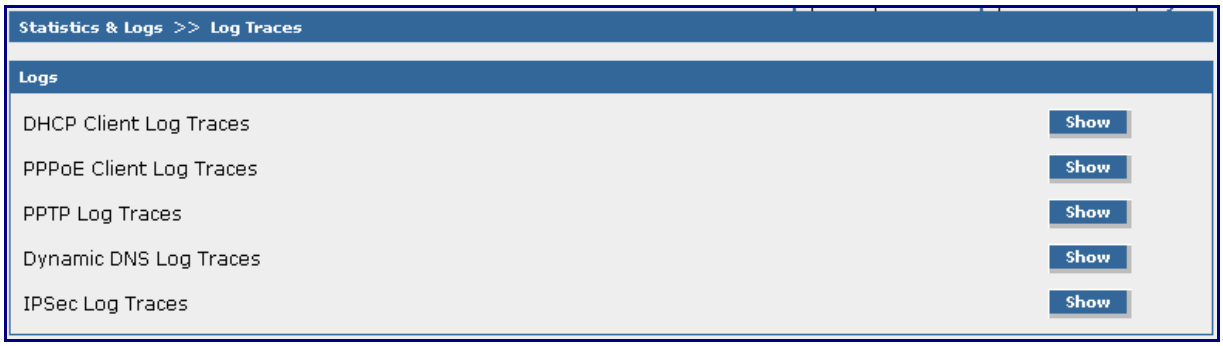
The PPP Cellular/Analog Log gives information about the modem connection:

Statistics & Logs › WLAN Client Live Log

The WLAN Client Live Log lists current WLAN connections.

Statistics & Logs › Log Traces

Log Traces provides information about the following connections.



Logs

DHCP Client Log Traces

Click the **Show** button to view connection events between the DHCP Client and the DHCP Server.

PPPoE Client Log Traces

Click the **Show** button to view connection events between the PPPoE Client and the DHCP Server.

PPTP Log Traces

Click the **Show** button to view PPTP connection events.

Dynamic DNS Log Traces

Click the **Show** button to view DDNS connection events.

IPSec Log Traces

Click the **Show** button to view IPSec connection events and key negotiations.

Chapter 6 – Troubleshooting

This chapter provides a list of common problems encountered while installing, configuring or administering the RouteFinder. In the event you are unable to resolve your problem, refer to the Warranty information on the Multi-Tech Web site. For Technical Support, see the copyright page for information about contacting our Technical Support representatives.

System Diagnostics *as a Troubleshooting Tool*

The ***System Diagnostics*** function performs a check-up on the SOHO RouteFinder to make sure that it is functioning properly.

To display this screen, launch your Web browser and enter the RouteFinder's IP address (**http://192.168.2.1**) in the browser's address box.

You might want to print this page before you call Technical Support.

Problem #1

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 RouteFinder 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 click **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 #2

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 RouteFinder.
- Use Web browser interface 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 #3

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 section in the User Guide for the appropriate initialization string.

Problem #4

My RouteFinder dials-up a connection but can't seem to communicate 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 the RouteFinder Web browser management interface to set the baud rate to a lower rate and retry the connection.
- If your connection still doesn't work, contact your ISP.

Problem #5

Sometimes when I try to 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 RouteFinder, 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 Web browser management interface 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 #6

After installing my RouteFinder, 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 Web browser management interface to view the number of concurrent client connections to your ISP.

Problem #7

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

- The RouteFinder 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 RouteFinder to dial-up your ISP. To determine which computer on your network is processing a request for an Internet connection, use the RouteFinder Web browser management interface. The event messages will provide information about which computer is causing the RouteFinder to dial and which service (port #) the computer is requesting.

Problem #8

The **Please set the Device IP** screen displays while configuring the RouteFinder.

- The system detects that the RouteFinder's LAN Ethernet IP address is not in the same subnet as the PC's. Use RouteFinder Web browser management interface to set the RouteFinder's IP address to the same network as your PC's.

Problem #9

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

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

Chapter 7 – Frequently Asked Questions

Where is the xDSL/Cable 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.

Does the 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.

Does the WAN connection of the xDSL/Cable 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.

What Is Network Address Translation and How Is It Used?

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.

Does the xDSL/Cable Router support any operating system other than Windows 2000+ and 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.

Does the Router pass PPTP packets or actively route PPTP sessions?

The Router lets PPTP packets pass through.

What is the maximum number of users supported by the Router?

The Router supports up to 253 users.

Is the Router cross-platform compatible?

Any platform that supports Ethernet & TCP/IP is compatible with the router.

Will the Router function in a Mac environment?

Yes, as long as you have a browser to configure the router.

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.

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.

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.

Which modems are compatible with the router?

The Router is compatible with any cable modem or DSL modem that supports Ethernet.

How do I access the Router's setup pages with a Mac?

The router's setup pages are accessible to the Mac through a browser. Use the default address 192.168.2.1.

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.

Does Multi-Tech provide syslog support?

Yes.

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

Consult your ISP to confirm this data.

Does the Router support PPP over Ethernet (PPPoE)?

Yes, the router does support PPPoE.

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.

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 for the RouteFinder at www.multitech.com.
- Reset the Router's factory default by holding down the reset button until the lights start blinking.
- Flash the firmware again to the RouteFinder to ensure that it was successfully written to the unit.

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.

Does the Router support IPSec?

The RouteFinder supports IPSec endpoint/gateway.

What type of firewall is the router equipped with?

The Router uses NAT.

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.

Appendix A – Table of Commonly Supported Subnet Addresses

This table lists commonly supported Subnets organized by Address.

	Network Number	Hosts Available	Broadcast Address
255.255.255.128	N.N.N.0	N.N.N.1-126	N.N.N.127
/25	N.N.N.128	N.N.N.129-254	N.N.N.255

	Network Number	Hosts Available	Broadcast Address
255.255.255.192	N.N.N.0	N.N.N.1-62	N.N.N.63
/26	N.N.N.64	N.N.N.65-126	N.N.N.127
	N.N.N.128	N.N.N.129-190	N.N.N.191
	N.N.N.192	N.N.N.193-254	N.N.N.255

	Network Number	Hosts Available	Broadcast Address
255.255.255.224	N.N.N.0	N.N.N.1-30	N.N.N.31
/27	N.N.N.32	N.N.N.33-62	N.N.N.63
	N.N.N.64	N.N.N.65-94	N.N.N.95
	N.N.N.96	N.N.N.97-126	N.N.N.127
	N.N.N.128	N.N.N.129-158	N.N.N.159
	N.N.N.160	N.N.N.161-190	N.N.N.191
	N.N.N.192	N.N.N.193-222	N.N.N.223
	N.N.N.224	N.N.N.225-254	N.N.N.255

	Network Number	Hosts Available	Broadcast Address
255.255.255.240	N.N.N.0	N.N.N.1-14	N.N.N.15
/28	N.N.N.16	N.N.N.17-30	N.N.N.31
	N.N.N.32	N.N.N.33-46	N.N.N.47
	N.N.N.48	N.N.N.49-62	N.N.N.63
	N.N.N.64	N.N.N.65-78	N.N.N.79
	N.N.N.80	N.N.N.81-94	N.N.N.95
	N.N.N.96	N.N.N.97-110	N.N.N.111
	N.N.N.112	N.N.N.113-126	N.N.N.127
	N.N.N.128	N.N.N.129-142	N.N.N.143
	N.N.N.144	N.N.N.145-158	N.N.N.159
	N.N.N.160	N.N.N.161-174	N.N.N.175
	N.N.N.176	N.N.N.177-190	N.N.N.191
	N.N.N.192	N.N.N.193-206	N.N.N.207
	N.N.N.208	N.N.N.209-222	N.N.N.223
	N.N.N.224	N.N.N.225-238	N.N.N.239
	N.N.N.240	N.N.N.241-254	N.N.N.255

	Network Number	Hosts Available	Broadcast Address
255.255.255.248	N.N.N.0	N.N.N.1-6	N.N.N.7
/29	N.N.N.8	N.N.N.9-14	N.N.N.15
	N.N.N.16	N.N.N.17-22	N.N.N.23
	N.N.N.24	N.N.N.25-30	N.N.N.31
	N.N.N.32	N.N.N.33-38	N.N.N.39
	N.N.N.40	N.N.N.41-46	N.N.N.47
	N.N.N.48	N.N.N.49-54	N.N.N.55
	N.N.N.56	N.N.N.57-62	N.N.N.63
	N.N.N.64	N.N.N.65-70	N.N.N.71
	N.N.N.72	N.N.N.73-78	N.N.N.79
	N.N.N.80	N.N.N.81-86	N.N.N.87
	N.N.N.88	N.N.N.89-94	N.N.N.95
	N.N.N.96	N.N.N.97-102	N.N.N.103
	N.N.N.104	N.N.N.105-110	N.N.N.111
	N.N.N.112	N.N.N.113-118	N.N.N.119
	N.N.N.120	N.N.N.121-126	N.N.N.127
	N.N.N.128	N.N.N.129-134	N.N.N.135
	N.N.N.136	N.N.N.137-142	N.N.N.143
	N.N.N.144	N.N.N.145-150	N.N.N.151
	N.N.N.152	N.N.N.153-158	N.N.N.159
	N.N.N.160	N.N.N.161-166	N.N.N.167
	N.N.N.168	N.N.N.169-174	N.N.N.175
	N.N.N.176	N.N.N.177-182	N.N.N.183
	N.N.N.184	N.N.N.185-190	N.N.N.191

	N.N.N.192	N.N.N.193-198	N.N.N.199
	N.N.N.200	N.N.N.201-206	N.N.N.207
	N.N.N.208	N.N.N.209-214	N.N.N.215
	N.N.N.216	N.N.N.217-222	N.N.N.223
	N.N.N.224	N.N.N.225-230	N.N.N.231
	N.N.N.232	N.N.N.233-238	N.N.N.239
	N.N.N.240	N.N.N.241-246	N.N.N.247
	N.N.N.248	N.N.N.249-254	N.N.N.255
	Network Number	**Hosts Available**	**Broadcast Address**
255.255.255.252 /30	N.N.N.0	N.N.N.1-2	N.N.N.3
	N.N.N.4	N.N.N.5-6	N.N.N.7
	N.N.N.8	N.N.N.9-10	N.N.N.11
	N.N.N.12	N.N.N.13-14	N.N.N.15
	N.N.N.16	N.N.N.17-18	N.N.N.19
	N.N.N.20	N.N.N.21-22	N.N.N.23
	N.N.N.24	N.N.N.25-26	N.N.N.27
	N.N.N.28	N.N.N.29-30	N.N.N.31
	N.N.N.32	N.N.N.33-34	N.N.N.35
	N.N.N.36	N.N.N.37-38	N.N.N.39
	N.N.N.40	N.N.N.41-42	N.N.N.43
	N.N.N.44	N.N.N.45-46	N.N.N.47
	N.N.N.48	N.N.N.49-50	N.N.N.51
	N.N.N.52	N.N.N.53-54	N.N.N.55
	N.N.N.56	N.N.N.57-58	N.N.N.59
	N.N.N.60	N.N.N.61-62	N.N.N.63
	N.N.N.64	N.N.N.65-66	N.N.N.67
	N.N.N.68	N.N.N.69-70	N.N.N.71
	N.N.N.72	N.N.N.73-74	N.N.N.75
	N.N.N.76	N.N.N.77-78	N.N.N.79
	N.N.N.80	N.N.N.81-82	N.N.N.83
	N.N.N.84	N.N.N.85-86	N.N.N.87
	N.N.N.88	N.N.N.89-90	N.N.N.91
	N.N.N.92	N.N.N.93-94	N.N.N.95
	N.N.N.96	N.N.N.97-98	N.N.N.99
	N.N.N.100	N.N.N.101-102	N.N.N.103
	N.N.N.104	N.N.N.105-106	N.N.N.107
	N.N.N.108	N.N.N.109-110	N.N.N.111
	N.N.N.112	N.N.N.113-114	N.N.N.115
	N.N.N.116	N.N.N.117-118	N.N.N.119
	N.N.N.120	N.N.N.121-122	N.N.N.123
	N.N.N.124	N.N.N.125-126	N.N.N.127
	N.N.N.128	N.N.N.129-130	N.N.N.131
	N.N.N.132	N.N.N.133-134	N.N.N.135
	N.N.N.136	N.N.N.137-138	N.N.N.139
	N.N.N.140	N.N.N.141-142	N.N.N.143
	N.N.N.144	N.N.N.145-146	N.N.N.147
	N.N.N.148	N.N.N.149-150	N.N.N.151
	N.N.N.152	N.N.N.153-154	N.N.N.155
	N.N.N.156	N.N.N.157-158	N.N.N.159
	N.N.N.160	N.N.N.161-162	N.N.N.163
	N.N.N.164	N.N.N.165-166	N.N.N.167
	N.N.N.168	N.N.N.169-170	N.N.N.171
	N.N.N.172	N.N.N.173-174	N.N.N.175
	N.N.N.176	N.N.N.177-178	N.N.N.179
	N.N.N.180	N.N.N.181-182	N.N.N.183
	N.N.N.184	N.N.N.185-186	N.N.N.187
	N.N.N.188	N.N.N.189-190	N.N.N.191
	N.N.N.192	N.N.N.193-194	N.N.N.195
	N.N.N.196	N.N.N.197-198	N.N.N.199
	N.N.N.200	N.N.N.201-202	N.N.N.203
	N.N.N.204	N.N.N.205-206	N.N.N.207
	N.N.N.208	N.N.N.209-210	N.N.N.211
	N.N.N.212	N.N.N.213-214	N.N.N.215
	N.N.N.216	N.N.N.217-218	N.N.N.219
	N.N.N.220	N.N.N.221-222	N.N.N.223
	N.N.N.224	N.N.N.225-226	N.N.N.227
	N.N.N.228	N.N.N.229-230	N.N.N.231
	N.N.N.232	N.N.N.233-234	N.N.N.235
	N.N.N.236	N.N.N.237-238	N.N.N.239
	N.N.N.240	N.N.N.241-242	N.N.N.243
	N.N.N.244	N.N.N.245-246	N.N.N.247
	N.N.N.248	N.N.N.249-250	N.N.N.251
	N.N.N.252	N.N.N.253-254	N.N.N.255

Appendix B – Antenna for the Wireless RouteFinder

The Antenna

Your ship kit for the wireless RouteFinders (RF820-AP and RF830-AP) includes a 2.4 GHz 5dBi SWI-Reverse-F Swivel Antenna.

Important Notes:

- The antenna for this product must be a reverse polarity SMA antenna.
- The antenna must be attached in order for the RouteFinder to be operational.

Antenna Electrical Characteristics

Frequency:	2400 to 2500 MHZ
Gain:	4.5dBi (nominal)
VSWR:	≤ 2
Polarization:	Linear, Vertical
Maximum Power:	20W
Impedance:	50 Ω
Connector:	RP-SMA Plug Reverse Polarity Meets FCC Part 15.203 Requirements

Mechanical

Testing Condition Note: Non-operating during test.

Endurance

Number of connection/disconnection of the connector: 500 cycles

Number of 360° rotation of the connector: 1000 cycles

Mandatory: Guaranty of functionalities after test

Bending

Number of 90° at the hinge parts and bending on one direction with 1kg force: 1000 cycles

Mandatory: No mechanical damage tolerated. Guaranty of functionalities after test.

Antenna Resistance

Tests are applicable to all parts and both sides.

Traction

Tractions force applied 3 times on plugs during 15 seconds: 5kg

Mandatory: No mechanical damage tolerated. Guaranty of functionalities after test.

Environmental

Storage

Condition: Non-operating during test.

Cold: -40°C during 72h (IEC 68-2-1 standard Ab/Ad test)

Dry Heat: +80°C during 96h (IEC 68-2-2 standard Bb/Bd test)

Humidity: +40°C at 95% R.H. during 4 days (IEC 68-2-56 standard Cb test)

Mandatory: No mechanical or visible damage tolerated. Guaranty of functionalities after test.

Operation

Condition: Operating during test.

Cold: -10°C during 48h (IEC 68-2-1 standard Ab/Ad test)

Dry Heat: +55°C during 48h (IEC 68-2-2 standard Bb/Bd test)

Humidity: -10°C to +55°C at 95% R.H. 4 cycles (IEC 68-2-30 standard Nb test)

Mandatory: No mechanical or visible damage tolerated. Guaranty of functionalities during and after test.

Appendix C – Waste Electrical and Electronic Equipment Directive (WEEE)

Waste Electrical and Electronic Equipment (WEEE) Directive

The WEEE directive places an obligation on manufacturers, distributors and retailers to take-back electronic products at the end of their useful life. A sister Directive, ROHS (Restriction of Hazardous Substances), complements the WEEE Directive by banning the presence of specific hazardous substances in the products at the design phase. The WEEE Directive covers all Multi-Tech products being sold into the EU as of August 13, 2005. Manufacturers, distributors and retailers are obliged to finance the costs of recovery from municipal collection points, reuse, and recycling of specified percentages per the WEEE requirements.

Instructions for Disposal of WEEE by Users in the European Union

The symbol shown below is on the product or on its packaging which indicates that this product must not be disposed of with other waste. Instead, it is the user's responsibility to dispose of the user's waste equipment by handing it over to a designated collection point for the recycling of electrical and electronic waste equipment. The separate collection and recycling of waste equipment at the time of disposal will help to conserve natural resources and ensure that it is recycled in a manner that protects human health and the environment. For more information about where you can drop off your waste equipment for recycling, please contact your local city office, your household waste disposal service or the seller from whom you purchased the product.

06/27/2005

Glossary

A

AES
AES (Advanced Encryption Standard), also known as Rijndael, is a block cipher adopted as an encryption standard.

Authentication
The process of determining the identity of a user attempting to access a system and the process of verifying that a particular name really belongs to a particular entity.

Asynchronous
A method of transmitting data which allows characters to be sent at irregular intervals.

B

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

Blocked Cipher
Cipher that encrypts data in blocks of a fixed size: DES, IDEA, and SKIPJACK are block ciphers.

C

Client
A computing entity in a network that seeks service from other entities on the network. Client software generally resides on personal workstations and is used to contact network servers to retrieve information and perform other actives.

D

Data Encryption Standard (DES)
Block cipher that is widely used in commercial systems. It is a Federal standard so it is deemed acceptable by many financial institutions.

Data Key
Crypto key that encrypts data as opposed to a key that encrypts other keys. Also called a session key.

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 dialog box in RouteFinder Web browser management interface. 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 the DNS translator, you need to know the IP address of your ISP's DNS Server.

Domain Name
The textual name assigned to a host on the Internet. The Domain Name Service (DNS) protocol translates between domain names and numerical IP addresses.

Dynamic Routing
Routing is the process of selecting the correct path for a message. Dynamic routing adjusts automatically to changes in network topologies or traffic. It automatically accomplishes load balancing and optimizes performance of the network “on the fly.”

E

Encryption
In general use, the transformation of data into a form unreadable by anyone without a secret decryption key. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it is not intended.

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

F

Filtering
An operating parameter used in LAN bridges and routers that when set will cause these devices to block the transfer of packets from one LAN to another.

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 Web browser management 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.

G

Gateway
An entrance and exit into a communications network.

I

IKE
Internet Key Exchange – a procedure by which the value of a key is shared between two or more parties.

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.

IPSec
A collection of IP security measures that comprise an optional tunneling protocol for IPv6. IPSec supports authentication through an “authentication header” which is used to verify the validity of the originating address in the header of every packet of every packet stream.

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 RouteFinder 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 firewall function of the RouteFinder 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.

PING
A program that tests whether a particular network destination on the Internet is online (that is, working) by bouncing a “signal” off a specified IP destination address.

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.

PPPoE
Point-to-point protocol over the Ethernet. It is a means of connecting from your premises to your Internet Service Provider. Its main advantage is that it determines the need for the ISP to manage the allocation of IP addresses.

PPTP
Point-to-Point Tunneling Protocol – An IP tunneling protocol designed to encapsulate the LAN protocols IPX and Apple Talk within IP for transmission across the Internet and other IP-based networks.

Private Key
Key used in public key crypto that belongs to an individual entity and must be kept secret.

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 is, therefore, an Internet Access Server.

SSID
An SSID is the name of a wireless local area network (WLAN). All wireless devices on a WLAN must employ the same SSID in order to communicate with each other. SSIDs are case sensitive, consist of a sequence of alphanumeric characters (letters and numbers), and have a maximum length of 32 characters. Example: Multi-Tech.

Static Routing
Involves the selection of a route for data traffic on the basis of routing options preset by the network administrator.

Subnet
A portion of a network that shares a common address component. On TCP/IP networks, subnets are all devices whose IP Addresses have the same prefix. For example, all devices with IP addresses starting with 213.0.0 are 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.

TKIP
TKIP (Temporal Key Integrity Protocol) is a security protocol used in Wi-Fi Protected Access (WPA).

Triple DES (3DES)
Cipher that applies the DES cipher three times with either two or three different DES keys.

Tunneling
As an Internet term, tunneling means to provide a secure temporary path over the Internet or other IP-based network in a VPN (Virtual Private Network) scenario. In this context, tunneling is the process of encapsulating an encrypted data packet in an IP packet for secure transmission across an inherently insecure IP network, such as the Internet.

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.

V

Virtual Private Network
A private network built atop a public network. Hosts within the private network use encryption to talk to other hosts; the encryption excludes hosts from outside the private network even if they are on the public network.

W

WAN (Wide Area Network)
A network that connects host computers and sites across a wide geographical area.

WEP
WEP (Wired Equivalency Privacy) offers the privacy equivalent to that of a wired LAN. If activated, data is encrypted before transmission, and then the receiving station, such as an access point or another radio, performs decryption upon arrival of the data. 802.11 WEP encrypts data only between 802.11 stations.

WLAN (Wireless Local Area Network)
A LAN without wires.

WPA-PSK
Wi-Fi Protected Access (WPA and WPA2) is a class of systems to secure wireless (Wi-Fi) computer networks. WPA is designed for use with an IEEE 802.1x authentication server, which distributes different keys to each user. However, it can also be used in a less secure "pre-shared key" (PSK) mode, where every user is given the same passphrase. Pre-Shared Key mode (PSK, also known as personal mode) is designed fro home and small networks that cannot afford the cost and complexity of an 802.1x authentication server. Each user must enter a passphrase to access the network.

Index

T

U

V

W