Dual-Band Wireless VPN Router with GbE Switch

RV220W

User's Guide

Table of Contents

Document Version: 1.0

Chapter 1

Introduction

This Chapter provides an overview of the Dual-Band Wireless-N VPN Router's features and capabilities.

Congratulations on the purchase of your new Dual-Band Wireless-N VPN Router. The Dual-Band Wireless-N VPN Router is a multi-function device providing the following services:

- ***Shared Broadband Internet Access*** for all LAN users.
- ***Wireless Access Point*** for 802.11a, 802.11b, 802.11g and 802.11n Wireless Stations.
- ***4-Port Switching Hub*** for 10BaseT, 100 or 1000BaseT connections.

Dual-Band Wireless-N VPN Router Features

The Dual-Band Wireless-N VPN Router incorporates many advanced features, carefully designed to provide sophisticated functions while being easy to use.

Internet Access Features

- ***Shared Internet Access.*** All users on the LAN or WLAN can access the Internet through the Dual-Band Wireless-N VPN Router, using only a single external IP Address. The local (invalid) IP Addresses are hidden from external sources. This process is called NAT (Network Address Translation).
- ***DSL & Cable Modem Support.*** The Dual-Band Wireless-N VPN Router has a 10/100/1000BaseT Ethernet port for connecting a DSL or Cable Modem. All popular DSL and Cable Modems are supported.
- ***PPPoE, PPTP and L2TP Support.*** The Internet (WAN port) connection supports PPPoE (PPP over Ethernet), PPTP (Peer-to-Peer Tunneling Protocol) and L2TP, as well as "Direct Connection" type services.
- ***Fixed or Dynamic IP Address.*** On the Internet (WAN port) connection, the Dual-Band Wireless-N VPN Router supports both Dynamic IP Address (IP Address is allocated on connection) and Fixed IP Address.

Advanced Internet Functions

- ***Application Level Gateways (ALGs).*** Applications which use non-standard connections or port numbers are normally blocked by the Firewall. The ability to define and allow such applications is provided, to enable such applications to be used normally.
- ***Port Triggering.*** This feature, also called Special Applications, allows you to use Internet applications which normally do not function when used behind a firewall.
- ***Port Forwarding.*** This feature allows Internet users to access Internet servers on your LAN. The required setup is quick and easy.
- ***Dynamic DNS Support.*** DDNS, when used with the Virtual Servers feature, allows users to connect to Servers on your LAN using a Domain Name, even if you have a dynamic IP address which changes every time you connect.
- ***URL Filter.*** Use the URL Filter to block access to undesirable Web sites by LAN users.

- ***Access Control.*** Using the Access Control feature, you can assign LAN users to different groups, and determine which Internet services are available to each group.
- ***Scheduling.*** Both the URL Filter and Firewall rules can be scheduled to operate only at certain times. This provides great flexibility in controlling Internet -bound traffic.
- ***Logs.*** Define what data is recorded in the Logs, and optionally send log data to a Syslog Server. Log data can also be E-mailed to you.
- ***QoS Support*** Quality of Service can be used to handle packets so that more important connections receive priority over less important one.

VPN Features

- ***IPSec Support.*** IPSec is the most common protocol.
- ***Easy Configuration.*** The configuration required to allow 2 Routers to establish a VPN connection between them is easy accomplished.

Wireless Features

- ***Standards Compliant.*** The Wireless Access Point complies with the IEEE802.11g and IEEE802.11n draft 2.0 specifications for Wireless LANs.
- ***Supports Pre-N Wireless Stations.*** The 802.11n Draft standard provides for backward compatibility with the 802.11b standard, so 802.11n, 802.11a, 802.11b and 802.11g Wireless stations can be used simultaneously. The Router supports both the 2.4GHz and 5.0GHz (802.11a) bands.
- ***VLAN Support.*** The 802.1Q VLAN standard is supported, allowing traffic from different sources to be segmented. Combined with the multiple SSID feature, this provides a powerful tool to control access to your LAN.
- ***WEP support.*** Support for WEP (Wired Equivalent Privacy) is included. Key sizes of 64 Bit and 128 Bit are supported. WEP encrypts any data before transmission, providing protection against snoopers.
- ***WPA- Personal support.*** Like WEP, WPA-Personal encrypts any data before transmission, providing protection against snoopers. The WPA- Personal is a later standard than WEP, and provides both easier configuration and greater security than WEP.
- ***WPA2- Personal support.*** Support for WPA2 is also included. WPA2 uses the extremely secure AES encryption method.
- ***802.1x Support.*** Support for 802.1x mode is included, providing for the industrial-strength wireless security of 802.1x authentication and authorization.
- ***Wireless MAC Access Control.*** The Wireless Access Control feature can check the MAC address (hardware address) of Wireless stations to ensure that only trusted Wireless Stations can access your LAN.
- ***Simple Configuration.*** If the default settings are unsuitable, they can be changed quickly and easily.
- ***WPS Support.*** WPS (Wi-Fi Protected Setup) can simplify the process of connecting any device to the wireless network by using the push button configuration (PBC) on the Wireless Access Point, or entering a PIN code if there's no button.

LAN Features

- ***4-Port Switching Hub.*** The Dual-Band Wireless-N VPN Router incorporates a 4-port 10/100/1000BaseT switching hub, making it easy to create or extend your LAN.

- ***DHCP Server Support.*** **D**ynamic **H**ost **C**onfiguration **P**rotocol provides a dynamic IP address to PCs and other devices upon request. The Dual-Band Wireless-N VPN Router can act as a **DHCP Server** for devices on your local LAN and WLAN.

Configuration & Management

- ***Easy Setup.*** Use your WEB browser from anywhere on the LAN or WLAN for configuration.
- ***Configuration File Upload/Download.*** Save (download) the configuration data from the Dual-Band Wireless-N VPN Router to your PC, and restore (upload) a previously-saved configuration file to the Dual-Band Wireless-N VPN Router.
- ***Remote Management.*** The Dual-Band Wireless-N VPN Router can be managed from any PC on your LAN or Wireless LAN. And, if the Internet connection exists, it can also (optionally) be configured via the Internet.
- ***Network Diagnostics.*** You can use the Dual-Band Wireless-N VPN Router to perform a *Ping* or *DNS lookup*.
- ***UPnP Support.*** UPnP (Universal Plug and Play) allows automatic discovery and configuration of the Dual-Band Wireless-N VPN Router. UPnP is supported by Windows ME, XP, or later.

Security Features

- ***Password - protected Configuration***. Password protection is provided to prevent unauthorized users from modifying the configuration data and settings.
- ***Wireless LAN Security***. WPA-PSK, WEP and Wireless access control by MAC address are all supported. The MAC-level access control feature can be used to prevent unknown wireless stations from accessing your LAN.
- ***NAT Protection.*** An intrinsic side effect of NAT (Network Address Translation) technology is that by allowing all LAN users to share a single IP address, the location and even the existence of each PC is hidden. From the external viewpoint, there is no network, only a single device - the Dual-Band Wireless-N VPN Router.
- ***Firewall.*** All incoming data packets are monitored and all incoming server requests are filtered, thus protecting your network from malicious attacks from external sources.
- ***Protection against DoS attacks.*** DoS (Denial of Service) attacks can flood your Internet connection with invalid packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable. The Dual-Band Wireless-N VPN Router incorporates protection against DoS attacks.

Package Contents

The following items should be included. If any of these items are damaged or missing, please contact your dealer immediately.

- The Dual-Band Wireless-N VPN Router Unit
- RJ45 (LAN) cable
- Power Adapter
- Warranty Card
- CD-ROM containing the user manual.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of thefollowing measures:
-Reorient or relocate the receiving antenna.
-Increase the separation between the equipment and receiver.
-Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
-Consult the dealer or an experienced radio/TV technician for help.

You are cautioned that changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

FCC RF Radiation Exposure Statement:
1. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.2. This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

According to FCC 15.407(e), the device is intended to operate in the frequency band of 5.15GHz to 5.25GHz under all conditions of normal operation. Normal operation of this device is restricted to indoor used only to reduce any potential for harmful interference to co-channel MSS operations.

Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

RSS-GEN 7.1.4:
User Manual for Transmitters with Detachable Antennas The user manual of transmitter devices equipped with detachable antennas shall contain the followinginformation in a conspicuous location:
This device has been designed to operate with the antennas listed below, and having a maximum gain of [2.0] dB. Antennas not included in this list or having a gain greater than [2.0] dB are strictly prohibited for use with this device. The required antenna impedance is [50] ohms.

RSS-GEN 7.1.5
To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that permitted for successful communication.

IC RF Radiation Exposure Statement:
1. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.2. This equipment complies with IC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimumdistance of 20 centimeters between the radiator and your body.

except above RF exposure statement, for devices used at 5.15-5.25GHz should add the following □ wording at their user manual.□

□

According to RSS-210, the device is intended to operate in the frequency band of 5.15GHz to □ 5.25GHz under all conditions of normal operation. Normal operation of this device is restricted to □ indoor used only to reduce any potential for harmful interference to co-channel MSS operations.□

□

□

□

□

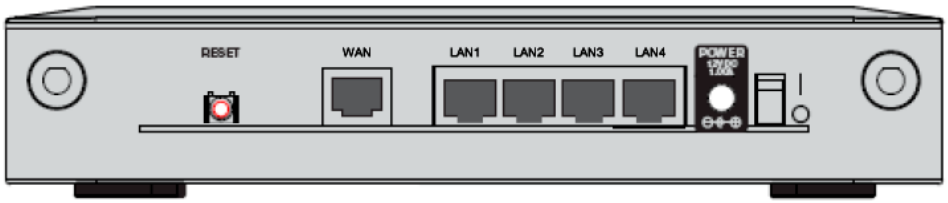
□

Physical Details

Front-mounted LEDs

POWER (Green)	**On** - Power on. **Off** - No power.
DIAG (Red)	**On** - System problem. **Off** - Normal operation. **Flashing** - System rebooting or firmware upgrading.
DMZ (Green)	**On** - DMZ enabled. **Off** - DMZ disabled.
WIRELESS (Green)	**On** - Wireless enabled. **Off** - No Wireless connections currently exist. **Flashing** - Data is being transmitting or receiving via the Wireless connection.
LAN (1~4)	Each port has 3 LEDs: • **10** - This will be ON if the LAN connection is using 10BaseT, and blinking if data is being transferred via the corresponding LAN port. • **100** - This will be ON if the LAN connection is using 100BaseT, and blinking if data is being transferred via the corresponding LAN port. • **1000** - This will be ON if the LAN connection is using 1000BaseT, and blinking if data is being transferred via the corresponding LAN port. If neither LED is on, there is no active connection on the corresponding LAN port.
WAN(Green)	The **WAN** LED lights up the appropriate LED depending upon the speed of the device that is attached to the Internet port. If the Router is connected to a cable or DSL modem, typically the 10 LED will be the only LED lit up (i.e. 10Mbps). The LED Flashes during activity.

Rear Panel



RESET button	The Reset button can be used in one of two ways: • If the Router is having problems connecting to the Internet, press the Reset button for just a second with a paper clip or a pencil tip. This is similar to pressing the Reset button on your PC to reboot it. • If you are experiencing extreme problems with the Router and have tried all other troubleshooting measures, press and hold in the Reset button for 10 seconds. This will restore the factory defaults and clear all of the Router's settings, such as port forwarding or a new password.
WAN	Connect the DSL or Cable Modem here. If your modem came with a cable, use the supplied cable. Otherwise, use a standard LAN cable.
LAN 1-4 (10/100/1000BaseT)	Use standard LAN cables (RJ45 connectors) to connect your PCs to these ports.
POWER	Connect the supplied power adapter here.

Chapter 2

Installation

2

This Chapter covers the physical installation of the Dual-Band Wireless-N VPN Router.

Requirements

- Network cables. Use standard 10/100/1000BaseT network (UTP) cables with RJ45 connectors.
- TCP/IP protocol must be installed on all PCs.
- For Internet Access, an Internet Access account with an ISP, and a DSL connection.
- To use the Wireless Access Point, all Wireless devices must be compliant with the IEEE 802.11a, IEEE 802.11g, IEEE 802.11b or IEEE 802.11n Draft specifications.

Procedure

1. Choose an Installation Site

Select a suitable place on the network to install the Dual-Band Wireless-N VPN Router. Make sure that the Router is powered off.

For best Wireless reception and performance, the Dual-Band Wireless-N VPN Router should be positioned in a central location with minimum obstructions between the Dual-Band Wireless-N VPN Router and the PCs.

2. Connect LAN Cables

Use standard LAN cables to connect PCs to the ports on the Dual-Band Wireless-N VPN Router. 10BaseT, 100BaseT and 1000BaseT connections can be used simultaneously.

3. Connect ADSL Cable

Connect the DSL or Cable modem to the INTERNET port on the Dual-Band Wireless-N VPN Router. Use the cable supplied with your DSL/Cable modem. If no cable was supplied, use a standard cable.

4. Power Up

Connect the supplied power adapter to the Dual-Band Wireless-N VPN Router. Use only the power adapter provided. Using a different one may cause hardware damage.

5. Check the LEDs

- The *Power* LED should be ON.
- The *LAN* LED should be ON (provided the PC is also ON.)
- The *WIRELESS* LED should be ON if Wireless PC is connected.

- The *WAN* LED may be OFF. After configuration, it should come ON.

Antennas and Positions

Positions

The Router can be placed in three different positions: stackable, standalone, or wall-mount.

Standalone

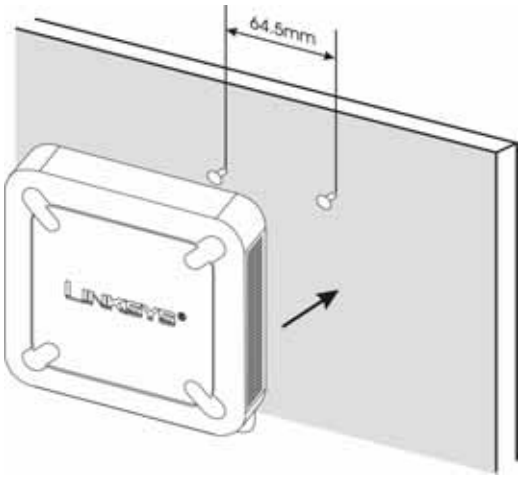
1. Locate the Router's left side panel.
2. The Router includes two stands. With the two large prongs facing outward, insert the short prongs into the little slots in the Router, and push the stand upward until it snaps into place.

Wall-mount

You will need two suitable screws to mount the Router. Make sure the screw size can fit into the crisscross wall-mount slots.

1. On the Wireless Router's back panel are two crisscross wall-mount slots.
2. Determine where you want to mount the Wireless Router, and install two screws that are 2-9/16 in (64.5mm) apart.

3. Line up the Wireless Router so that the wall-mount slots line up with the two screws.



4. Place the wall-mount slots over the screws and slide the Wireless Router down until the screws fit snugly into the wall-mount slots.

Chapter 3

Setup

This Chapter provides Setup details of the Dual-Band Wireless-N VPN Router.

Configuration Program

The Dual-Band Wireless-N VPN Router contains an HTTP server. This enables you to connect to it, and configure it, using your Web Browser. **Your Browser must support JavaScript**.

The configuration program has been tested on the following browsers:

- Netscape 7.1 or later
- Mozilla 1.6 or later
- Internet Explorer V5.5 or later

Preparation

Before attempting to configure the Dual-Band Wireless-N VPN Router, please ensure that:

- Your PC can establish a physical connection to the Dual-Band Wireless-N VPN Router. The PC and the Dual-Band Wireless-N VPN Router must be directly connected (using the Hub ports on the Dual-Band Wireless-N VPN Router) or on the same LAN segment.
- The Dual-Band Wireless-N VPN Router must be installed and powered ON.
- If the Dual-Band Wireless-N VPN Router's default IP Address (192.168.1.1) is already used by another device, the other device must be turned OFF until the Dual-Band Wireless-N VPN Router is allocated a new IP Address during configuration.

Using your Web Browser

To establish a connection from your PC to the Dual-Band Wireless-N VPN Router:

1. After installing the Dual-Band Wireless-N VPN Router in your LAN, start your PC. If your PC is already running, restart it.
2. Start your WEB browser.
3. In the *Address* box, enter "HTTP://" and the IP Address of the Dual-Band Wireless-N VPN Router, as in this example, which uses the Dual-Band Wireless-N VPN Router's default IP Address:

   `HTTP://192.168.1.1`
4. When prompted for the User name and Password, enter values as follows:
   - User name `admin`
   - Password `admin`

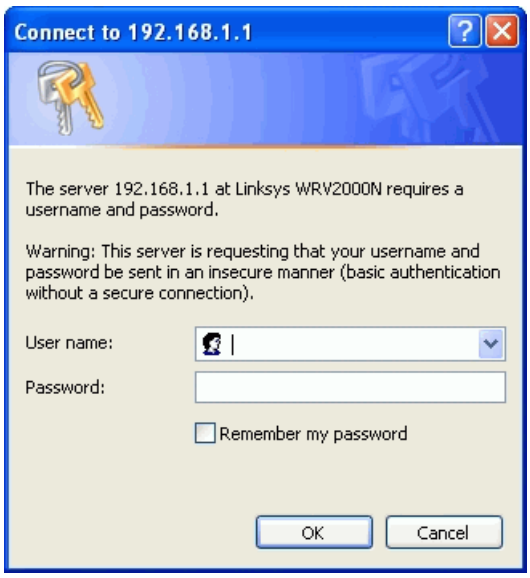


Figure 1: Login Screen

If you can't connect

If the Dual-Band Wireless-N VPN Router does not respond, check the following:

- The Dual-Band Wireless-N VPN Router is properly installed, LAN connection is OK, and it is powered ON. You can test the connection by using the "Ping" command:
  - Open the MS-DOS window or command prompt window.
  - Enter the command:
    ```
    ping 192.168.1.1
    ```
    If no response is received, either the connection is not working, or your PC's IP address is not compatible with the Dual-Band Wireless-N VPN Router's IP Address. (See next item.)
- If your PC is using a fixed IP Address, its IP Address must be within the range 192.168.1.2 to 192.168.1.254 to be compatible with the Dual-Band Wireless-N VPN Router's default IP Address of 192.168.1.1. Also, the *Network Mask* must be set to 255.255.255.0. See *Chapter 4 - PC Configuration* for details on checking your PC's TCP/IP settings.
- Ensure that your PC and the Dual-Band Wireless-N VPN Router are on the same network segment. (If you don't have a router, this must be the case.)
- Ensure you are using the wired LAN interface. The Wireless interface can only be used if its configuration matches your PC's wireless settings.

Setup Tab

The Setup screen contains all of the Router's basic setup functions. The Router can be used in most network settings without changing any of the default values. Some users may need to enter additional information in order to connect to the Internet through an ISP (Internet Service Provider) or broadband (DSL, cable modem) carrier.

Setup - Summary

The first screen that appears is the System Summary screen, which displays the Router's current status and settings. This information is read-only. Underlined text is hyperlinked to related setup pages, so if you click a hyperlink, the related setup screen will appear. On the right-hand side of this screen and all other screens of the utility is a link to the Site Map, which has links to all of the utility's tabs.

Figure 2: Summary Screen

Data - Summary Screen

System Information	
Firmware Version	It displays the current firmware version installed on this Router.
CPU	Displayed here are the type and speed of the processor installed on the Router.
System Up Time	This is the length of time in days, hours, and minutes that the Router has been active. The current time and date are also displayed.
DRAM	Displayed here is the size of DRAM installed on the Router's motherboard.
FLASH	Displayed here is the size of flash memory installed on the Router's board.
Port Statistics	
Port Statistics	This section displays the following color-coded status information on the Router's Ethernet ports: • **Green** - Indicates that the port has a connection. • **Black** - Indicates that the port has no connection.
Networking Setting Status	
LAN IP	Displays the IP address of the Router's LAN interface.
WAN IP	Displays the IP address of the Router's WAN interface. If this address was assigned using DHCP, click *DHCP Release* to release the address, or click *DHCP Renew* to renew the address.
Mode	Displays the operating mode, Gateway or Router.
Gateway	Displays the Gateway address, which is the IP address of your ISP's server.
DNS 1-2	The IP addresses of the Domain Name System (DNS) server(s) that the Router is using.
DDNS	Indicates whether the Dynamic Domain Name System (DDNS) feature is enabled.
DMZ	Indicates whether the DMZ Hosting feature is enabled.
Firewall Setting Status	
DOS (Denial of Service)	Indicates whether the DoS Protection feature is enabled to block DoS attacks.
Block WAN Request	Indicates whether the Block WAN Request feature is enabled.
Remote Management	Indicates whether the Remote Management feature is enabled.
VPN Setting Status	
Tunnel(s) Used	Displays the number of VPN tunnels currently being used.
Tunnel(s) Available	Displays the number of VPN tunnels that are available.

Setup - WAN Screen

DHCP

By default, the Router's Configuration Type is set to Automatic Configuration - DHCP, and it should be kept only if your ISP supports DHCP or you are connecting through a dynamic IP address.

Figure 3: DHCP Screen

Optional Settings	
Host Name	Enter a host name for the Router.
Domain Name	Enter a domain name for the Router.
MTU	This setting specifies the largest packet size permitted for network transmission. In most cases, keep the default, **Auto**. To specify the MTU, select **Manual**, and then enter the value in the **Size** field.

DDNS Service	Select the desired option from the list.
	• **Disabled** - If selected, no DDNS service will be used.
	• **DynDNS**
	  • **User Name, Password, Host Name** - Enter the User Name, Password, and Host Name of the account you set up with DynDNS.org.
	  • **Custom DNS** - Enable the checkbox if you want to use this feature.
	  • **Status** - The status of the DDNS service connection is displayed here.
	• **TZO**
	  • **E-mail Address, TZO Password, Domain Name** - Enter the E-mail Address, Password, and Domain Name of the account you set

	up with TZO. • **Status** - The status of the TZO service connection is displayed here.
Connect Button	When DDNS is enabled, the **Connect** button is displayed. Use this button to manually update your IP address information on the DDNS server. The Status area on this screen also updates.

Static IP

If you are required to use a permanent IP address, select Static IP.

Figure 4: Static IP

Static IP Settings	
Internet IP Address	This is the Router's IP address on the WAN port that can be reached from the Internet.
Subnet Mask	Enter the Subnet mask to match the IP address above.
Default Gateway	Your ISP will provide you with the Default Gateway (Router) to reach the Internet.
Primary DNS	Your ISP will provide you with at least one DNS (Domain Name System) Server IP Address to resolve host name to IP address mapping.
Secondary DNS	The secondary DNS will only be used if the primary DNS is not available.

PPPoE

Most DSL-based ISPs use PPPoE (Point-to-Point Protocol over Ethernet) to establish Internet connections. If you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoE. If they do, you will have to enable PPPoE.

Figure 5: PPPoE

PPPoE Settings	
Username	Enter the User Name provided by your ISP for PPPoE authentication.
Password	Enter the Password by your ISP for PPPoE authentication.
Connect on Demand	You can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, click the Connect on Demand option and enter the number of minutes you want to have elapsed before your Internet connection terminates in the **Max Idle Time** field. Use this option to minimize your DSL connection time if it is charged based on time.
Keep Alive	This option allows the Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, click the option next to Keep Alive. In the Redial Period field, you specify how often you want the Router to check the Internet connection. This option is enabled by default and the default Redial Period is 30 seconds. Use this option to minimize your Internet connection response time since it will always be connected.

PPTP

Point-to-Point Tunneling Protocol (PPTP) is a service that applies to connections in Europe and Israel only.

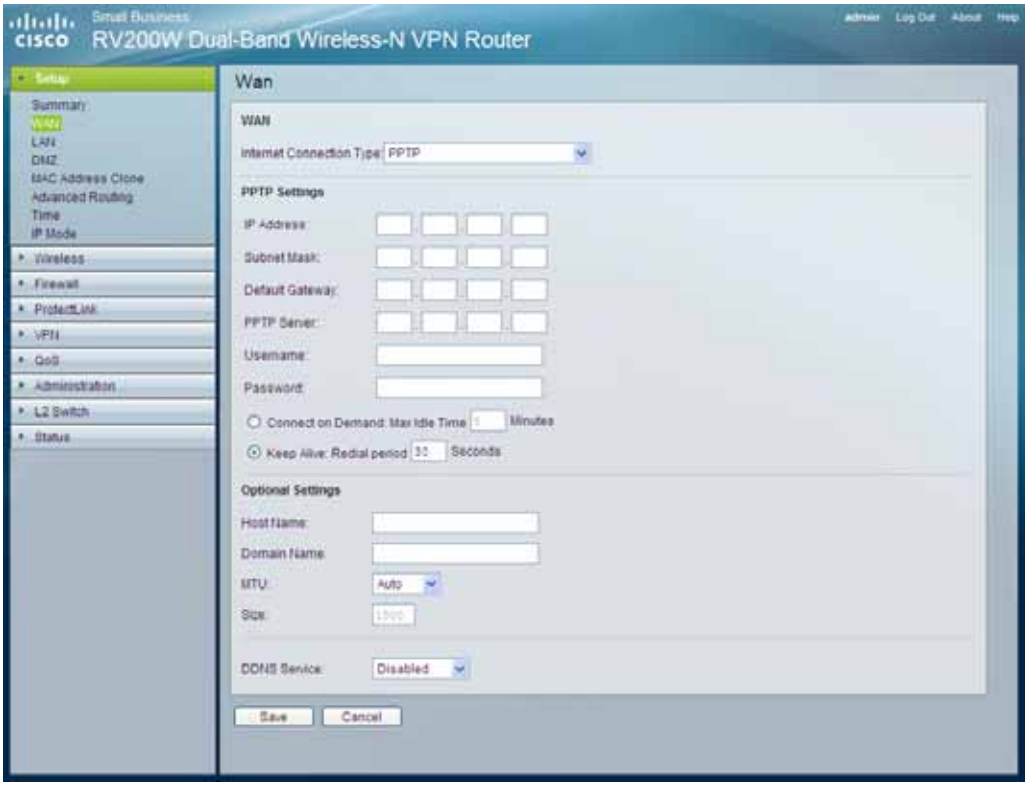


Figure 6: PPTP

PPTP Settings	
IP Address	This is the Router's IP address, when seen from the WAN, or the Internet. Your ISP will provide you with the IP Address you need to specify here.
Subnet Mask	This is the Router's Subnet Mask. Your ISP will provide you the Subnet Mask and your IP address.
Default Gateway	Your ISP will provide you with the Default Gateway IP Address.
PPTP Server	Enter the IP address of the PPTP server.
Username	Enter the User Name provided by your ISP.
Password	Enter the Password provided by your ISP.
Connect on Demand	You can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, click the Connect on Demand option and enter the number of minutes you want to have elapsed before your Internet connec-

	tion terminates in the **Max Idle Time** field. Use this option to minimize your DSL connection time if it is charged based on time.
Keep Alive	This option allows the Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, click the option next to Keep Alive. In the Redial Period field, you specify how often you want the Router to check the Internet connection. This option is enabled by default and the default Redial Period is 30 seconds. Use this option to minimize your Internet connection response time since it will always be connected.

L2TP

Layer 2 Tunneling Protocol (L2TP) is a service that tunnels Point-to-Point Protocol (PPP) across the Internet. It is used mostly in European countries. Check with your ISP for the necessary setup information.

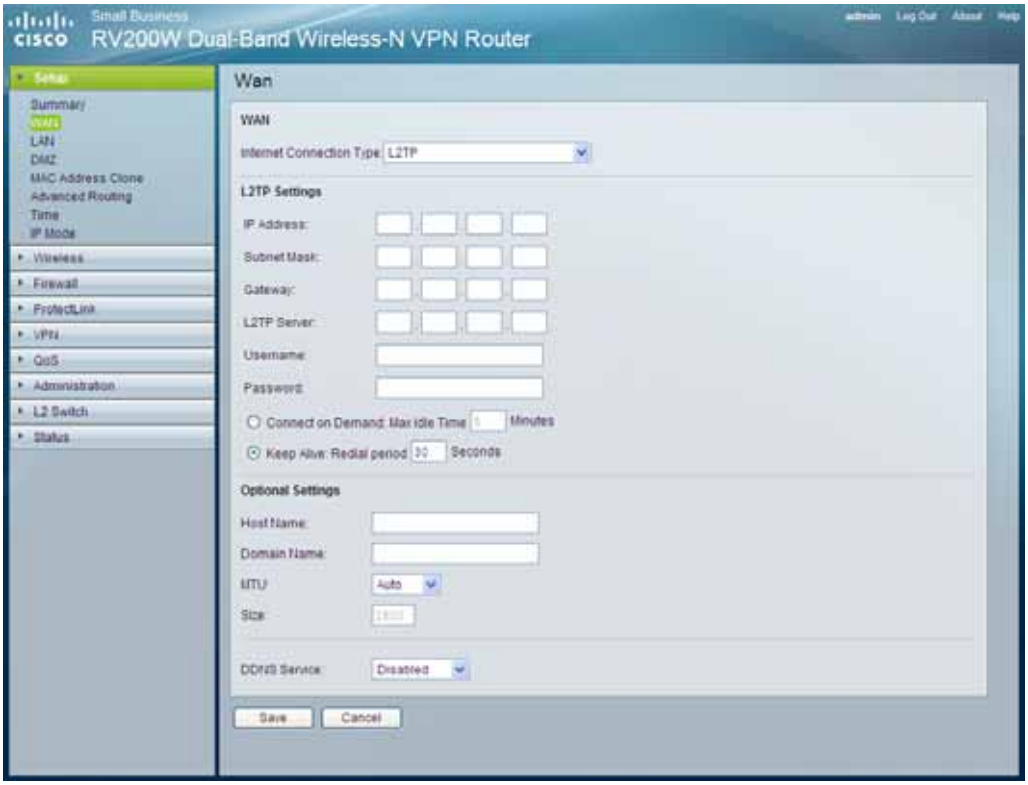


Figure 7: L2TP

L2tp Settings	
IP Address	This is the Router's IP address, when seen from the WAN, or the Internet. Your ISP will provide you with the IP Address you need to specify here.
Subnet Mask	This is the Router's Subnet Mask. Your ISP will provide you the Subnet Mask and your IP address.
Gateway	Your ISP will provide you with the Default Gateway IP Address.

L2TP Server	Enter the IP address of the L2TP server
Username	Enter the User Name provided by your ISP.
Password	Enter the Password provided by your ISP.
Connect on Demand	You can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, click the Connect on Demand option and enter the number of minutes you want to have elapsed before your Internet connection terminates in the **Max Idle Time** field. Use this option to minimize your DSL connection time if it is charged based on time.
Keep Alive	This option allows the Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, click the option next to Keep Alive. In the Redial Period field, you specify how often you want the Router to check the Internet connection. This option is enabled by default and the default Redial Period is 30 seconds. Use this option to minimize your Internet connection response time since it will always be connected.

Setup - LAN Screen

The LAN Setup section allows you to change the Router's local network settings for the four Ethernet ports.

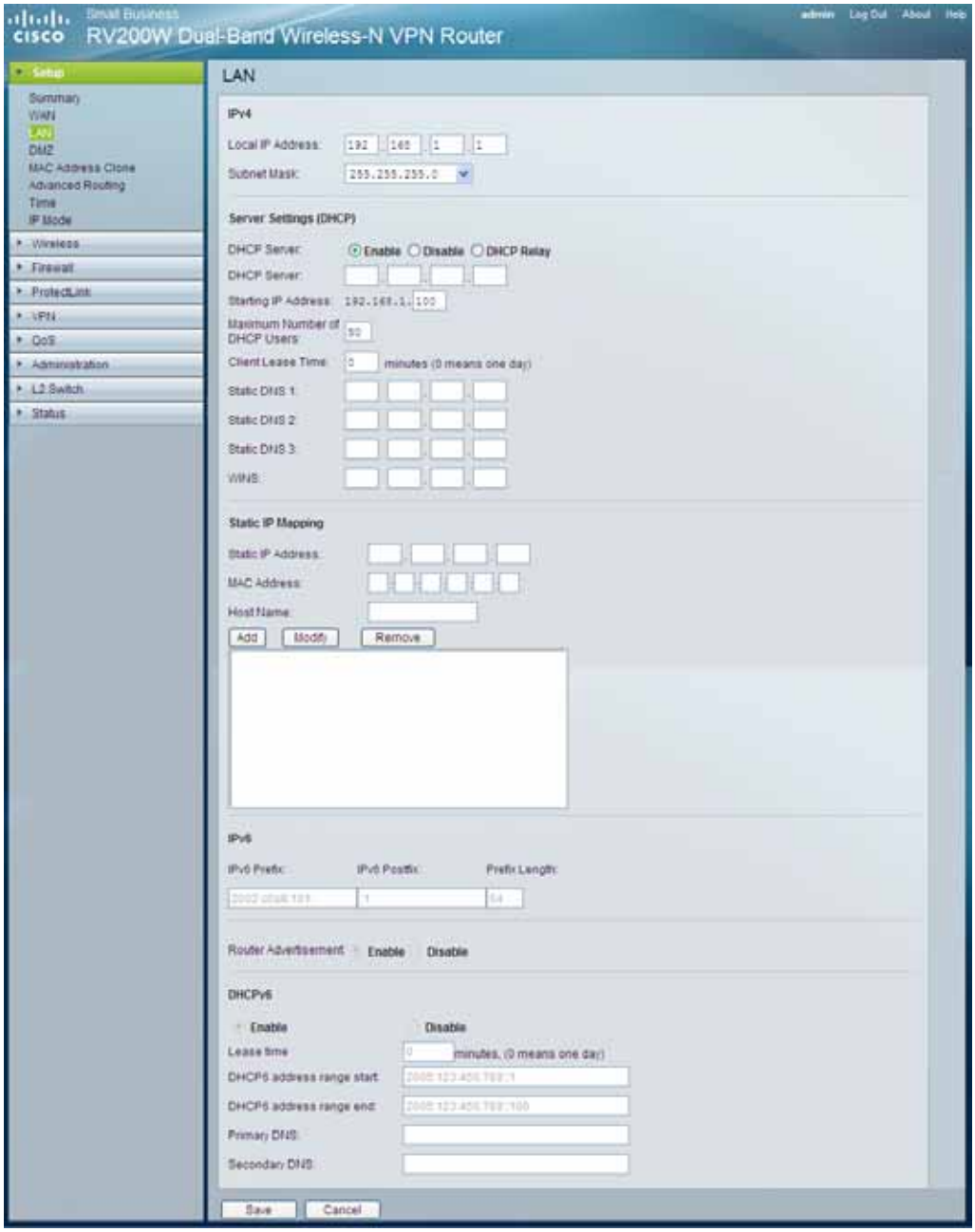


Figure 8: LAN Screen

Data - LAN Screen

IPv4	
Local IP Address	Enter the IPv4 address on the LAN side. The default value is 192.168.1.1.

Subnet Mask	Select the subnet mask from the drop-down menu. The default value is 255.255.255.0.
Server Settings (DHCP)	
DHCP Server	DHCP is enabled by default. If you already have a DHCP server on your network, or you don't want a DHCP server, then select **Disabled** (no other DHCP features will be available). If you already have a DHCP server on your network, and you want the Router to act as a Relay for that DHCP Server, select **DHCP Relay**, then enter the **DHCP Server IP Address**.
Starting IP Address	Enter a value for the DHCP server to start with when issuing IP addresses. This value will automatically follow your local IP address settings. Normally, you assign the first IP address for the Router (e.g. 192.168.1.1) so that you can assign an IP address to other devices starting from the 2nd IP address (e.g. 192.168.1.2). The last address in the subnet is for subnet broadcast (e.g. 192.168.1.255) so that the address cannot be assigned to any host.
Maximum Number of DHCP Users	Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. This number cannot be greater than the available host addresses in the subnet (e.g. 253 for /24 subnet). In order to determine the DHCP IP Address range, add the starting IP address (e.g., 100) to the number of DHCP users.
Client Lease Time	This is the amount of time a DHCP client can keep the assigned IP address before it sends a renewal request to the DHCP server. The default value is 0, which actually means one day.
Static DNS (1~3)	If applicable, enter the IP address(es) of your DNS server(s).
WINS	Windows Internet Naming Service (WINS) is a service that resolves NetBIOS names to IP addresses. WINS is assigned if the computer (DHCP client) requests one. Enter the IP address of the WINS server.
Static IP Mapping	
Static IP Address	Enter the static IP address.
MAC Address	Enter the MAC address of the device.
Host Name	Enter a descriptive name for the device.
Add, Modify, Remove buttons	Click **Add**, and configure as many entries as you would like, up to a maximum of 100. To delete an entry, select it and click **Remove**. Select the desired entry and click the **Modify** to change the settings.
IPv6	
IPv6 Prefix	Enter the IPv6 prefix.
IPv6 Postfix	Enter the IPv6 postfix.
Prefix Length	Enter the IPv6 prefix length. The default is 64, which should not need to be changed.
Router Advisement	Enabling this option allows the Router to send out IPv6 Router Advertisement packets periodically. This helps IPv6 hosts to learn their IPv6 prefix and setup their IPv6 Address automatically.

DHCPv6	
DHCPv6	Enabled or Disabled as required.
Lease Time	Enter the desired value. The default is 0, which actually means one day.
DHCP address range start	Enter the start IP address of the DHCP range.
DHCP address range end	Enter the end IP address of the DHCP range.
Primary DNS	Your ISP will provide you with at least one DNS (Domain Name System) Server IP Address to resolve host name to IP address mapping.
Secondary DNS	The secondary DNS will only be used if the primary DNS is not available.

Setup - DMZ Screen

The DMZ screen allows one local PC to be exposed to the Internet for use of a special-purpose service, such as Internet gaming and video-conferencing. DMZ hosting forwards traffic to all the ports for the specified PC simultaneously, unlike Port Range Forwarding that can only forward a maximum of 10 ranges of ports.

Figure 9: DMZ Screen

Data - DMZ Screen

DMZ	
DMZ Hosting	This feature allows one local PC to be exposed to the Internet for use of a special-purpose service such as Internet gaming and video-conferencing. To use this feature, select *Enable*. To disable the DMZ feature, select *Disable*.
DMZ Host IP Address	To expose one PC, enter the computer's IP address.

Setup - MAC Address Clone Screen

Some ISPs require that you register a MAC address. This feature clones your PC network adapter's MAC address onto the Router, and prevents you from having to call your ISP to change the registered MAC address to the Router's MAC address. The Router's MAC address is a 6-byte hexadecimal number assigned to a unique piece of hardware for identification.

Figure 10: MAC Address Clone Screen

Data - MAC Address Clone Screen

MAC Address Clone	
MAC Address Clone	Select *Enabled* or *Disabled*.
MAC Address	Enter the MAC Address registered with your ISP in this field.
Clone My PC's MAC	When Mac Address Clone is enabled, click this to copy the MAC address of the network adapter in the computer that you are using to connect to the Web-based utility.

Setup - Advanced Routing Screen

Figure 11: Advanced Routing Screen

Data - Advanced Routing Screen

Operating Mode	
Operating Mode	• **Gateway** - This is the normal mode of operation. This allows all devices on your LAN to share the same WAN (Internet) IP address. In the Gateway mode, the NAT (Network Address Translation) mechanism is enabled. • **Router** - You either need another Router to act as the Gateway, or all PCs on your LAN must be assigned (fixed) Internet IP addresses. In Router mode, the NAT mechanism is disabled.
Dynamic Routing	
RIP	The Router, using the RIP protocol, calculates the most efficient route for the network's data packets to travel between the source and the destination based upon the shortest paths.
RIP Send Packet Version	Choose the version of RIP packets you want to send to peers: RIPv1 or RIPv2. This should match the version supported by other Routers on your LAN.
RIP Recv Packet Version	Choose the version of RIP packets you want to receive from peers: RIPv1 or RIPv2. This should match the version supported by other Routers on your LAN.

Static Routing	
Select Set Number	Sometimes you will prefer to use static routes to build your routing table instead of using dynamic routing protocols. Static routes do not require CPU resources to exchange routing information with a peer router. You can also use static routes to reach peer routers that do not support dynamic routing protocols. Static routes can be used together with dynamic routes. Be careful not to introduce routing loops in your network. To set up static routing, you should add route entries in the routing table that tell the Router where to forward packets to specific IP destinations. Enter the following data to create a static route entry: 1. **Select Set Number**. Select the set number (routing table entry number) that you wish to view or configure. If necessary, click Delete This Entry to clear the entry. 2. **Destination IP Address**. Enter the network address of the remote LAN segment. For a standard Class C IP domain, the network address is the first three fields of the Destination LAN IP, while the last field should be zero. 3. **Subnet Mask**. Enter the Subnet Mask used on the destination LAN IP domain. For Class C IP domains, the Subnet Mask is 255.255.255.0. 4. **Gateway**. If this Router is used to connect your network to the Internet, then your gateway IP is the Router's IP Address. If you have another router handling your network's Internet connection, enter the IP Address of that router instead. 5. **Hop Count**. This value gives the number of routers that a data packet passes through before reaching its destination. It is used to define the priority on which route to use if there is a conflict between a static route and dynamic route. **Show Routing Table** button. Click this button to show the routing table established either through dynamic or static routing methods.
Inter-VLAN Routing	
Inter-VLAN Routing	Select *Enable* to allow packets to be routed between VLANs that are in different subnets. The default is *Enable*.

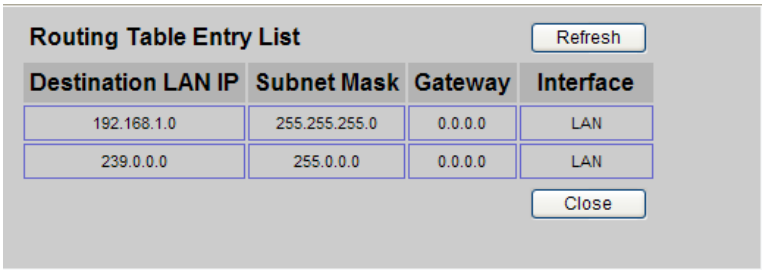


Figure 12: Routing Table

Setup - Time Screen

You can either define your Router's time manually or automatically through Time Server.

Figure 13: Time Screen

Data - Time Screen

Time	
Time	• **Set the local time Manually** - If you wish to enter the time and date manually, enter the *Day*, *Month*, *Year*, *Hour*, *Minute*, and *Second* in the Time field using 24 hour format (example 10:00pm would be entered 22:0:0). • **Set the local time using Network Time Protocol (NTP) Automatically** - Select the time zone for your location and your setting synchronizes over the Internet with public NTP (Network Time Protocol) Servers.
Time Zone	Select the time zone for your location.
Auto Daylight Saving	To use the daylight saving feature, select Enabled. Enter the Month and Day of the start date, and then enter the Month and Day of the end date.
User-defined NTPServer	If you want to use your own NTP server, select the Enabled option. The default is Disabled.
NTP Serve IP	Enter the IP address of your own NTP server.

Setup - IP Mode Screen

You can either define your Router's time manually or automatically through Time Server.

Figure 14: IP Mode Screen

Data - IP Mode Screen

IP Mode	
IPv4 Only	This option utilizes IPv4 on the Internet and local network.
Dual-Stack IP	This option utilizes IPv4 over the Internet and IPV4 and IPv6 on the local network. Then select how the IPv6 hosts will connect to the Internet: • **NAPT-PT** - This allows an IPv6-only host on your LAN to connect to IPv4-only hosts on the WAN using address translation and protocol-translation (per RFC2766). • **6-4 Tunnel** - This allows your IPv6 network to connect to other IPv6 networks via tunnels through IPv4 (per RFC3056). The remote router also needs to support 6to4.
6 to 4 Gateway Access Control	Select the desired option to match your needs. Enter the related data in the following fields if required. • Disabled • Permit following sites: Enter the IP addresses that you want to permit in the following section. • Block following sites: Enter the IP addresses that you want to block in the following section.

Wireless - Basic Settings Tab

The Dual-Band Wireless-N VPN Router's settings must match the other Wireless stations.

Note that the Dual-Band Wireless-N VPN Router will automatically accept both 802.11b and 802.11g connections, and no configuration is required for this feature.

To change the Dual-Band Wireless-N VPN Router's default settings for the Wireless Access Point feature, use the *Wireless* link on the main menu to reach the ***Wireless*** screen. An example screen is shown below.

Figure 15: Basic Settings

Data - Basic Settings Screen

Basic Settings	
Wireless Radio Band	Select *2.4GHz Wireless* or *5GHz Wireless* from the list to configure.

Wireless Network Mode	Select the desired mode:
	• **2.4GHz Wireless**
	  • **B-Only** - All the wireless client devices can be connected to the Wireless Router at Wireless-B data rates with a maximum speed of 11Mbps.
	  • **G-Only** - Both Wireless-N and Wireless-G client devices can be connected at Wireless-G data rates with a maximum speed of 54Mbps. Wireless-B clients cannot be connected in this mode.
	  • **N-Only** - Only Wireless-N client devices can be connected at Wireless-N data rates with a maximum speed of 300Mbps.
	  • **B/G/N-Mixed** - All the wireless client devices can be connected at their respective data rates in this mixed mode.
	• **5GHz Wireless**
	  • **A-Only** - All the wireless client devices can be connected to the Wireless Router at Wireless-A data rates with a maximum speed of 11Mbps.
	  • **N-Only** - Only Wireless-N client devices can be connected at Wireless-N data rates with a maximum speed of 300Mbps.
	  • **A/N-Mixed** - All the wireless client devices can be connected at their respective data rates in this mixed mode.

Wireless Channel	Select the appropriate channel to be used between your Wireless Router and your client devices. The default is channel 6. You can also select *Auto* so that your Wireless Router will select the channel with the lowest amount of wireless interference while the system is booting up. Auto channel selection will start when you click the *Save Settings* button, and it will take several seconds to scan through all the channels to find the best channel.
Multiple BSSID	Select *Enabled* or *Disabled*. The default is *Disabled*
SSID Name	The SSID is the unique name shared between all devices in a wireless network. It is case-sensitive, must not exceed 32 alphanumeric characters, and may be any keyboard character. Make sure this setting is the same for all devices in your wireless network. The default SSID name is linksys-n.
SSID Broadcast	This option allows the SSID to be broadcast on your network. You may want to enable this function while configuring your network, but make sure that you disable it when you are finished. With this enabled, someone could easily obtain the SSID information with site survey software or Windows XP and gain unauthorized access to your network. Click *Enabled* to broadcast the SSID to all wireless devices in range. Click *Disabled* to increase network security and prevent the SSID from being seen on networked PCs. The default is *Enabled* in order to help users configure their network before use.

Wireless - Security Settings

Change the Wireless Router's wireless security settings on this screen.

Figure 16: Disabled

Data - Security Settings Screen

WEP Data Encryption	
Select SSID	Select the desired SSID from the drop-down list.
Wireless Isolation (Between SSID w/o VLAN)	Select Enabled to use this feature.
Security Mode	Select the wireless security mode you want to use, **WEP, WPA-Personal**, **WPA2-Personal**, **WPA-Enterprise**, **WPA2-Enterprise**, or **Radius**. (WPA stands for Wi-Fi Protected Access, which is a security standard stronger than WEP encryption and forward compatible with IEEE 802.11e. WEP stands for Wired Equivalent Privacy, Enterprise refers to using RADIUS server for authentication, while RADIUS stands for Remote Authentication Dial-In User Service.) Refer to the appropriate instructions below after you select the Authentication Type and SSID Interoperability settings. To disable wireless security completely, select **Disabled**. The default is **Disabled**.
Wireless Isolation (Within SSID)	When disabled, wireless PCs that are associated to the same network name (SSID), can see and transfer files between each other. By enabling this feature, Wireless PCs will not be able to see each other. This feature is very useful when setting up a wireless hotspot location. The default is Disabled.

WEP

Figure 17: WEP

Data - WEP Screen

WEP Data Encryption	
Authentication Type	Normally, this should be left at the default value of "Automatic". If changed to "Open System" or "Shared Key", ensure that your Wireless Stations use the same setting.
WEP Data Encryption	Select the desired option, and ensure the Wireless Stations use the same setting. • **40/64-bit (10 Hex digits)** - data is encrypted, using the default key, before being transmitted. You must enter at least the default key. For 64 Bit Encryption, the key size is 10 chars in HEX (0~9 and A~F). • **104/128-bit (26 Hex digits)** - data is encrypted, using the default key, before being transmitted. You must enter at least the default key. For 128 Bit Encryption, the key size is 26 chars in HEX (0~9 and A~F).
Passphrase	If desired, you can generate a key from a phrase, instead of entering the key value directly. Enter the desired phrase, and click the "Generate" button.
Key (1~4)	If you want to manually enter WEP keys, then complete the fields provided. Each WEP key can consist of the letters “A” through “F” and the numbers “0” through “9”. It should be 10 characters in length for 64-bit encryption or 26 characters in length for 128-bit encryption.
TX Key	Select one of the keys to be used for data encryption (when you manually enter multiple WEP keys).

WPA-Personal

Figure 18: WPA-Personal

Data - WPA-Personal Screen

Encryption	The WPA-Personal standard allows different encryption methods to be used. Select the desired option. Wireless Stations must use the same encryption method.
Shared Secret	Enter a WPA Shared Key of 8-63 characters.
Key Renewal	Enter a Key Renewal Timeout period, which instructs the Wireless Router how often it should change the encryption keys. The default is **3600** seconds.

WPA2-Personal

Figure 19: WPA2-Personal

Data - WPA2-Personal Screen

Encryption	The WPA2-Personal standard allows different encryption methods to be used. Select the desired option. Wireless Stations must use the same encryption method.
Shared Secret	Enter a WPA Shared Key of 8-63 characters.
Key Renewal	Enter a Key Renewal Timeout period, which instructs the Wireless Router how often it should change the encryption keys. The default is **3600** seconds.

WPA-Enterprise

Figure 20: WPA-Enterprise

Data - WPA-Enterprise Screen

Encryption	WPA offers you two encryption methods, TKIP and AES for data encryption. Select the type of algorithm you want to use, TKIP or AES.
RADIUS Server	Enter the server address here.
RADIUS Port	Enter the port number used for connections to the Radius Server.
Shared Key	Enter the shared key. Data is encrypted using a key derived from the network key. Other Wireless Stations must use the same key. The key must be from 8 to 63 characters in length.
Key Renewal	Enter a Key Renewal Timeout period, which instructs the Wireless Router how often it should change the encryption keys. The default is **3600** seconds.

WPA2-Enterprise

Figure 21: WPA2-Enterprise

Data - WPA2-Enterprise Screen

Encryption	WPA2 always uses AES for data encryption.
RADIUS Server	Enter the server address here.
RADIUS Port	Enter the port number used for connections to the Radius Server.
Shared Key	Enter the shared key. Data is encrypted using a key derived from the network key. Other Wireless Stations must use the same key. The key must be from 8 to 63 characters in length.
Key Renewal	Enter a Key Renewal Timeout period, which instructs the Wireless Router how often it should change the encryption keys. The default is 3600 seconds.

Radius Server

Figure 22: Radius Server

Data - Radius Server Screen

RADIUS Server	Enter the server address here.
RADIUS Port	Enter the port number used for connections to the Radius Server.
Shared Key	Enter the shared key. Data is encrypted using a key derived from the network key. Other Wireless Stations must use the same key. The key must be from 8 to 63 characters in length.
Authentication Type	Normally, this should be left at the default value of "Automatic". If changed to "Open System" or "Shared Key", ensure that your Wireless Stations use the same setting.
Encryption	Select the desired option, and ensure the Wireless Stations use the same setting. • **40/64-bit (10 Hex digits)** - data is encrypted, using the default key, before being transmitted. You must enter at least the default key. For 64 Bit Encryption, the key size is 10 chars in HEX (0~9 and A~F). • **104/128-bit (26 Hex digits)** - data is encrypted, using the default key, before being transmitted. You must enter at least the default key. For 128 Bit Encryption, the key size is 26 chars in HEX (0~9 and A~F).
Passphrase	If desired, you can generate a key from a phrase, instead of entering the key value directly. Enter the desired phrase, and click the "Generate" button.
Key (1~4)	If you want to manually enter keys, then complete the fields provided. Each key can consist of the letters “A” through “F” and the numbers “0” through “9”. It should be 10 characters in length for 64-bit encryption or 26 characters in length for 128-bit encryption.

TX Key	Select one of the keys to be used for data encryption (when you manually enter multiple keys).

Wireless - Connection Control

This screen allows you to configure the Connection Control List to either permit or block specific wireless client devices connecting to (associating with) the Wireless Router.

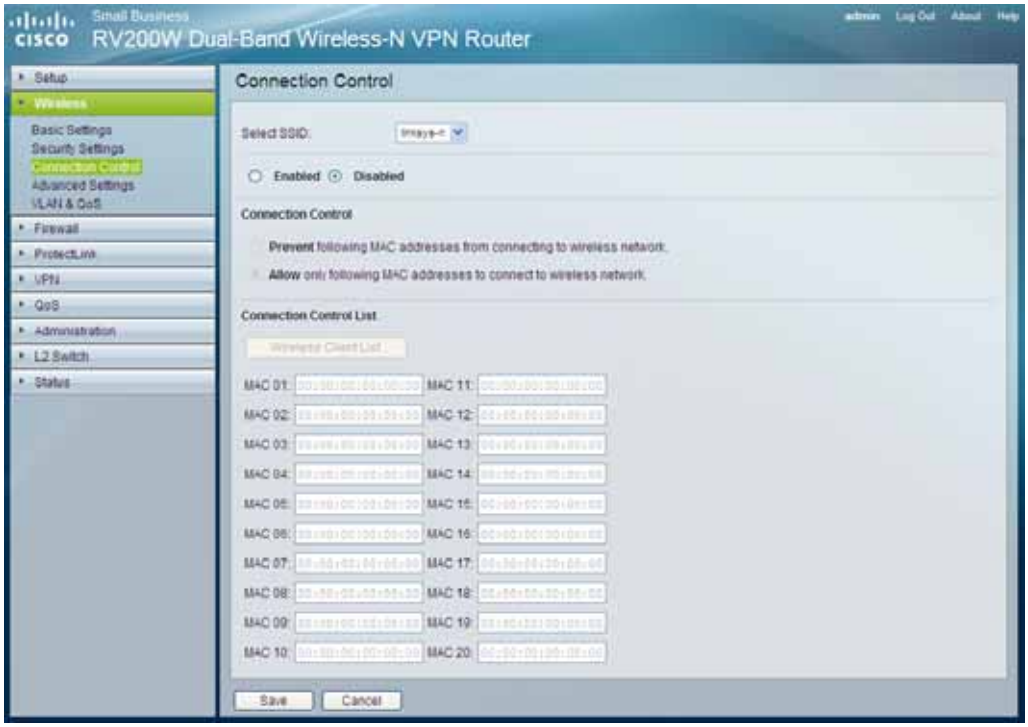


Figure 23: Connection Control

Data - Connection Control

Select SSID	Select the desired SSID from the drop-down list.
Enabled/Disabled	Enable or disable wireless connection control. The default is Disabled.
Connection Control	There are two ways to control the connection (association) of wireless client devices. You can either prevent specific devices from connecting to the Wireless Router, or you can allow only specific client devices to connect to the Wireless Router. The client devices are specified by their MAC addresses. The default is to allow only specific client devices.
Wireless Client List	Instead of manually entering the MAC addresses of each client, the Wireless Router provides a convenient way to select a specific client device from the client association table. Click this button and a window appears to let you select a MAC address from the table. The selected MAC address will be entered into the Connection Control List.
MAC (01~20)	Enter the MAC addresses of the wireless client devices you want to control.

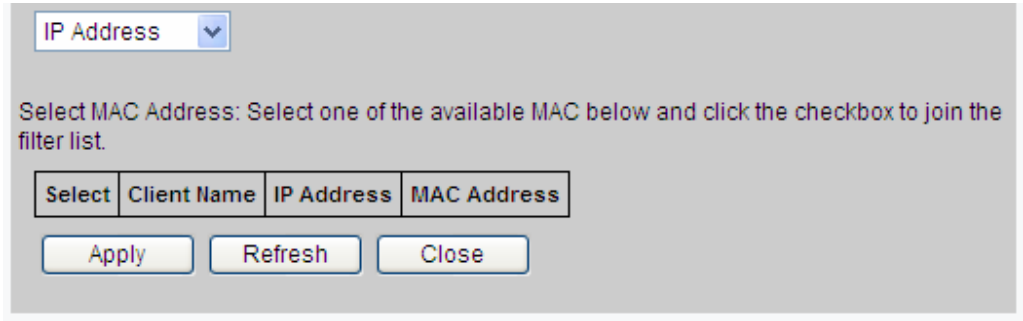


Figure 24: Wireless Client List

Wireless - Advanced Settings

This screen allows you to configure the advanced settings for the Wireless Router. The Wireless-N Router adopts several new parameters to adjust the channel bandwidth and guard intervals to improve the data rate dynamically. Linksys recommends to let your Wireless Router automatically adjust the parameters for maximum data throughput.

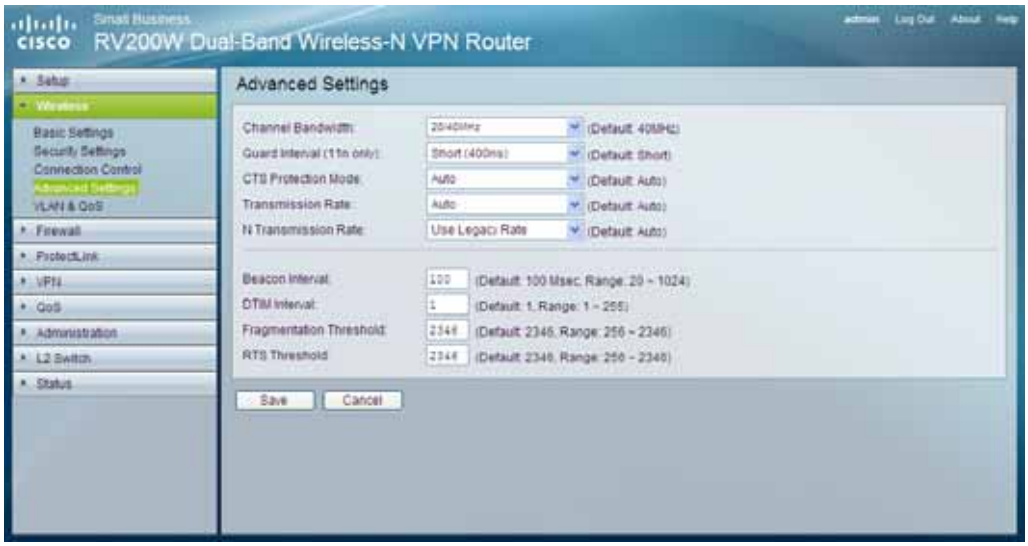


Figure 25: Advanced Settings Screen

Channel Bandwidth	You can select the channel bandwidth manually for Wireless-N connections. When it is set to 20MHz, only the 20MHz channel is used. When it is set to 40MHz, Wireless-N connections will use 40MHz channel but Wireless-B and Wireless-G will still use 20MHz channel. The default is 20MHz.
Guard Interval	You can select the guard interval manually for Wireless-N connections. The two options are Short (400ns) and Long (800ns). The default is Short.
CTS Protection Mode	CTS (Clear-To-Send) Protection Mode function boosts the Wireless Router's ability to catch all wireless transmissions, but will severely decrease performance. Keep the default setting, Auto, so the Wireless Router can use this feature as needed, when the Wireless-N/G products are not able to transmit to the Wireless Router in an environment with heavy 802.11b traffic. Select Disabled if you want to permanently disable this feature.
Transmission Rate	Select the desired transmission rate from the drop-down list. The default is *Auto*.
N Transmission Rate	Select the desired rate from the drop-down list. The default is *Auto*.
Beacon Interval	This value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the Wireless Router to keep the network synchronized. A beacon includes the wireless networks service area, the Wireless Router address, the Broadcast destination addresses, a time stamp, Delivery Traffic Indicator Maps, and the Traffic Indicator

	Message (TIM). The default is 100 Msec.
DTIM Interval	This value indicates how often the Wireless Router sends out a Delivery Traffic Indication Message (DTIM). Lower settings result in more efficient networking, while preventing your PC from dropping into power-saving sleep mode. Higher settings allow your PC to enter sleep mode, thus saving power, but interferes with wireless transmissions. The default is 1 ms.
Fragmentation Threshold	Enter the preferred setting between 256 and 2346. Normally, this can be left at the default value.
RTS Threshold	This setting determines how large a packet can be before the Wireless Router coordinates transmission and reception to ensure efficient communication. This value should remain at its default setting of 2346. If you encounter inconsistent data flow, only minor modifications are recommended.

Wireless - VLAN & QoS

This screen allows you to configure the Qos and VLAN settings for the Router. The QoS (Quality of Service) feature allows you specify priorities for different traffic. Lower priority traffic will be slowed down to allow greater throughput or less delay for high priority traffic. The 802.1Q VLAN feature is allowing traffic from different sources to be segmented. Combined with the multiple SSID feature, this provides a powerful tool to control access to your LAN.

Figure 26: VLAN &QoS Screen

VLAN	
Enabled/Disabled	You can enable this feature only if the hubs/switches on your LAN support the VLAN standard.
AP Management VLAN	Define the VLAN ID used for management.
VLAN ID	Enter the VLAN ID.
QoS	
Default CoS (Priority)	Select Enabled or Disabled as required.
U-PSD (WMM Power Save)	Select Enabled or Disabled as required.
Default CoS	Select the desired value for the Default CoS.
Tx Rate Limiting	Select the desired rate limiting from the list.
WMM	Wi-Fi Multimedia is a QoS feature defined by WiFi Alliance before IEEE 802.11e was finalized. Now it is part of IEEE 802.11e. When it is enabled, it provides four priority queues for different types of traffic. It automatically maps the incoming packets to the appropriate

	queues based on QoS settings (in IP or layer 2 header). WMM provides the capability to prioritize traffic in your environment. The default is Enabled.

Firewall Tab

The Firewall Tab allows you to configure software security features like SPI (Stateful Packet Inspection) Firewall, IP based Access List, restriction LAN users on Internet (WAN port) access, and NAPT (Network Address Port Translation) Settings (only works when NAT is enabled) to limited services to specific ports.

Note that for WAN traffic, NAPT settings are applied first, then it will pass the SPI Firewall settings, followed by IP based Access List (which requires more CPU power).

Firewall - Basic Settings

Figure 27: Basic Settings Screen

Basic Settings	
Firewall	SPI (Stateful Packet Inspection) Firewall, when you enable this feature, the Router will perform deep packet inspection on all the traffic going through the Router.
DoS Protection	When enabled, the Router will prevent DoS (Denial of Service) attacks coming in from the Internet. DOS attacks are making your Router's CPU busy such that it cannot provide services to regular traffic. The default is *Enable*.
Block WAN Request	When enabled, the Router will ignore PING Request from the Internet so it seems to be hidden. The default is *Enable*.
Remote Management	When enabled, the Router will allow the Web-based Utility to be accessed from the Internet. The default is *Disable*. The default value of *Port* field is **8080**.
Multicast Pass-through	When enabled, the Router will allow IP Multicast traffic to come in from the Internet. The default is *Disable*.
Block	Select the Web features that you wish to restrict. All those features

	could place security concern to your PCs on the LAN side. You have to balance your needs on those applications and security. The default is unselected. • **Java**: Java is a programming language for websites. If you deny Java, you run the risk of not having access to Internet sites created using this programming language. • **Cookies**: A cookie is data stored on your PC and used by Internet sites when you interact with them, so you may not want to deny cookies. • **ActiveX**: ActiveX is a Microsoft (Internet Explorer) programming language for websites. If you deny ActiveX, you run the risk of not having access to Internet sites using this programming language. Also, Windows Update uses ActiveX, so if this is blocked, Windows update will not work. • **Access to Proxy HTTP Server**: If local users have access to WAN proxy servers, they may be able to circumvent the Router's content filters and access Internet sites blocked by the Router. Denying Proxy will block access to any WAN proxy servers.

Firewall - IP Based ACL

This screen shows a summary of configured IP based Access List. The Access List is used to restrict traffic going through the Router either from WAN or LAN port. There are two ways to restrict data traffic. You can block specific types of traffic according to your ACL definitions. Or you can allow only specific types of traffic according to your ACL definition. The ACL rules will be read according to its priority. If there is a match for a packet, the action will be taken and following lower priority rules will not be checked against this packet.

Note that the higher the number of rules that need to be checked against packets, the lower the throughput. Use ACL rules with caution.

There are two default rules in the table that cannot be deleted. The first rule will allow all traffic coming in from LAN port to pass the Router. The second rule will allow all traffic coming in from WAN port. These two rules have the lowest priority, so without adding any user defined rules, all the packets can be passed through from both WAN and LAN sides.

The rule will be enabled when the Enable button is checked, and when Date and Time are matched. If any of conditions are not met, the rule will not be used to check against packets.

Figure 28: IP Based ACL Screen

IP Based ACL	
Page Selection	You can select specific page of ACL list from the drop-down menu to be displayed. Or you can navigate them page by page through *Previous Page* and *Next Page* button.
Priority	This defines the order on which rule is checked against first. The smaller number has higher priority. The default rules will always be checked last.

Enable	This tells the Router if the rule is active or not. You can have rules defined in the ACL Table but in an inactive state. The administrator can decide on when to enable specific ACL rules manually.
Action	This defines how the rule is to affect the traffic. It can be either Allow or Deny. If the rule is matched and the action is Allow, the packet will be forwarded. If the rule is matched and the action is Deny, the packet will be dropped.
Service	You can either select one of the pre-defined services in the drop-down menu or you can define new services by clicking the Service Management button. Once you defined your own service, it will be listed on the top of the drop-down menu. You can also select ALL to allow or block all types of IP traffic. The User-defined Service GUI page can be either accessed from the New Rule screen by clicking Service Management button, or you can access it directly from the 2nd layer tab under Firewall.
Source Interface	Select LAN, WAN, or ANY interface.
Source	This is the source IP address to be matched against. You can define a Single IP address, a Range of IP addresses (start IP and end IP), a Network (IP Prefix and Network Mask), or ANY IP addresses.
Destination	This is the destination IP address to be matched against. You can define a Single IP address, a Range of IP addresses (start IP and end IP), a Network (IP Prefix and Network Mask), or ANY IP addresses.
Time	Displays the time period this rule will be enabled (used together with Date). It can be set to Any Time.
Day	Displays the days in a week this rule will be enabled (used together with Time). It can be set to Any Day.
Edit Button	Use this button to go to Edit IP ACL Rule screen and modify this rule.
Delete Button	Use this button to delete the ACL rule from the list.
Add New Rule	Click this button to enter the page to define a new ACL rule.
Disable All Rule	Click this page to disable all the user-defined rules.
Delete All Rules	Click this page to delete all the user-defined rules.

Edit IP ACL Rule

This Web page can be entered only through IP Based ACL Tab. You can enter this page by clicking **Add New Rule** button on that page.

Figure 29: Edit IP ACL Rule

New Rule	
Action	Select either *Allow* or *Deny*. Default is *Allow*.
Service	Select ALL or pre-defined (or user-defined) services from the drop-down menu.
Log	If checked, this ACL rule will be logged when a packet match happens.
Log Prefix	This string will be attached in front of the log for the matched event.
Source Interface	Select *LAN*, *WAN*, or *ANY* interface.
Source IP	The source IP address to be matched against. You can define a Single IP address, a Range of IP addresses (start IP and end IP), a Network (IP Prefix and Network Mask), or ANY IP addresses.
Destination IP	The destination IP address to be matched against. You can define a Single IP address, a Range of IP addresses (start IP and end IP), a Network (IP Prefix and Network Mask), or ANY IP addresses.
Service Management Button	Click this button and the Service Tab to add new service type to the Service drop-down menu.
Scheduling	
Time	Enter the time period this rule will be applied (used together with Date). It can be set to Any Time.
Date	Enter the days in a week this rule will be applied (used together with Time). It can be set to Any Day.

Firewall - Internet Access Policy

Access to the Internet can be managed by policies. A policy consists of four components. You need to define the PCs (MAC or IP address) to apply this policy, either Deny or Allow Internet service, what time and date to enable this policy, and what URLs or Keywords to apply this policy.

Use the settings on this screen to establish an access policy. Selecting a policy from the drop-down menu will display that policy's settings. You can then perform the following operations:

- Create a Policy - see instructions below.
- Delete the current policy - click the Delete button.
- View all policies - click the Summary button. On the Summary screen, the policies are listed with the following information: No., Policy Name, Days, Time, and a checkbox to delete (clear) the policy. To delete a policy, check the checkbox in the Delete column, and click the Delete button
- View or change the PCs covered by the current policy - click the Edit List of PCs button.

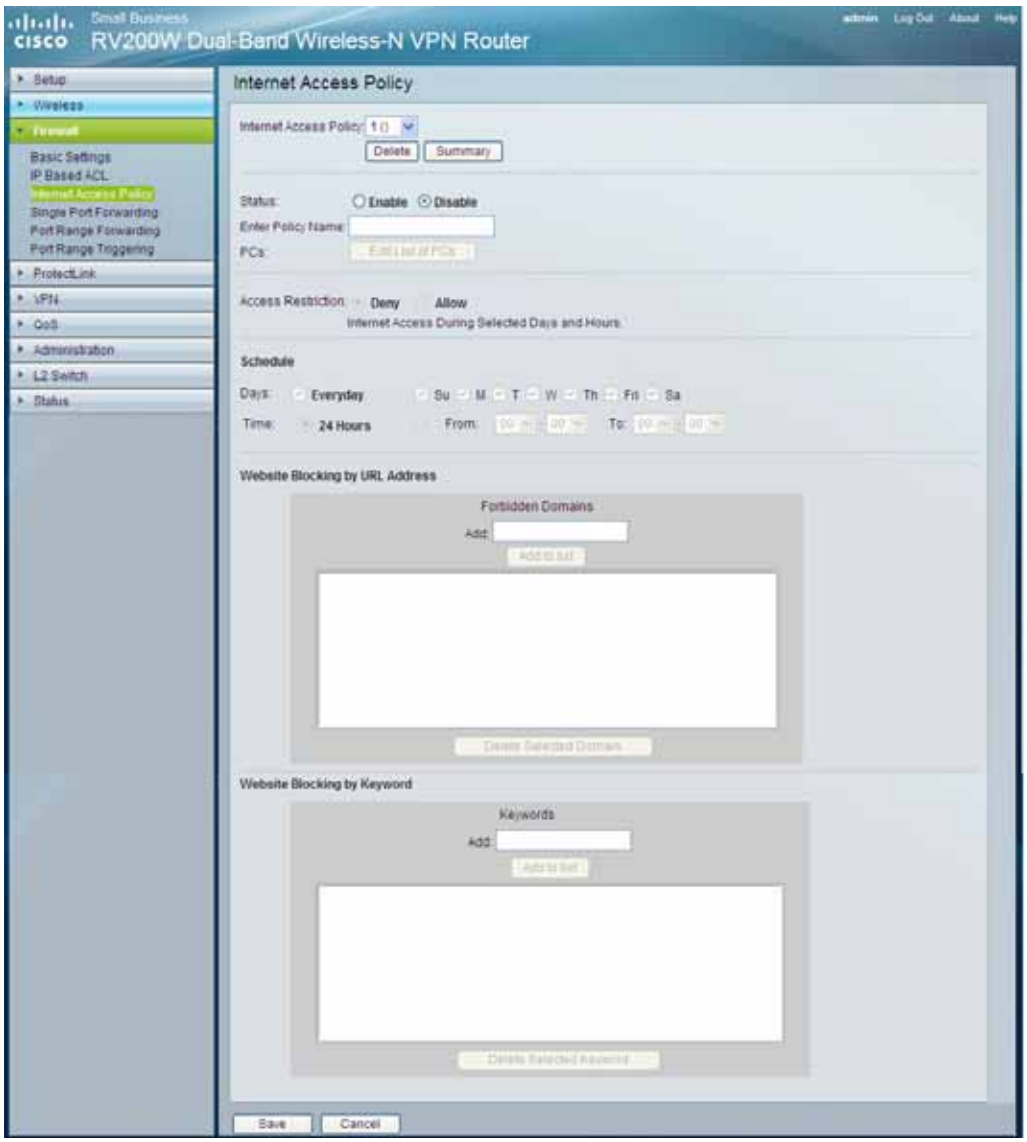


Figure 30: Internet Access Policy Screen

On the List of PCs screen, you can define PCs by MAC Address or IP Address. You can also enter a range of IP Addresses if you want this policy to affect a group of PCs.

To create an Internet Access policy:

1. Select the desired policy number from the Internet Access Policy drop-down menu.
2. Enter a Policy Name in the field provided.
3. To enable this policy, select the Enable option.
4. Click the *Edit List of PCs* button to select which PCs will be affected by the policy. The List of PCs screen will appear in a sub-window. You can select a PC by MAC Address or IP Address. You can also enter a range of IP Addresses if you want this policy to affect a group of PCs. After making your changes, click the Save Settings button to apply your changes.
5. Click the appropriate option, Deny or Allow, depending on whether you want to block or allow Internet access for the PCs you listed on the List of PCs screen.

6. Decide what Days and what Times you want this policy to be enforced. Select the individual days during which the policy will be in effect, or select Everyday. Enter a range of hours and minutes during which the policy will be in effect, or select 24 Hours.
7. If you wish to block access to Web sites, use the Website Blocking by URL Address or Website Blocking by Keyword feature.
   - Website Blocking by URL Address. Enter the URL or Domain Name of the web sites you wish to block.
   - Website Blocking by Keyword. Enter the keywords you wish to block in the fields provided. If any of these Keywords appears in the URL of a web site, access to the site will be blocked. Note that only the URL is checked, not the content of each Web page.
8. Click the *Save Settings* button to save the policy settings.

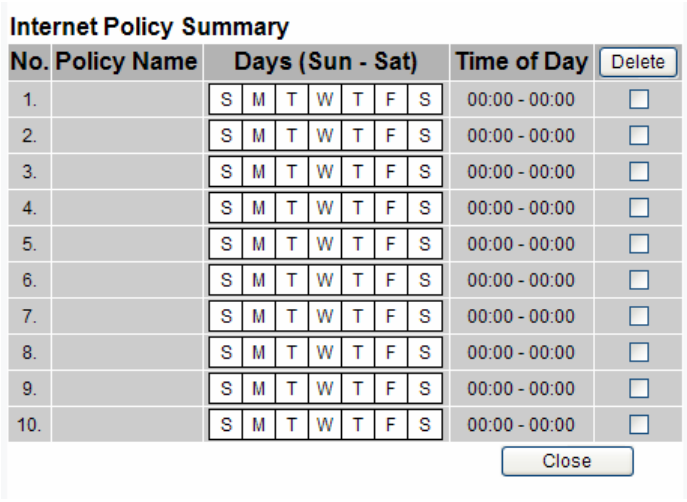


Figure 31: Summary

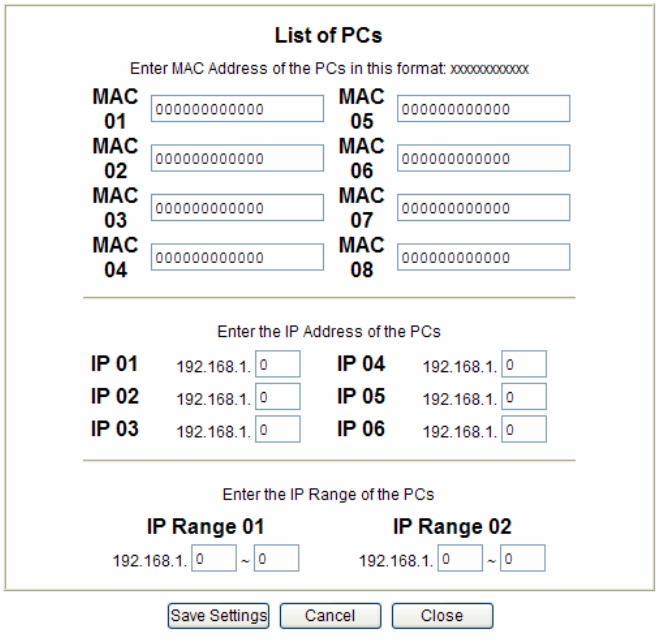


Figure 32: Internet Access PC List

Firewall - Single Port Forwarding

This is one of the NAPT (Network Address Port Translation) feature. Use the Single Port Forwarding screen when you want to open specific services (that use single port). This allows users on the Internet to access this server by using the WAN port address and the matched external port number. When users send these types of request to your WAN port IP address via the Internet, the NAT Router will forward those requests to the appropriate servers on your LAN.

Figure 33: Single Port Forwarding Screen

Single Port Forwarding	
Application	Enter the name of the application you wish to configure.
External Port	This is the port number used by the service or Internet application. Internet users must connect using this port number. Check with the software documentation of the Internet application for more information.
Internal Port	This is the port number used by the Router when forwarding Internet traffic to the PC or server on your LAN and is usually the same as the External Port number. If it is different, the Router performs a Port Translation, so that the port number used by Internet users is different from the port number used by the server or Internet application. For example, you could configure your Web Server to accept connections on both port 80 (standard) and port 8080. Then, enable Port Forwarding, set the External Port to 80 and the Internal Port to 8080. Now, any traffic from the Internet to your Web server will be using port 8080, even though the Internet users used the standard port, 80. (Users on the local LAN can and should connect to your Web Server

	using the standard port 80.)
Protocol	Select the protocol used for this application, TCP and/or UDP.
IP Address	For each application, enter the IP address of the PC running the specific server application.
Enabled	Select Enabled to enable port forwarding for the relevant server application.

Firewall - Port Range Forwarding

This is one of the NAPT (Network Address Port Translation) features. The Port Range Forwarding screen allows you to set up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications that use one or multiple port numbers (e.g. video conference). The port numbers being used will not change while forwarding to the local network. This allows users on the Internet to access this server by using the WAN port IP address and the pre-defined port numbers. When users send these types of requests to your WAN port IP address via the Internet, the NAT Router will forward those requests to the appropriate servers on your LAN.

Figure 34: Port Range Forwarding Screen

Port Range Forwarding	
Application	Enter the name of the application you wish to configure.
Start	This is the beginning of the port range. Enter the beginning of the range of port numbers (external ports) used by the server or Internet application. Check with the software documentation of the Internet application for more information if necessary.
End	This is the end of the port range. Enter the end of the range of port numbers (external ports) used by the server or Internet application. Check with the software documentation of the Internet application for more information if necessary.
Protocol	Select the protocol(s) used for this application, TCP and/or UDP.
IP Address	For each application, enter the IP address of the PC running the specific application.
Enabled	Select Enabled to enable port range forwarding for the relevant application.

Firewall - Port Range Triggering

This is one of the NAPT (Network Address Port Translation) feature. Port Range Triggering is used for special applications that can request a port to be opened on demand. For this feature, the Wireless Router will watch outgoing packets for specific port numbers. This will trigger the Wireless Router to allow the incoming packets within the specified forwarding range and forward those packets to the triggering PC. One of the example applications is QuickTime. It would use port 1000 for outgoing packets and 2000 for incoming packets.

Figure 35: Port Range Triggering Screen

Port Range Triggering	
Application Name	Enter the name of the application you wish to configure.
Triggered Range	For each application, list the triggered port number range. These are the ports used by outgoing traffic. Check with the Internet application documentation for the port number(s) needed. In the first field, enter the starting port number of the Triggered Range. In the second field, enter the ending port number of the Triggered Range.
Forwarded Range	For each application, list the forwarded port number range. These are the ports used by incoming traffic. Check with the Internet application documentation for the port number(s) needed. In the first field, enter the starting port number of the Forwarded Range. In the second field, enter the ending port number of the Forwarded Range.
Enabled	Select Enabled to enable port range triggering for the relevant application.

Security Protection - Web Protection

The Web Protection features are provided by the Router. Configure the website filtering settings on this screen.

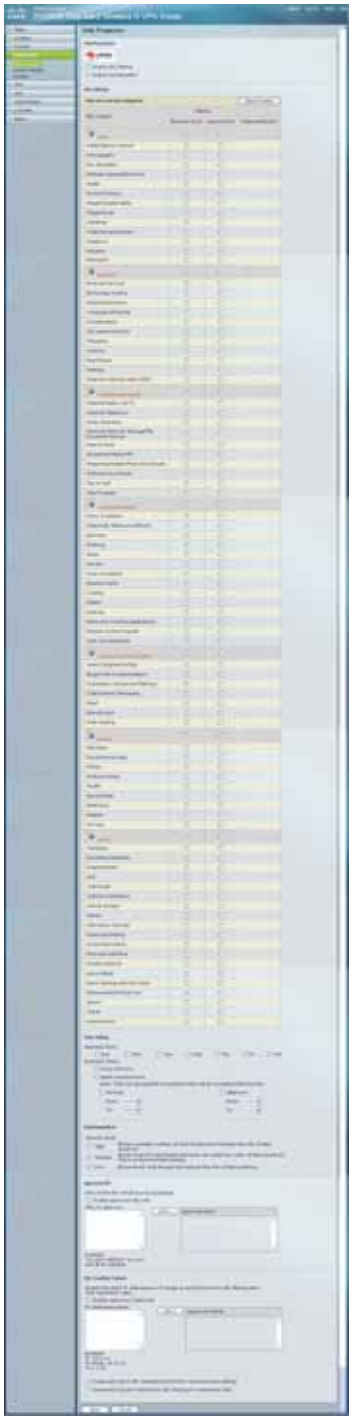


Figure 36: Web Protection

Web Protection	
Enable URL Filtering	To filter website addresses (URLs), select this option.
Enable Web Reputation	To block potentially malicious websites, select this option.
URL Filtering	
Reset Counter	The Router counts the number of attempted visits to a restricted URL. To reset the counter to zero, click Reset Counter.
URL Category	For each URL category, select the appropriate Filtering option. If you want to filter a sub-category, click + to view the sub-categories for each category. Then select the appropriate Filtering option.
Business Hours	To filter this URL category during the business hours you have specified, select this option.
Leisure Hours	To filter this URL category during non-business hours, select this option.
Instances Blocked	The number of attempted visits is displayed.
Business Days	Select the appropriate days. The default days are Mon. through Fri.
Business Times	To specify entire days, keep the default, All day (24 hours). To specify hours, select Specify business hours. For morning hours, select *Morning*, and then select the appropriate From and To times. For afternoon hours, select *Afternoon*, and then select the appropriate From and To times.
Web Reputation	
High	This level blocks a higher number of potentially malicious websites but also increases the risk of false positives. (A false positive is a website that can be trusted but seems potentially malicious.)
Medium	This level blocks most potentially malicious websites and does not create too many false positives. The default is Med um and is the recommended setting.
Low	This level blocks fewer potentially malicious websites and reduces the risk of false positives.
Approved URLs	
Enable Approved URL list	To set up a list of always accessible URLs, select this option.
URL(s) to approve	Enter the trusted URL(s). Separate multiple URLs with semicolons (“;”).
Add>>	To add the URLs, click Add.
Approved URLs list	The trusted URLs are displayed. To delete a URL, click its trash can icon.
URL Overflow Control	
Enable Approved Client list	To set up a list of trusted clients, select this option.

IP Addresses/range	Enter the appropriate IP addresses or ranges. Separate multiple URLs with semicolons (“;”). For a range of IP addresses, use a hyphen (“-”). Example: 10.1.1.0-10.1.1.10.
Add>>	To add the IP addresses or ranges, click Add.
Approved Clients list	The IP addresses or range of trusted clients are displayed. To delete an IP address or range, click its trash can icon.
Temporarily block URL requests	If there are too many URL requests, the overflow will be held back until they can be processed. This is the default setting.
Temporarily bypass Trend Micro URL Filtering for requested URLs	If there are too many URL requests, the overflow will be allowed without verification.

Security Protection - Email Protection

The Email Protection features are provided by an online service called IMHS, which stands for InterScan™ Messaging Hosted Security. It checks your e-mail messages so spam, viruses, and inappropriate content are filtered out. After you have configured the IMHS settings, your email messages will be checked online before appropriate messages are forwarded to your network.

Note: To have your e-mail checked, you will need to provide the domain name and IP address of your e-mail server. If you do not know this information, contact your ISP.

Figure 37: Email Protection Screen

Email Protection	
https://us.imhs.trendmicro.com/linksys	To set up e-mail protection, click this link. You will be redirected to the Trend Micro ProtectLink Gateway website. Then follow the on-screen instructions.

Security Protection - License

The license for the Trend Micro ProtectLink Gateway service (Email Protection and Web Protection) is valid for one year from the time the activation code for Web Protection is generated. If you do not provide the necessary information to activate Email Protection during registration, please provide that information as soon as possible because Email Protection and Web Protection will expire at the same time.

Note: For example, if you provide the information needed for Email Protection one month after receiving the activation code for Web Protection, then you will receive only 11 months of Email Protection.

On the License screen, license information is displayed. Use this screen to renew your license, add seats, or view license information online.

Figure 38: License Screen

License	
Update Information	To refresh the license information displayed on-screen, click Update Information.
License Information	
View detailed license online	To view license information online, click this link.
Status	The status of your license, Activated or Expired, is displayed.
Platform	The model type, Gateway Service, is automatically displayed.
License expires on	The date and time your license expires are displayed.
Renew	To renew your license, click Renew. Then follow the on-screen instructions.
Add Seats	Each seat allows an e-mail account to use Email Protection. To add

	seats to your license, click Add Seats. Then follow the on-screen instructions.

VPN - Summary Tab

Figure 39: Summary Screen

Summary	
Tunnel(s) Used	Displays the number of tunnels used.
Tunnel(s) Available	Displays the number of available tunnels.
Tunnel Status	
No.	Displays the number of the tunnel.
Name	Displays the name of the tunnel, as defined by the Tunnel Name field on the VPN > IPSec VPN screen.
Status	Displays the tunnel's status: Connected, Hostname Resolution Failed, Resolving Hostname, or Waiting for Connection.
Phase2 Enc/Auth	Displays the Phase 2 Encryption type (3DES), Authentication type (MD5 or SHA1), and Group (768-bit, 1024-bit, or 1536-bit) that you chose in the VPN > IPSec VPN screen.
Local Group	Displays the IP address and subnet of the local group.
Remote Group	Displays the IP address and subnet of the remote group.
Remote Gateway	Displays the IP address of the remote gateway.
Tunnel Test	Click Connect to verify the tunnel status; the test result is updated in the Status column. If the tunnel is connected, you can disconnect the IPSec VPN connection by clicking Disconnect.
Config.	Click Edit to change the tunnel's settings. Click Trash to delete all of the tunnel's settings.

VPN Clients Status	
No.	Displays the user number from 1 to 5.
Username	Displays the username of the VPN Client.
Status	Displays the connection status of the VPN Client.
IP Address	Displays the IP address of the VPN Client.
Start Time	Displays the start time of the most recent VPN session for the specified VPN Client.
End Time	Displays the end time of a VPN session if the VPN Client has disconnected.
Duration	Displays the total connection time of the latest VPN session.
Disconnect	Check the Disconnect checkbox at the end of each row in the VPN Clients Table and click the *Disconnect* button to disconnect a VPN Client session.

VPN - IPSec VPN Tab

Use this screen to create VPN tunnels between the Router to the remote Router. All Linksys Routers with Ipsec VPN support can be used as a remote Router (e.g. RVS4000, WRV54G, RV042). The Router supports VPN tunnels using IPsec (IP Security) technologies. You can create, delete, or modify a VPN tunnel on this page.

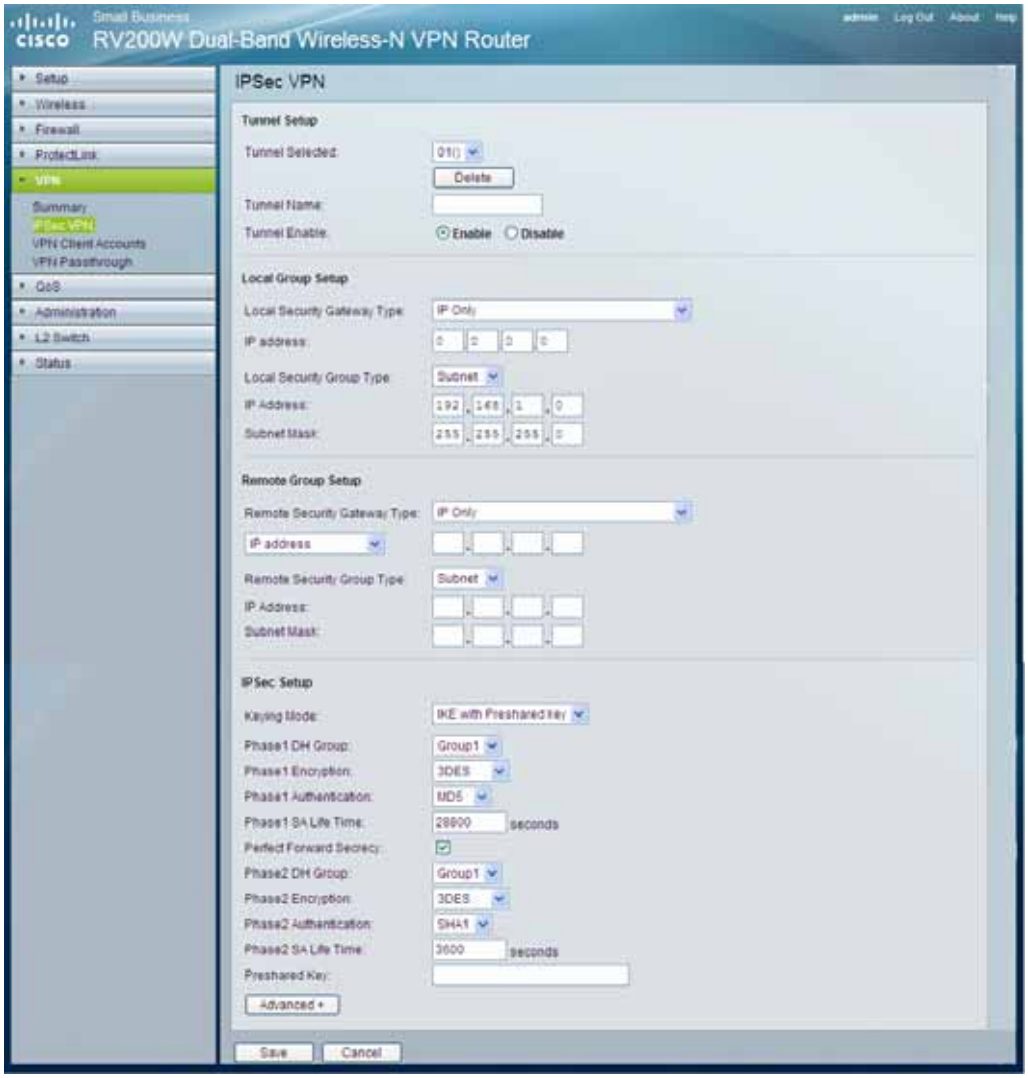


Figure 40: IPSec VPN Screen

IPSec VPN	
Tunnel Selected	Select a tunnel to configure or create a new tunnel.
Delete Button	Click this button to delete the selected tunnel.
Tunnel Name	For each application, list the forwarded port number range. These are the ports used by incoming traffic. Check with the Internet application documentation for the port number(s) needed. In the first field, enter the starting port number of the Forwarded Range. In the second field, enter the ending port number of the Forwarded Range.

Tunnel Enable	Select Enable to enable this tunnel.
Local Security Group	
Local Security Gateway Type	This has two settings, **IP Only** and **IP + Domain Name (FQDN) Authentication**. • **IP Only** If this is selected, the Wireless Router's WAN IP address automatically appears in the *IP Address* field. • **IP + Domain Name (FQDN) Authentication** This is the same as IP Only, but includes a domain name for greater security. Enter an arbitrary domain name in the *Domain Name* field. The Router's WAN IP address automatically appears in the IP Address field.
Local Security Group Type	Select the local LAN user(s) behind the Router that can use this VPN tunnel. This may be a single IP address. Notice that the Local Security Group must match or cover the other router's Remote Security Group.
IP Address	Enter the IP address on the local network.
Subnet Mask	If the Local Security Group Type is set to *Subnet*, enter the mask to determine the IP addresses on the local network.
Remote Security Group	
Remote Security Gateway Type	Select either **IP Only** or **IP + Domain Name (FQDN) Authentication**. The setting should match the Local Security Gateway Type for the VPN device at the other end of the tunnel. • **IP Only** Select this to specify the remote device that will have access to the tunnel. Then either select IP Address from the drop-down menu and enter the remote gateway's WAN IP address in the *IP Address* field, or select *IP by DNS Resolved* from the dropdown menu and enter the remote gateway's domain name in the *Domain Name* field. • **IP + Domain Name (FQDN) Authentication** This is the same as IP Only but includes a domain name for greater security. Enter an arbitrary domain name in the *Domain Name* field. Then select either *IP Address* or *IP by DNS Resolved* from the drop-down menu, and fill in the *IP Address* field or *Domain Name* field.
Remote Security Group Type	Select the remote LAN user(s) behind the remote gateway who can use this VPN tunnel. This may be a single IP address or a Subnetwork. Note that the Remote Security Group Type must match the other router's Local Security Group Type.
IP Address	Enter the IP address on the remote network.
Subnet Mask	If the Remote Security Group Type is set to Subnet, enter the mask to determine the IP addresses on the remote network.
IPSec Setup	
Keying Mode	The Router supports both automatic and manual key management. When choosing automatic key management, IKE (Internet Key Exchange) protocols are used to negotiate key material for SA (Security Association). If manual key management is selected, no

	key negotiation is needed. Basically, manual key management is used in small static environments or for troubleshooting purpose. Notice that both sides must use the same Key Management method (both Auto or both Manual). For Manual key management, all the configurations need to match on both sides.

Manual	• **Incoming/Outgoing SPI**
	The SPI (Security Parameter Index) is carried in the IPsec ESP header. This enables the receiver to select the SA (Security Association), under which a packet should be processed. The SPI is a 32-bit value. Both decimal and hexadecimal values are acceptable. e.g. “987654321” or “0x3ade68b1”. Each tunnel must have unique an Inbound SPI and Outbound SPI. No two tunnels share the same SPI. Notice that Inbound SPI must match the other Router's Outbound SPI, and vice versa.
	• **Encryption**
	The Encryption method determines the complexity to encrypt/decrypt data packets. Only 3DES is supported. Notice that both sides must use the same Encryption method.
	• **Authentication**
	Authentication determines a method to authenticate the data packets to make sure they come from a trusted source. Either MD5 or SHA1 may be selected. Notice that both sides (VPN endpoints) must use the same Authentication method.
	  • MD5 - A one way hashing algorithm that produces a 128-bit digest.
	  • SHA1 - A one way hashing algorithm that produces a 160-bit digest.
	• **Encryption Key**
	This field specifies a key used to encrypt and decrypt data packets. Both characters and hexadecimal values are acceptable in this field.
	Note: that both sides must use the same Encryption Key.
	• **Authentication Key**
	This field specifies a key used to authenticate IP traffic. Both characters and hexadecimal values are acceptable in this field.
	Note: that both sides must use the same Authentication Key.

IKE with Preshared Key	• **Phase1 DH Group** Phase 1 is used to create a security association (SA). DH (Diffie-Hellman) is a key exchange protocol that used during phase 1 of the authentication process to establish pre-shared keys. There are three groups of different prime key lengths. Group 1 is 768 bits, Group 2 is 1,024 bits and Group 5 is 1,536 bits. If network speed is preferred, select Group 1. If network security is preferred, select Group 5. • **Phase 1 Encryption** There are five methods of encryption, DES, 3DES, AES-128, AES-192 and AES-256. The Encryption method determines the length of the key used to encrypt/decrypt ESP packets. DES is 56-bit encryption, 3DES is 168-bit encryption, AES-128 is 128-bit encryption, AES-192 is 192-bit encryption and AES-256 is 256-bit encryption. DES is faster than 3DES, but 3DES is more secure than DES. Both sides must use the same Encryption

method.

- **Phase 1 Authentication**
  Authentication determines a method to authenticate the data packets to make sure they come from a trusted source. Either MD5 or SHA1 may be selected. Notice that both sides (VPN endpoints) must use the same Authentication method.
  - MD5 - A one way hashing algorithm that produces a 128-bit digest.
  - SHA1 - A one way hashing algorithm that produces a 160-bit digest.
- **Phase 1 SA Life Time**
  This field allows you to configure the length of time a VPN tunnel is active in Phase 1. The default value is 28,800 seconds.
- **Perfect Forward Secrecy**
  If PFS is enabled, IKE Phase 2 negotiation will generate a new key material for IP traffic encryption and authentication. Note that both sides must have this selected.
- **Phase2 DH Group**
  There are three groups of different prime key lengths. Group1 is 768 bits, Group2 is 1,024 bits and Group 5 is 1,536 bits. If network speed is preferred, select Group 1. If network security is preferred, select Group 5. You can choose the different Group with the Phase 1 DH Group you chose. If Perfect Forward Secrecy is disabled, there is no need to setup the Phase 2 DH Group since no new key generated, and the key of Phase 2 will be same with the key in Phase 1.
- **Phase 2 Encryption**
  Phase 2 is used to create one or more IPSec SAs, which are then used to key IPSec sessions. There are five methods of encryption, DES, 3DES, AES-128, AES-192 and AES-256. The Encryption method determines the length of the key used to encrypt/decrypt ESP packets. DES is 56-bit encryption, 3DES is 168-bit encryption, AES-128 is 128-bit encryption, AES-192 is 192-bit encryption and AES-256 is 256-bit encryption. DES is faster than 3DES, but 3DES is more secure than DES. Both sides must use the same Encryption method. If users enable the AH Hash Algorithm in Advanced, it is recommended to select Null to disable encrypt/decrypt ESP packets in Phase 2 for most users, but both sides of tunnel must use the same setting.
- **Phase 2 Authentication**
  Authentication determines a method to authenticate the data packets to make sure they come from a trusted source. Either MD5 or SHA1 may be selected. Notice that both sides (VPN endpoints) must use the same Authentication method.
  - MD5 - A one way hashing algorithm that produces a 128-bit digest.
  - SHA1 - A one way hashing algorithm that produces a 160-bit digest.
- **Phase 2 SA Life Time**
  This field allows you to configure the length of time a VPN tunnel is active in Phase 2. The default value is 3,600 seconds.

	• **PreShared Key** IKE uses the Pre-shared Key field to authenticate the remote IKE peer. Both characters and hexadecimal values are acceptable in this field. e.g. “My_@123” or “0x4d795f40313233” Note that both sides must use the same Pre-shared Key.
Advanced	
Aggressive Mode	There are two types of Phase 1 exchanges: Main mode and Aggressive mode. Aggressive Mode requires half of the main mode messages to be exchanged in Phase 1 of the SA exchange. If network security is preferred, select Main mode. When users select the Dynamic IP in Remote Security Gateway Type, it will be limited as Aggressive Mode.
Compress	The router supports IP Payload compression Protocol. IP Payload Compression is a protocol to reduce the size of IP datagrams. If Compress is enabled, the router will propose compression when initiating a connection. If the responders reject this propose, the router will not implement the compression. When the router works as a responder, the router will always accept compression even without enabling compression.
AH Hash Algorithm	AH (Authentication Header) protocol describes the packet format and the default standards for packet structure. With the use of AH as the security protocol, protected is extended forward into IP header to verify the integrity of the entire packet by use of portions of the original IP header in the hashing process. There are two algorithms, MD5 and SHA1. MD5 produces a 128-bit digest to authenticate packet data and SHA1 produces a 160-bit digest to authenticate packet data. Both sides of tunnel should use the same algorithm.
NetBIOS broadcast	Check the box to enable NetBIOS traffic to pass through the VPN tunnel. By default, the router blocks these broadcasts.
Dead Peer Detection	When DPD is enabled, the router will send the periodic HELLO/ACK messages to prove the tunnel liveliness when both peers of VPN tunnel provide DPD mechanism. Once a dead peer detected, the router will disconnect the tunnel so the connection can be re-established. The Interval is the number of seconds between DPD messages. The default is DPD enabled, and default Interval is 10 seconds.

VPN - VPN Client Accounts Tab

You can allow remote users to easily establish a VPN connection to your Router using the Linksys QuickVPN client utility without using a compatible VPN Router with IPsec VPN settings. This is achieved by creating user accounts on the Router and authenticate users through Username and Password. After creating user accounts, it will be summarized in the table below.

For users using QuickVPN, it will first establish an SSL connection with remote Wireless Router to get authenticated. Then QuickVPN will automatically negotiate IPsec settings with the remote Router. All the data packets will be encrypted using IPsec thereafter.

The Wireless Router supports up to five Linksys QuickVPN clients by default. Additional QuickVPN Client licenses can be purchased separately.

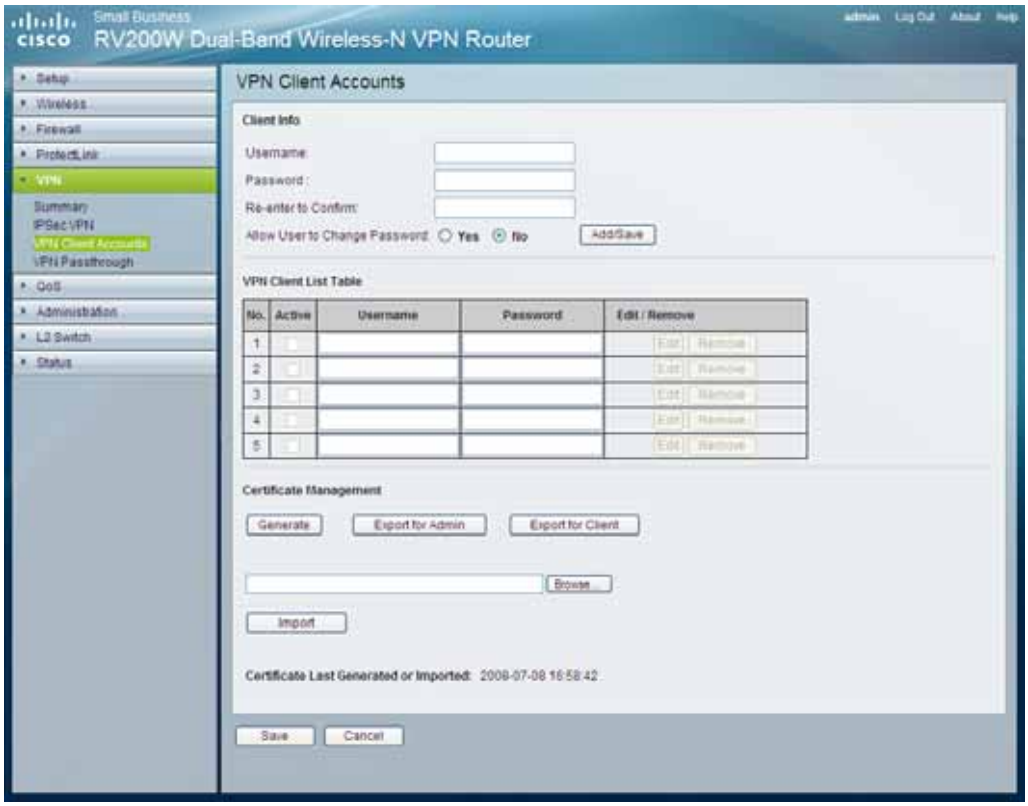


Figure 41: VPN Client Accounts Screen

VPN Client Accounts	
Username	Enter the username using any combination of keyboard characters.
Password	Enter the password you would like to assign to this user.
Re-enter to Confirm	Retype the password to ensure that it has been entered correctly.
Allow User to Change Password	This option determines whether the user is allowed to change their password.

VPN Client List Table	
No	Displays the user number.
Active	When checked, the designated user can connect, otherwise the VPN client account is disabled.
Username	Displays the username.
Password	Displays the password.
Edit Button	This button is used to modify the username, password, or toggle between whether the user is allowed to change their password.
Remove Button	This button is used to delete a user account.
Certificate Management	
Generate	Click this button to generate a new certificate to replace the existing certificate on the router.
Export to Admin	Click this button to export the certificate for administrator. A dialog will ask you to specify where you want to store your certificate. The default file name is “RV220W_Admin.pem” but you can use another name. The certificate for administrator contains the private key and needs to be stored in a safe place as a backup. If the router’s configuration is reset to the factory default, this certificate can be imported and restored on the router.
Export to Client	Click this button to export the certificate for client. A dialog will ask you where you want to store your certificate. The default file name is “RV220W_Client. pem” but you can use another name. For QuickVPN users to securely connect to the router, this certificate needs to be placed in the install directory of the QuickVPN client.
Import	Click this button to import a certificate previously saved to a file using Export for Admin or Export for Client. Enter the file name in the field or click Browse to locate the file on your computer, then click Import.
Certificate Last Generated or Imported	This displays the date and time when a certificate was last generated or imported.

VPN - VPN Passthrough

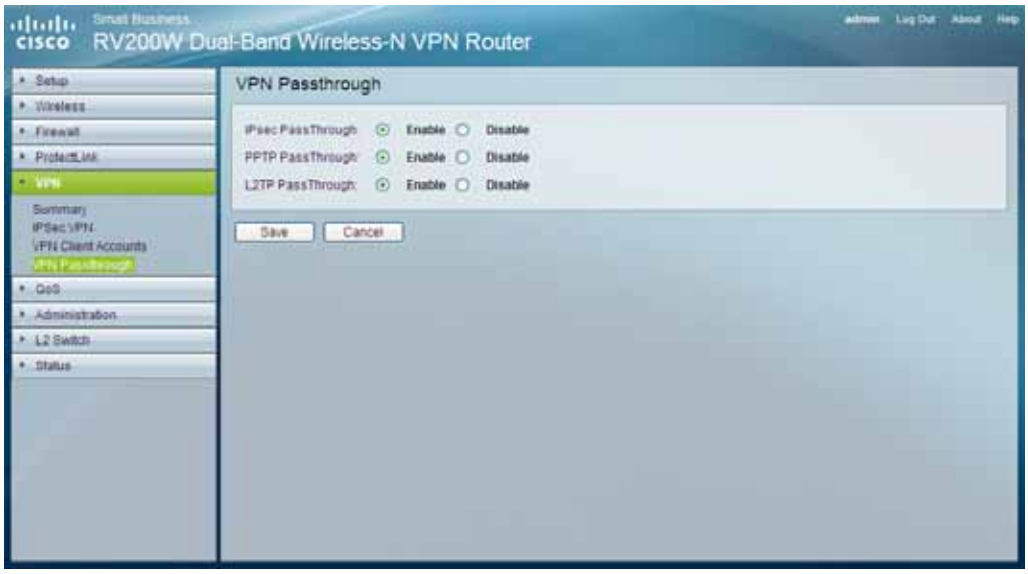


Figure 42: VPN Passthrough Screen

VPN Passthrough	
IPSec PassThrough	Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. IPSec Passthrough is enabled by default to allow IPSec tunnels to pass through the Router. To disable IPSec Passthrough, select Disabled.
PPTP PassThrough	Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. PPTP Passthrough is enabled by default. To disable it, select Disabled.
L2TP PassThrough	Layer 2 Tunneling Protocol is the method used to enable Point-to-Point sessions via the Internet on the Layer 2 level. L2TP Passthrough is enabled by default. To disable L2TP Passthrough, select Disabled.

QoS Tab

QoS (Quality of Service) allows you to perform Bandwidth Management, by either Rate Control or Priority. You can also configure QoS Trust Mode and the DSCP settings.

QoS - Bandwidth Management

Figure 43: Bandwidth Management Screen

Setup	
Bandwidth Management	QoS (Quality of Service) is disabled by default. When enabled, this option allows you to assign priority based on the application type.
Bandwidth	This section lets you specify the maximum bandwidth provided by the ISP on the WAN interface, for both the upstream and downstream directions.
Bandwidth Management Type	
Type	The desired type of bandwidth management, either *Rate Control* or *Priority*. Depending on your selection, the lower portion of the screen displays either the Rate Control section or the Priority section.
Rate Control	
Service	Select the service from the drop-down menu. If it does not contain the service you need, click *Service Management* to add the service.
IP	Enter the IP address or IP range you need to control. The default is zero, which includes all internal IP addresses.
Direction	Select Upstream for outbound traffic or Downstream for inbound traffic.

Mini. Rate	Enter the minimum rate for the guaranteed bandwidth.
Max. Rate	Enter the maximum rate for the guaranteed bandwidth.
Enable	Check this box to enable this Rate Control Rule.
Add to List	After a rule is set up, click this button to add it to the list. The list can contain a maximum of 15 entries.
Delete selected application	Click this button to delete a rule from the list.
Priority	
Service	Select the service from the drop-down menu. If it does not contain the service you need, click Service Management to add the service.
Direction	Select Upstream for outbound traffic or Downstream for inbound traffic.
Priority	Select *High*, *Medium*, *Normal*, or *Low* priority for the service. The default is Medium.
Enable	Check this box to enable this Priority Rule.
Service Man-agement	Click this button to open a sub screen to add, delete or modify services settings.
Add to List	After a rule is set up, click this button to add it to the list. The list can contain a maximum of 15 entries.
Delete selected application	Click this button to delete a rule from the list.

Figure 44: Service Management

QoS - QoS Setup

The QoS Setup screen allows users to configure QoS Trust Mode for each LAN port.

Figure 45: QoS Setup Screen

QoS Setup	
Port ID	The number of the LAN port.
Trust Mode	Select either CoS or DSCP. The default is CoS.
Priority	If Trust Mode is set to Port, select the port priority from 0 to 7 from the drop-down menu. If Trust Mode is set to CoS, select the default CoS priority 0 from the drop-down menu.
CoS Setup	
Priority	The CoS priority from 0 to 7.
Queue	Select the desired traffic forwarding queue from the list.

QoS - Queue Settings

Figure 46: Queue Settings

QoS Setup Queue Settings	
Queue	The number of the Queue.
Strict Priority	Select either *Strict Priority* or *WRR*. The default is *Strict Priority*.
WRR	If WRR enabled, enter the values for *WRR Weight* and *% of WRR Bandwidth*.

QoS - DSCP Setup

Figure 47: DSCP Setup Screen

DSCP Setup	
DSCP	The Differentiated Services Code Point value in the incoming packet.
Priority	Select the traffic forwarding queue, 1 to 7, to which the DSCP priority is mapped.
Restore Defaults	Click this button to restore the default DSCP values.

Administration Tab

The Administration tab provides access to system administration settings and tools.

Administration - Management

Figure 48: Management Screen

Local Gateway Access	
Gateway Userlist	Select the desired Gateway User List.
Gateway Username	Enter the user name here.
Gateway Password	Enter the password.
Re-enter to Confirm	Retype the password in this field.
SNMP	
SNMP	Select Enable if you wish to use SNMP. To use SNMP, you need SNMP software on your PC.
System Name	Enter a suitable name. This name will be used to identify this device, and will be displayed by your SNMP software.
System Contact	Enter contact information for the system.
System Location	Enter the location of the system.
Read Community	Enter the SNMP community name for SNMP “Get” commands.

Write Community	Enter the SNMP community name for SNMP “Set” commands.
Trap Community	Enter the SNMP community name for SNMP “Trap” commands.
Trap To	Enter the IP Address of the SNMP Manager to which traps will be sent. If desired, this may be left blank.
UPnP	
UPnP	If you want to use UPnP, keep the default setting, Enable. Otherwise, select Disable.
WLAN	
Management Via WLAN	Select *Enable* or *Disable*. The default setting is *Disable*.

Administration - Log

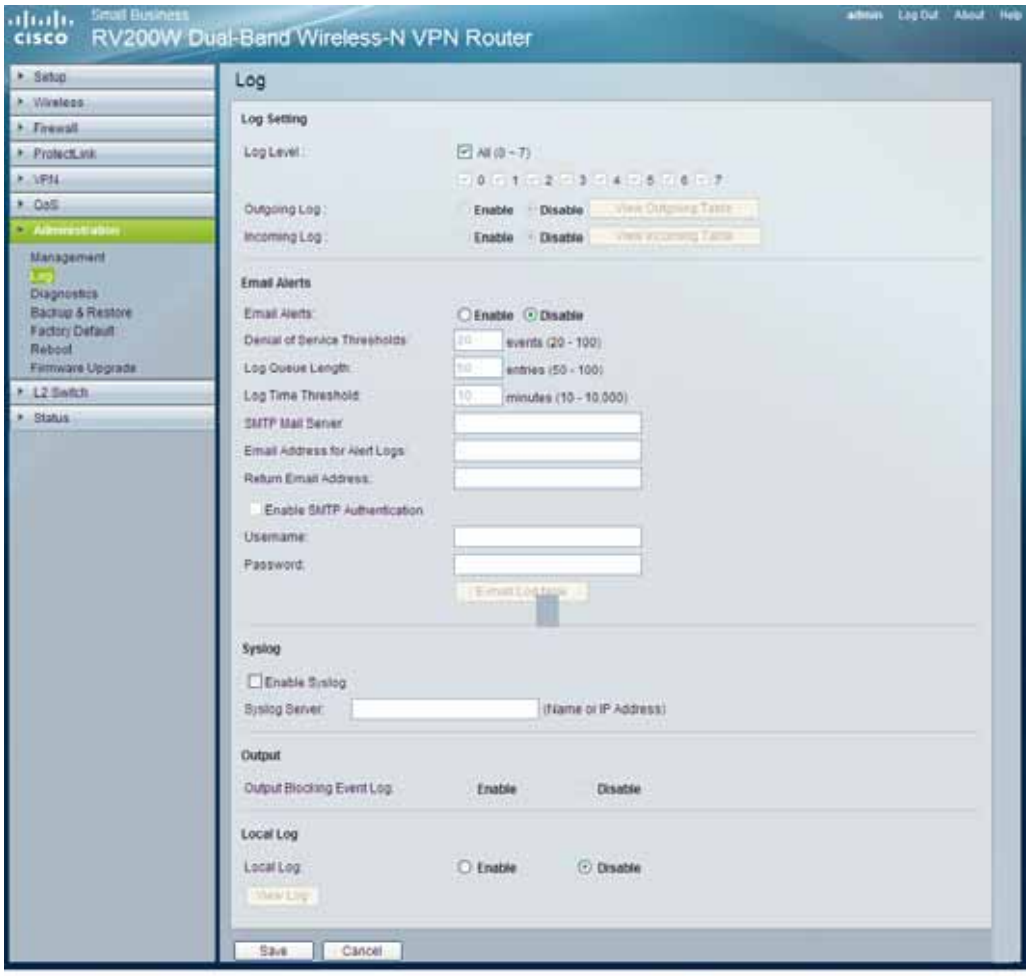


Figure 49: Log Screen

Log Setting	
Log Level	Select the log level(s) that the Router should record.
Outgoing Log	Select Enable to cause all outgoing packets to be logged. You can then click *View Outgoing Table* to display information on the outgoing packets including Source IP, Destination IP, and Service/Port number.
Incoming Log	Select Enable to cause all incoming packets to be logged. You can then click *View Incoming Table* to display information on incoming packets including Source IP, Destination IP, and Service/Port number.
Email Alerts	
Email Alerts	Select Enable to cause an e-mail to be sent immediately if a DoS (Denial of Service) attack is detected. If enabled, fill in the e-mail address information in the remaining fields in this section.

Denial of Service Thresholds	Enter the number of DoS (Denial of Service) attacks which need to be blocked by the built-in Firewall before an e-mail alert is sent. The minimum value is 20, the maximum value is 100.
Log Queue Length	The default is 0 entries (Router will e-mail the log if there are more than 50 entries).
Log Time Threshold	The default is 0 minutes (Router will e-mail the log every 10 minutes).
SMTP Mail Server	Enter the address (domain name) or IP address of the SMTP (Simple Mail Transport Protocol) Server you use for outgoing e-mail.
Email Address for Alert Logs	Enter the e-mail address the Log is to be sent to.
Return Email Address	The e-mail will show this address as the Sender's address.
Enable SMTP Authentication	If your SMTP server requires Authentication, you can enable it here, and enter the Username and Password.
Email Log Now	Press this button to cause the log to be e-mailed immediately.
Syslog	
Enable Syslog	Select the checkbox if you want to use this feature.
Syslog Server	Enter the IP Address in this field when Enable Syslog is checked.
Output Blocking Event Log	Select Enable to use this feature.
Local Log	
Local Log	Enable this if you want to see a log of all incoming and outgoing URLs or IP addresses.
View Log	Click this button when you wish to view the logs. A new window will appear with the log data.

Administration - Diagnostic

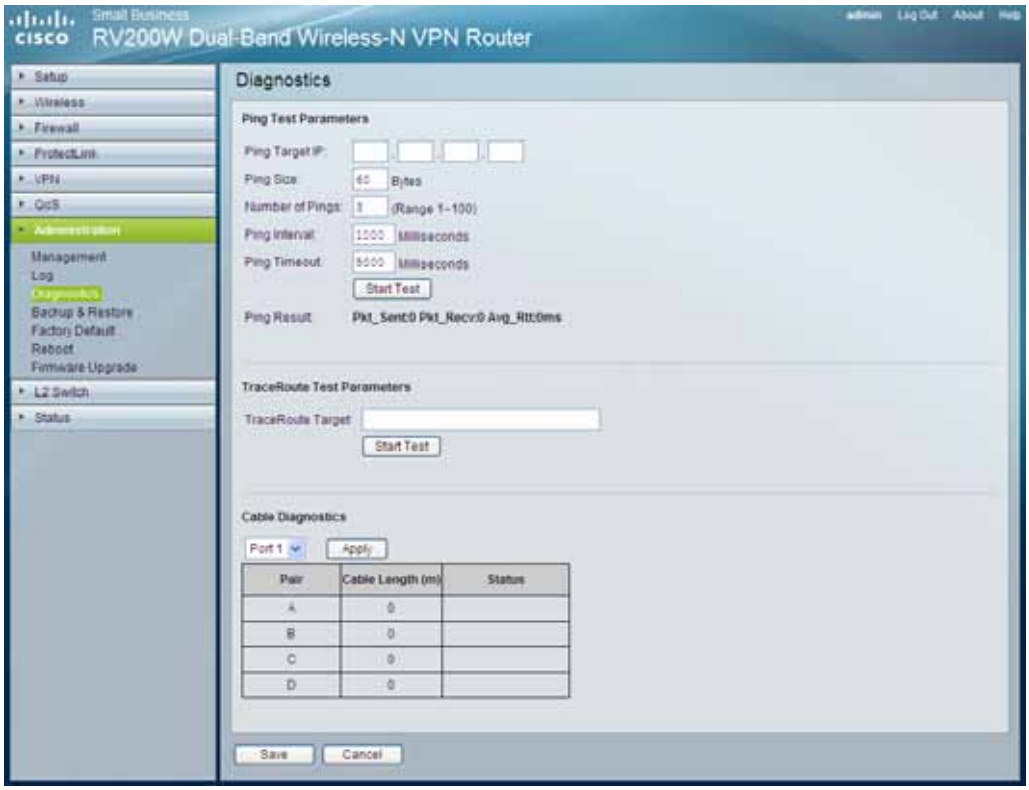


Figure 50: Diagnostic Screen

Ping Test Parameters	
Ping Target IP	Enter the IP address or URL that you want to ping.
Ping Size	Enter the size of the packet you want to use.
Number of Pings	Enter the number of times you wish to ping the target device.
Ping Interval	Enter the time period (milliseconds) between each ping.
Ping Timeout	Enter the desired time period (milliseconds). If a response is not received within the defined ping period, the ping is considered to have failed.
Start Test	Click this button to begin the test. A new screen will appear and display the test results.
Ping Result	Displays the Ping status.
Traceroute Test Parameters	
Traceroute Target	Enter the target IP address for the traceroute test.
Start Test	Click this button to begin the test. A new screen will appear and display the test results.
Cable Diagnostic	
Port	Select the port number from the drop-down menu.

Pair	Identifies a specific pair (A, B, C, or D) in the cable. Each cable consists of 8 pins (4 pairs).
Cable Length	Displays the length of the cable in meters.
Status	Displays the status of the pair.

Administration - Backup & Restore

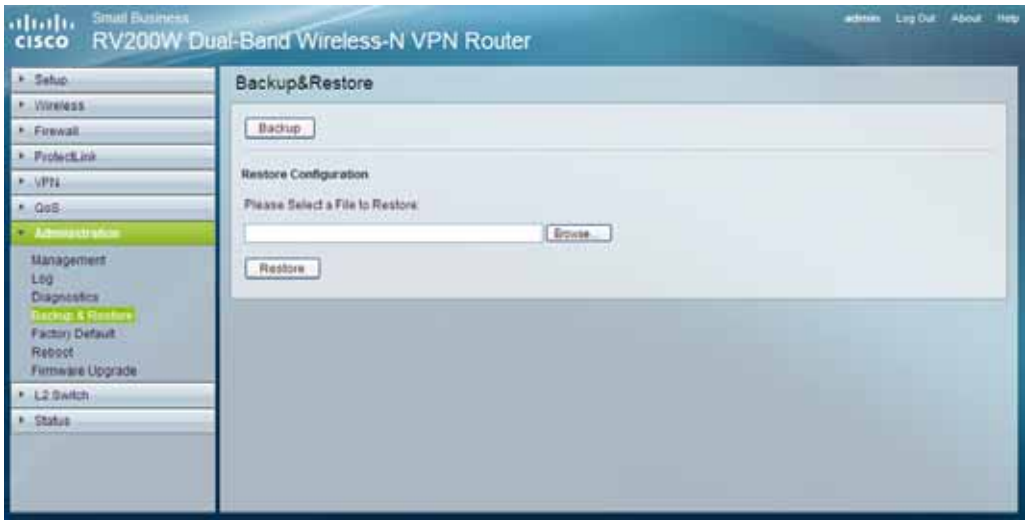


Figure 51: Backup & Restore Screen

Backup & Restore	
Backup & Restore	To download a copy of the current configuration and store the file on your PC, click *Backup* to start the download.
Restore & Configuration	
Restore & Configuration	To restore a previously saved config file back to the Router, enter the file name in the field or click Browse to select the config file, then click *Restore* to upload the config file.

Administration - Factory Defaults

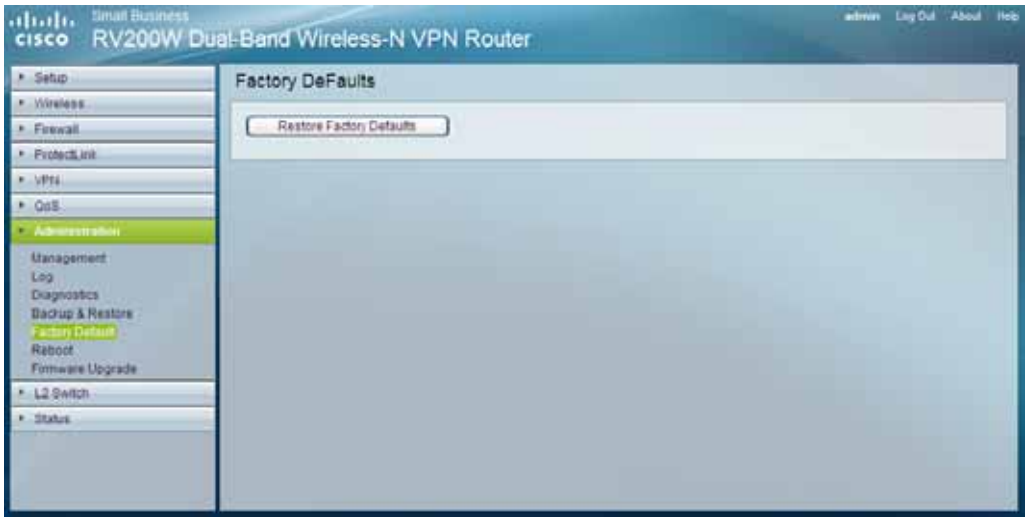


Figure 52: Factory Defaults Screen

Factory Defaults	
Restore Factory Defaults Button	Click this button to reset all configuration settings to their factory default values. Any settings that have been saved will be lost when the default settings are restored. After clicking the button, another screen will appear. Click OK to continue. Another screen will appear while the system reboots.

Administration - Reboot

Figure 53: Reboot Screen

Reboot	
Reboot	Click this button to reboot the Router. This operation will not cause the Router to lose any of its stored settings.

Administration - Firmware Upgrade

To upgrade firmware, download the latest firmware for the product from www.linksys.com, extract it to your computer, and perform the steps below.

Figure 54: Firmware Upgrade Screen

Firmware Upgrade	
File	Type in the name of the extracted firmware upgrade file or click *Browse* to locate the file.
Start to Upgrade	Once you have selected the appropriate file, click *Start to Upgrade* and follow the on-screen instructions to upgrade your firmware.

L2 Switch - Create VLAN

VLANs are logical subgroups of a Local Area Network (LAN) created via software rather than defining a hardware solution. VLANs combine user stations and network devices into a single domain regardless of the physical LAN segment to which they are attached. VLANs allow network traffic to flow more efficiently within subgroups. VLANs managed through software reduce the amount of time in which network changes are implemented.

VLANs have no minimum number of ports, and can be created per unit, per device, per stack, or any other logical connection combination, as VLANs are software based and not defined by physical attributes.

VLANs function at layer 2. Since VLANs isolate traffic within the VLAN, a Layer 3 router is needed to allow traffic flow between VLANs. Layer 3 routers identify segments and coordinate with VLANs. VLANs are broadcast and multicast domains. Broadcast and multicast traffic is transmitted only in the VLAN in which the traffic is generated.

Figure 55: Create VLAN Screen

VLAN Configuration	
VLAN ID	The VLAN ID number. This can be any number from 2 to 3290, or from 3293 to 4094. (VLAN ID 1 is reserved for the default VLAN, which is used for untagged frames received on the interface. VLAN IDs 3291-3292 are reserved and cannot be used.) To create VLAN, enter the ID number and click Add VLAN.
VLAN ID Range	To create multiple VLANs with a range of ID numbers, enter the starting and ending ID numbers and click *Add Range*.
Deleted Selected VLAN	To delete a VLAN, select it form the VLAN list and click Delete Selected VLAN.

L2 Switch - VLAN & Port Assignment

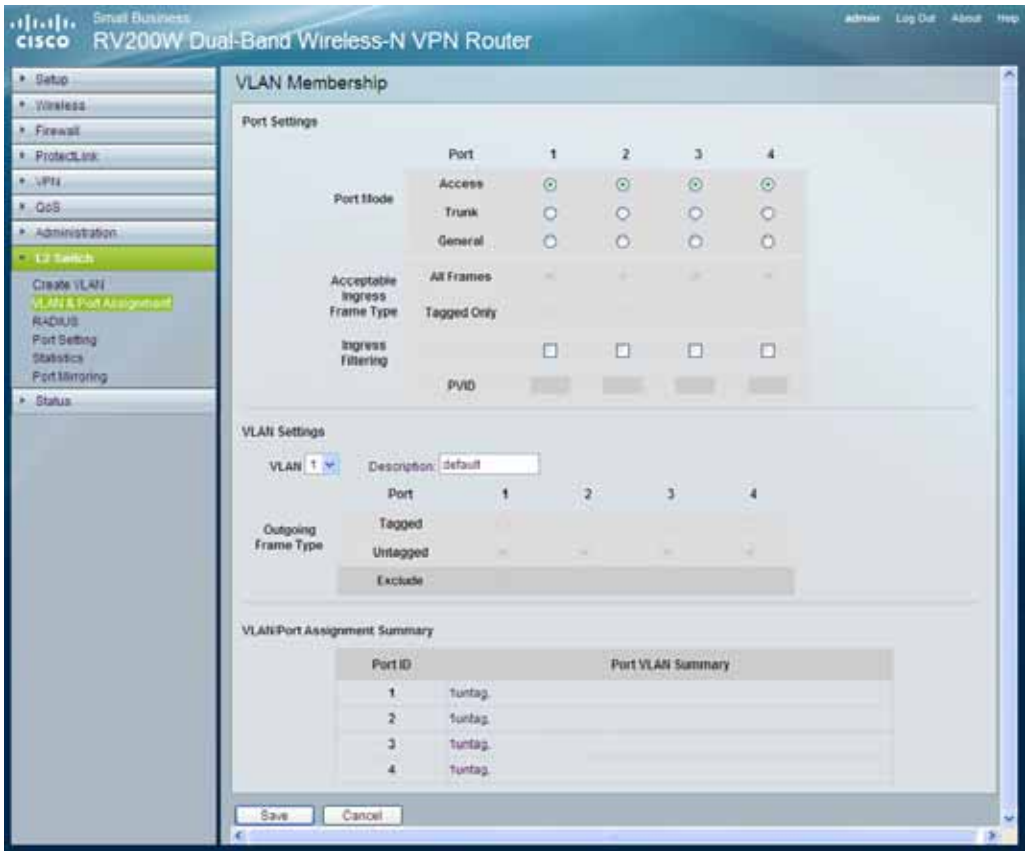


Figure 56: VLAN & Port Assignment Screen

Port Settings	
Port Mode	The table indicates each port's current mode (Access, Trunk, or General e). Wireless can be enabled in Access Mode.
Acceptable Ingress Frame Type	Configure which kind of packet can be accepted in the port.
Ingress Filtering	Select the checkbox if you want to use Ingress Filtering.
PVID	Configure the PVID setting.
VLAN Settings	
VLAN	Select the VLAN whose membership you want to configure.
Description	Enter a VLAN group name of up to 50 characters.
Outgoing Frame Type	The table indicates each port's outgoing frame type (Untagged, Tagged, or Exclude).
VLAN/Port Assignment Summary	
Table	Displays the table of summary.

L2 Switch - Radius

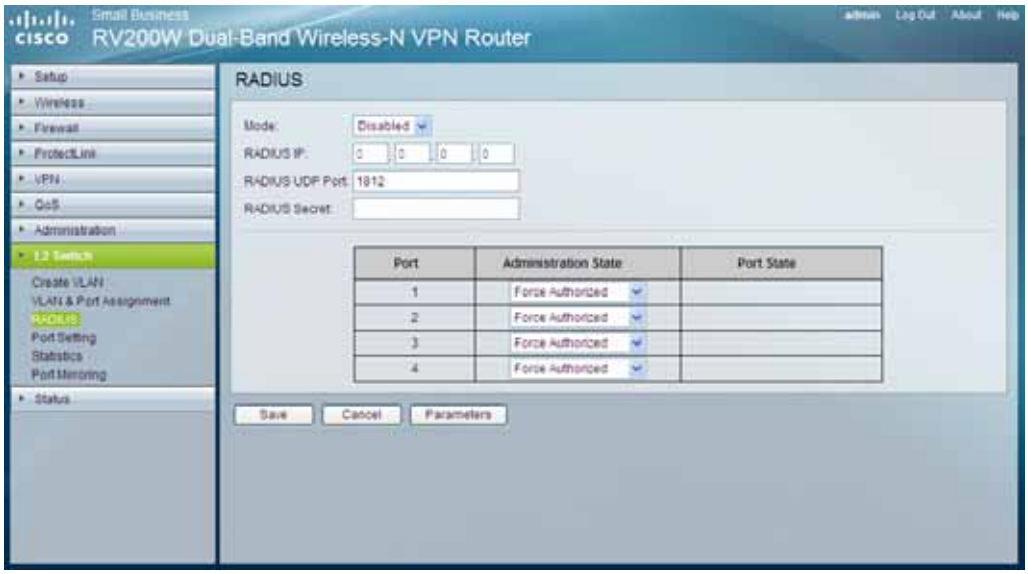


Figure 57: Radius Screen

Radius	
Mode	Select *Enabled* or *Disabled* from the drop-down menu to enable or disable RADIUS.
Radius IP	Enter the Server IP address.
Radius UDP Port	Enter the UDP port. The UDP port is used to verify the RADIUS server authentication.
Radius Secret	Enter the Key string used for authenticating and encrypting all RADIUS communications between the device and the RADIUS server. This key must match the RADIUS server encryption key. If no host-specific value is specified, the global value applies to each host.
Administration State	Specifies the port authorization state. The possible field values are: • **Auto** - The controlled port state is set by the Authentication method. • **Force Authorized** - The controlled port state is set to Force-Authorized (forward traffic). • **Force Unauthorized** - The controlled port state is set to Force-Unauthorized (discard traffic).
Port State	Displays the state of the selected port.

L2 Switch - Port Setting

Figure 58: Port Setting Screen

Port Setting	
Port	Displays the physical port number.
Link	Displays the port duplex mode and speed. Full Duplex indicates that the interface supports transmission between the device and its link partner in both directions simultaneously. Half Duplex indicates that the interface supports transmission between the device and the client in only one direction at a time.
Mode	Select the port duplex mode and speed from the drop-down menu. You can also select *Auto Negotiation*, which is a protocol between two link partners that enables a port to advertise its transmission rate, duplex mode and flow control abilities to its partner.
Flow Control	Displays the flow control status on the port. Operates when port is in Full duplex mode.
Jumbo Frame	Displays the maximum frame size the port can receive and send.

L2 Switch - Statistics

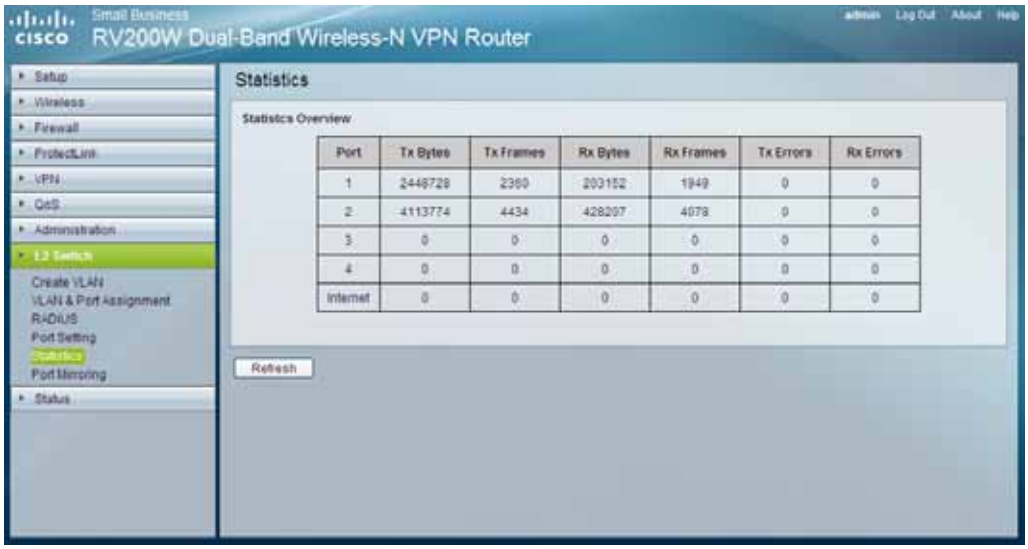


Figure 59: Statistics Screen

Statistics	
Tx Bytes	Displays the number of Bytes transmitted from the selected port.
Tx Frames	Displays the number of Frames transmitted from the selected port.
Rx Bytes	Displays the number of Bytes received on the selected port.
Rx Frames	Displays the number of Frames received on the selected port.
Tx Errors	Displays the number of error packets transmitted from the selected port.
Rx Errors	Displays the number of error packets received from the selected port.

L2 Switch - Port Mirroring

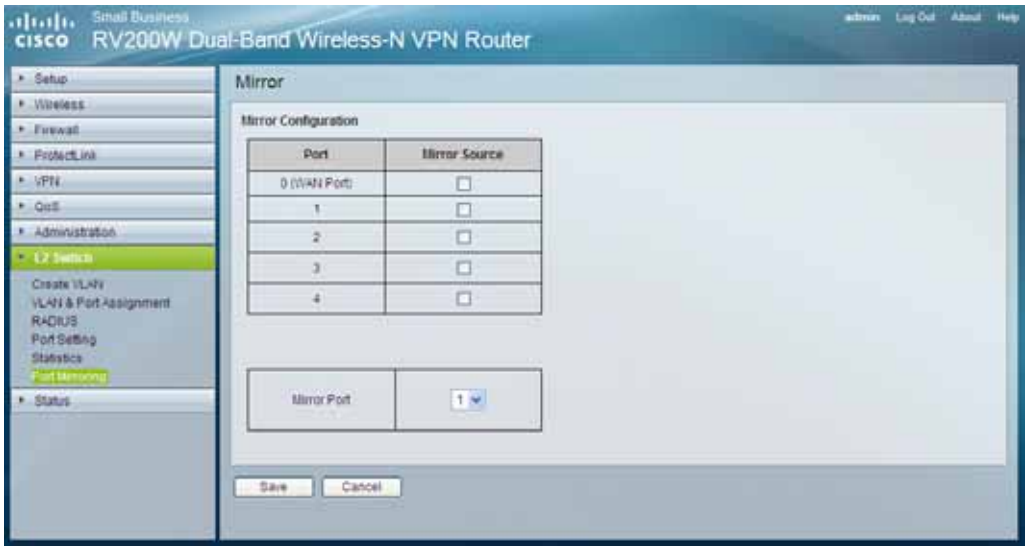


Figure 60: Port Mirroring Screen

Mirror Configuration	
Mirror Source	Use this to enable or disable source port mirroring for each port on the Router. To enable source port mirroring on a port, check the box next to that port. To disable source port mirroring on a port, leave the box unchecked. The default is disabled.
Mirror Port	Select the mirror destination port from the drop-down menu.

Status - Gateway

Figure 61: Gateway Screen

WAN/Gateway	
Firmware Version	Displays the Gateway's current firmware.
Mac Address	Displays the Gateway MAC Address, as seen by your ISP.
Current Time	Displays the time, based on the time zone you selected on the Setup tab.
Internet Connection	
Connection Type	Displays the type of the connection.
Interface	Displays the Gateway Internet Interface.
IP Address	Displays the Gateway Internet IP Address.
Subnet Mask	Displays the Subnet Mask that is associated with the IP address above.
Default Gateway	Displays your ISP's Gateway.
DNS 1-2	Displays the DNS (Domain Name System) IP addresses currently used by this Gateway.
DHCP Release	Click this button to release IP address on WAN port if using DHCP.
DHCP Renew	Click this button to renew IP address on the WAN port if using

	DHCP.
IP Conntrack	Click this button to display the IP Conntrack screen.

IP Conntrack

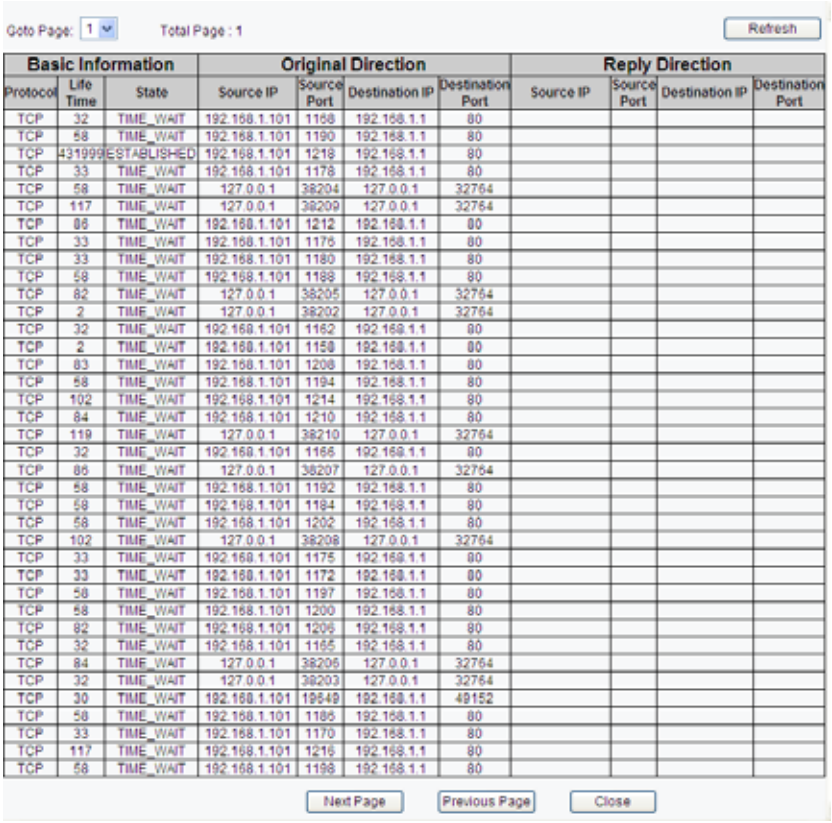


Figure 62: IP Conntrack

The IP Conntrack (Connection Tracking) screen displays information about TCP/UDP connections, such as source and destination IP address and port number pairs (known as socket pairs), protocol types (TCP/UDP/ICMP), connection state and timeouts. To see more information, click Next Page or Previous Page, or select the page from the Goto Page drop-down menu. To see the latest information, click Refresh. Click Close to return to the Status > Gateway screen.

Status - Local Network

Figure 63: Local Network Screen

Local Network	
Current IP Address System	This shows the current system.
Mac Address	This is the Router MAC Address, as seen on your local, Ethernet network.
IP Address	The Internet IP Address is displayed here.
Subnet Mask	This Subnet Mask is associated with the IP address above.
IPv6 Address	This shows the IPv6 IP address, if applicable.
DHCP Server	The status of the Router's DHCP server function is displayed here.
Start IP Address	This shows the beginning of the range of IP addresses used by the DHCP Server.
End IP Address	This shows the end of the range of IP addresses used by the DHCP Server.
DHCP Client Table	Clicking this button will open a screen showing you which PCs are utilizing the Router as a DHCP server. On the DHCP Client Table screen, you will see a list of DHCP clients (PCs and other network devices) with the following information: Client Names, Interfaces, IP Addresses, MAC Addresses, and the length of time before their assigned IP addresses expire.
ARP/RARP Table	Clicking this button will open a screen showing you which PCs are utilizing the Router as an ARP/RARP server. On the ARP/RARP Table screen, you will see a list of ARPs/RARPs (PCs and other network devices) with the following information: IP Addresses and MAC Addresses.

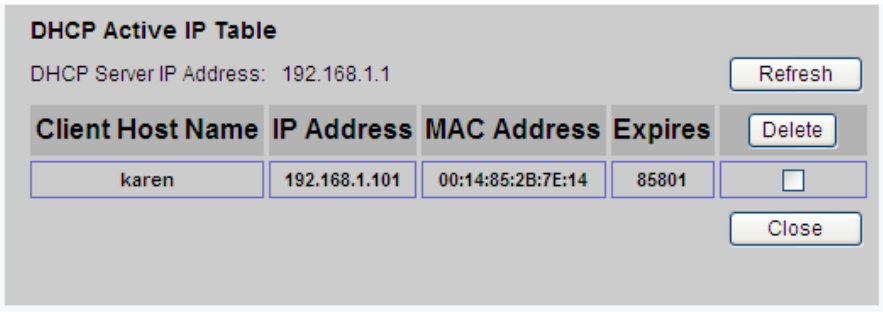


Figure 64: DHCP Client Table

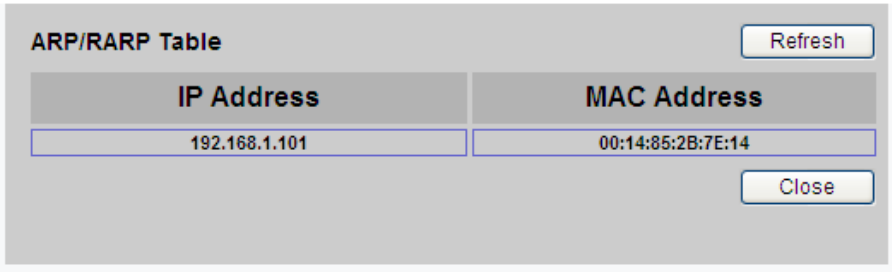


Figure 65: ARP/RARP Table

Status - Wireless LAN

This screen provides some basic information on the Wireless LAN of this Wireless Router.

Figure 66: Wireless LAN Screen

Wireless LAN	
Wireless IP Address	Displays the IP address on the Wireless LAN interface.
Mac Address	Displays the MAC address on the Wireless LAN interface.
Network Mode	Displays the Wireless network operating mode (e.g. B/G/N-Mixed).
Wireless SSID	Displays the Wireless network name.
Channel Bandwidth	Displays the wireless channel bandwidth setting.
Wireless Channel	Displays the radio channel number used.
Security	Displays the Wireless Security mode.
SSID Broadcast	This shows the beginning of the range of IP addresses used by the DHCP Server.

Status - System Performance

This screen provides data packet statistics on the LAN switch and Wireless LAN of the Router.

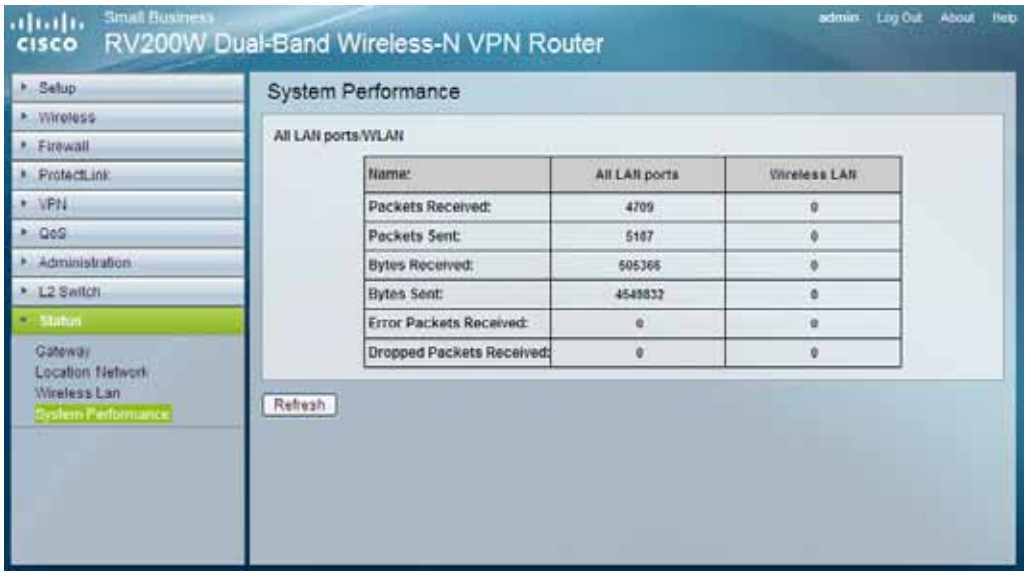


Figure 67: System Performance Screen

All LAN ports / WLAN	
Packets Received	This shows the number of packets received.
Packets Sent	This shows the number of packets sent.
Bytes Received	This shows the number of bytes received.
Bytes Sent	This shows the number of bytes sent.
Error Packets Received	This shows the number of error packets received.
Dropped Packets Received	This shows the number of packets being dropped after they were received.

Appendix A

Specifications

Dual-Band Wireless-N VPN Router

General	
Model	RV220W
Ports	10/100/1000 Base-T Ethernet, 12V DC Power
Buttons	Reset
Cabling Type	Type UTP CAT 5
LEDs	Power, Diag, DMZ, Wireless, ETHERNET 1-4, Internet
Wireless	
Transmit Power	IEEE 802.11a: 23.92 dBm draft 802.11n Standard-20 MHz Channel mode: 24.52 dBm draft 802.11n Wide-40 MHz Channel mode: 23.82 dBm IEEE 802.11b: 19.26 dBm IEEE 802.11g: 20.74 dBm draft 802.11n Standard-20 MHz Channel mode: 20.65 dBm draft 802.11n Wide-40 MHz Channel mode: 18.79 dBm
Modulation Technique & Transmit Data Rate	IEEE 802.11a: OFDM (QPSK, BPSK, 16-QAM, 64-QAM) (54, 48, 36, 24, 18, 12, 9, 6 Mbps) draft 802.11n Standard-20 MHz Channel mode: OFDM (6.5, 7.2, 13, 14.4, 14.44, 19.5, 21.7, 26, 28.89, 28.9, 39, 43.3, 43.33 52, 57.78, 57.8, 58.5, 65.0, 72.2, 78, 86.67, 104, 115.56, 117, 130, 144.44 Mbps) draft 802.11n Wide-40 MHz Channel mode: OFDM (13.5, 15, 27, 30, 40.5, 45, 54, 60, 81, 90, 108, 120, 121.5, 135, 150, 162, 180, 216, 240, 243, 270, 300 Mbps) IEEE 802.11b mode: DSSS (1, 2, 5.5 and 11 Mpbs) IEEE 802.11g mode: OFDM (6, 9, 12, 18, 24, 36, 48 and 54 Mpbs) draft 802.11n Standard-20 MHz Channel mode: OFDM (6.5, 7.2, 13, 14.4, 14.44, 19.5, 21.7, 26, 28.89, 28.9, 39, 43.3, 43.33 52, 57.78, 57.8, 58.5, 65.0, 72.2, 78, 86.67, 104, 115.56, 117, 130, 144.44 Mbps) draft 802.11n Wide-40 MHz Channel mode: OFDM (13.5, 15, 27, 30, 40.5, 45, 54, 60, 81, 90, 108, 120, 121.5, 135, 150, 162, 180, 216, 240, 243, 270, 300 Mbps)
Antenna Specification	1. Dipole Antenna / 2 dBi MIMO: 2dBi + 10 log (2) = 5 dBi (Numeric gain: 3.16) 2. PIFA Antenna / 6.6 dBi (RX only)
Performance	
NAT Throughput	800 Mb/s

Setup/Config	
Web User Interface	WebUI Built in Web UI for Easy browser-based configuration (HTTP/HTTPS)
Management	
SNMP Version	SNMP Version 1, 2c
Event Logging	Local, Syslog, E-mail Alerts
Web F/W upgrade	Firmware Upgradable Through Web-Browser
Diagnostics	DIAG LED for Flash and RAM failure; Ping Test for network diagnostics
Security	
VPN	5 QuickVPN Tunnels for remote client access 5 IPSec Gateway-to-Gateway Tunnels for branch office connectivity 3DES Encryption MD5/SHA1 Authentication IPSec NAT-T VPN Passthrough of PPTP, L2TP, IPSec
Access Control	IP-based ACL, Internet Access Policy Control
Firewall	SPI stateful packet inspection firewall
Content Filtering	URL blocking, keyword blocking
IPS (Intrusion Prevention System)	IP Sweep Detection, Application Anomaly Detection (HTTP, FTP, Telnet, RCP), P2P Control, Instant Messenger Control, L3-L4 Protocol (IP, TCP, UDP, ICMP) Normalization, L7 Signature Matching
Signature Update	Manual download from the web (Free download for 1 year)
Secure Management	HTTPS, Username/Password
802.1x	Port-based Radius Authentication (EAP-MD5, EAP-PEAP)
NAT	PAT, NAPT, ALG support, NAT Traversal
QoS	
Prioritization types	Port-based and Application-based Priority
Queues	4 queues
Network	
VLAN Support	Port-based VLAN
DHCP	DHCP Server, DHCP Client, DHCP Relay Agent
DNS	DNS Relay, Dynamic DNS (DynDNS, TZO)
DMZ	Any host IP address on LAN side
Routing	Static and RIP v1, v2

Environment	
Device Dimensions	(W x H x D) 170 x 131 x 170 mm
Weight	0.99 lbs (0.45kg)
Power	12V 1.25A
Certification	FCC class B, CE, ICES-003
Operating Temp.	0ºC to 40ºC (32ºF to 104ºF)
Storage Temp.	-20ºC to 70ºC (-4ºF to 158ºF)
Operating Humidity	10% to 85% Non-Condensing
Storage Humidity	5% to 90% Non-Condensing