



ADMINISTRATION GUIDE

Cisco Small Business

WRV210 Wireless-G VPN Router with RangeBooster

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco Ironport, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0907R)

Chapter 1: Introduction	6
Product Overview	6
Features	6
Front Panel	7
Back Panel	8
Initial Installation	8
Placement Options	9
Desktop Option	9
Wall Option	9
Connecting the Equipment	9
Verifying the Hardware Installation	11
Configuring the Internet Connection	12
Securing the Wireless Network	13
Getting Started in the Configuration Utility	16
Logging In	16
Navigating through the Pages	17
Saving Your Changes	17
Viewing the Help Files	17
Chapter 2: Setting Up the Network	18
Configuring the Basic Settings	18
Localizing the Configuration Utility	19
Setting Up the Internet Connection	20
Setting Up the Local Network	23
Adjusting the Time Settings	24
Setting Up Virtual LANs	25
Using DDNS to Map Domain Names to Your Network	26
DynDNS.org Setup	27
TZO.com Setup	28
Cloning a MAC Address for Your Internet Connection	29
Setting Up Advanced Routing	30
Configuring Dynamic Routing	31

Setting Up Static Routing	32
Chapter 3: Configuring the Wireless Network	34
A Note About Wireless Security	34
Wireless Security Tips	34
General Network Security Guidelines	36
Enabling Your Wireless Networks	37
Wireless > Wireless Security	39
Controlling Access to the Wireless Network	43
Adjusting the Advanced Wireless Settings	45
Configuring a Wireless Distribution System (WDS)	47
Chapter 4: Configuring the Firewall	49
Preventing Attacks	50
Enabling Port Forwarding to Allow Access to Services	51
Using Port Triggering to Allow Access to Applications	54
Configuring a DMZ to Allow Access to All Ports of a Server	55
Restricting Users' Access to the Internet	57
Blocking Web Access with URL Filtering	59
Chapter 5: Configuring a Virtual Private Network (VPN)	61
Managing the VPN Users and Certificates	61
Managing the VPN Users	63
Managing VPN Certificates	65
Configuring VPN Passthrough	66
VPN > IPSec VPN	68
Monitoring the IPSec VPN Tunnels	73
Chapter 6: Configuring Quality of Service (QoS)	75
Configuring QoS Settings for Specified Applications	75
Priority Queue QoS Type	76

Bandwidth Allocation QoS	77
Configuring QoS Settings for Specified Ports	78

Chapter 7: Administration **80**

Managing Access and Configuring Other Management Options	80
Resetting the Admin Password	81
Managing LAN and WAN Access to the Configuration Utility	82
Configuring SNMP Settings for Status Reporting	84
Configuring Universal Plug and Play (UPnP) Settings	85
Backing and Restoring a Configuration	86
Setting Up Alerts and System Logs	87
Performing Diagnostic Tests	89
Reverting to the Factory Default Settings	91
Upgrading the Firmware	92
Rebooting the Router	94

Chapter 8: Monitoring the Status of the Network **95**

Monitoring the Router Status	96
Monitoring the LAN	97
Monitoring the Wireless Network	99
Monitoring the System Performance	100
Monitoring the QuickVPN Clients	102

Appendix A: Specifications **103**

Appendix B: Where to Go From Here **107**

Introduction

This chapter provides information to familiarize you with the product features, guide you through the installation process, and get started using the web-based Configuration Utility.

- [Product Overview, page 6](#)
- [Initial Installation, page 8](#)
- [Getting Started in the Configuration Utility, page 16](#)

Product Overview

Thank you for choosing the Wireless-G VPN Router with RangeBooster. The WRV210 is a VPN router with a Wireless-G access point for small offices and home offices. The 10/100 Ethernet WAN interface connects directly to your broadband DSL or Cable modem. For the LAN interface, there is a built-in 4-port, full-duplex 10/100 Ethernet switch that can connect up to four devices.

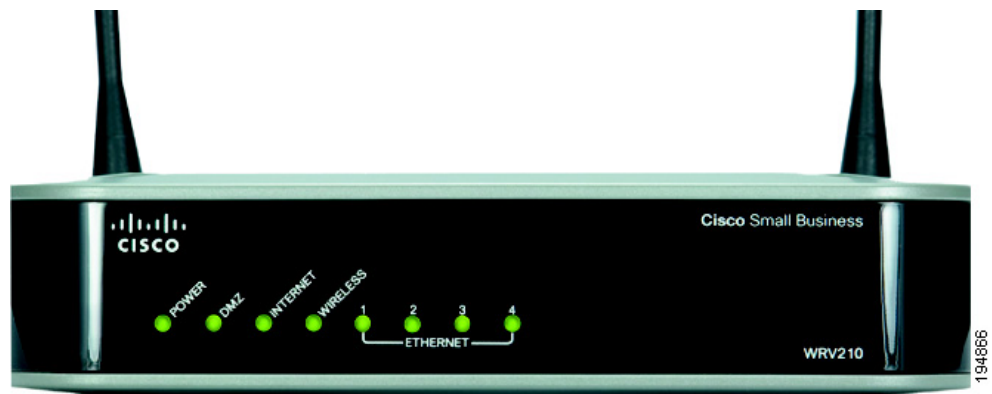
Features

The wireless Access Point supports 802.11b/g and incorporates RangeBooster technology, which utilizes a MIMO antennae configuration to provide increased coverage and reliability over standard 802.11g.

The WRV210 has the advanced security functions needed for business networking. It has a SPI based firewall with DoS prevention, but also a Virtual Private Networking (VPN) engine for secure communication between mobile or remote workers and branch offices. For your wired and wireless local area network, there is support for multiple SSIDs and VLANs for traffic separation. The WRV210 Wireless Access Point implements WPA2-PSK, WPA2-ENT, and WEP encryption, along with other security features including enabling/disabling SSID Broadcasts and MAC-based filtering.

Wireless networking in business environments requires additional flexibility. The WRV210 has the capability to expand or reduce the area of your wireless network. There is support for Wireless Distribution System (WDS), which allows the wireless coverage to be expanded without wires through wireless bridging between it and select Cisco Small Business stand-alone access points. That, along with the ability to increase or decrease the RF output power, allows for optimal wireless coverage.

Front Panel



POWER—(Green) The Power LED lights up when the Router is powered on.

DMZ—(Green) The DMZ LED lights up when the Router has an available DMZ port. If the LED is flashing, the Router is sending or receiving data over the DMZ port.

INTERNET—(Green) The Internet LED lights up when the Router is connected to your cable or DSL modem. If the LED is flashing, the Router is sending or receiving data over the Internet port.

WIRELESS—(Green) The Wireless LED lights up whenever there is a successful wireless connection. If the LED is flashing, the Router is actively sending or receiving data over the wireless network.

1-4 (ETHERNET)—(Green) These four LEDs correspond to the four Ethernet ports of the Router. If the LED is continuously lit, the Router is connected to a device through the corresponding port (1, 2, 3, or 4). If the LED is flashing, the Router is actively sending or receiving data over that port.

Back Panel



POWER—The Power port is where you connect the AC power cable.

RESET—The Reset button has two functions.

- If pressed for one second, the Reset button causes a warm reboot—the Router restarts without losing any of the current configuration settings.
- If pressed for approximately 15 seconds, the Reset button resets the Router's factory defaults.

You can also restore the factory defaults from the *Administration > Factory Defaults* screen of the Router's Configuration Utility.

INTERNET—The Internet port connects to your cable or DSL modem.

1-4 (ETHERNET)—The four Ethernet ports connect to your PCs and other network devices.

Initial Installation

Follow the instructions below to connect the equipment and configure the Internet connection and wireless network.

- **“Placement Options” on page 9**
- **Connecting the Equipment, page 9**
- **Verifying the Hardware Installation, page 11**
- **Configuring the Internet Connection, page 12**

- [Securing the Wireless Network, page 13](#)

Placement Options

You can place the router horizontally on a desktop or mount it on the wall.

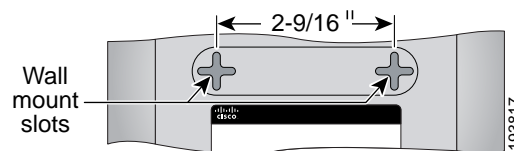
Desktop Option

For desktop placement, place the router horizontally on a surface so it sits on its four rubber feet.

Wall Option

To mount the router on the wall, follow these steps.

- STEP 1** Determine where you want to mount the router.
- STEP 2** Install two screws (not supplied) 2-9/16 in. apart (approximately 6.45 cm.) Leave about 1/8 in. (about 3 mm) of the head exposed.
- STEP 3** With the back panel pointing up (if installing vertically), position the router so that the wall-mount crisscross slots on the bottom panel line up with the two screws.



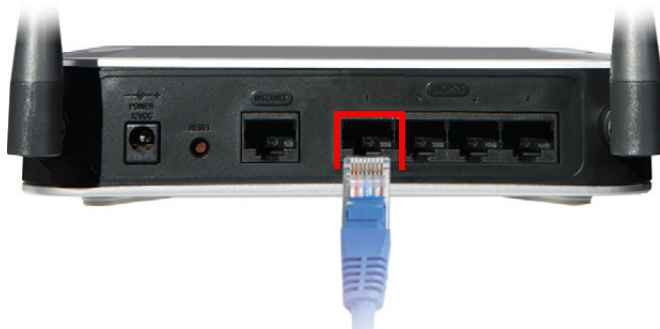
- STEP 4** Place the wall-mount slots over the screws and slide the router down until the screws fit snugly into the wall-mount slots.

Connecting the Equipment

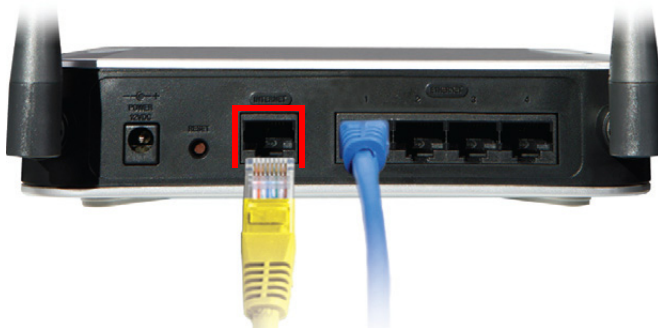
- STEP 1** Make sure that all of the network hardware is powered off, including the Router, PCs, and cable or DSL modem.
- STEP 2** Connect one end of an Ethernet network cable to one of the LAN ports (labeled 1-4) on the back of the Router, and the other end to an Ethernet port on a PC.



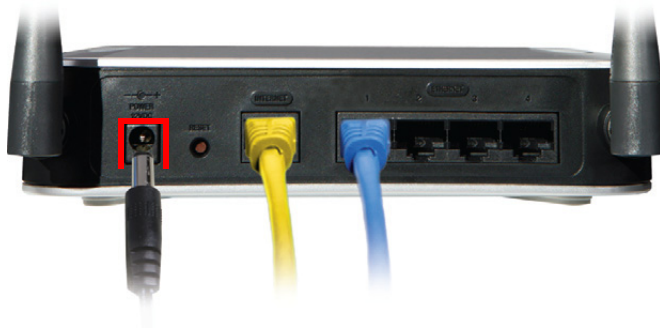
NOTE You must connect one computer with an Ethernet cable for the purpose of the initial configuration. After you complete the initial configuration, administrative tasks can be performed from a wireless connection.



STEP 3 Repeat the previous step to connect more PCs, a switch, or other network devices to the Router.



STEP 4 Connect an Ethernet network cable from the cable or DSL modem to the Internet port on the Router's back panel.



STEP 5 Power on the cable or DSL modem.

STEP 6 Connect the power adapter to the Router's Power port, and then plug the other end into an electrical outlet.



NOTE Use only the power adapter that is supplied with the Router. Using a different power adapter could damage the Router.

The Power and Internet LEDs on the front panel will light up green as soon as the power adapter is connected properly.

STEP 7 Power on the PCs.

The hardware installation is now complete.

Verifying the Hardware Installation

To verify the hardware installation, complete the following tasks:

- Check the cable connections.
- Check the LED states, as described in **Front Panel, page 7**.



NOTE If you need help resolving a problem, visit the Cisco Small Business Support Community at www.cisco.com/go/smallbizsupport. For technical documentation and other links, see **Appendix B, "Where to Go From Here."**

Configuring the Internet Connection

Before you begin, make sure that you have the setup information for the specific type of Internet connection. The installation technician from the Internet Service Provider (ISP) should have provided this information when installing the broadband connection. If not, call your ISP to request the settings.

- STEP 1** Using one of the PCs that you previously connected to LAN port on the back panel of the Router, start your web browser.



NOTE You must complete the initial installation from a PC that is physically connected to the Router. You cannot configure the Router from a PC that is connected wirelessly.

- STEP 2** To connect to the web-based Configuration Utility, enter **http://192.168.1.1** in the Address field, and press **Enter**.

A password request screen appears.

- STEP 3** In the User Name and Password fields, enter the default user name and password, admin, in lowercase letters. Then click **OK**.

For added security, you should later set a new password using the web-based Configuration Utility (Administration > Management).

The web-based Configuration Utility appears with the *Setup* tab selected.

- STEP 4** If requested by the ISP (usually cable ISPs), complete the Host Name and Domain Name fields, and the MTU and MTU Size fields. Otherwise, leave the default values.

- STEP 5** From the Internet Configuration Type drop-down menu, select a connection type, as described below.

- **Automatic Configuration DHCP:** If you are connecting through DHCP or a dynamic IP address from the ISP, keep this default setting.
- **Static IP:** If the ISP assigns you a static IP address, select Static IP from the drop-down menu. Complete the Internet IP Address, Subnet Mask, Default Gateway, and DNS fields. Enter at least one DNS address.
- **PPPoE:** If you are connecting through PPPoE, select PPPoE from the drop-down menu. Complete the User Name and Password fields.

- **PPTP:** PPTP is a service used in Europe only. If you are using a PPTP connection, check with the ISP for the necessary setup information.
- **L2TP:** L2TP is used mostly in Europe. Check with the ISP for the necessary setup information.
- **Heart Beat Signal:** Heart Beat Signal is a service used in Australia. Check with the ISP for the necessary setup information.

STEP 6 When you are finished entering the Internet connection settings, click **Save Settings** to save the changes.

STEP 7 Restart the computer.

STEP 8 To test the Internet connection, start a web browser on any connected computer and entering a valid website address, such as www.cisco.com.

Securing the Wireless Network

STEP 1 To choose the security options for your network, click **Wireless > Wireless Security** in the navigation tree.

STEP 2 From the **Select SSID** drop-down list, choose the SSID that you want to configure. You will need to repeat this procedure for each SSID that you enabled on the Basic Wireless Settings page.

STEP 3 Choose the **Security Mode**. Cisco recommends using the highest level of security that is supported by your network devices. Choose from the following options:

- **WEP:** Weak security with a basic encryption method that is not as secure as WPA. WEP may be required if your network devices do not support WPA.
- **WPA Personal:** Provides strong wireless security with advanced encryption. Choose **WPA Personal** (TKIP or AES encryption), **WPA2 Personal** (AES encryption), **WPA2 Personal Mixed** (TKIP or AES encryption).
- **WPA Enterprise:** Strong security using authentication by a RADIUS server that is connected to the router. Choose **WPA Enterprise** (TKIP or AES encryption), **WPA2 Enterprise** (AES), or **WPA2 Enterprise Mixed** (TKIP or AES encryption).

- **RADIUS (WEP):** Weak security (WEP) with a basic encryption method that is not as secure as WPA. WEP may be required if your network devices do not support WPA. Authentication is provided by a RADIUS server that is connected to the router.

STEP 4 From the **Wireless Isolation within SSID** drop-down list, choose **Enabled** to allow communication and file transfers between all wireless PCs that are connected to this SSID. This feature is useful when setting up a wireless hotspot location. Choose **Disabled** (the default option) to prevent communication and file transfers between the PCs.

STEP 5 In the final section of the page, enter the required information, based on the chosen security mode, as described below.

For WPA Enterprise modes and RADIUS (WEP) mode:

RADIUS Server IP Address:	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
RADIUS Server Port:	<input type="text" value="1812"/>

- **RADIUS Server IP Address:** Enter the IP address for the RADIUS server.
- **RADIUS Server Port:** Enter the port number for the RADIUS server.

For WPA Personal modes and WPA Enterprise modes:

Encryption:	<input type="text" value="TKIP"/>
Shared Secret:	<input type="text"/>
Key Renewal:	<input type="text" value="3600"/> seconds

- **Encryption:** For WPA Personal and WPA Enterprise, choose either TKIP or AES encryption. The encryption method is chosen automatically for the other WPA modes.
- **Shared Secret:** Enter 8-32 characters. The Shared Secret is also known as a Pre-Shared Key.
 - For WPA Personal, this key also must be configured in the wireless clients who want to connect to the network.
 - For WPA Enterprise and RADIUS, this key is shared between the router and the RADIUS server.

- **Key Renewal:** For all security modes except WEP, enter the interval in seconds. The Key Renewal instructs the router how often it should change the encryption keys. The default is 3600 seconds, which is 1 hour.

For WEP mode and RADIUS (WEP) mode:

The screenshot shows a configuration interface for WEP. It includes the following fields and options:

- Authentication Type:** A dropdown menu currently set to "Open System".
- Default Transmit Key:** Four radio buttons labeled 1, 2, 3, and 4. Radio button 1 is selected.
- Encryption:** A dropdown menu currently set to "64 bits". To the right of the dropdown is the text "(10 hex digits or 5 ASCII characters)".
- Passphrase:** A text input field followed by a "Generate" button.
- Key 1:** A text input field.
- Key 2:** A text input field.
- Key 3:** A text input field.
- Key 4:** A text input field.

- **Authentication Type:** Choose one of the following options:
 - **Open System:** A wireless client doesn't need to provide a shared key in order to access the wireless network. Any client can associate to the router.
 - **Share Key:** A wireless client must provide the correct shared key in order to access the wireless network.
- **Default Transmit Key:** To indicate which WEP key to use, select the appropriate Default Transmit Key number.
- **Encryption:** Choose the level of WEP encryption, 64 bits (10 hex digits) or 128 bits (26 hex digits). Higher encryption levels offer higher levels of security, but due to the complexity of the encryption, they may decrease network performance.
- **Passphrase:** If you want to generate a key instead of entering a key manually, type a passphrase in the field. You can enter up to 32 alphanumeric characters. Then click **Generate**. A valid key appears in each of the Key 1 - Key 4 fields.
- **Key 1 - Key 4:** If you did not use the Generate feature, enter a valid WEP key. Do not leave a field blank, and do not enter all zeroes; they are not valid key values.
 - If you chose 64-bit WEP encryption, the key must be exactly 10 hexadecimal characters in length.

- If you chose 128-bit WEP encryption, the key must be exactly 26 hexadecimal characters in length. Valid hexadecimal characters are “0” to “9” and “A” to “F”.

STEP 6 Keep the default values for all other settings.

STEP 7 Click **Save** to save the changes.

STEP 8 To test the wireless setup, use the wireless client on any computer to enter the correct SSID and shared key for your wireless network. Verify that you can connect by entering a website address, such as www.cisco.com.

Congratulations! The installation of the Wireless-G VPN router with RangeBooster is complete. Use this Administration Guide to configure other settings, as needed.

Getting Started in the Configuration Utility

Logging In

To access the Configuration Utility, launch Internet Explorer or Firefox, and enter the Router's default IP address, **192.168.1.1**, in the Address field. Then press **Enter**.



NOTE

The default IP address is **192.168.1.1**. If the IP address has been changed, enter the assigned IP address instead.

A password request page appears. (Windows XP users see a similar screen.) The first time you open the Configuration Utility, enter the default login information, as shown below, and then click **OK**.

- **User Name:** admin
- **Password:** admin



NOTE

You can change the password later from the Administration > Management page. See “**Managing Access and Configuring Other Management Options**” on page 80.

After you log in, the Configuration Utility displays the Setup > Basic Settings page.

Navigating through the Pages

Use the navigation tree in the left pane to open the configuration pages.

Saving Your Changes

When you finish making changes on a configuration page, click **Save** to save the changes, or click **Cancel** to undo your changes.

Viewing the Help Files

To view more information about a configuration page, click the **Help** link near the top right corner of the page.

Setting Up the Network

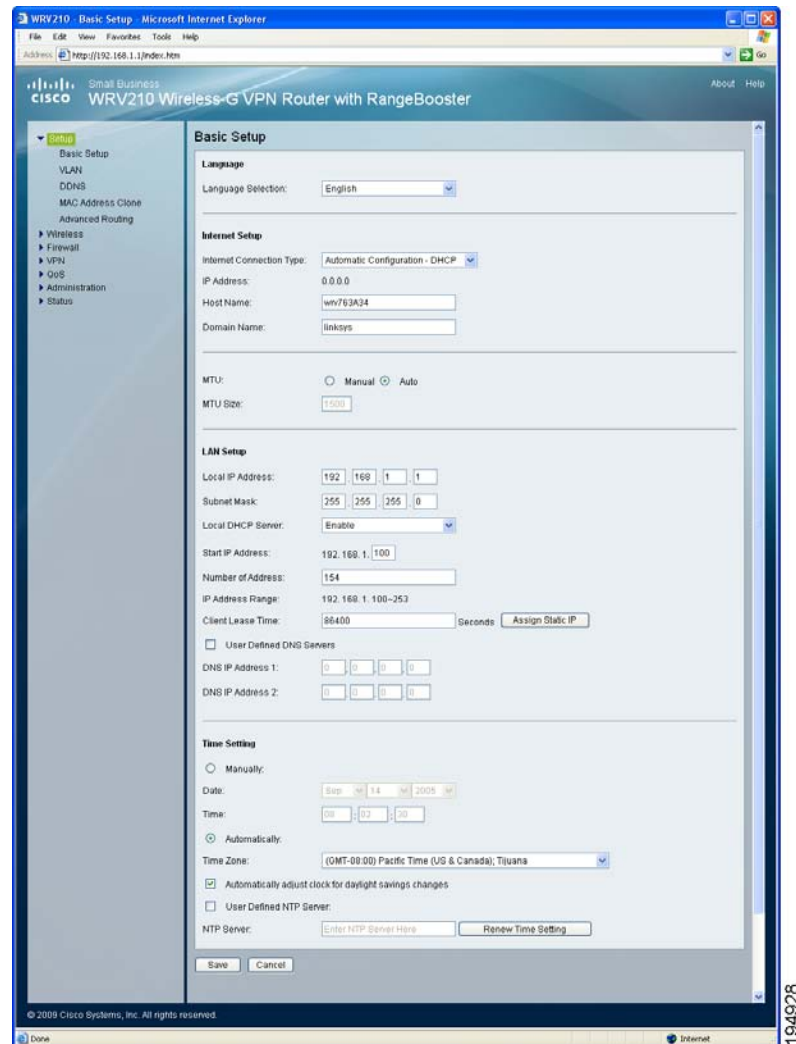
Use the Setup module to configure the Internet connection, local network settings, VLANs, DDNS, MAC Address cloning, and advanced routing.

- [Configuring the Basic Settings, page 18](#)
- [Setting Up Virtual LANs, page 25](#)
- [Using DDNS to Map Domain Names to Your Network, page 26](#)
- [Cloning a MAC Address for Your Internet Connection, page 29](#)
- [Setting Up Advanced Routing, page 30](#)

Configuring the Basic Settings

Use the Setup > Basic Settings page to perform the following basic tasks:

- [“Localizing the Configuration Utility” on page 19](#)
- [“Setting Up the Internet Connection” on page 20](#)
- [“Setting Up the Local Network” on page 23](#)
- [“Adjusting the Time Settings” on page 24](#)



Localizing the Configuration Utility

You can change the language that appears on the configuration pages.

STEP 1 Click **Setup > Basic Settings** in the navigation tree.

STEP 2 From the **Language Selection** drop-down list, choose one of the following languages: **English** (default), **French**, **German**, **Italian**, **Portuguese**, or **Spanish**.

- STEP 3** Click **Save** to save your settings, or click **Cancel** to refresh the page with the previously saved settings.
—OR— Complete other sections of the Basic Settings page before saving your settings.

Setting Up the Internet Connection

Use the information provided by your ISP to configure your Internet Connection.

-
- STEP 1** Click **Setup > Basic Settings** in the navigation tree.
- STEP 2** In the **Internet Setup** section, choose the Internet Connection Type required by your ISP. Then enter the required information for the selected connection. The Router supports six types of connections, as described below.
- **Automatic Configuration - DHCP:** Select this option if your ISP supports DHCP or you are connecting through a dynamic IP address. This option is selected by default.
 - **Static IP:** If your ISP provided you with a permanent (public) IP address, then select **Static IP**. Also enter the following information, as provided by your ISP:
 - **IP Address:** Enter the IP address that your ISP provided to you.
 - **Subnet Mask:** Enter the Router's Subnet Mask, as seen by external users on the Internet (including your ISP).
 - **Default Gateway:** Enter the Default Gateway Address, which is the ISP server's IP address.
 - **Primary DNS (Required) and Secondary DNS (Optional):** Enter at least one DNS (Domain Name System) Server IP Address.
 - **PPPoE:** This type of connection is required by some DSL-based ISPs. Enter the following information, as provided by your ISP:
 - **Account to be Used:** You can have dual PPPoE profiles to allow easy switching between two separate PPPoE accounts. Select either **Primary** (default) or **Secondary**. Then configure the settings for the selected profile.

- **User Name and Password/Confirm Password:** Enter the User Name and the Password provided by your ISP. Then, enter the password again to confirm it.
- **Service Name:** If your service provider has given you this information, enter it in this field. If you are not sure if your service provider requires this information, or if you do not know the service name, leave this field blank.
- **Connect on Demand and Max Idle Time:** You can configure the Router to disconnect the Internet connection after it has been inactive for a specified period of time (Max Idle Time). The Router automatically re-establishes the connection when a user attempts to access the Internet again. If you select this option, specify the Max Idle Time by entering the number of seconds of inactivity that can elapse before the Internet connection is terminated automatically.
- **Keep Alive:** Select this option to enable the Router to periodically check your Internet connection. If you are disconnected, then the Router automatically re-establishes your connection.
- **PPTP:** Point-to-Point Tunneling Protocol (PPTP) is a service that applies to connections in Europe and Israel. Enter the following information, as provided by your ISP:
 - **IP Address:** Enter the IP address that your ISP provided to you.
 - **Subnet Mask:** Enter the Router's Subnet Mask, as seen by external users on the Internet (including your ISP).
 - **Default Gateway:** Enter the Default Gateway Address, which is the ISP server's IP address.
 - **PPTP Server IP:** Enter the IP address of the ISP's PPTP server.
 - **User Name and Password:** Enter the User Name and Password provided by your ISP.
 - **Connect on Demand and Max Idle Time:** You can configure the Router to disconnect the Internet connection after it has been inactive for a specified period of time (Max Idle Time). The Router automatically re-establishes the connection when a user attempts to access the Internet again. If you select this option, specify the Max Idle Time by entering the number of seconds of inactivity that can elapse before the Internet connection is terminated automatically.

- **Keep Alive:** Select this option to enable the Router to periodically check your Internet connection. If you are disconnected, then the Router automatically re-establishes your connection.
- **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. Enter the following information, as provided by your ISP:
 - **IP Address:** Enter the IP address that your ISP provided to you.
 - **Subnet Mask:** Enter the Router's Subnet Mask, as seen by external users on the Internet (including your ISP).
 - **Default Gateway:** Enter the Default Gateway Address, which is the ISP server's IP address.
 - **L2TP Server IP:** Enter the IP address of the L2TP server.
 - **User Name and Password:** Enter the User Name and Password provided by your ISP.
 - **Connect on Demand and Max Idle Time:** You can configure the Router to disconnect the Internet connection after it has been inactive for a specified period of time (Max Idle Time). The Router automatically re-establishes the connection when a user attempts to access the Internet again. If you select this option, specify the Max Idle Time by entering the number of seconds of inactivity that can elapse before the Internet connection is terminated automatically.
 - **Keep Alive:** Select this option to enable the Router to periodically check your Internet connection. If you are disconnected, then the Router automatically re-establishes your connection.
- **Heart Beat Signal:** Heart Beat Signal is a service used in Australia. Enter the following information, as provided by your ISP:
 - **User Name and Password:** Enter the User Name and Password provided by your ISP.
 - **Authentication Server:** Enter the IP address of the Heart Beat authentication server.

STEP 3 If required by your ISP, enter the following information in the Optional Settings section. Verify with your ISP before making any changes.

- **Host Name and Domain Name:** Some ISPs require these names as identification. In most cases, you can leave these fields blank.

- **MTU:** The MTU (Maximum Transmission Unit) setting specifies the largest packet size permitted for network transmission. Select **Enabled** and enter the value desired. It is recommended that you leave this value in the 1200 to 1500 range. For most DSL users, it is recommended to use the value 1492. By default, MTU is set at **1500** when disabled.
- **MTU Size:** When **Manual** is selected in the MTU field, this option is enabled. It is recommended that you set this value within the range of 1200 to 1500, but the value can be defined between 128 and 1500.

STEP 4 Click **Save** to save your settings, or click **Cancel** to refresh the page with the previously saved settings.
—OR— Complete other sections of the Basic Settings page before saving your settings.

Setting Up the Local Network

STEP 1 Click **Setup > Basic Settings** in the navigation tree.

STEP 2 In the **LAN Setup** section, configure the Router's local network settings. In most cases, you can keep the defaults.

- **Local IP Address:** Enter the IP address for the router on your network. The default address is 192.168.1.1.
- **Subnet Mask:** Enter the subnet mask for your network. The default value is 255.255.255.0.
- **Local DHCP Server:** The Router can be used as your network's DHCP (Dynamic Host Configuration Protocol) server, which automatically assigns an IP address to each connected device. Unless you already have a DHCP server, it is highly recommended that you enable the DHCP server. This is the default setting. If you already have a DHCP server on your network, choose **Disabled**. If you disable DHCP, use the other router's configuration utility to assign a static IP address to the WRV210.
- **Start IP Address:** Enter the first IP address in the range of addresses that are assigned by the DHCP server. Assuming that you are using the default router IP address of 192.168.1.1, the Start IP address must be greater than 192.168.1.1 but smaller than 192.168.1.255, which is reserved as the broadcast IP address.

- **Number of Address:** Enter the maximum number of PCs that you want the DHCP server to assign IP addresses. This number cannot be greater than 253. The IP Address Range is determined by adding this number to the Start IP Address.
- **IP Address Range:** The range of DHCP addresses that will be assigned, based on your entries in the Start IP Address field and the Number of Address field.
- **Client Lease Time:** Enter the number of seconds that a DHCP client can keep an assigned IP address before it sends a renewal request to the DHCP server. The default value is 86400 seconds, which is 24 hours.
- **Assign Static IP:** Click this button if you need to assign fixed IP addresses to particular network devices. When the Static Table appears, enter the Static IP Address and the MAC address of the device, then click **Add**. To edit an entry, highlight the entry in the table, click **Edit**, make your changes in the fields, then click **Add**. To remove an entry, highlight the entry, then click **Remove**.
- **User Defined DNS Servers:** Check this box if you want to specify particular DNS servers for your network. Then enter the DNS IP addresses in the spaces provided.

STEP 3 Click **Save** to save your settings, or click **Cancel** to refresh the page with the previously saved settings.
—OR— Complete other sections of the Basic Settings page before saving your settings.

Adjusting the Time Settings

STEP 1 Click **Setup > Basic Settings** in the navigation tree.

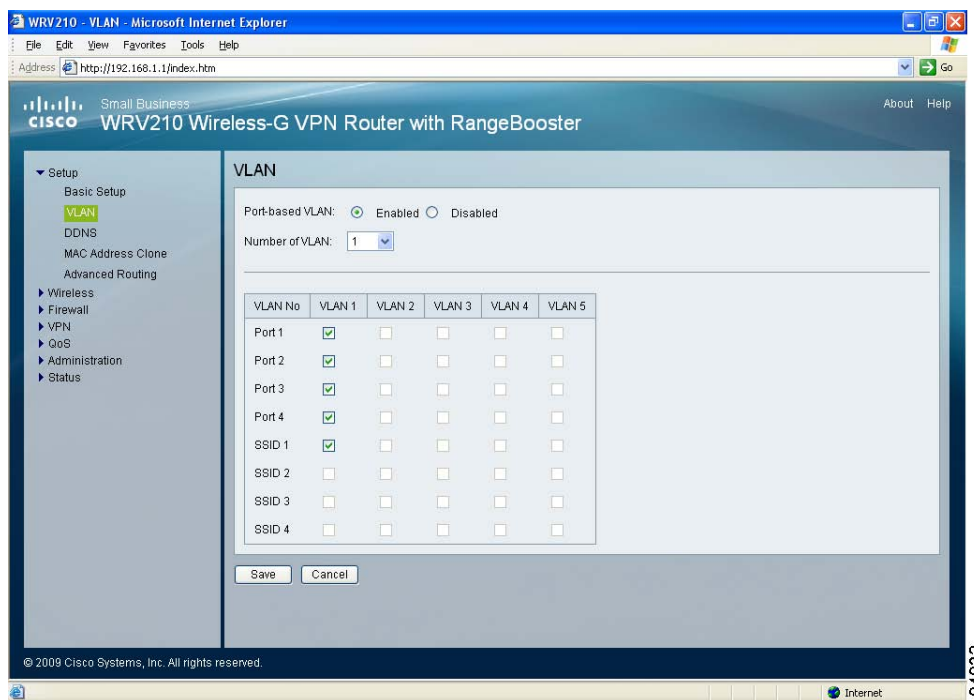
STEP 2 In the Time Configuration section, enter the following information:

- **Manually:** Select the date from the Date drop-down menus. Then enter the time in the Time fields.
- **Automatically:** Select your time zone from the Time Zone drop-down menu. If you want to enable the Automatic Daylight Savings feature, click **Automatically adjust clock for daylight savings changes**. If you want to use a Network Time Protocol (NTP) server to set the time automatically, click **User Define NTP Server**, then enter the IP address of the NTP server in the field.

- STEP 3** Click **Save** to save your settings, or click **Cancel** to refresh the page with the previously saved settings.
—OR— Complete other sections of the Basic Settings page before saving your settings.

Setting Up Virtual LANs

You can create virtual LANs (VLANs) on each port of the Router. Each VLAN is a separate subnet.



- STEP 1** Click **Setup > VLAN** in the navigation tree.

- STEP 2** Enter the following information:

- **Port-based VLAN:** Select **Enabled** to enable the feature. When enabled, and a VLAN is selected, VLAN1 is enabled as a default VLAN, so you have two VLANs. Select **Disabled** to disable the feature. When this feature is disabled, all LAN ports are on the same LAN.

- **Number of VLAN:** Select the number of the VLAN from the drop-down menu.
- **VLAN No.:** Select the VLAN number to associate with the desired port.

STEP 3 Click **Save** to save your settings, or click **Cancel** to refresh the page with the previously saved settings.

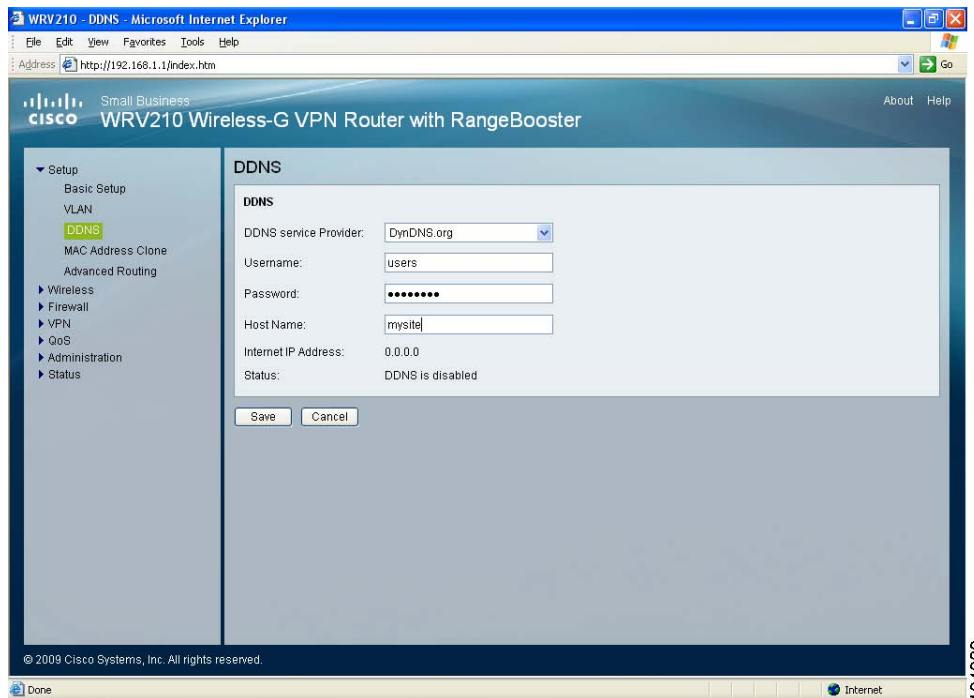
Using DDNS to Map Domain Names to Your Network

The Router offers a Dynamic Domain Name System (DDNS) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other server behind the Router and your ISP does not give you a fixed IP address.

Before you can use this feature, you need to sign up for DDNS service at one of two DDNS service providers, DynDNS.org or TZO.com.

- [DynDNS.org Setup, page 27](#)
- [TZO.com Setup, page 28](#)

DynDNS.org Setup



STEP 1 Click **Setup > DDNS** in the navigation tree.

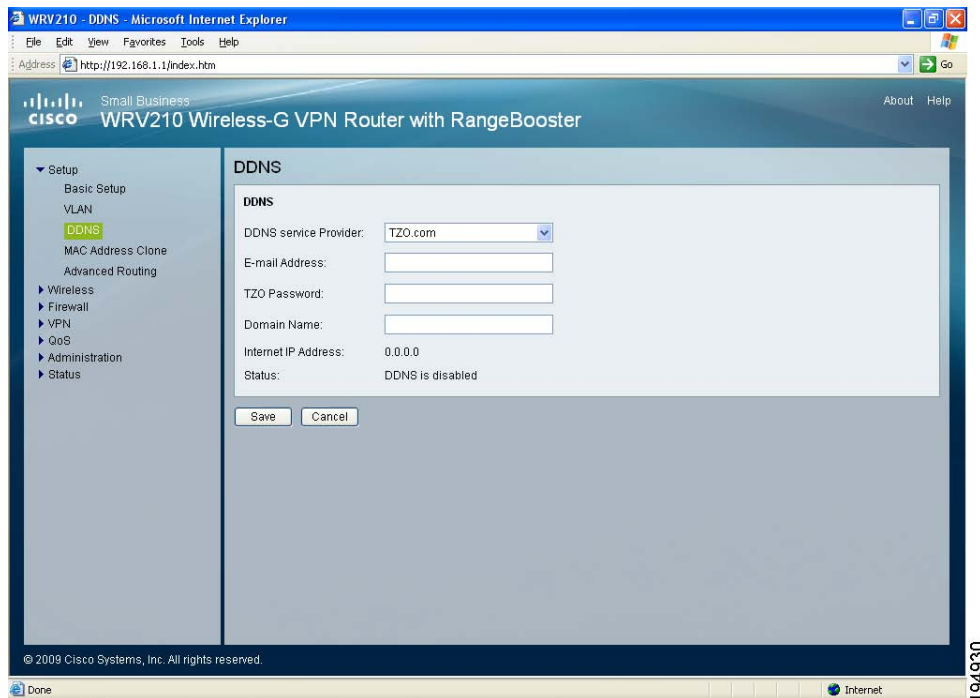
STEP 2 From the **DDNS Service Provider** drop-down list, choose **DynDNS.org**.

STEP 3 Enter the following information:

- **User Name, Password, and Host Name:** Enter the User Name, Password, and Host Name of the account you set up with DynDNS.org.
- **Internet IP Address:** The Router's current Internet IP Address is displayed here. Because it is dynamic, it changes.
- **Status:** The status of the DDNS service connection is displayed here.

STEP 4 Click **Save** to save your settings, or click **Cancel** to refresh the page with the previously saved settings.

TZO.com Setup



STEP 1 Click **Setup > DDNS** in the navigation tree.

STEP 2 From the **DDNS Service Provider** drop-down list, choose **TZO.com**.

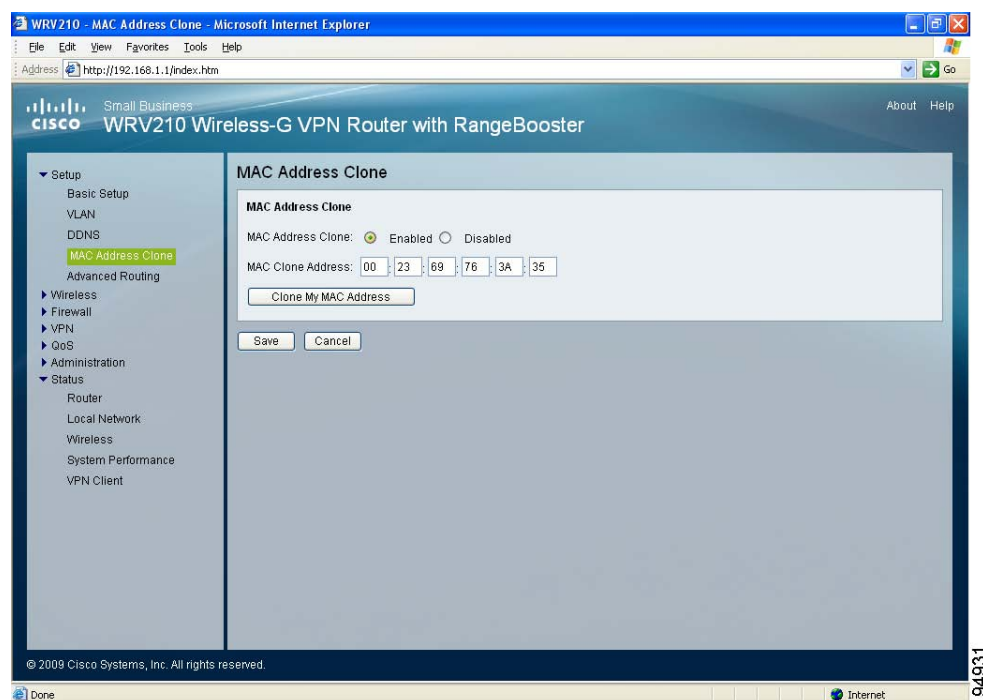
STEP 3 Enter the following information:

- **Email, TZO Password Key, and Domain Name:** Enter the E-mail Address, TZO Password Key, and Domain Name of the service you set up with TZO.
- **Internet IP Address:** The Router's current Internet IP Address is displayed here. Because it is dynamic, it changes.
- **Status:** The status of the DDNS service connection is displayed here.

STEP 4 Click **Save** to save your settings, or click **Cancel** to refresh the page with the previously saved settings.

Cloning a MAC Address for Your Internet Connection

Some ISPs require that you register a MAC address, which is a unique 12-digit code assigned to a network device for identification. If you previously registered a different router's MAC address with your ISP, you can use the MAC Address Clone feature to associate the registered MAC address with your WRV210 Router. This feature saves you the trouble of contacting your ISP to change the registered MAC address to the Router's MAC address.



STEP 1 Click **Setup > MAC Address Clone** in the navigation tree.

STEP 2 To use MAC address cloning, select **Enabled** in the **MAC Address Clone** field.

STEP 3 Enter the following information:

- **MAC Clone Address:** Enter the MAC Address that is registered with your ISP for your Internet account.
- **Clone My MAC Address:** Click this button if you want to clone the MAC address of the PC you are currently using to configure the Router. The Router automatically detects your PC's MAC address. You do not have to call your ISP to change the registered MAC address to the Router's MAC

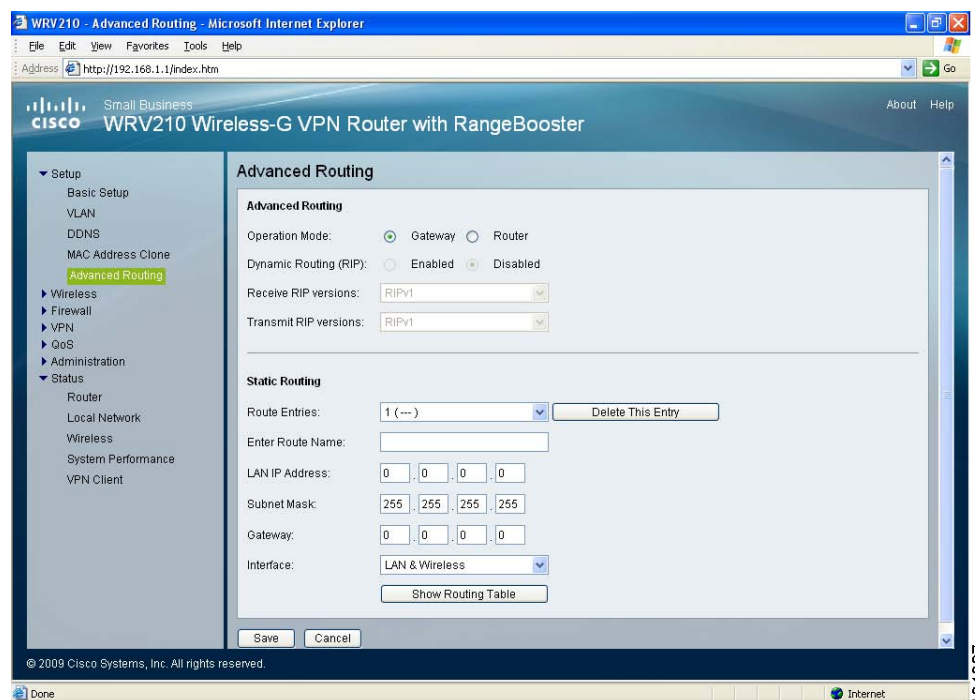
address. It is recommended to use the PC registered with the ISP for this operation.

- STEP 4** Click **Save** to save your settings, or click **Cancel** to refresh the page with the previously saved settings.

Setting Up Advanced Routing

Use the Advanced Routing page to configure dynamic routing and static routing.

- [Configuring Dynamic Routing, page 31](#)
- [Setting Up Static Routing, page 32](#)



Configuring Dynamic Routing

If another router on your network is hosting your Internet connection, you can configure dynamic routing. The Router, using the RIP protocol, determines the network packets' route based on the fewest number of hops between the source and the destination. The RIP protocol regularly broadcasts routing information to other routers on the network.

STEP 1 Click **Setup > Advanced Routing** in the navigation tree.

STEP 2 To support dynamic routing, change the **Operation Mode** to **Router**. This selection indicates that another router on your network hosts your Internet connection.



NOTE If this Router is hosting your network's connection to the Internet, leave the default selection, **Gateway**. This setting enables NAT (Network Address Translation) to map your private network addresses to the IP address that is provided by your ISP. This setting does not allow dynamic routing.

STEP 3 In the **Dynamic Routing** field, click **Enabled** to allow the Router to automatically adjust to physical changes in the network's layout.

STEP 4 Configure the following settings:

- **Receive RIP Versions:** To use dynamic routing when receiving network data, select a protocol: RIPv1 or RIPv2.
- **Transmit RIP Versions:** To use dynamic routing when transmitting network data, select a protocol: RIPv1 or RIPv2.

STEP 5 Click **Save** to save your settings, or click **Cancel** to refresh the page with the previously saved settings.

Setting Up Static Routing

You can configure static routes to direct packets to the destination network. A static route is a pre-determined pathway that a packet must travel to reach a specific host or network.

STEP 1 Click **Setup > Advanced Routing** in the navigation tree.

STEP 2 In the **Static Routing** section, enter the following information:

- **Route Entries:** From the drop-down list, select the identification number of the static route that you want to set up. You can create up to five static route entries.



NOTE To delete a static route, select it from the drop-down list, and then click **Delete This Entry**.

- **Enter Route Name:** Enter a descriptive name for this route.
- **LAN IP Address:** Enter the address of the remote network or host to which you want to assign this static route. If you are building a route to an entire network, be sure that the network portion of the IP address is set to 0. For example, the Router's standard IP address is 192.168.1.1. Based on this address, the address of the routed network is 192.168.1, with the last digit determining the Router's place on the network. Therefore you would enter the IP address 192.168.1.0 if you wanted to route to the Router's entire network, rather than just to the Router.
- **Subnet Mask:** Enter the subnet mask (also known as Network Mask). This mask determines which portion of an IP address is the network portion, and which portion is the host portion. Take, for example, a network in which the subnet mask is 255.255.255.0. This determines (by using the values 255) that the first three numbers of a network IP address identify this particular network, while the last digit (from 1 to 254) identifies the specific host.
- **Gateway:** Enter the IP address of the gateway device that allows for contact between the Router and the remote network or host.
- **Interface:** Select the interface that is used to connect to the destination. Choose one of the following options:
 - **LAN & Wireless:** The destination device is connected to your LAN or wireless network.

- **Internet:** The destination device is on a network that you reach through your Internet connection.
- **Show Routing Table:** Click the **Show Routing Table** button to open a screen displaying how packets are routed through your local network. For each route, the Destination LAN IP address, Subnet Mask, Gateway, and Interface are displayed. Click **Refresh** to update the information. Click **Close** to exit this screen.

STEP 3 Click **Save** to save your settings, or click **Cancel** to refresh the page with the previously saved settings.

Configuring the Wireless Network

Use the Wireless module to configure your wireless network.

- [“A Note About Wireless Security” on page 34](#)
- [“Enabling Your Wireless Networks” on page 37](#)
- [“Adjusting the Advanced Wireless Settings” on page 45](#)
- [“Configuring a Wireless Distribution System \(WDS\)” on page 47](#)

A Note About Wireless Security

Wireless networks are convenient and easy to install, so homes with high-speed Internet access are adopting them at a rapid pace. Because wireless networking operates by sending information over radio waves, it can be more vulnerable to intruders than a traditional wired network. Like signals from your cellular or cordless phones, signals from your wireless network can also be intercepted. The following information will help you to improve your security:

- [“Wireless Security Tips” on page 34](#)
- [“General Network Security Guidelines” on page 36](#)

Wireless Security Tips

Since you cannot physically prevent someone from connecting to your wireless network, you need to take some additional steps to keep your network secure.

- Change the default wireless network name or SSID

Wireless devices have a default wireless network name or Service Set Identifier (SSID) set by the factory. This is the name of your wireless network, and can be up to 32 characters in length. Linksys wireless products use linksys as the default wireless network name. You should change the wireless network name to something unique to distinguish your

wireless network from other wireless networks that may exist around you, but do not use personal information (such as your Social Security number) because this information may be available for anyone to see when browsing for wireless networks.

- Change the default password

For wireless products such as access points, routers, and gateways, you will be asked for a password when you want to change their settings. These devices have a default password set by the factory. The Linksys default password is admin. Hackers know these defaults and may try to use them to access your wireless device and change your network settings. To thwart any unauthorized changes, customize the device's password so it will be hard to guess.

- Enable MAC address filtering

Linksys routers and gateways give you the ability to enable Media Access Control (MAC) address filtering. The MAC address is a unique series of numbers and letters assigned to every networking device. With MAC address filtering enabled, wireless network access is provided solely for wireless devices with specific MAC addresses. For example, you can specify the MAC address of each computer in your home so that only those computers can access your wireless network.

- Enable encryption

Encryption protects data transmitted over a wireless network. Wi-Fi Protected Access (WPA/WPA2) and Wired Equivalency Privacy (WEP) offer different levels of security for wireless communication. Currently, devices that are Wi-Fi certified are required to support WPA2, but are not required to support WEP.

A network encrypted with WPA/WPA2 is more secure than a network encrypted with WEP, because WPA/WPA2 uses dynamic key encryption. To protect the information as it passes over the airwaves, you should enable the highest level of encryption supported by your network equipment.

WEP is an older encryption standard and may be the only option available on some older devices that do not support WPA.

- Keep wireless routers, access points, or gateways away from exterior walls and windows.

- Turn wireless routers, access points, or gateways off when they are not being used (at night, during vacations).
- Use strong passphrases that are at least eight characters in length. Combine letters and numbers to avoid using standard words that can be found in the dictionary.

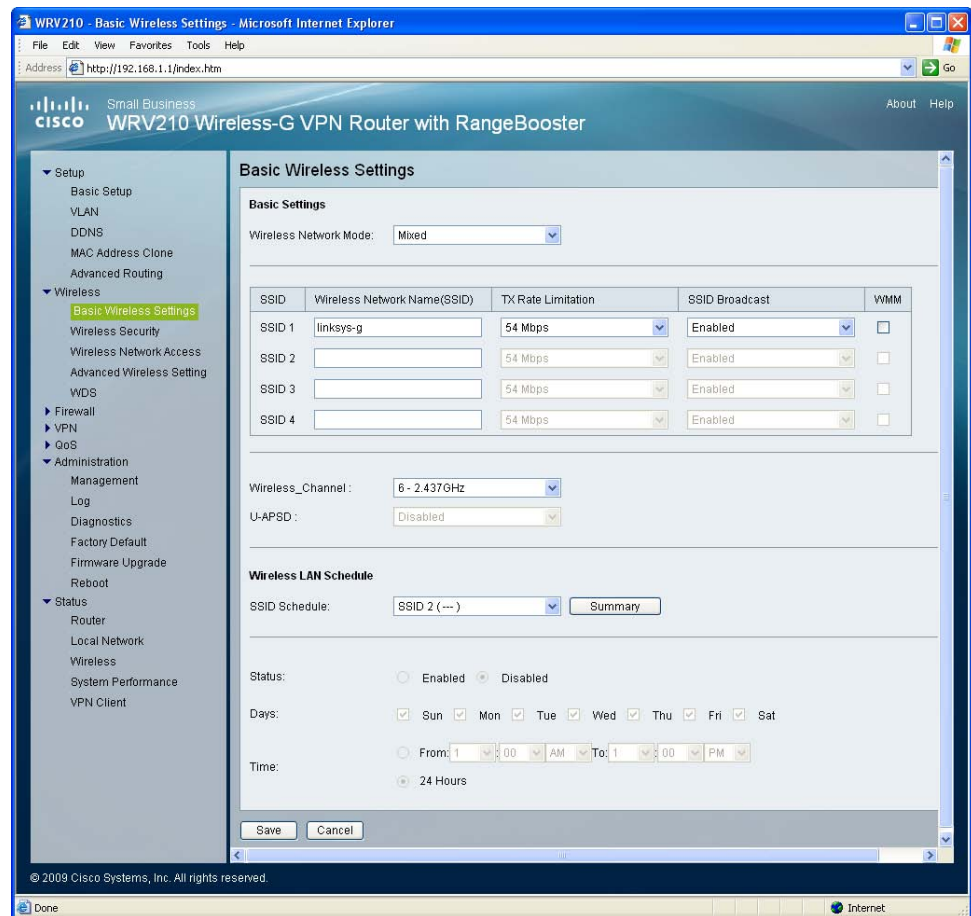
General Network Security Guidelines

Wireless network security is useless if the underlying network is not secure. Cisco recommends that you take the following precautions:

- Password protect all computers on the network and individually password protect sensitive files.
- Change passwords on a regular basis.
- Install anti-virus software and personal firewall software.
- Disable file sharing (peer-to-peer). Some applications may open file sharing without your consent and/or knowledge.

Enabling Your Wireless Networks

Use the Basic Wireless Settings page to configure the wireless network mode, the SSIDs, the channels, and the schedules for up to four wireless networks. You may wish to set up multiple networks to segment the network traffic, to allow different levels of access, such as guest access, or to allow access for different functions such as accounting, billing, and so on.



STEP 1 Click **Wireless > Basic Wireless Settings** in the navigation tree.

STEP 2 From the **Wireless Network Mode** drop-down list, choose the wireless standards running on your network.

- **Mixed:** Choose this option if you have both 802.11g and 802.11b devices in your network.

- **G-Only:** Choose this option if you have only 802.11g devices in your network.
- **B-Only:** Choose this option if you have only 802.11b devices in your network.
- **Disable:** Choose this option if there are no 802.11g or 802.11b devices and you do not wish to enable the wireless network.

STEP 3 In the SSID section, configure up to four wireless networks by entering the SSID (network name) and other settings:

- **Wireless Network Name (SSID):** Enter a unique name for this wireless network. Include up to 32 characters, using any of the characters on the keyboard. For added security, you should change the default SSID1 (ciscosb) to a unique name.
- **TX Rate Limitation:** Choose the rate of data transmission. The Router negotiates the connection speed between the Router and a wireless client by this rate.
- **SSID Broadcast:** Enable this feature if you want to allow all wireless clients within range to be able to detect this wireless network when they are scanning the local area for available networks. Disable this feature if you do not want to make the SSID known. When this feature is disabled, wireless users can connect to your wireless network only if they know the SSID (and provide the required security credentials).
- **WMM:** Check this box if you want to enable WMM (Wi-Fi Multimedia). This feature prioritizes traffic for voice and media applications, such as Wi-Fi phones.
- **Wireless Channel:** Select the appropriate channel from the drop-down menu. All devices in your wireless network must transmit using the same channel in order to function correctly. You may need to change the wireless channel to improve the communication quality if there is interference from nearby wireless access points.
- **U-APSD:** Select **Enable** if you want to use the Unscheduled Automatic Power Save Delivery (U-APSD) feature to conserve power.

STEP 4 In the **Wireless LAN Schedule**, set up schedules when your the SSID2-SSID4 networks are available.



NOTE

SSID 1 is the default and is always operational, unless the *Wireless Network Mode* option is set to **Disable**.

- **SSID Schedule:** Select the SSID that you want to operate according to this schedule.
- **Summary:** Click this button to display a list of all currently defined schedules.
- **Status:** Select **Enabled** to activate the SSID schedule feature for the selected SSID.
- **Days:** Check the box for each day when the wireless network is available. Uncheck the box for each day when the network is unavailable.
- **Time:** Use the drop-down lists to set the range of times when the network is available. In the following example, the network is enabled from 8 a.m. to 5 p.m., Monday through Friday and is unavailable on Saturday and Sunday.

Status: ☒ Enabled ☐ Disabled

Days: ☐ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☐ Sat

Time: ☒ From: 8 : 00 AM To: 5 : 00 PM ☐ 24 Hours

STEP 5 Click **Save** to save your settings, or click **Cancel** to refresh the page with the previously saved settings.

Wireless > Wireless Security

The Wireless Security settings configure the security of your wireless network. There are eight wireless security mode options supported by the Router: WPA-Personal, WPA2-Personal, WPA Enterprise, WPA2 Enterprise, WPA2-Personal-Mixed, WPA2-Enterprise Mixed, RADIUS, and WEP.

WPA (Wi-Fi Protected Access) is a stronger security standard than WEP (Wired Equivalent Privacy). RADIUS (Remote Authentication Dial-In User Service) can be used with either WPA or WEP to authenticate users from a database on a RADIUS server. For detailed instructions on configuring wireless security for the Router, see **[“A Note About Wireless Security” on page 34.](#)**



NOTE

If you configured multiple networks (SSIDs), repeat this procedure for each one.

- STEP 1** Click **Wireless > Wireless Security** in the navigation tree.
- STEP 2** From the **Select SSID** drop-down list, choose the SSID for the network that you want to configure.
- STEP 3** From the **Security Mode** drop-down list, select the appropriate security mode for your network. All devices on your network must use the same security mode and settings to work correctly. Cisco recommends using the highest level of security that is supported by the devices in your network.
- **WPA Personal:** Provides strong wireless security with advanced encryption. Choose **WPA Personal** (TKIP or AES encryption), **WPA2 Personal** (AES encryption), **WPA2 Personal Mixed** (TKIP or AES encryption).
 - **WPA Enterprise:** Strong security using authentication by a RADIUS server that is connected to the Router. Choose **WPA Enterprise** (TKIP or AES encryption), **WPA2 Enterprise** (AES), or **WPA2 Enterprise Mixed** (TKIP or AES encryption).
 - **RADIUS (WEP):** Weak security (WEP) with a basic encryption method that is not as secure as WPA. WEP may be required if your network devices do not support WPA. Authentication is provided by a RADIUS server that is connected to the Router.
 - **WEP:** Weak security with a basic encryption method that is not as secure as WPA. WEP may be required if your network devices do not support WPA.
- STEP 4** From the **Wireless Isolation within SSID** drop-down list, choose **Enabled** to allow communication and file transfers between all wireless PCs that are connected to this SSID. This feature is useful when setting up a wireless hotspot location. Choose **Disabled** (the default option) to prevent communication and file transfers between the PCs.
- STEP 5** Enter the required information, based on the chosen mode:

For WPA Enterprise modes and RADIUS (WEP) mode:

RADIUS Server IP Address:	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
RADIUS Server Port:	<input type="text" value="1812"/>

- **RADIUS Server IP Address:** Enter the IP address for the RADIUS server.
- **RADIUS Server Port:** Enter the port number for the RADIUS server.

For WPA Personal modes and WPA Enterprise modes:

Encryption:	TKIP	▼
Shared Secret:	<input type="text"/>	
Key Renewal:	3600	seconds

- **Encryption:** For WPA Personal and WPA Enterprise, choose either TKIP or AES encryption. The encryption method is chosen automatically for the other WPA modes.
- **Shared Secret:** Enter 8-32 characters. The Shared Secret is also known as a Pre-Shared Key.
 - For WPA Personal, this key also must be configured in the wireless clients who want to connect to the network.
 - For WPA Enterprise and RADIUS, this key is shared between the Router and the RADIUS server.
- **Key Renewal:** For all security modes except WEP, enter the interval in seconds. The Key Renewal instructs the Router how often it should change the encryption keys. The default is 3600 seconds, which is 1 hour.

For WEP mode and RADIUS (WEP) mode:

Authentication Type:	Open System	▼
Default Transmit Key:	<input checked="" type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4	
Encryption:	64 bits	▼ (10 hex digits or 5 ASCII characters)
Passphrase:	<input type="text"/>	<input type="button" value="Generate"/>
Key 1:	<input type="text"/>	
Key 2:	<input type="text"/>	
Key 3:	<input type="text"/>	
Key 4:	<input type="text"/>	

- **Authentication Type:** Choose one of the following options:
 - **Open System:** A wireless client doesn't need to provide a shared key in order to access the wireless network. Any client can associate to the router.

- **Share Key:** A wireless client must provide the correct shared key in order to access the wireless network.
 - **Default Transmit Key:** To indicate which WEP key to use, select the appropriate Default Transmit Key number.
 - **Encryption:** Choose the level of WEP encryption, 64 bits (10 hex digits) or 128 bits (26 hex digits). Higher encryption levels offer higher levels of security, but due to the complexity of the encryption, they may decrease network performance.
 - **Passphrase:** If you want to generate a key instead of entering a key manually, type a passphrase in the field. You can enter up to 32 alphanumeric characters. Then click **Generate**. A valid key appears in each of the Key 1 - Key 4 fields.
 - **Key 1 - Key 4:** If you did not use the Generate feature, enter a valid WEP key. Do not leave a field blank, and do not enter all zeroes; they are not valid key values.
 - If you chose 64-bit WEP encryption, the key must be exactly 10 hexadecimal characters in length.
 - If you chose 128-bit WEP encryption, the key must be exactly 26 hexadecimal characters in length. Valid hexadecimal characters are “0” to “9” and “A” to “F”.
- STEP 6** Click **Save** to save your settings, or click **Cancel** to refresh the page with the previously saved settings.

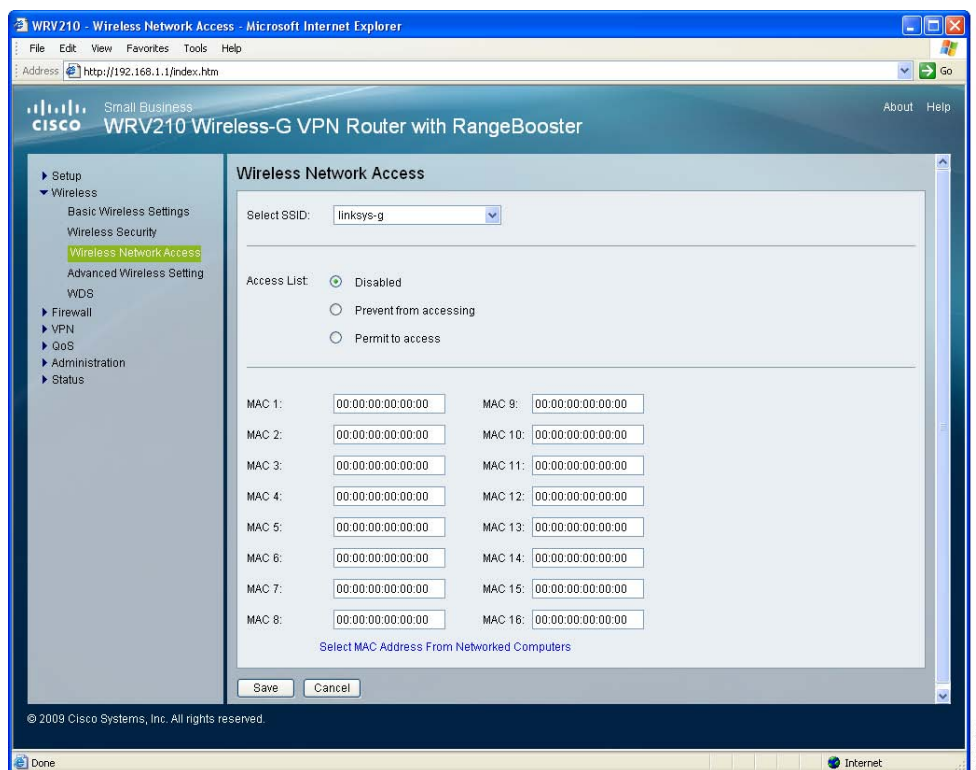
Controlling Access to the Wireless Network

This screen allows you to control access to your wireless network for each SSID.



NOTE

If you configured multiple networks (SSIDs), repeat this procedure for each one.



STEP 1 Click **Wireless > Wireless Network Access** in the navigation tree.

STEP 2 From the **Select SSID** drop-down list, choose the SSID for the network that you want to configure.

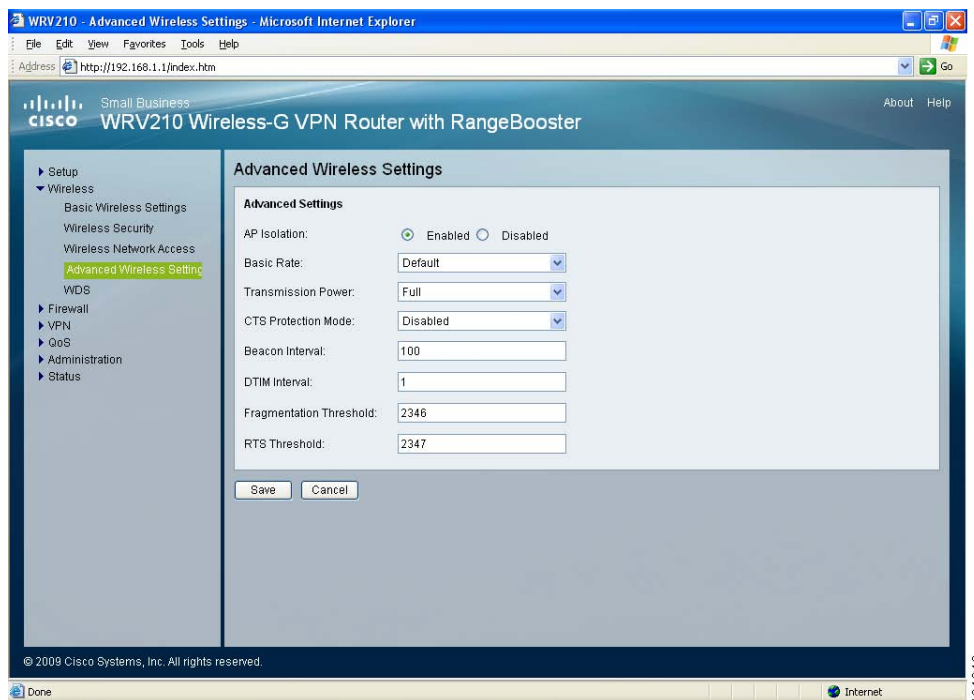
- **Access List:** Choose the type of access policy that you want to create, as described below.
 - **Disabled:** Choose this option if you do not want to use an access policy. Any client that provides the correct security credentials can connect. This option is the default selection.

- **Prevent from accessing:** Choose this option to prevent the specified computers from accessing your wireless network.
- **Permit to access:** Choose this option to allow only the specified computers to access your network.
- **MAC 1 to MAC 16:** To specify the computers that are subject to your policy, enter the MAC addresses. For a more convenient way to add MAC addresses, click the **Select MAC Address From Networked Computers** link below the table. When the Select MAC Address screen appears, select the MAC Addresses that you want to add to the policy. Then click **Apply**. Click **Refresh** if you want to refresh the screen. Click **Close** to return to the previous screen.

STEP 3 Click **Save** to save your settings, or click **Cancel** to refresh the page with the previously saved settings.

Adjusting the Advanced Wireless Settings

Use the Advanced Wireless Settings page to set up the Router's advanced wireless functions. These settings should only be adjusted by an advanced user as incorrect settings can reduce wireless performance.



STEP 1 Click **Wireless > Advanced Wireless Settings** in the navigation tree.

STEP 2 Enter the following settings, as needed:

- **AP Isolation:** This feature isolates all wireless clients and wireless devices on your network from each other. Wireless devices can communicate with the Router but not with one another. To use this function, click **Enabled**. AP Isolation is disabled by default.
- **Basic Rate:** The Basic Rate setting is not actually one rate of transmission but a series of rates at which the Router can transmit. The Router advertises its Basic Rate to the other wireless devices in your network, so they know which rates can be used. The Router also advertises that it automatically selects the best rate for transmission. The default setting is **Default**, when the Router can transmit at all standard wireless rates (1-2Mbps, 5.5Mbps, 11Mbps, 18Mbps, and 24Mbps). Other options are **1-2Mbps**, for use with

older wireless technology, and **All**, when the Router can transmit at all wireless rates. The Basic Rate is not the actual rate of data transmission. If you want to specify the Router's rate of data transmission, configure the Transmission Rate setting.

- **Transmission Power:** The amount of transmission power should be set so that the Router uses only as much power as needed to reach the farthest device in your wireless network. This setting can help to prevent unwanted eavesdropping on your wireless network. You can select from a range of power levels, from **Full**, **Half**, **Quarter**, **Eighth**, or **Min**. The default setting is **Full**.
- **CTS Protection Mode:** CTS (Clear-To-Send) Protection Mode's default setting is **Auto**. The Router automatically uses CTS Protection Mode when your Wireless-G products are experiencing severe problems and are not able to transmit to the Router in an environment with heavy 802.11b traffic. This function boosts the Router's ability to catch all Wireless-G transmissions but severely decreases performance.
- **Beacon Interval:** The default value is **100**. Enter a value between 1 and 65,535 milliseconds. The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the Router to synchronize the wireless network.
- **DTIM Interval:** The default value is **3**. This value, between 1 and 255, indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages.
- **Fragmentation:** Threshold In most cases, this value should remain at its default value of **2346**. It specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor reduction of the default value is recommended.
- **RTS Threshold:** The RTS Threshold value should remain at its default value of **2347**. Should you encounter inconsistent data flow, only minor reduction of the default value, 2347, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism is not enabled. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame.

After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission.

STEP 3 Click **Save** to save your settings, or click **Cancel** to refresh the page with the previously saved settings.

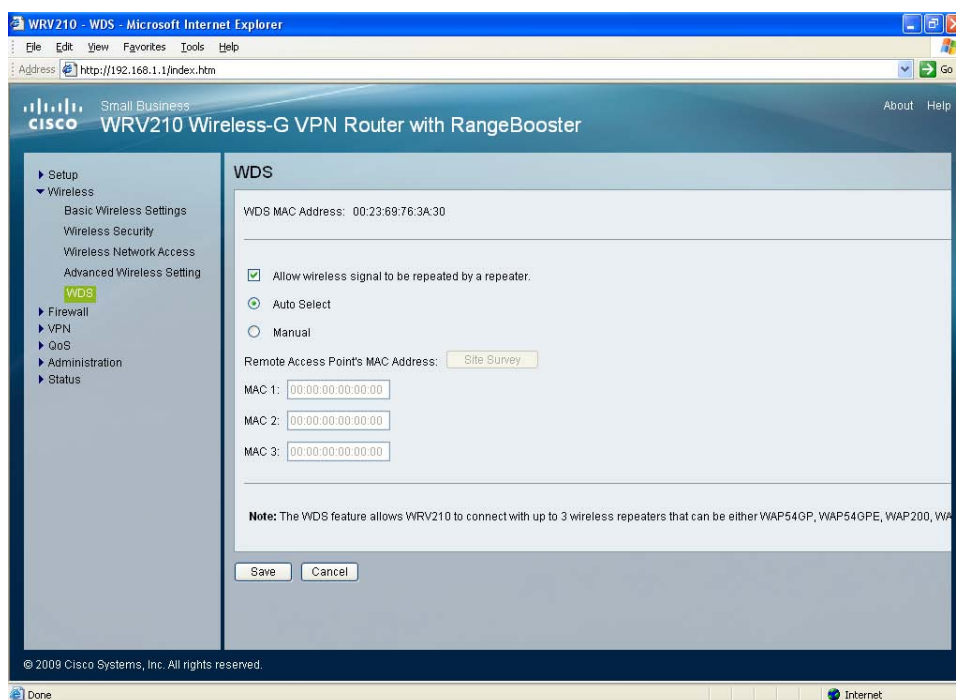
Configuring a Wireless Distribution System (WDS)

If you need to extend the coverage of the Router by using a repeater, you can use the WDS page to configure a Wireless Distribution System. This mode allows a wireless client to connect to the Router through an access point, such as WAP54GP or WAP54GPE, when operating in the Repeater Mode. You can install up to three repeaters.



NOTE

WDS works *only* with SSID1. Make sure that the channel and security settings are the same for all WDS-enabled devices.



-
- STEP 1** Click **Wireless > WDS** in the navigation tree.
- STEP 2** To enable WDS, check the **Allow wireless signal to be repeated by a repeater** check box.
- STEP 3** Choose the method for allowing repeaters to connect:
- **Auto Select:** Choose this option to automatically allow access from an access point that is operating in Repeater Mode.
 - **Manual:** Choose this option if you want to allow access only from specified access points. Then enter the MAC address of up to three access points. Alternatively, click the **Site Survey** button to view the available access points.
- STEP 4** Click **Save** to save your settings, or click **Cancel** to refresh the page with the previously saved settings.
-

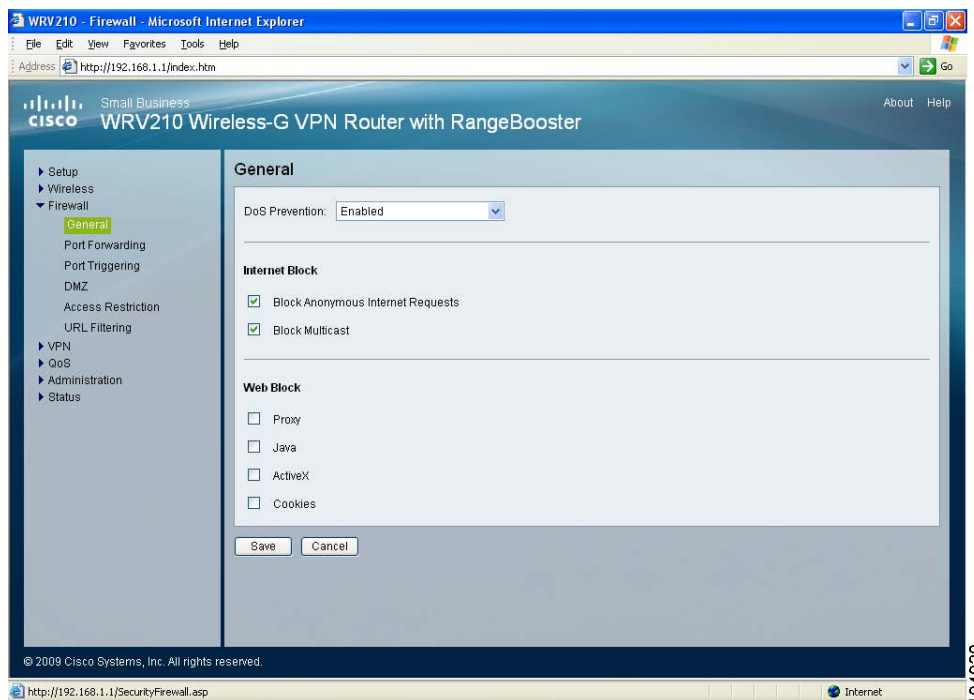
Configuring the Firewall

Use the Firewall module to prevent attacks and to control your users' access to the Internet.

- [Preventing Attacks, page 50](#)
- [Enabling Port Forwarding to Allow Access to Services, page 51](#)
- [Using Port Triggering to Allow Access to Applications, page 54](#)
- [Configuring a DMZ to Allow Access to All Ports of a Server, page 55](#)
- [Restricting Users' Access to the Internet, page 57](#)
- [Blocking Web Access with URL Filtering, page 59](#)

Preventing Attacks

The Router's firewall enhances the security of your network. You can implement a Stateful Packet Inspection (SPI) firewall, block anonymous Internet requests, and enable block mechanisms.



STEP 1 Click **Firewall > General** in the navigation tree.

STEP 2 Enter the following settings, as needed:

- **DoS Prevention:** Denial of Service (DoS) Prevention checks incoming packets before allowing them to enter your network. To use this feature, select **Enabled** from the drop-down menu. If you do not want DoS Prevention, select **Disabled**. This feature is enabled by default.
- **Block Anonymous Internet Requests:** This feature prevents your network from being “pinged” or detected and reinforces your network security by hiding your network ports. This feature makes it more difficult for intruders to work their way into your network. Check the box to enable this feature, or uncheck the box to disable it. This feature is enabled by default.
- **Block Multicast:** Multicasting allows a transmission to be forwarded automatically to multiple recipients at the same time. Check the box to

prevent multicasting, or uncheck the box to allow multicasting. This feature is enabled by default.

- **Web Block:** Check the box for each type of web component that you want to block. Uncheck the box for each feature that you want to allow. All of the options are unchecked by default.
 - **Proxy:** Use of WAN proxy servers may compromise the Router's security. Check the box to disable access to any WAN proxy servers. Uncheck the box to proxies.
 - **Java:** Java is a programming language for websites. If you deny Java applets, you run the risk of not having access to Internet sites created using this programming language. Check the box to prevent Java applets from being downloaded by a web browser. Uncheck the box to allow Java applets.
 - **ActiveX:** ActiveX is a programming language for websites. If you deny ActiveX, you run the risk of not having access to Internet sites created using this programming language. Check the box to prevent ActiveX controls from being downloaded by a web browser. Uncheck the box to allow ActiveX controls.
 - **Cookies:** A cookie is data that is stored on a PC and used by Internet sites. Check the box to prevent cookies from being downloaded by a web browser. Uncheck the box to allow cookies.

STEP 3 Click **Save** to save your settings, or click **Cancel** to refresh the page with the previously saved settings.

Enabling Port Forwarding to Allow Access to Services

By default, the Router's firewall prevents access from the Internet to your private network. You can use the Port Forwarding screen to allow public access from the Internet to your network resources, such as web servers, FTP servers, e-mail servers, or other specialized Internet applications. Specialized Internet applications are any applications that use Internet access to perform functions such as video conferencing or online gaming. Some Internet applications may not require any forwarding.

When users send this type of request to your network via the Internet, the Router forwards those requests to the appropriate PC. Any PC whose port is being forwarded must have its DHCP client function disabled and must have a new static IP address assigned to it because its IP address may change when using the DHCP function.



NOTE

Port Forwarding and DMZ are used for similar purposes. However, Port Range Forwarding can forward to a maximum of 10 ranges of ports on different PCs, while a DMZ can forward all the ports for one PC. For information about DMZ, see [Configuring a DMZ to Allow Access to All Ports of a Server, page 55](#).

Application Name	Start ~ End	Protocol	IP address	Enable
None		TCP	192.168.1.0	<input type="checkbox"/>
None		TCP	192.168.1.0	<input type="checkbox"/>
None		TCP	192.168.1.0	<input type="checkbox"/>
None		TCP	192.168.1.0	<input type="checkbox"/>
None		TCP	192.168.1.0	<input type="checkbox"/>
		TCP	192.168.1.0	<input type="checkbox"/>
		TCP	192.168.1.0	<input type="checkbox"/>
		TCP	192.168.1.0	<input type="checkbox"/>
		TCP	192.168.1.0	<input type="checkbox"/>
		TCP	192.168.1.0	<input type="checkbox"/>
		TCP	192.168.1.0	<input type="checkbox"/>
		TCP	192.168.1.0	<input type="checkbox"/>
		TCP	192.168.1.0	<input type="checkbox"/>
		TCP	192.168.1.0	<input type="checkbox"/>
		TCP	192.168.1.0	<input type="checkbox"/>
		TCP	192.168.1.0	<input type="checkbox"/>
		TCP	192.168.1.0	<input type="checkbox"/>
		TCP	192.168.1.0	<input type="checkbox"/>
		TCP	192.168.1.0	<input type="checkbox"/>
		TCP	192.168.1.0	<input type="checkbox"/>

STEP 1 Click **Firewall > Port Forwarding** in the navigation tree.

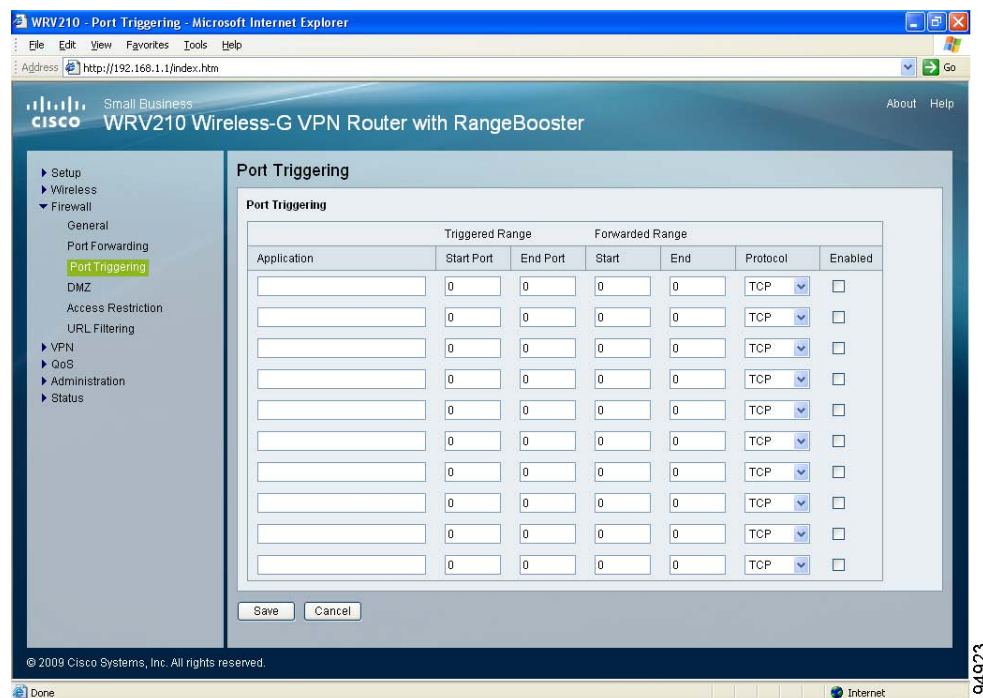
STEP 2 Enter the following information:

- **Application Name:** In this field, enter the name you wish to give the application. Each name can be up to 12 characters.
- **Start~End:** Use these two fields to enter the port range. In the **Start** field, enter the first port number in the range. In the **End** field, enter the final port number in the range.
- **Protocol:** Enter the protocol used for this application. The options are **TCP**, **UDP**, or **Both**.
- **IP Address:** For each application, enter the IP Address of the PC that hosts the specified application.
- **Enabled:** Check the box to enable port forwarding for the relevant application. Uncheck the box to disable this feature.

STEP 3 Click **Save** to save your settings, or click **Cancel** to refresh the page with the previously saved settings.

Using Port Triggering to Allow Access to Applications

Port Triggering is used for special Internet applications that use different ports to transmit and receiving data. For this feature, the Router watches outgoing data for specific port numbers. The Router remembers the IP address of the computer that sends a transmission requesting data, so that when the requested data returns through the Router, the data is pulled back to the proper computer by way of IP address and port mapping rules.



STEP 1 Click **Firewall > Port Triggering** in the navigation tree.

- **Application:** Enter a name for the application. Each name can be up to 12 characters.
- **Triggered Range:** Use these two fields to enter the range for the ports that receive a transmission requesting data. In the **Start Port** field, enter the first port number in the range. In the **End Port** field, enter the final port number in the range.
- **Forwarded Range:** Use these two fields to enter the port range for the ports where the Router forwards the data. In the **Start** field, enter the first

port number of the range. In the **End** field, enter the final port number in the range.

- **Protocol:** Enter the protocol used for this application. The options are **TCP**, **UDP**, or **Both**.
- **Enabled:** Check the box to enable port forwarding for the relevant application. Uncheck the box to disable this feature.

STEP 2 Click **Save** to save your settings, or click **Cancel** to refresh the page with the previously saved settings.

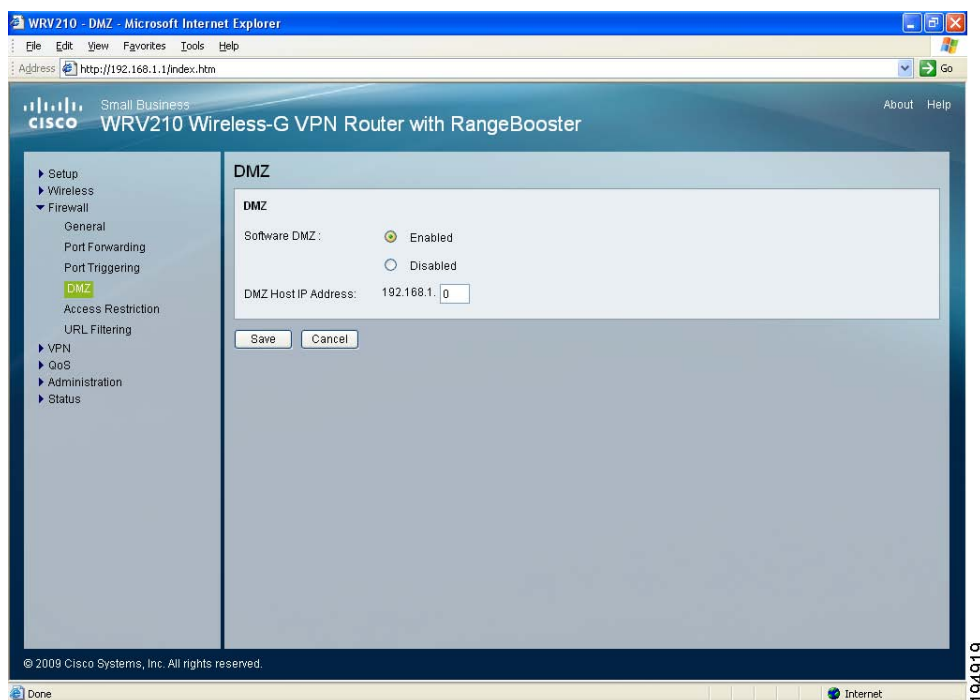
Configuring a DMZ to Allow Access to All Ports of a Server

By default, the Router's firewall prevents access from the Internet to your private network. You can use the DMZ page to configure a Demilitarized Zone or Demarcation Zone, which allows one local PC to be exposed to the Internet while protecting the rest of your private network. Typically a DMZ is used for a special-purpose service such as Internet gaming and video conferencing.



NOTE

DMZ and Port Forwarding are used for similar purposes. However, Port Range Forwarding can forward to a maximum of 10 ranges of ports on different PCs, while a DMZ can forward all the ports for one PC. For information about Port Forwarding, see [Enabling Port Forwarding to Allow Access to Services, page 51](#).



STEP 1 Click **Firewall > DMZ** in the navigation tree.

STEP 2 In the **Software DMZ**, click **Enabled**.



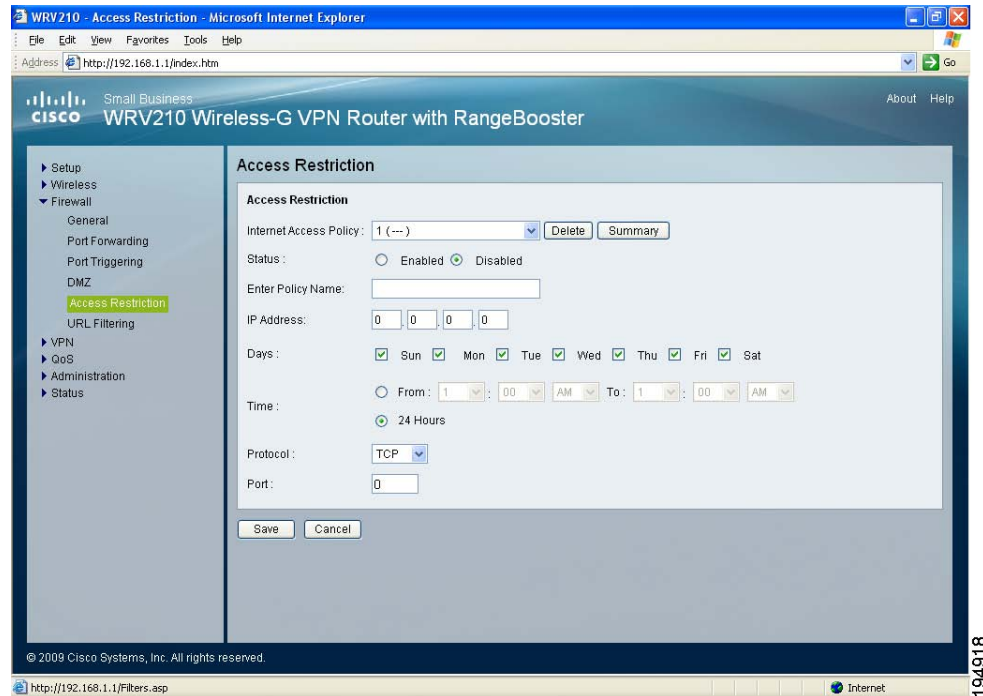
NOTE You can disable a DMZ at any time by clicking **Disabled** and saving the settings.

STEP 3 Enter the IP address of the PC that hosts the service that you want to expose to Internet traffic.

STEP 4 Click **Save** to save your settings, or click **Cancel** to refresh the page with the previously saved settings.

Restricting Users' Access to the Internet

By default, the Router's firewall allows your users to access the Internet. You can use the Access Restriction page to block or allow specific kinds of Internet usage and traffic during specific days and times.



STEP 1 Click **Firewall > Access Restriction** in the navigation tree.

STEP 2 From the **Internet Access Policy** drop-down list, choose the policy that you want to configure. You can configure up to eight policies.



NOTE To delete a policy, select the policy, and then click **Delete**. To view all the policies, click **Summary**.

STEP 3 Enter the following settings for the chosen policy:

- **Status:** Click **Enabled** to enable the policy, or click **Disabled** to disable it. Policies are disabled by default.
- **Enter Policy Name:** Type a name to identify the policy. After you save the policy, this name will appear with the policy number in the Internet Access Policy drop-down list.
- **IP Address:** Enter the IP address that will be affected by this policy.
- **Days:** Check the box for each day when the policy is enforced. Uncheck the box for each day when the policy is not enforced.
- **Time:** Use the drop-down lists to set the range of times when the policy is enforced. In the following example, the network is enabled from 8 a.m. to 5 p.m., Monday through Friday and is unavailable on Saturday and Sunday.

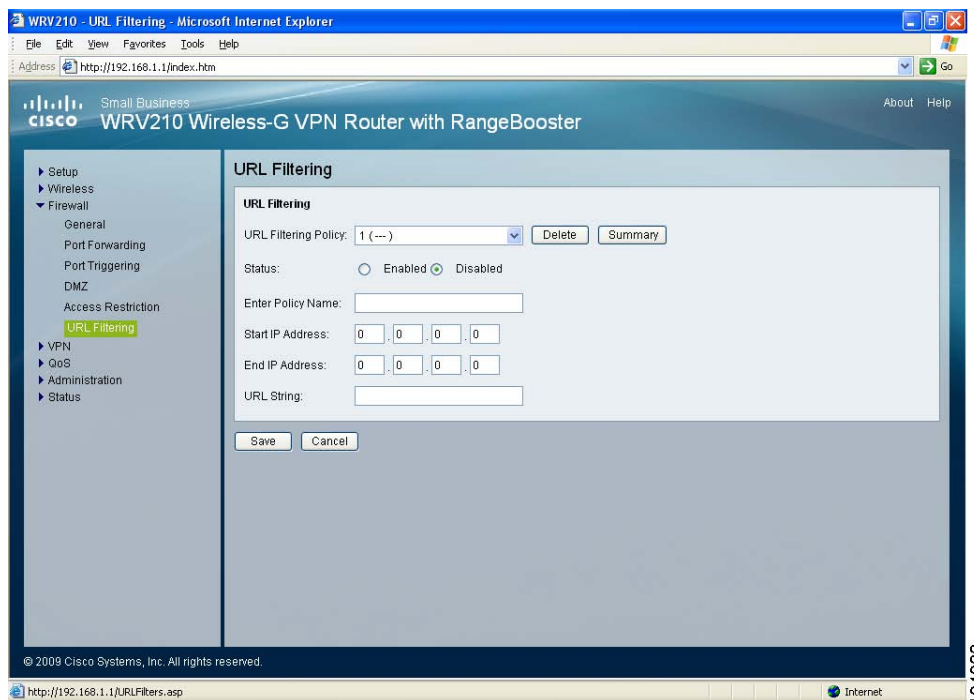
The screenshot shows a configuration window with three sections: Status, Days, and Time. The Status section has two radio buttons: 'Enabled' (selected) and 'Disabled'. The Days section has checkboxes for each day of the week: Sun (unchecked), Mon (checked), Tue (checked), Wed (checked), Thu (checked), Fri (checked), and Sat (unchecked). The Time section has two radio buttons: 'From: 8:00 AM To: 5:00 PM' (selected) and '24 Hours' (unchecked). The time values are displayed in dropdown menus.

- **Protocol:** Specify the protocol that this policy affects. The choices are **TCP**, **UDP**, **All**.
- **Port:** If this policy applies to traffic through a specific port, enter the port number. Otherwise, leave 0 in the field.

STEP 4 Click **Save** to save your settings, or click **Cancel** to refresh the page with the previously saved settings.

Blocking Web Access with URL Filtering

You can use the Firewall > URL Filtering page to block access to specified websites.



STEP 1 Click **Firewall > URL Filtering** in the navigation tree.

STEP 2 From the **URL Filtering Policy** drop-down list, choose the policy that you want to configure. You can configure up to 8 policies.



NOTE To delete a policy, select the policy, and then click **Delete**. To view all the policies, click **Summary**.

STEP 3 Enter the following settings for the chosen policy:

- **Status:** Click **Enabled** to enable the policy, or click **Disabled** to disable it. Policies are disabled by default.
- **Enter Policy Name:** Type a name to identify the policy. After you save the policy, this name will appear with the policy number in the Internet Access Policy drop-down list.
- **Start IP Address and End IP Address:** Enter the IP address of the PCs that are subject to this policy.

STEP 4 In the **URL String** field, enter the URL of the Internet site to block.



NOTE You can enter part of a URL, such as *yahoo*, to filter all URLs that contain that string, or you can enter the full URL, such as *www.yahoo.com*, to block only the specific URL as entered.

STEP 5 Click **Save** to save your settings, or click **Cancel** to refresh the page with the previously saved settings.

Configuring a Virtual Private Network (VPN)

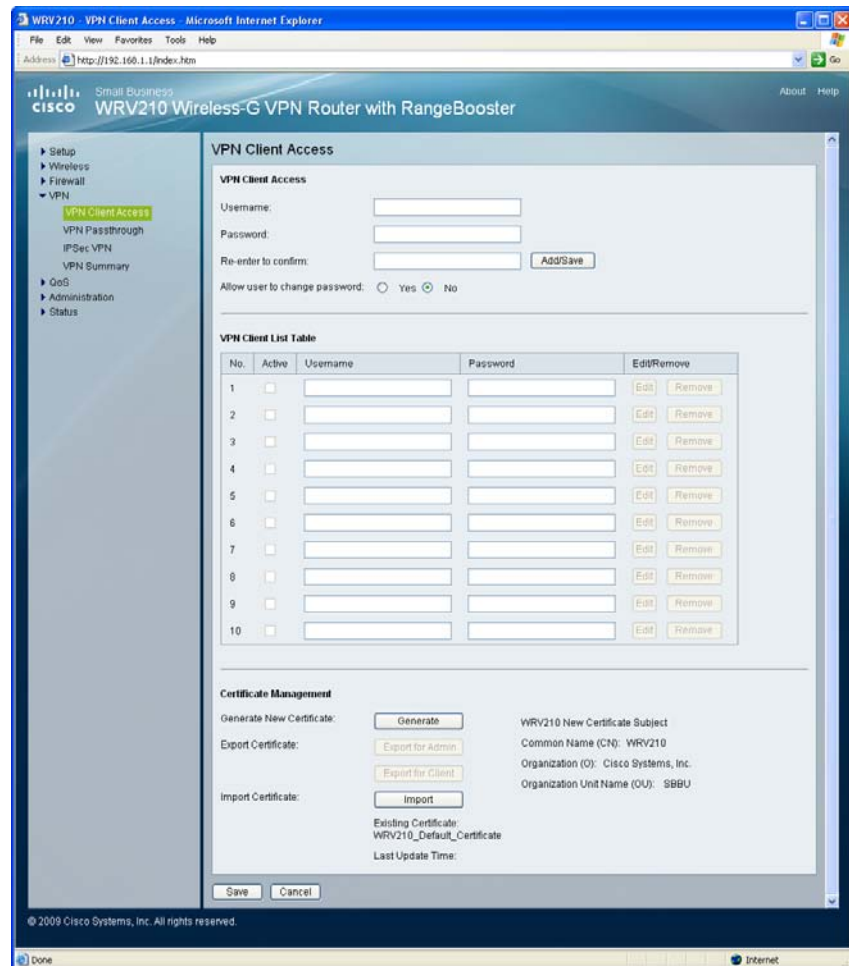
Virtual Private Networking (VPN) is a security measure that creates a secure connection between two remote locations. The security is created by the very specific settings for the connection. Use the VPN module to configure your VPN settings to make your network more secure.

This chapter includes the following sections:

- **[“Managing the VPN Users and Certificates” on page 61](#)**
- **[“Configuring VPN Passthrough” on page 66](#)**
- **[“VPN > IPSec VPN” on page 68](#)**
- **[“Monitoring the IPSec VPN Tunnels” on page 73](#)**

Managing the VPN Users and Certificates

The Router offers a QuickVPN Client utility for Windows 2000, XP, or Vista. QuickVPN allows remote workers to log on securely to the corporate network from anywhere on the Internet. You can use the VPN > VPN Client Access page to manage the VPN users and to generate certificates for added security.



Refer to the following topics:

- [Managing the VPN Users, page 63](#)
- [Managing VPN Certificates, page 65](#)

Managing the VPN Users

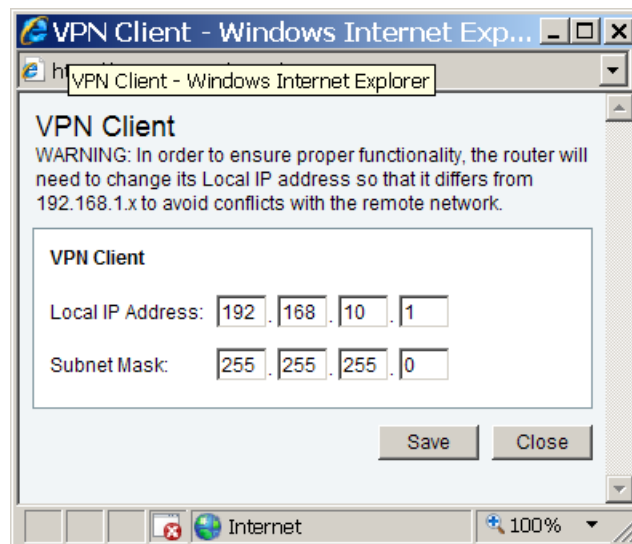
The Router supports up to 10 remote users. They use QuickVPN software to connect to your local network through the VPN tunnel.

STEP 1 Click **VPN > VPN Client Access** in the navigation tree.

STEP 2 To add a user, enter the username and password, and then click **Add/Save**.

- **User Name:** Enter a name for the VPN client.
- **Password:** Enter a password for the VPN client.
- **Re-enter to confirm:** Enter the password again to confirm it.
- **Allow user to change password?** If you want to let the user change his or her password from the user's QuickVPN client, select **Yes**.

STEP 3 If this is the first VPN client you have added, read the warning message and complete the steps below.



- a. Optionally, enter a new **Local IP Address** and **Subnet Mask** for your router, and then click **Save**.



NOTE IMPORTANT: You need to ensure that the local router and the remote router have different IP addresses. Otherwise a VPN tunnel cannot be established. If you are confident that the remote router has a different IP address, you can click **Close** to close the window without changing the IP address.

- b. When the second warning appears, click **OK**.



- c. To reconnect to the Configuration Utility, close your web browser, reopen it, and enter the new IP address.

STEP 4 To manage existing users, perform the following tasks:

- **To update the username or password:** Find the username in the table, and then click **Edit**.
- **To delete a user:** Find the username in the table, and then click **Remove**.
- **To activate a user's account:** Check the **Active** box.
- **To deactivate a user's account:** Uncheck the **Active** box.

STEP 5 Add or edit users, as needed.

STEP 6 Click **Save** to save your settings, or click **Cancel** to refresh the page with the previously saved settings.

Managing VPN Certificates

Certificates are used to secure the communication between the router and the QuickVPN clients. Use the VPN Certificates area of the VPN Client Access page to generate and manage the certificates.

**NOTE**

Certificates are used if you want additional security beyond the user name and password. The certificate must be installed on the client PC.

You can use the export function to save a copy of an admin certificate or a client certificate. You can use the import function to restore a previously saved certificate as the active certificate.

STEP 1 Click **VPN > VPN Client Access** in the navigation tree.

STEP 2 Perform the following tasks, as needed:

- **Generate:** Click this button to generate a new certificate to replace the existing certificate on the router.
- **Export for Admin:** Click this button to export the certificate for administrator. A dialog prompts you to specify where you want to store your certificate. The default file name is “WRV210_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 for Client:** Click this button to export the certificate for client. A dialog prompts you to specify where to store your certificate. The default file name is “WRV210_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 revert to a previous version of the certificate that you saved by 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**.

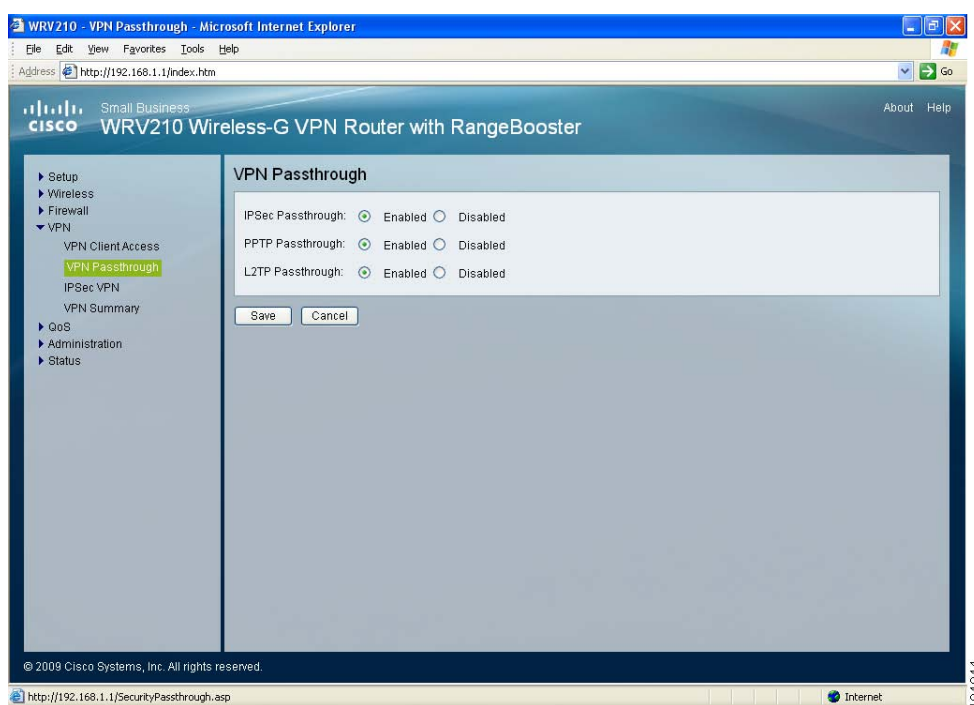
STEP 3 Click **Save** to save your settings, or click **Cancel** to refresh the page with the previously saved settings.

Configuring VPN Passthrough

Use the VPN Passthrough page to allow VPN tunnels to pass through the Router's firewall using IPSec, L2TP, or PPTP protocols.

**NOTE**

Disabling passthrough may prevent VPN clients from connecting to your network.



STEP 1 Click **VPN > VPN Passthrough** in the navigation tree.

STEP 2 Enable the protocol that you need for your network traffic:

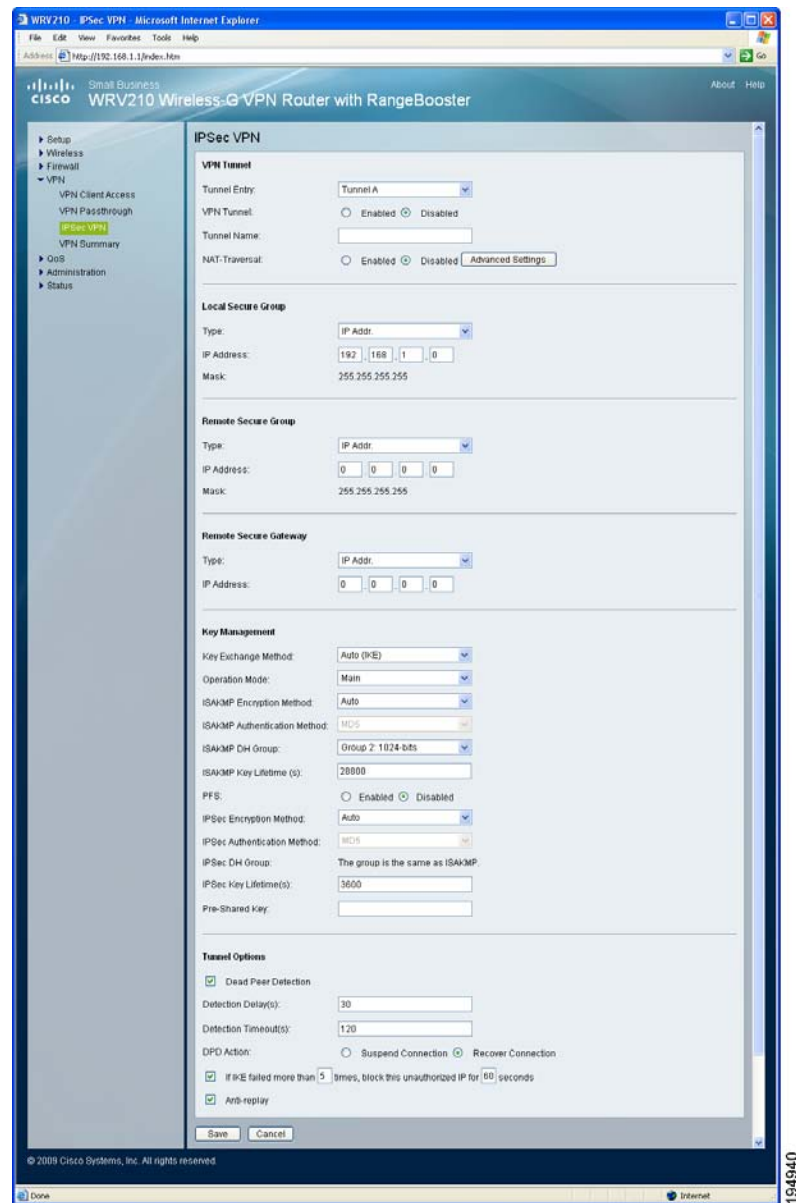
- **IPSec Passthrough:** Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. IPSec Passthrough is enabled by default to allow IPSec tunnels to pass through the Router. To disable IPSec Passthrough, select **Disabled**.
- **PPTP Passthrough:** 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**.

STEP 3 Click **Save** to save your settings, or click **Cancel** to refresh the page with the previously saved settings.

VPN > IPSec VPN

Use the VPN > IPSec VPN page to create and configure a Virtual Private Network (VPN) tunnel for site-to-site VPN. For example, you can use IPSec VPN to connect two offices of your company that are in different locations. You can configure up to 5 tunnels.





NOTE Repeat this procedure for each tunnel that you want to configure.

STEP 1 Click **VPN > IPSec VPN** in the navigation tree.

STEP 2 In the **VPN Tunnel** section, enter the following settings:

- **Tunnel Entry:** From the drop-down list, select the tunnel that you want to configure. You can configure up to 5 tunnels, indicated by the letters A through E.

- **VPN Tunnel:** Click **Enabled** to enable this tunnel, or click **Disabled** to disable this tunnel

- **Tunnel Name:** Enter a name for this tunnel, such as “Anaheim Office.”

NAT-Traversal: Click **Enabled** if you need to establish a VPN tunnel with a device that is behind an NAT firewall. NAT-T must be enabled for another private network to be able set up a site-to-site IPSec tunnel with your WRV210. Click **Disabled** if the remote device is not behind an NAT firewall.



NOTE If NAT traversal is enabled, the Remote Secure Group and Remote Secure Gateway must be set to **Any**.

If you want to limit access to specified IP addresses, click the **Advanced Settings** button. IPSec communication will be interrupted while you configure the NAT settings. Click **OK** to acknowledge the warning message that appears. In the NAT-Traversal Advanced Settings window, click **By Manual Setting**. Then enter each IP address and mask. Click the **Enabled** box to enable. Finally, click **Save** to save your settings in this window, or click **Cancel** to close the window without saving the settings.

STEP 3 In the **Local Secure Group** section, identify the computer(s) on your LAN that can access the tunnel. Choose a **Type**, and then enter the required information:

- **IP Addr.:** Allows a specified computer to access the tunnel. Enter the IP Address of the local VPN Router. The Mask appears.
- **Subnet:** Allows the entire network to access the tunnel. Enter the **IP Address** and **Mask** of the local VPN Router in the fields provided. To allow access to the entire IP subnet, enter **0** for the last octet of the IP Address, as in the following example: 192.168.1.0.

- **Host:** Directs the traffic, using port forwarding, to the correct computer. The VPN tunnel terminates at the router with this setting. Use Port Range Forwarding to direct traffic to the correct computer. For more information, see [“Enabling Port Forwarding to Allow Access to Services” on page 51](#).

STEP 4 In the **Remote Secure Group** section, enter the following information to identify the computer(s) on the remote end of the tunnel that can access the tunnel.

From the drop-down menu, choose the option that you want:

- **IP Addr.:** Allows a specified computer to access the tunnel. Enter the IP Address of the remote VPN router. The Mask appears.
- **Subnet:** Allows the entire network to access the tunnel. Enter the IP Address and Mask of the remote VPN router in the fields provided. To allow access to the entire IP subnet, enter **0** for the last set of IP Address, as in the following example: 192.168.1.0.
- **Host:** Terminates VPN at the Router, instead of the PC. Use Port Range Forwarding to direct traffic to the correct computer. For more information, see [“Enabling Port Forwarding to Allow Access to Services” on page 51](#).
- **Any:** Allows any computer to access the tunnel.

STEP 5 In the **Remote Secure Gateway** section, identify the VPN device, such as a second VPN router, on the remote end of the VPN tunnel. Enter the IP Address of the VPN device at the other end of the tunnel.



NOTE The remote VPN device can be another VPN router, a VPN server, or a computer with VPN client software that supports IPSec. The IP address may either be static (permanent) or dynamic, depending on the settings of the remote VPN device.

- If the IP Address is static, select **IP Addr.** and enter the IP address. Make sure that you have entered the IP address correctly, or the connection cannot be made. Remember, this is NOT the IP address of the local VPN Router; it is the IP address of the remote VPN router or device with which you wish to communicate.
- If the IP address is dynamic, select **FQDN** for DDNS or **Any**.
 - If FQDN is selected, enter the domain name of the remote router, so the Router can locate a current IP address using DDNS.
 - If **Any** is selected, then the Router accepts requests from any IP address.

STEP 6 In the **Key Management** section, enter the following information to configure the security for the IPSec VPN tunnel.

- **Key Exchange Method:** IKE is an Internet Key Exchange protocol used to negotiate key material for Security Association (SA). IKE uses the Pre-shared Key to authenticate the remote IDE peer. **Auto (IKE)** automatically negotiates the correct protocol.
- **Operation Mode:** Use this option to set the operation mode to **Main** (default) or **Aggressive**. Main Mode operation is supported in ISAKMP SA establishment.
- **ISAKMP Encryption Method:** There are four different types of encryption: **3DES**, **AES-128**, **AES-192**, or **ES-256**. You may choose any of these, but it must be the same type of encryption that is being used by the VPN device at the other end of the tunnel.
- **ISAKMP Authentication Method:** There are two types of authentication: MD5 and SHA (SHA is recommended because it is more secure). As with encryption, either of these may be selected, provided that the VPN device at the other end of the tunnel is using the same type of authentication.
- **ISAKMP DH Group:** This field specifies the Diffie-Hellman key negotiation. Seven groups are available for ISAKMP SA establishment. Group 1024, 1536, 2048, 3072, 4096, 6144, and 8192 represent different bits used in Diffie-Hellman mode operation. The default value is **1024**.
- **ISAKMP Key Lifetime(s):** Specify how long an ISAKMP key channel should be kept, before being renegotiated. The default is **28800** seconds, which is 8 hours.
- **PFS:** PFS (Perfect Forward Secrecy) ensures that the initial key exchange and IKE proposals are secure. Click **Enabled** to use PFS, or click **Disabled** to disable this feature.
- **IPSec Encryption Method:** Using encryption also helps make your connection more secure. There are four different types of encryption: **3DES**, **AES-128**, **AES-192**, **AES-256** or **Auto**. You may choose any of these, but you must choose the same type of encryption that is being used by the VPN device at the other end of the tunnel. **Auto** automatically negotiates the encryption method with the remote gateway.
- **IPSec Authentication Method:** Authentication acts as another level of security. There are two types of authentication: MD5 and SHA. SHA is recommended because it is more secure. The VPN device at the other end of the tunnel must be configured to use the same type of authentication. Or, both ends of the tunnel may choose to disable authentication.

- **IPSec DH Group:** This setting is the same as the ISAKMP DH Group setting.
- **IPSec Key Lifetime(s):** Optionally, you can choose to have the key expire at the end of a specified time period. Enter the number of seconds you'd like the key to be used until a re-key negotiation between each endpoint is completed. The default is **3600** seconds, which is 1 hour.
- **Pre-shared Key:** Enter a series of numbers or letters in the *Pre-shared Key* field. The same key must be entered at both ends of the tunnel. Based on this key, a key is generated to scramble (encrypt) the data being transmitted over the tunnel, where it is unscrambled (decrypted). You may use any combination of up to 24 numbers or letters in this field. No special characters or spaces are allowed.

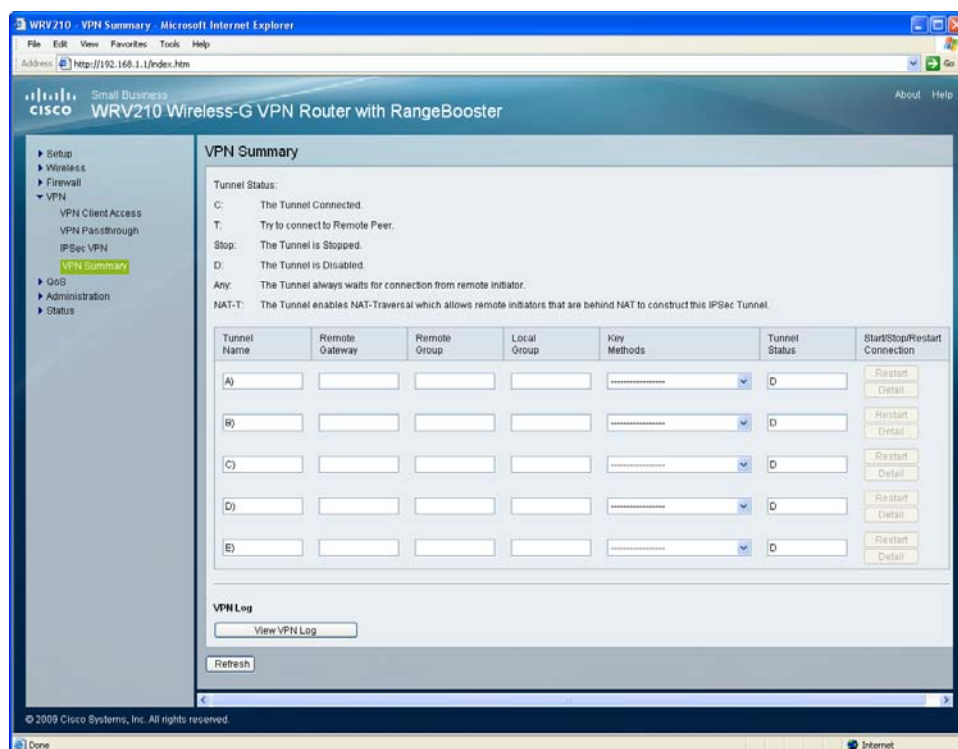
STEP 7 In the **Tunnel Options** section, enter the following settings:

- **Dead Peer Detection:** Dead Peer Detection (DPD) detects the status of a remote peer. DPD issues DPD packets (ISAKMP format) to query a remote peer, and waits for a reply to recognize that the peer is still alive. Check the box to enable DPD, or uncheck the box to disable this feature.
- **Detection Delay(s):** Specify the interval between DPD query packets. The default value is **30** seconds.
- **Detection Timeout(s):** Specify the length of timeout when DPD cannot hear any DPD reply. The default value is **120** seconds.
- **DPD Action:** Specify the action that is taken when the DPD Timeout setting expires. Select **Suspend Connection** to stop passively recovering the connection or select **Recover Connection**.
- **If IKE failed more than _times, block this unauthorized IP for _ seconds:** This feature enables the Router to block unauthorized IP addresses. Specify the number of **times** IKE must fail before the Router blocks that unauthorized IP address. also specify the number of **seconds** that the unauthorized IP address is blocked. This feature is enabled by default. You can uncheck the box if you want to disable this feature.
- **Anti-replay:** This feature protects the Router from anti-replay attacks, when people try to capture your authentication packets in an attempt to gain access. The feature is enabled by default. You can uncheck the box if you want to disable this feature.

STEP 8 Click **Save** to save your settings, or click **Cancel** to refresh the page with the previously saved settings.

Monitoring the IPsec VPN Tunnels

Use the VPN Summary page to review the settings and monitor the status of all IPsec tunnels. You also can stop, start, or restart a connection.



To open this page, click **VPN > VPN Summary** in the navigation tree. Refer to the following descriptions of the fields and buttons:

- **Tunnel Name:** The field displays the name of the tunnel.
- **Remote Gateway:** The field displays the remote gateway. If the pre-configured type is IP Addr., the field displays the IP address of remote gateway. If the pre-configured type of remote gateway is Any, the field displays ANY. If the pre-configured type is FQDN, the field displays the FQDN string directly.
- **Remote Group:** The field displays the remote peer that is designated for VPN communication after a IPsec VPN tunnel is established. If the pre-configured type of the remote group is IP Addr., the field displays the IP address of the remote peer. If the pre-configured type of the remote group is Subnet, the field displays the subnet type "IP Address/Mask". If the pre-

configured type of remote group is Host or Any, the field displays the “Host” or “Any” directly.

- **Local Group:** The field displays the local peer that is designated for VPN communication after an IPSec VPN tunnel is established. If the pre-configured type of local group is IP Addr., the field displays the IP address of the local peer. If the pre-configured type of local group is Subnet, the field displays the subnet type “IP Address/Mask”. If the pre-configured type of local group is Host, the field displays the “Host” directly.
- **Key Methods:** The field displays the IPSec authentication and encryption key methods of the Key exchange Method that is followed with the setting value of the Password Forward Secrecy.
- **Tunnel Status:** The field displays the status of IPSec Tunnel as follows.
 - **C:** The tunnel is connected.
 - **T:** The tunnel is trying to connect to remote peer.
 - **Stop:** The tunnel is stopped.
 - **D:** The tunnel is disabled.
 - **Any:** The tunnel always waits for the connection from the remote initiator.
 - **NAT-T:** The tunnel enables the NAT-Traversal to allow the remote initiator that is behind the NAT to construct this IPSec Tunnel.
- **Start/Stop/Restart Connection:** The name of the button changes, depending on the previous actions you have performed. For troubleshooting, you can click the button to start, stop, or restart the connection according to pre-configured tunnel settings. If the pre-configured type of remote gateway or remote group is either **Any** or **NAT-Traversal**, the **Detail** button can also examine Remote Security Gateway information.
- **Detail:** This button becomes available when the Tunnel Status is C, T, Any, or NAT-T. Click **Detail** to view the VPN Advanced Tunnel Information page. This page provides more detailed information for advanced configuration and management.
- **VPN Log:** Click this button to check the overall related VPN behaviors and contact messages of a VPN Tunnel and VPN Client. After viewing the log information, you can clear it by clicking **Clear Log Now**.
- **Refresh:** Click this button to update the page with current VPN status information.

Configuring Quality of Service (QoS)

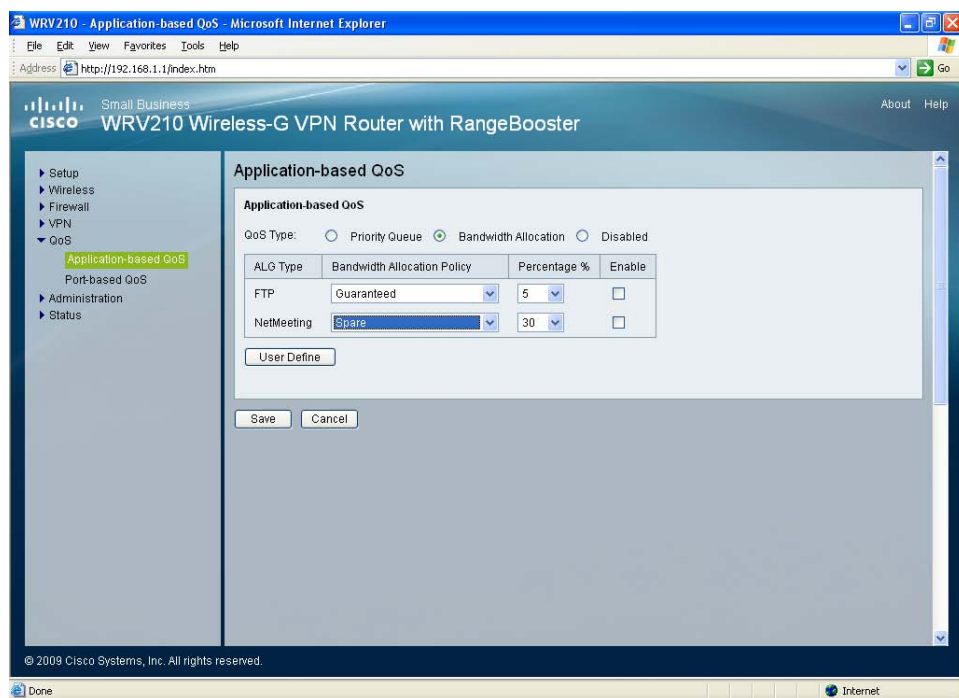
Quality of Service (QoS) ensures better service to high-priority service. Use the QoS module to configure the Router's QoS settings.

- [Configuring QoS Settings for Specified Applications, page 75](#)
- [Configuring QoS Settings for Specified Ports, page 78](#)

Configuring QoS Settings for Specified Applications

Application-based QoS involves Internet traffic, which may involve demanding, real-time applications, such as video conferencing. To enable Application-based QoS, you can select either **Priority Queue** or **Bandwidth Allocation**. The remaining fields in the screen depend on the selection.

- [“Priority Queue QoS Type” on page 76](#)
- [“Bandwidth Allocation QoS” on page 77](#)



Priority Queue QoS Type

With the Priority Queue option, you can manage QoS by specifying the priority of each application. There are five preset applications (FTP, HTTP, TELNET, SMTP, and POP3). You also can add custom applications.

- STEP 1** Click **QoS > Application-based QoS** in the navigation tree.
- STEP 2** For **QoS Type**, choose **Priority Queue**.
- STEP 3** Enter the following settings.
 - For the preset applications, choose **High Priority** or **Low Priority**.
 - For each custom application, enter a name, classify it as **High Priority** or **Low Priority**, and enter the port number that is used by the application.
- STEP 4** Click **Save** to save your settings, or click **Cancel** to refresh the page with the previously saved settings.

Bandwidth Allocation QoS

With the Bandwidth Allocation option, you can manage QoS by controlling the bandwidth utilization of each Application Layer Gateway (ALG).

FTP and NetMeeting appear by default. You can add additional applications requiring ALG. You must enable the ALG to apply the QoS settings.

STEP 1 Click **QoS > Application-based QoS** in the navigation tree.

STEP 2 For **QoS Type**, choose **Priority Queue**.

STEP 3 Enter the following settings:

- **Bandwidth Allocation Policy:** Choose **Guaranteed** or **Spare**.
 - **Guaranteed:** Choose this option to reserve exactly the specified percentage of bandwidth for the application.
 - **Spare:** Choose this option to reserve the specified percentage of bandwidth along with any available bandwidth that is available.
- **Percentage:** Specify the percentage bandwidth utilization from LAN to WAN.
- **Enable:** Check the box to enable the policy, or uncheck the box to disable the policy.

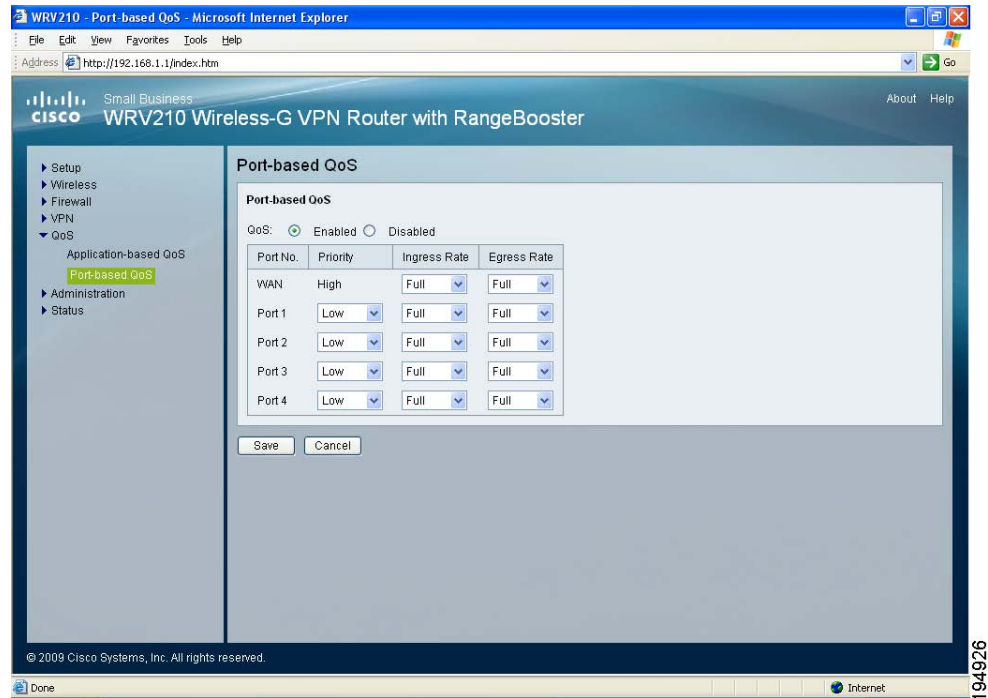
STEP 4 Optionally, if you want to configure advanced policies, click **User Define**. You can configure up to 5 policies.

- Specify the source IP address or the destination IP address, the subnet mask, and the protocol.
- Specify the port range, the Bandwidth Allocation Policy (Spare or Guaranteed), and the Percentage, as described above.
- Optionally, you can mark the DSCP field with specific value to egress packets. The bandwidth utilization could be controlled from LAN to WAN.
- Check the **Enable** box for each policy that you want to enforce.
- When you are finished entering the policies, click **Save** to save the Advanced Settings, or click **Close** to close the window without saving the settings.

STEP 5 Click **Save** to save your settings, or click **Cancel** to refresh the page with the previously saved settings.

Configuring QoS Settings for Specified Ports

Port-based QoS ensures better service to specified LAN ports. For example, if there is an email server connected to a particular port, you can prioritize traffic to that server.



STEP 1 Click **QoS > Port-based QoS** in the navigation tree.

STEP 2 Choose **Enabled** to enable port-based QoS, or choose **Disabled** to disable this feature.

STEP 3 For each port, enter the following settings:

- **Priority:** Select the QoS priority for each LAN port. This feature queues all egress packets from this port according to the specified priority value. If you select High for a port, the packets received from the port are put into High Priority Queue.



NOTE The WAN port has High priority, and this setting cannot be changed.

- **Ingress Rate:** Choose the input data rate for a port. Packets exceeding this rate are dropped. The rates can be 128kbps, 256kbps, 512kbps, 1Mbps, 2Mbps, 4Mbps, 8Mbps, 16Mbps, 32Mbps, Full (highest), or no rate control. Full is the default.
- **Egress Rate:** This setting lets the user choose the output data rate for a port. Packets exceeding this rate are dropped. The rates can be 128kbps, 256kbps, 512kbps, 1Mbps, 2Mbps, 4Mbps, 8Mbps, 16Mbps, 32Mbps, Full (highest), or no rate control.

STEP 4 Click **Save** to save your settings, or click **Cancel** to refresh the page with the previously saved settings.

Administration

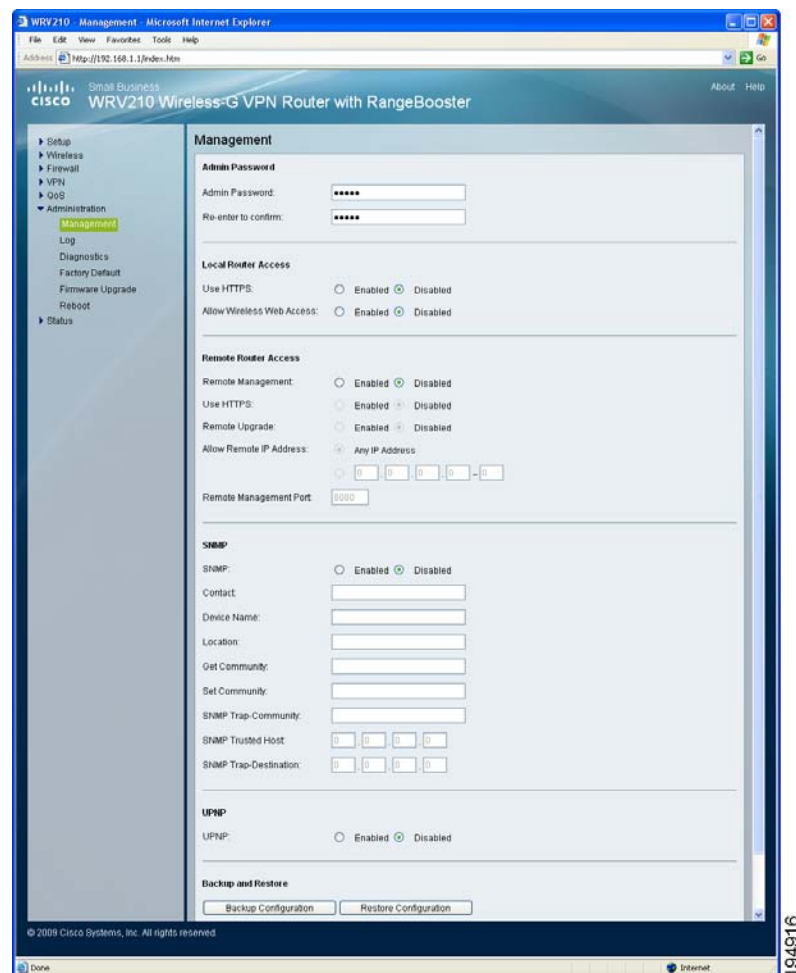
The Administration module provides access to system administration settings and tools.

- [Managing Access and Configuring Other Management Options, page 80](#)
- [Setting Up Alerts and System Logs, page 87](#)
- [Performing Diagnostic Tests, page 89](#)
- [Reverting to the Factory Default Settings, page 91](#)
- [Upgrading the Firmware, page 92](#)
- [Rebooting the Router, page 94](#)

Managing Access and Configuring Other Management Options

Use the Administration > Management page to reset the admin password, control access to the Configuration Utility, configure various management options, and back up or restore the configuration.

- [Resetting the Admin Password, page 81](#)
- [Managing LAN and WAN Access to the Configuration Utility, page 82](#)
- [Configuring SNMP Settings for Status Reporting, page 84](#)
- [Configuring Universal Plug and Play \(UPnP\) Settings, page 85](#)
- [Backing and Restoring a Configuration, page 86](#)



Resetting the Admin Password

To ensure the Router's security, you are prompted for your password when you access the Router's Configuration Utility. The default user name and password is **admin**. You should change this setting to prevent unauthorized access.

Make these changes in the **Admin Password** section of the Administration > Management page.

Admin Password	
Admin Password:	<input type="password" value="....."/>
Re-enter to confirm:	<input type="password" value="....."/>

STEP 1 Click **Administration > Management** in the navigation tree.

STEP 2 In the **Admin Password** section, enter and confirm the new password.

- **Admin Password:** Enter the new password. The password can include any alphanumeric characters.
- **Re-enter to confirm:** Re-enter the Router's new Password to confirm it.

STEP 3 Click **Save** to save your settings, or click **Cancel** to refresh the page with the previously saved settings.

Managing LAN and WAN Access to the Configuration Utility

With the default settings, the Configuration Utility can be accessed only from a computer that is physically connected to one of the Router's LAN ports. You can adjust the LAN access to enable access through a wireless connection, and enable WAN access from a computer at another site. For LAN and WAN access, you also can specify other settings.

Managing Access and Configuring Other Management Options, page 80 Configure these settings in the **Local Router Access** section and the **Remote Router Access** section of the Administration > Management page.

The screenshot shows two configuration sections: 'Local Router Access' and 'Remote Router Access'. In 'Local Router Access', 'Use HTTPS' and 'Allow Wireless Web Access' are both set to 'Disabled' (radio button selected). In 'Remote Router Access', 'Remote Management' is set to 'Disabled'. 'Use HTTPS' is set to 'Disabled'. 'Remote Upgrade' is set to 'Disabled'. 'Allow Remote IP Address' is set to 'Any IP Address' (radio button selected). Below this, there is an option to specify an IP range, which is currently set to '0.0.0.0 ~ 0.0.0.0'. The 'Remote Management Port' is set to '8080'.

Local Router Access	
Use HTTPS:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Allow Wireless Web Access:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

Remote Router Access	
Remote Management:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Use HTTPS:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Remote Upgrade:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Allow Remote IP Address:	<input checked="" type="radio"/> Any IP Address
	<input type="radio"/> 0 . 0 . 0 . 0 ~ 0 . 0 . 0 . 0
Remote Management Port:	8080

STEP 1 Click **Administration > Management** in the navigation tree.

STEP 2 In the **Local Router Access** section, configure the following settings:

- **Use HTTPS:** To use SSL encryption, select **Enabled**. After HTTPS is enabled, http requests to the Router's LAN IP are redirected to HTTPS.
- **Allow Wireless Web Access:** Click **Enabled** to allow access through a wireless connection, or click **Disabled** to prevent access through a wireless connection. This feature is disabled by default.

STEP 3 In the **Remote Router Access** section, configure the following settings:

- **Remote Management:** Click **Enabled** to allow access to manage the Router from a remote location, via the Internet. Click **Disabled** to disable this feature.
- **Use HTTPS:** Click **Enabled** to use the SSL encryption, or click **Disabled** to disable this feature.
- **Remote Upgrade:** If you enabled Remote Management, click **Enabled** to allow access to upgrade the Router remotely from outside the local network. Otherwise, keep the default setting, **Disabled**. This option is available only if the Remote Management feature enabled.
- **Allow Remote IP Address:** If you enabled Remote Management, you can allow access from any IP address, from a single IP address, or from a range of IP addresses. Choose one of the following options:
 - **To allow remote access from any site:** Click **Any IP Address**.
 - **To allow access from a single IP address:** Click the radio button next to the first text box, and then enter the IP address in the text boxes. Ignore the final text box after the ~ symbol.
 - **To allow access from a range of IP addresses:** Click the radio button next to the first text box. Enter the first IP address in the first four text boxes, and then enter the final octet of the final IP address in the text box next to the ~ symbol. The following example illustrates a range from 209.165.200.225 to 209.165.200.230.

Allow Remote IP Address: ☒ Any IP Address ☐ ~

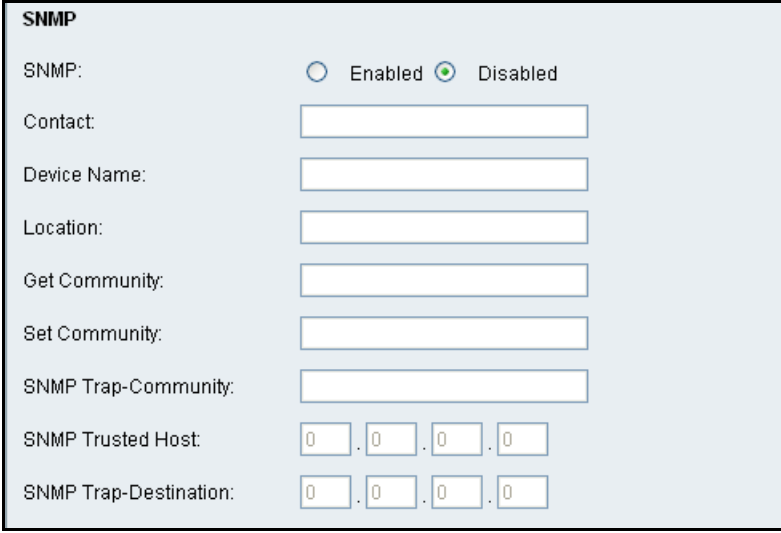
- **Remote Management Port:** Enter the port number that is open to outside access. The default setting is **8080**.

STEP 4 Click **Save** to save your settings, or click **Cancel** to refresh the page with the previously saved settings.

Configuring SNMP Settings for Status Reporting

SNMP, Simple Network Management Protocol, is a network protocol that provides network administrators with the ability to monitor the status of the Router and receive notification of any critical events as they occur on the network.

Configure this feature in the **SNMP** section of the Administration > Management page.



STEP 1 Click **Administration > Management** in the navigation tree.

STEP 2 In the **SNMP** section, configure the following settings:

- **SNMP:** To enable SNMP, check the **Enabled** box. To disable this feature, click **Disabled**.
- **SNMP:** Select **Enable** if you wish to use SNMP. To use SNMP, you need SNMP software on your PC.
- **Contact:** Enter the contact information for the Router.

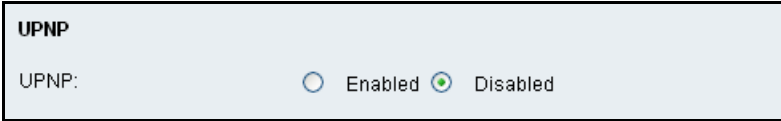
- **Device Name:** Enter a suitable name to identify this device in the SNMP software.
- **Location:** Enter the location of the Router.
- **Get Community:** Enter the SNMP community name for SNMP “Get” commands.
- **Write Community:** Enter the SNMP community name for SNMP “Set” commands.
- **SNMP Trap-Community:** Enter the SNMP community name for SNMP “Trap” commands.
- **SNMP Trusted Host:** Enter the IP address of the machine where you are running the SNMP software.
- **SNMP Trap-Destination:** Enter the IP address of the SNMP Manager to send traps to. If desired, this may be left blank.

STEP 3 Click **Save** to save your settings, or click **Cancel** to refresh the page with the previously saved settings.

Configuring Universal Plug and Play (UPnP) Settings

Universal Plug and Play (UPnP) can be used to set up public services on your network. When the UPnP function is enabled, Windows XP can add or delete entries to the underlined UPnP Forwarding Table. Some Internet games require enabling UPnP.

Manage this feature in the **UPNP** section of the Administration > Management page.



UPNP

UPNP: ☐ Enabled ☒ Disabled

STEP 1 Click **Administration > Management** in the navigation tree.

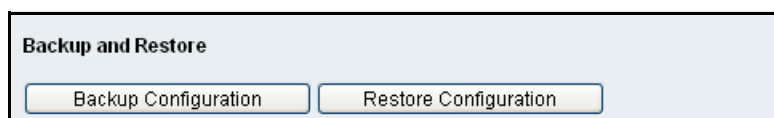
STEP 2 In the **UPNP** section, click **Enabled** to enable UPnP, or click **Disabled** to disable this feature.

- STEP 3** Click **Save** to save your settings, or click **Cancel** to refresh the page with the previously saved settings.

Backing and Restoring a Configuration

Cisco recommends that you periodically back up your configuration. This practice is especially helpful before you make significant changes in the settings. If you are dissatisfied with the results, you easily can restore the previous configuration from your backup file.

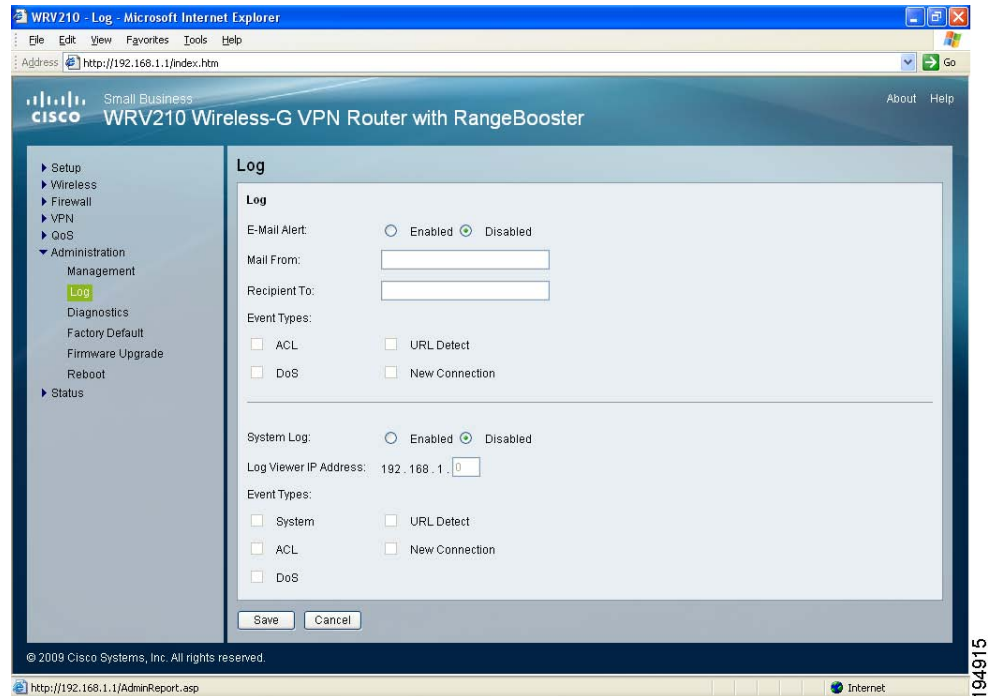
Manage these files in the **Backup and Restore** section of the Administration > Management page.



- STEP 1** Click **Administration > Management** in the navigation tree.
- STEP 2** In the **Backup and Restore** section, use the buttons to back up or restore your configuration, as needed:
- **To back up your current configuration:** Click **Backup Configuration**. When the **File Download** window appears, click **Save**. Find the location where you want to save the file, and then click **Save**. A message appears when the download is complete. The file is a .bin file. You can change the filename before saving, if you choose to do so.
 - **To restore a previously saved configuration:** Click **Restore Configuration**. click **Restore Configuration**. When the **File Path** field appears, type the file path or click **Browse** to find the .bin file that you saved in the previous backup operation. Finally, click **Load**. After a few minutes, a message appears: *Your changes have been saved. System Rebooting... Please wait.* When the Basic Setup page appears, the process is finished.
- STEP 3** Click **Save** to save your settings, or click **Cancel** to refresh the page with the previously saved settings.

Setting Up Alerts and System Logs

Use the Administration > Log page to log system activity. You can choose to enable email alerts for specified events, and you can configure the system log to send the information to a syslog server.



You can choose the following types of events:

- **ACL:** A violation of an access policy, as set on the Wireless > Wireless Network Access page
- **DoS:** A Denial of Service attack, assuming that DoS prevention is enabled on the Firewall > General page
- **URL Detect:** A violation of URL filtering, as set on the Firewall > URL Filtering page
- **New Connection:** May involve the following two scenarios: (1) remote management is enabled and a remote client establishes a management connection, and (2) port forwarding or DMZ is enabled, and traffic is allowed into the private network through this service

- **System** (for system logs only, not email alerts): May include system shutdown/startup, VPN connections, system processes, interface status changes, and DHCP events

STEP 1 Click **Administration > Log** in the navigation tree.

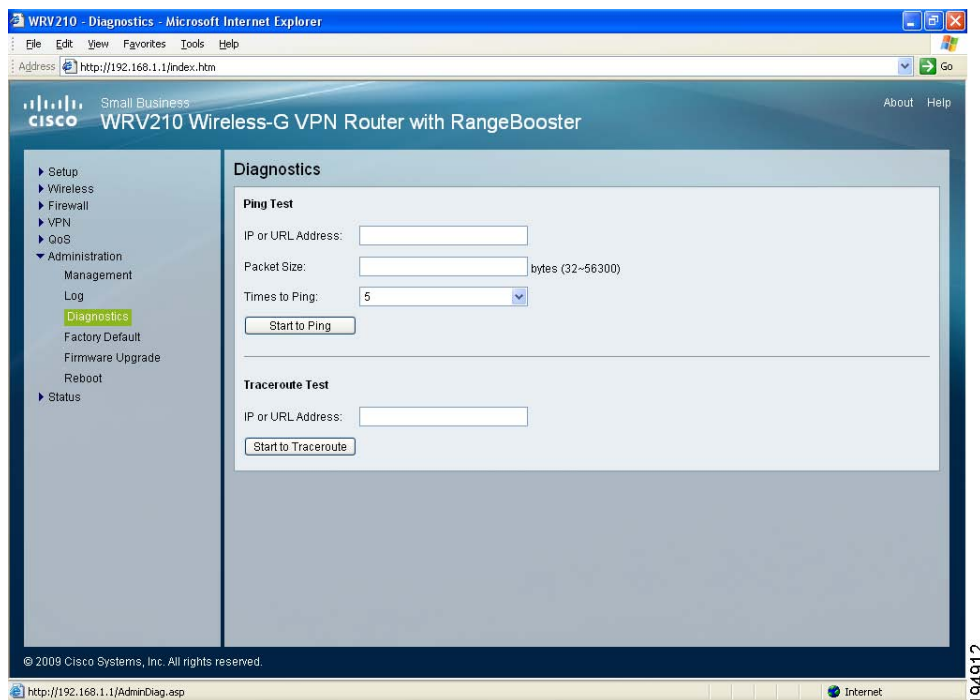
STEP 2 Configure the following settings, as needed:

- **E-Mail Alert:** Click **Enabled** to enable the router to send e-mail alerts when specified events occur. If you do not wish to have email alerts, select **Disabled**. If you enable this feature, also enter the following information:
 - **Mail From:** Enter the sender's email address to identify the message when it is sent to the Recipient.
 - **Recipient To:** Enter the email address where you want the alerts to be sent.
 - **Event Types:** Check the box for each type of event that will trigger an alert. Uncheck the box for each type of event that you do not want to include.
- **System Log:** Click **Enabled** to keep a log of the specified events. Click **Disabled** if you do not wish to keep a log. This feature requires the installation of an external log viewer or syslog viewer on your PC. If you enable the system log, also check the box for each type of event that you want to include in the log.
 - **Logviewer IP Address:** Enter the address where you want the system log to be sent.
 - **Event Types:** Check the box for each type of event to include in the log. Uncheck the box for each type of event that you do not want to include.

STEP 3 Click **Save** to save your settings, or click **Cancel** to refresh the page with the previously saved settings.

Performing Diagnostic Tests

Use the Administration > Diagnostics page to check the connections of your network components.



STEP 1 Click **Administration > Diagnostics** in the navigation tree.

STEP 2 Perform a Ping Test or a Traceroute Test, as described below:

Ping Test: To verify connectivity between devices, a ping utility sends a request, known as an ICMP echo-request packet, to the designated device. The device responds with an echo reply. If there is no connectivity to the device, the request times out.

a. Enter the following information:

- **IP or URL Address:** Enter the IP address or URL address of the network device whose connection status you wish to test.
- **Packet Size:** Enter the size of the ping packets, in bytes. Acceptable values are 32 to 56300.

- **Times to Ping:** Enter the number of times that you want to ping the device: **5, 10, 15, or Unlimited.**
- b. Click **Start to Ping** to start the test. The results of the test appear in a new window.
 - Click **Stop** to stop the test.
 - Click **Clear Log** to clear the results.
 - Click **Close** to return to the Administration > Diagnostics page.

Traceroute Test:

- a. In the **IP or URL Address** field, enter the IP or URL address of the network device whose performance you wish to test.
- b. Click **Start to Traceroute** to start the test. The results of the test appear in a new window.
 - Click **Stop** to stop the test.
 - Click **Clear Log** to clear the results.
 - Click **Close** to return to the Administration > Diagnostics page.

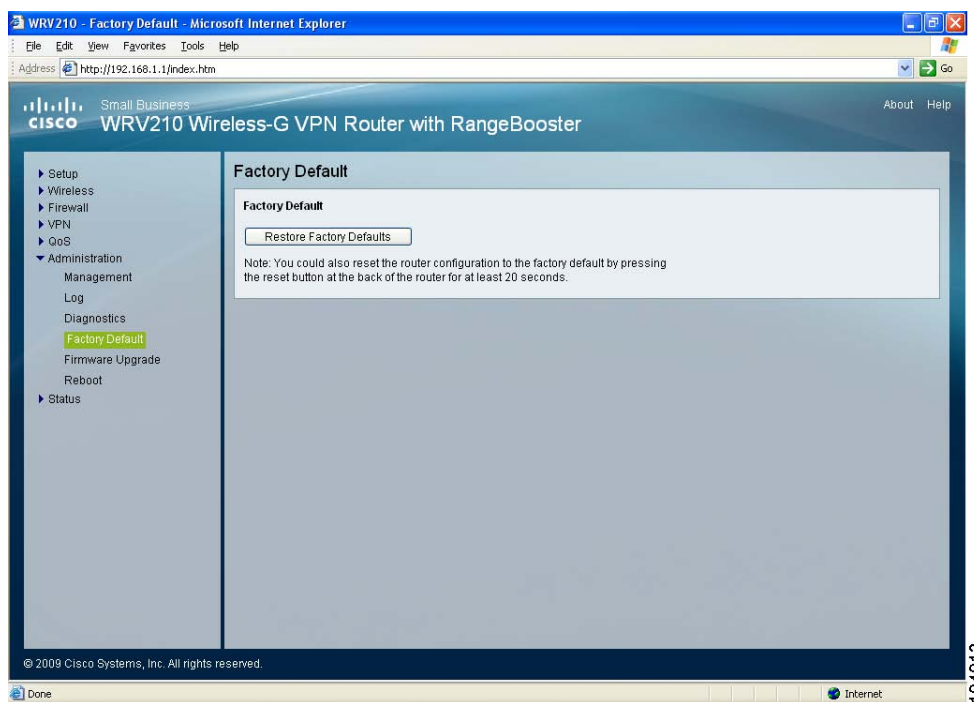
STEP 3 Click **Save** to save your settings, or click **Cancel** to refresh the page with the previously saved settings.

Reverting to the Factory Default Settings

The Administration > Factory Defaults page allows you to restore the Router's configuration to its factory default settings.

**NOTE**

Do not restore the factory defaults unless you are having difficulties with the Router and have exhausted all other troubleshooting measures. After the Router is reset, you have to re-enter all of your configuration settings, or use the Restore Configuration process to restore the settings from a previously saved file.



STEP 1 Click **Administration > Factory Default** in the navigation tree.

STEP 2 To reset all configuration settings to their factory default values, click **Restore Factory Defaults**.

STEP 3 Click **OK** to confirm the operation and continue.

When the operation is completed, all configuration settings revert to their original factory default values and all previous settings are lost.

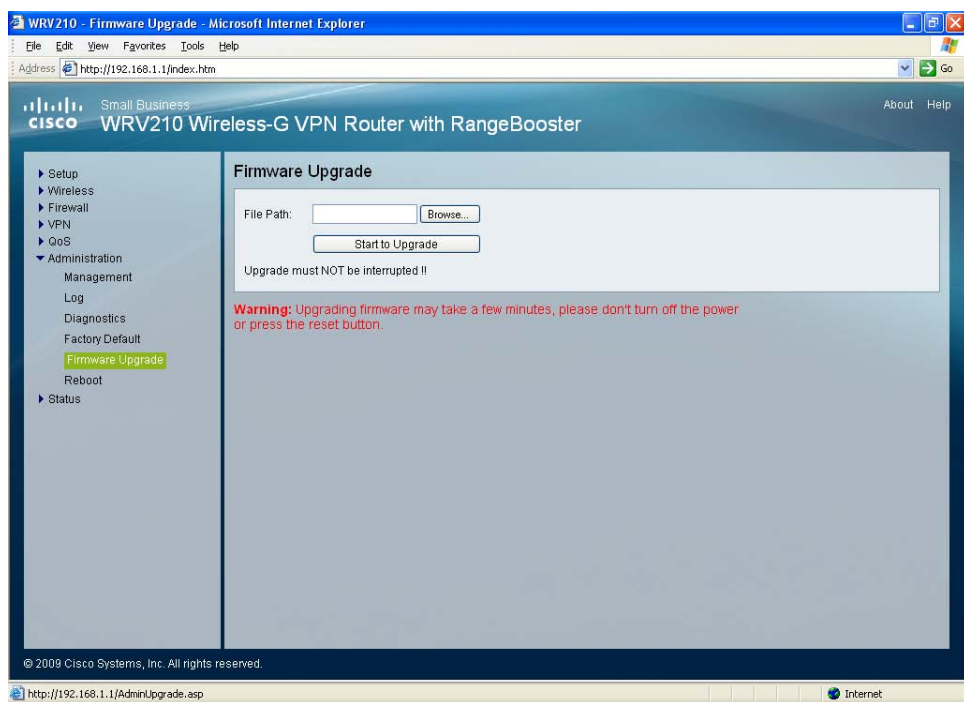
Upgrading the Firmware

Use the Administration > Firmware Upgrade page to upgrade the Router's firmware. Do not upgrade the firmware unless you are experiencing problems with the Router or the new firmware has a feature you want to use.



NOTE

If you upgrade the firmware, the Router loses all of the settings you have customized. Before performing the upgrade, be sure to back up your configuration as described below. After the upgrade, you can restore the saved configuration.



STEP 1 Back up the current configuration:

- a. In the Router Configuration Utility, click **Administration > Management**.
- b. In the **Backup and Restore** section, click **Backup Configuration**. When the **File Download** window appears, click **Save**. Find the location where you want to save the file, and click **Save**. A message appears when the download is complete. The file is a .bin file. You can change the filename before saving, if you choose to do so.

STEP 2 Download the new firmware:

- a. Start a web browser, and enter the following address:
tools.cisco.com/support/downloads
- b. When prompted, enter your Cisco online login.
- c. In the **Software Search** box, enter **WRV210**. Click **Go**.
- d. Follow the instructions to find the latest firmware and download it to your PC.

STEP 3 Perform the upgrade:

- a. Click **Administration > Firmware Upgrade**.
- b. Enter the **File Path** to the new firmware file. Alternatively, click **Browse**, locate the file, and then click **Open** to display the path in the field.
- c. Click **Start to Upgrade**. Once you have selected the appropriate file, click **Start to Upgrade**.



NOTE Do not turn off power or close your browser window during the upgrade process.

The progress is indicated in the status bar at the bottom of the browser window. After a few minutes, the following message appears: *Your changes have been saved. System Rebooting... Please wait.* When the Basic Setup page appears, the upgrade process is finished.

STEP 4 Verify the upgrade:

- a. Click **Status > Router** in the navigation tree.
- b. Verify that the **Software Version** matches the version number of the new firmware that you installed.

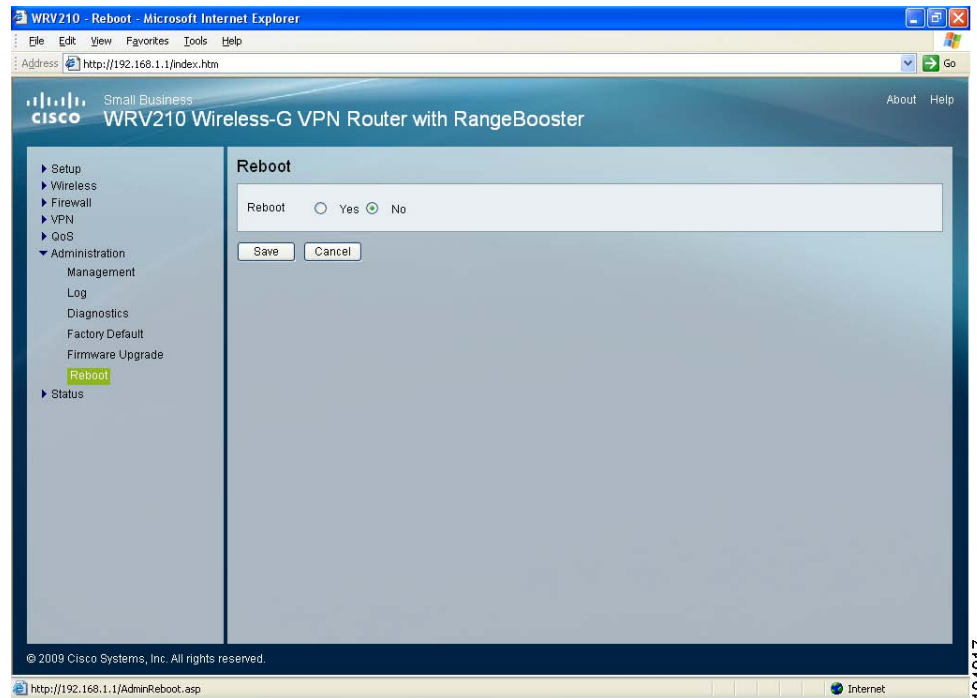
STEP 5 When the upgrade is finished, restore your previously saved settings:

- a. In the Router Configuration Utility, click **Administration > Management**.
- b. In the **Backup and Restore** section, click **Restore Configuration**. When the **File Path** field appears, type the file path or click **Browse** to find the .bin file that you saved in the previous backup operation. Finally, click **Load**.

After a few minutes, a message appears: *Your changes have been saved. System Rebooting... Please wait.* When the Basic Setup page appears, the process is finished.

Rebooting the Router

The Administration > Reboot page allows you to restart the Router without losing any of its stored settings. You may wish to reboot the router during remote troubleshooting.



STEP 1 Click **Administration > Reboot** in the navigation tree.

STEP 2 To reboot the router, click **Yes** to confirm and then click **Save**. If you do not want to reboot the router, click **No** or **Cancel**.

Monitoring the Status of the Network

Use the Status module to monitor your network.

- [Monitoring the Router Status, page 96](#)
- [Monitoring the LAN, page 97](#)
- [Monitoring the Wireless Network, page 99](#)
- [Monitoring the System Performance, page 100](#)
- [Monitoring the QuickVPN Clients, page 102](#)

Monitoring the Router Status

The Status > Router page displays information about the Router and its current settings. The on-screen information varies depending on the Internet Connection Type selected on the Basic Setup page.

**NOTE**

The page automatically refreshes every 10 seconds.

- **Hardware Version:** The installed version and date of the hardware
- **Software Version:** The installed version and date of the software
- **Current Time:** The current time
- **System Up Time:** The time elapsed since the last system reboot
- **MAC Address:** The MAC Address of the Router's Internet interface
- **Host Name:** The host name that was entered on the Basic Setup page, if applicable
- **Domain Name:** The domain name that was entered on the Basic Setup page, if applicable

- **Connection Type:** The Internet connection type
- **IP Address:** The Router's Internet IP Address
- **Subnet Mask and Default Gateway:** The Router's Subnet Mask and Default Gateway address for DHCP and static IP connections
- **DNS:** The DNS (Domain Name Server) IP addresses currently used by the Router
- **Release:** Click this button to release the current IP address of the device connected to the Router's Internet port. This button is available only if the Router has a DHCP connection.
- **Renew:** Click this button to renew the current IP address of the device that is connected to the Router's Internet port. This button is available only if the Router has a DHCP connection.
- **Refresh:** Click this button to update the on-screen information.

Monitoring the LAN

The Status > Local Network page displays information about the local network.



Local Network

- **Local MAC Address:** The MAC Address of the Router's LAN (local area network) interface
- **IP Address:** The Router's local IP address
- **Subnet Mask:** The Router's subnet mask

DHCP Server

- **DHCP Server:** The status of the DHCP server on the Router
- **Start IP:** The first IP address in the range of addresses that the DHCP server issues to connected devices on the local network
- **End IP:** The final IP address in the range of addresses that the DHCP server issues to connected devices on the local network
- **DHCP Clients Table:** Click this button to view a list of PCs that have been assigned IP addresses by the Router. The DHCP Active IP Table lists the DHCP Server IP Address, Computer Names, IP Addresses, MAC Addresses, and length of time until a computer's assigned IP address expires. Click **Close** to return to the Local Network page. Click **Refresh** to update the information.
- **Refresh:** Click this button to update the on-screen information.

Monitoring the Wireless Network

The Status > Wireless page displays status information about your wireless network. The information appears for each configured SSID (SSID1 through SSID4).



NOTE

The page automatically refreshes every 10 seconds.

- **Mode:** The wireless mode (Mixed, G-Only, or Disabled) used by the network
- **Wireless Channel:** The channel on which your wireless network is broadcasting
- **Wireless Network Name (SSID):** The SSID of your network
- **MAC Address:** The MAC Address of the SSID listed in the table and on your network
- **Security Mode:** The type of wireless security that is used by the Router
- **WMM:** The status of the Router's WMM feature: Enabled or Disabled

- **Refresh:** Click this button to update the on-screen information.

Monitoring the System Performance

The Status > System Performance page displays status information about network traffic for the Internet, wireless activities, and wired connectivity.

System Performance

Internet / Wireless

Name	Internet	SSID1	SSID2	SSID3	SSID4
Connection	Disconnected	Connected	Disconnected	Disconnected	Disconnected
Packets Received	0	0	0	0	0
Packets Sent	0	778	0	0	0
Bytes Received	0	0	0	0	0
Bytes Sent	0	95114	0	0	0
Error Packets Received	0	0	0	0	0
Drop Received Packets	0	0	0	0	0

LAN

Name	Port1	Port2	Port3	Port4
Connection	Connected	Disconnected	Disconnected	Disconnected
Packets Received	12999			
Packets Sent	17308			
Bytes Received	1455989			
Bytes Sent	11625556			
Error Packets Received	0			
Drop Received Packets	0			

Refresh

© 2009 Cisco Systems, Inc. All rights reserved.



NOTE

The page automatically refreshes every 10 seconds.

Internet/Wireless:

Statistics for the network traffic on the Internet connection and wireless connectivity are shown in five separate columns.

- **Connection:** The status of the connection

- **Packets Received:** The number of packets received
- **Packets Sent:** The number of packets sent
- **Bytes Received:** The number of bytes received
- **Bytes Sent:** The number of bytes sent
- **Error Packets Received:** The number of error packets received
- **Dropped Packets Received:** The number of dropped packets received

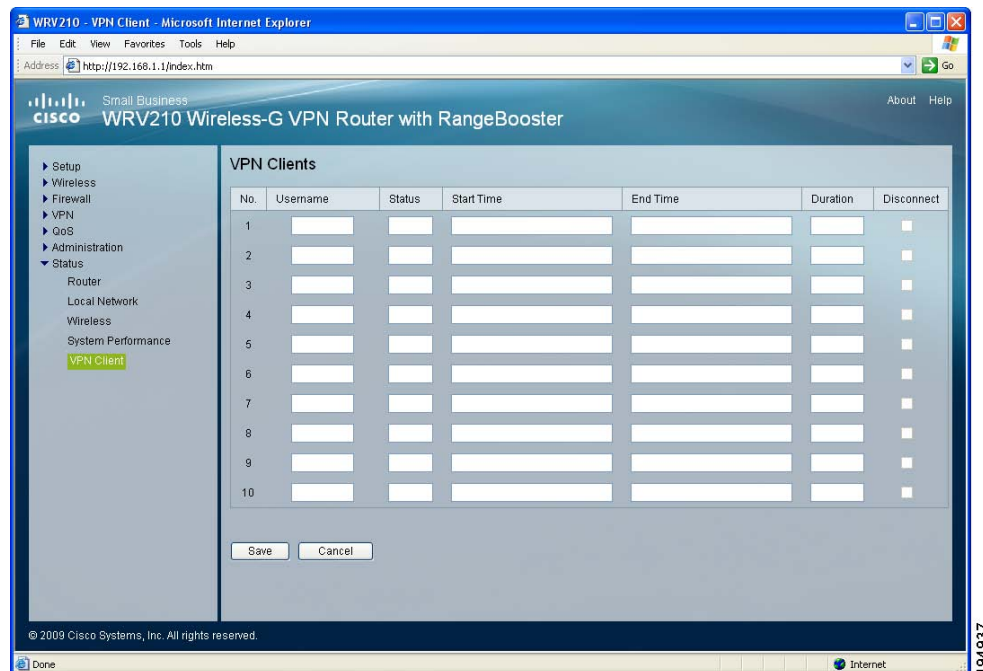
LAN

Statistics for the network traffic on each of the four LAN ports are shown in four separate columns.

- **Connection:** The status of the connection
- **Packets Received:** The number of packets received
- **Packets Sent:** The number of packets sent
- **Bytes Received:** The number of bytes received
- **Bytes Sent:** The number of bytes sent
- **Error Packets Received:** The number of error packets received
- **Dropped Packets Received:** The number of dropped packets received
- **Refresh:** Click this button to update the on-screen information.

Monitoring the QuickVPN Clients

The Status > VPN Client Status page displays status information about the Router's QuickVPN clients.



NOTE

The page automatically refreshes every 10 seconds.

- **No.:** The identification number assigned to the VPN client.
- **Username:** The Username assigned to the VPN client appears here
- **Status:** The status of the VPN connection
- **Start Time:** The time the VPN connection began
- **End Time:** The time the VPN connection ended
- **Duration:** The length of time that the VPN connection has lasted
- **Disconnect:** Check the **Disconnect** box for each VPN client that you want to disconnect. Then click the **Disconnect** button.
- **Refresh:** Click this button to update the on-screen information.

Specifications

Feature	Details
Specifications	
Model	WRV210
Standards	IEEE802.11g, IEEE802.11b, IEEE802.3, IEEE802.3u, 802.1x (Security Authentication), 802.11i (Security WPA2), 802.11e (Wireless QoS)
Ports	One Power port (12V 1A), Four 10/100 RJ-45 LAN ports, One 10/100 RJ-45 Internet port
Buttons	Reset
Cabling Type	UTP CAT 5
LEDs	Power, DMZ, Wireless, Internet, LAN 1-4
Operating System	Linux
Performance	
NAT Throughput	93 Mbps
IPSec Throughput	23 Mbps (3DES)
Setup/Config	
User Interface	Built-in Web UI for easy browser-based configuration (HTTP/HTTPS)
Management	
SNMP Version	SNMP version 1, 2c
Event Logging	Local, Syslog, E-mail

Feature	Details
Firmware Upgrade	Firmware Upgradeable Through Web Browser and TFTP Utility
Diagnostics	Flash, RAM, LAN, WLAN
Wireless	
Spec/Modulation	Radio and Modulation Type: 802.11b/DSSS, 802.11g/OFDM
Supported Data Rates	802.11b: 1, 2, 5.5, 11 Mbps 802.11g: 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
Operating Channels	11 North America, 13 Most of Europe (ETSI and Japan)
External Antennae	2 Omnidirectional
Antenna connector type	Fixed
Transmit Power	Transmit Power (adjustable) @ Normal Temp Range: 802.11g: -18 dBm (typical); 802.11b: -20 dBm (typical)
Adjustable Power	Yes
Antenna Gain	2 dBi
Receiver Sensitivity	802.11g: 54 Mbps @ -69 dBm (typical), 802.11b: 11 Mbps @ -82 dBm (typical)
Wireless QoS	WMM. 802.11e
Security Features	
802.1X RADIUS Auth.	802.1x - RADIUS (MD5, SHA1, TLS, TTLS, PEAP) Dynamically Varying Encryption
Access Control	Access Control List (ACL) Capability: MAC-based and IP-based
Firewall	SPI Stateful Packet Inspection Firewall
DoS	Denial of Service Prevention

Feature	Details
Secure Management	HTTPS, Username/Password
Network	
VLAN Support	4 LAN Ports and 4 SSIDs can be mapped to up to 5 VLANs
SSID Broadcast	SSID Broadcast Enable/Disable
Multiple SSID	Supports Multiple BSSIDs (4) which can operate on pre-defined schedules
Wireless VLAN Map	Supports SSID-to-VLAN Mapping with Wireless Client Isolation
WDS	Allows Wireless Signals to be Repeated by up to 3 Repeaters
DMZ Host	A LAN PC can be configured as a DMZ Host
PPPoE	Dual PPPoE User Profiles
ALG Support	FTP, PPTP, L2TP, IPSec
VPN	
Tunnels	10 IPSec Tunnels with QuickVPN support
Encryption	3DES/AES Encryption
Authentication	MD5/SHA1 Authentication
NAT Traversal	IPSec
Routing	
	Static and RIP v1, v2
Environmental	
Dimensions	6.69" x 1.65" x 7.62" (170 x 42 x 193.5 mm)
Unit Weight	0.78 lb (0.355 kg)

Feature	Details
Power	12V 1A
Certification	FCC Class B, CE, IC
Operating Temp.	32 to 104°F (0 to 40°C)
Storage Temp.	-4 to 158°F (-20 to 70°C)
Operating Humidity	10 to 85% Noncondensing
Storage Humidity	5 to 90% Noncondensing

Where to Go From Here

Cisco provides a wide range of resources to help you and your customer obtain the full benefits of the WRV210.

Product Resources

Support	
Cisco Small Business Support Community	www.cisco.com/go/smallbizsupport
Online Technical Support and Documentation (Login Required)	www.cisco.com/support
Phone Support Contacts	www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html
Software Downloads (Login Required)	Go to tools.cisco.com/support/downloads , and enter the model number in the Software Search box.
Product Documentation	
Cisco Small Business Routers (Login Required)	http://www.cisco.com/en/US/partner/products/ps9923/tsd_products_support_series_home.html
Cisco Small Business	
Cisco Partner Central for Small Business (Partner Login Required)	www.cisco.com/web/partners/sell/smb
Cisco Small Business Home	www.cisco.com/smb
Marketplace	www.cisco.com/go/marketplace