



ADMINISTRATION GUIDE

Cisco Small Business

WRVS4400N Wireless-N Gigabit Security Router
with VPN

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned 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. (1005R)

Chapter 1: Introduction	6
Chapter 2: Networking and Security Basics	8
An Introduction to LANs	8
The Use of IP Addresses	9
The Intrusion Prevention System (IPS)	11
Chapter 3: Planning Your Virtual Private Network (VPN)	13
Why do I need a VPN?	13
What is a VPN?	15
Chapter 4: Getting Started with the WRVS4400N Router	18
Front Panel	19
Back Panel	20
WRVS4400N Antennas	20
Placement Options	21
Installing the Router	24
Configuring the Router	26
Chapter 5: Setting Up and Configuring the WRVS4400N Wireless-N Router	28
Accessing the Web-Based Utility	29
Navigating the Utility	30
Setting Up Your Wireless-N Router	36
Configuring Wireless Settings	68
Configuring Firewall Settings	88
Configuring the ProtectLink Web Service	104
Configuring the VPN Settings	105
Configuring the QoS Settings	118
Configuring the Administration Settings	123
Configuring IPS Settings	135

Configuring the L2 Switch Settings	141
Viewing Status	152
Chapter 6: Using the VPN Setup Wizard	160
VPN Setup Wizard	160
Before You Begin	160
Running the VPN Router Software Wizard	161
Appendix A: Troubleshooting	178
Frequently Asked Questions	191
Appendix B: Using Cisco QuickVPN for Windows 2000, XP, or Vista	195
Overview	195
Before You Begin	196
Installing the Cisco QuickVPN Software	197
Using the Cisco QuickVPN Software	199
Distributing Certificates to QuickVPN Users	202
Appendix C: Configuring a Gateway-to-Gateway IPSec Tunnel	203
Introduction	203
Environment	204
Configuring the VPN Settings for the VPN Routers	204
Configuring the Key Management Settings	206
Configuring PC 1 and PC 2	207
Appendix D: Finding Out MAC and IP Addresses	208
Windows 98 or Me Instructions	208
Windows 2000 or XP Instructions	209
For the Router's Web-based Utility	209

Appendix E: Cisco ProtectLink Web Service	210
Overview	210
How to Access the Web-Based Utility	210
How to Purchase, Register, or Activate the Service	211
How to Use the Service	214
Appendix F: Specifications	219
General	219
Performance	220
Management	220
Security	221
QoS	221
Layer 2	222
Environmental	222
Appendix G: Where to Go From Here	223

Introduction

Thank you for choosing the Cisco WRVS4400N Wireless-N Gigabit Security Router with VPN. The Wireless-N Gigabit Security Router with VPN is an advanced Internet-sharing network solution for your small business needs. WRVS4400N lets multiple computers in your office share an Internet connection through both wired and wireless connections.

The WRVS4400N wireless router features a built-in 4-Port full-duplex 10/100/1000 Ethernet switch, which allows you to connect four personal computers directly, or you can connect more hubs and switches to create as big a network as you need.

You can use the WRVS4400N wireless router as an intranet router to aggregate traffic to a company backbone network.

The WRVS4400N wireless router has a built-in access point that supports the latest 802.11n draft specification by IEEE. The WRVS4400N wireless router also supports 802.11g and 802.11b clients in a mixed environment.

The built-in access point can support an 11n data rate of up to 300 Mbps. In addition to having a higher data rate, 802.11n technology also promises longer coverage by using multiple antennas to transmit and receive data streams in different directions.

The Cisco WRVS4400N Wireless-N Gigabit Security Router with VPN is equipped with advanced security technologies like Intrusion Prevention System (IPS), Stateful Packet Inspection (SPI) Firewall, IP based Access List (IP ACL), and Network Address Port Translation (NAPT, also called NAT as a more generic term).

These technologies work together by providing self-defensive strategy. They identify, classify, and stop malicious attack traffic in real time while passing through the WRVS4400N wireless router.

The SPI Firewall provides deep packet inspection to analyze packets in network layer (IP) and transport layer (TCP, UDP) to block illegal packet transactions. You can also use IP based ACL to limit traffic to a specific source, destination and protocol.

NAPT allows you to open specific TCP/UDP port numbers to the Internet to provide limited service while minimizing harmful traffic at the same time.

The Virtual Private Network (VPN) capability is another security feature that creates encrypted “tunnels” through the Internet, allowing up to five remote offices and five traveling users to securely connect into your office network from off-site.

Users connecting through a VPN tunnel are attached to your company’s network with secure access to files, e-mail, and your intranet as if they were in the building. You can also use the VPN capability to allow users on your small office network to securely connect out to a corporate network.

The QoS features of the Cisco WRVS4400N Wireless-N Gigabit Security Router with VPN provide consistent voice and video quality throughout your business.

This administration guide gives you all the information you need to connect, set up, and configure your router.

Networking and Security Basics

This chapter describes networking and security basics. It includes the following sections:

- [An Introduction to LANs, page 8](#)
- [The Use of IP Addresses, page 9](#)
- [The Intrusion Prevention System \(IPS\), page 11](#)

An Introduction to LANs

A router is a network device that connects two networks together.

The router connects your local area network (LAN), or the group of personal computers in your home or office, to the Internet. The router processes and regulates the data that travels between these two networks.

The router's Network Address Translation (NAT) technology protects your network of personal computers so users on the Internet cannot "see" your personal computers. This is how your LAN remains private. The router protects your network by inspecting the first packet coming in through the Internet port before delivery to the final destination on one of the Ethernet ports. The router inspects Internet port services like the web server, FTP server, or other Internet applications, and, if allowed, it will forward the packet to the appropriate personal computer on the LAN side.

You can use multiple Cisco WRVS4400N Wireless-N Gigabit Security Routers to connect multiple LANs together. This usually applies to a medium-sized or larger company where you want to divide your network into multiple IP subnets to increase the intranet throughput and reduce the size of the IP broadcast domain and its interference. In this case, you need one WRVS4400N wireless router for each subnetwork and you can connect all the WAN ports to a second level router or switch to the Internet.

The second level router only forwards data packets through a wired network so you don't have to use the Cisco WRVS4400N Wireless-N Gigabit Security Router. You can use any wired router in the Cisco family such as RVS4000 that has 4 LAN ports and 1 WAN port.



The Use of IP Addresses

IP stands for Internet Protocol. Every device in an IP-based network, including personal computers, print servers, and routers, requires an IP address to identify its location, or address, on the network. This applies to both the Internet and LAN connections.

There are two ways of assigning IP addresses to your network devices.

A static IP address is a fixed IP address that you assign manually to a personal computer or other device on the network. Since a static IP address remains valid until you disable it, static IP addressing ensures that the device assigned it will always have that same IP address until you change it. Static IP addresses are commonly used with network devices such as server personal computers or print servers.

If you use the router to share your cable or DSL Internet connection, contact your ISP to find out if they have assigned a static IP address to your account. If so, you will need that static IP address when configuring the router. You can get the information from your ISP.

A dynamic IP address is automatically assigned to a device on the network. These IP addresses are called dynamic because they are only temporarily assigned to the personal computer or other device. After a certain time period, they expire and may change. If a personal computer logs onto the network (or the Internet) and its dynamic IP address has expired, the DHCP server will assign it a new dynamic IP address.

A DHCP server can either be a designated personal computer on the network or another network device, such as the router. By default, the router's Internet Connection Type is **Obtain an IP automatically (DHCP)**.

The personal computer or network device obtaining an IP address is called the DHCP client. DHCP frees you from having to assign IP addresses manually every time a new user is added to your network.

For DSL users, many ISPs may require you to log on with a user name and password to gain access to the Internet. This is a dedicated, high-speed connection type called Point to Point Protocol over Ethernet (PPPoE). PPPoE is similar to a dial-up connection, but PPPoE does not dial a phone number when establishing a connection. It also will provide the router with a dynamic IP address to establish a connection to the Internet.

By default, a DHCP server (on the LAN side) is enabled on the router. If you already have a DHCP server running on your network, you **MUST** disable one of the two DHCP servers. If you run more than one DHCP server on your network, you will experience network errors, such as conflicting IP addresses. To disable DHCP on the router, see [Configuring Local Area Network \(LAN\) Settings, page 52](#)



NOTE Since the router is a device that connects two networks, it needs two IP addresses—one for the LAN, and one for the Internet. In this Administration Guide, you'll see references to the "Internet IP address" and the "LAN IP address".

Since the router uses NAT technology, the only IP address that can be seen from the Internet for your network is the router's Internet IP address. However, even this Internet IP address can be blocked so the router and network seem invisible to the Internet.

The Intrusion Prevention System (IPS)

IPS is an advanced technology to protect your network from malicious attacks. IPS works together with your SPI Firewall, IP Based Access Control List (ACL), Network Address Port Translation (NAPT), and Virtual Private Network (VPN) to achieve the highest level of security. IPS works by providing real-time detection and prevention as an in-line module in a router.

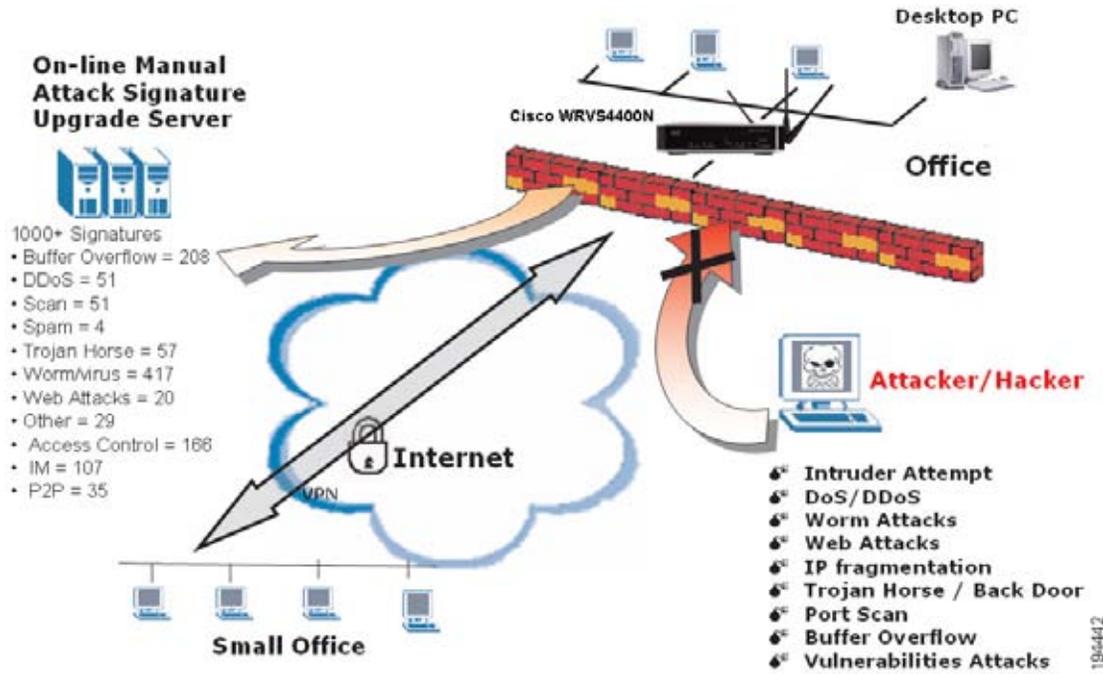
The WRVS4400N wireless router has hardware-based acceleration for real-time pattern matching for detecting malicious attacks. It actively filters and drops malicious TCP/UDP/ICMP/IGMP packets and can reset TCP connections. This protects your client personal computers and servers running various operating systems including Windows, Linux, and Solaris from network worm attacks. However, this system does not prevent viruses contained in e-mail attachments.

The P2P (peer to peer) and IM (instant messaging) control allows you to prevent network users from using those protocols to communicate with people over the Internet. This helps the administrators to set up company policies on how to use their Internet bandwidth wisely.

The signature file is the heart of the IPS system. It is similar to the virus definition files on your personal computer's Anti-Virus programs. IPS uses this file to match against packets coming in to the Router and performs actions accordingly. As of today, the Wireless-N Router is shipped with signature file version 1.3.8 and with a total of 1101 rules. The rules cover the following categories: DDoS, Buffer Overflow, Access Control, Scan, Trojan Horse, Misc., P2P, IM, Virus, Worm, and Web Attacks.

It is recommended that you update your IPS signature file regularly to thwart new attack types.

The following diagram illustrates a number of IPS scenarios.



Planning Your Virtual Private Network (VPN)

This chapter provides information for planning your VPN and includes the following sections:

- [Why do I need a VPN?, page 13](#)
- [What is a VPN?, page 15](#)

Why do I need a VPN?

Computer networking provides a flexibility not available when using an archaic, paper-based system. With this flexibility, however, comes an increased risk in security. This is why firewalls were first introduced. Firewalls help to protect data inside of a local network. But what do you do once information is sent outside of your local network, when e-mails are sent to their destination, or when you have to connect to your company's network when you are out on the road? How is your data protected?

That is when a VPN can help. VPNs are called Virtual Private Networks because they secure data moving outside of your network as if it were still within that network.

When data is sent out across the Internet from your computer, it is always open to attacks. You may already have a firewall, which will help protect data moving around or held within your network from being corrupted or intercepted by entities outside of your network, but once data moves outside of your network—when you send data to someone via e-mail or communicate with an individual over the Internet—the firewall will no longer protect that data.

At this point, your data becomes open to hackers using a variety of methods to steal not only the data you are transmitting but also your network login and security data. Some of the most common methods are as follows:

- [MAC Address Spoofing, page 14](#)
- [Data Sniffing, page 14](#)
- [Man in the Middle Attacks, page 14](#)

MAC Address Spoofing

Packets transmitted over a network, either your local network or the Internet, are preceded by a packet header. These packet headers contain both the source and destination information for that packet to transmit efficiently. A hacker can use this information to spoof (or fake) a MAC address allowed on the network. With this spoofed MAC address, the hacker can also intercept information meant for another user.

Data Sniffing

Data “sniffing” is a method used by hackers to obtain network data as it travels through unsecured networks, such as the Internet. Tools for just this kind of activity, such as protocol analyzers and network diagnostic tools, are often built into operating systems and allow the data to be viewed in clear text.

Man in the Middle Attacks

Once the hacker has either sniffed or spoofed enough information, he can now perform a “man in the middle” attack. This attack is performed, when data is being transmitted from one network to another, by rerouting the data to a new destination. Even though the data is not received by its intended recipient, it appears that way to the person sending the data.

These are only a few of the methods hackers use and they are always developing more. Without the security of your VPN, your data is constantly open to such attacks as it travels over the Internet. Data travelling over the Internet will often pass through many different servers around the world before reaching its final destination. That’s a long way to go for unsecured data and this is when a VPN serves its purpose.

What is a VPN?

A VPN, or Virtual Private Network, is a connection between two endpoints—a VPN router, for instance—in different networks that allows private data to be sent securely over a shared or public network, such as the Internet. This establishes a private network that can send data securely between these two locations or networks.

This is done by creating a “tunnel”. A VPN tunnel connects the two PCs or networks and allows data to be transmitted over the Internet as if it were still within those networks. Not a literal tunnel, it is a connection secured by encrypting the data sent between the two networks.

VPN was created as a cost-effective alternative to using a private, dedicated, leased line for a private network. Using industry standard encryption and authentication techniques—IPSec, short for IP Security—VPN creates a secure connection that, in effect, operates as if you were directly connected to your local network. VPN can be used to create secure networks linking a central office with branch offices, telecommuters, and/or professionals on the road (travelers can connect to a VPN router using any computer with the Cisco QuickVPN Client software.)

There are two basic ways to create a VPN connection:

- VPN router to VPN router
- Computer (using the Cisco QuickVPN Client software) to VPN router

The VPN router creates a “tunnel” or channel between two endpoints, so that data transmissions between them are secure. A computer with the Cisco QuickVPN Client software can be one of the two endpoints (refer to [Appendix B, “Using Cisco QuickVPN for Windows 2000, XP, or Vista”](#)). If you choose not to run the VPN client software, any computer with the built-in IPSec Security Manager (Microsoft 2000 and XP) allows the VPN router to create a VPN tunnel using IPSec (refer to [Appendix C, “Configuring a Gateway-to-Gateway IPSec Tunnel.”](#)). Other versions of Microsoft operating systems require additional, third-party VPN client software applications that support IPSec to be installed.

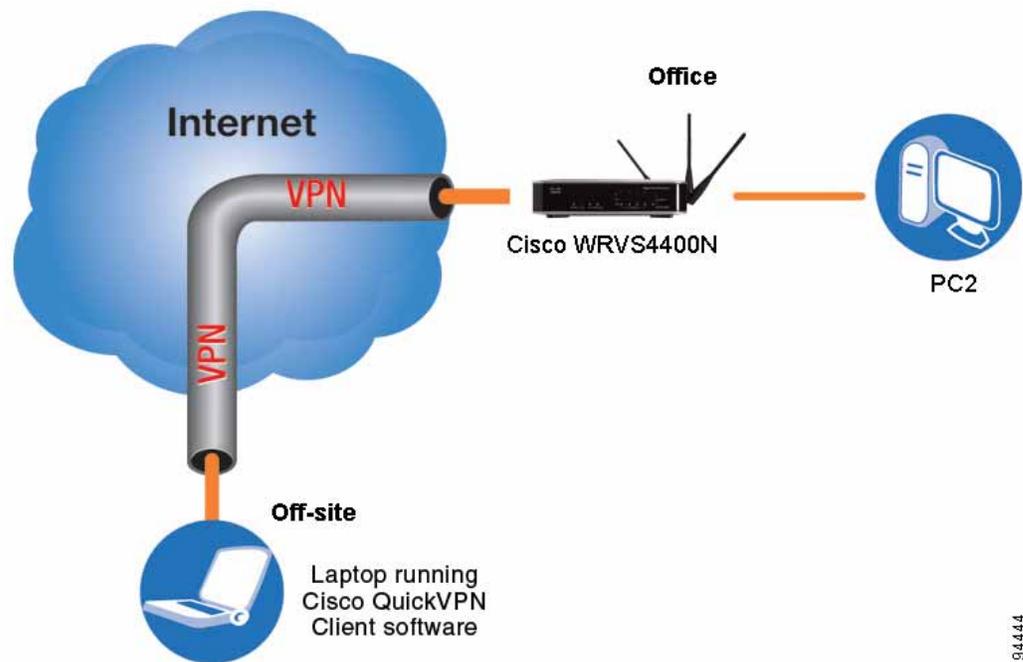
VPN Router to VPN Router

An example of a VPN router-to-VPN router VPN would be as follows. At home, a telecommuter uses his VPN router for his always-on Internet connection. His router is configured with his office's VPN settings. When he connects to his office's router, the two routers create a VPN tunnel, encrypting and decrypting data. As VPNs utilize the Internet, distance is not a factor. Using the VPN, the telecommuter now has a secure connection to the central office's network, as if he were physically connected. For more information, refer to [Appendix C, "Configuring a Gateway-to-Gateway IPSec Tunnel."](#)



Computer to VPN Router

The following is an example of a computer-to-VPN router VPN. In her hotel room, a traveling businesswoman connects to her ISP. Her notebook computer has the Cisco QuickVPN Client software, which is configured with her office's IP address. She accesses the Cisco QuickVPN Client software and connects to the VPN router at the central office. As VPNs utilize the Internet, distance is not a factor. Using the VPN, she now has a secure connection to the central office's network, as if she were physically connected.



For additional information and instructions about creating your own VPN, please visit www.cisco.com. You can also refer to **Appendix B, "Using Cisco QuickVPN for Windows 2000, XP, or Vista"**, and **Appendix C, "Configuring a Gateway-to-Gateway IPSec Tunnel."**

194444

Getting Started with the WRVS4400N Router

This chapter describes the physical features of the WRVS4400N router and provides information for installing the router. The following sections are included:

- [Front Panel, page 19](#)
- [Back Panel, page 20](#)
- [WRVS4400N Antennas, page 20](#)
- [Placement Options, page 21](#)
- [Installing the Router, page 24](#)
- [Configuring the Router, page 26](#)

Front Panel

The LEDs are located on the front panel of the router.

Front of Router



- POWER LED**—Lights up green to indicate the router is powered on. The LED flashes when the router is running a diagnostic test.
- DIAG LED**—If this light is off, the system is ready. The Diag LED blinks red during firmware upgrades.
- IPS LED**—The IPS LED lights up when the Intrusion Prevention System (IPS) function is enabled. If the LED is off, then IPS functions are disabled. The IPS LED flashes green when an external attack is detected. It flashes red when an internal attack is detected.
- Wireless LED**—The WIRELESS LED lights up when the wireless module is enabled. The LED is off when the wireless module is disabled. The WIRELESS LED flashes green when the data is transmitting or receiving on the wireless module.
- Ethernet Port LEDs 1-4**—For each LAN port, there are three LEDs. If a port LED is continuously lit green, the router is connected to a device at the speed indicated through the corresponding port (1, 2, 3, or 4). The LED flashes green when a router is actively sending or receiving data on that port.
- INTERNET LED**—The Internet LED lights up green to indicate the line speed of the device attached to the Internet port. If the router is connected to a cable or DSL modem, typically the 100 LED will be the only LED lit up, indicating 100 Mbps. Flashing indicates activity.

Back Panel

The Ethernet ports, Internet port, Reset button, and Power port are on the back panel of the router.



RESET Button—The Reset button can be used in two ways:

- If the router is having problems connecting to the Internet, press the Reset button for just a second with a paper clip or a pencil tip. This is similar to pressing the reset button on your personal computer to reboot it.
- If you are experiencing extreme problems with the router and have tried all other troubleshooting measures, press and hold in the Reset button for 10 seconds. This restores the factory defaults and clears all of the router settings, such as port forwarding or a new password.



INTERNET Port—Provides a WAN connection to a cable modem or DSL modem.



ETHERNET Ports 1-4—Provide a LAN connection to network devices, such as PCs, print servers, or additional switches.



POWER Port—Connects the router to power via the supplied AC power adapter.

WRVS4400N Antennas

The router has three non-detachable 1.8dBi omni-directional antennas. The three antennas have a base that can rotate 90 degrees when in the standing position.

The three antennas support 2X3 MIMO diversity in wireless-N mode.

Placement Options

You can place the router horizontally on the rubber feet, mount it in the stand, or mount it on the wall.

Desktop Option

For desktop placement, place the Cisco WRVS4400N router horizontally on a surface so it sits on its four rubber feet.



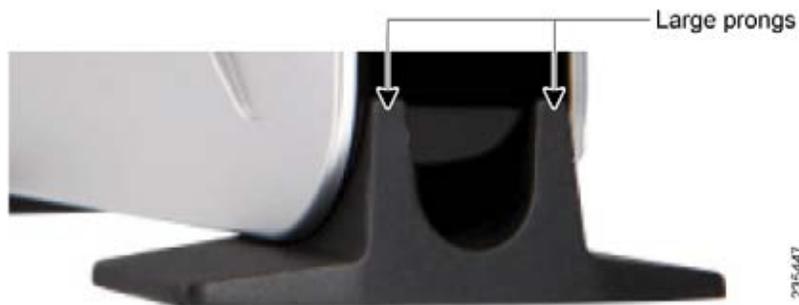
Stand Option

To install the router vertically in the supplied stands, follow the steps below.



To place the router vertically, follow these steps.

- STEP 1** Locate the left side panel of the router.
- STEP 2** With the two large prongs of one of the stands facing outward, insert the short prongs into the little slots in the router and push the stand upward until the stand snaps into place.

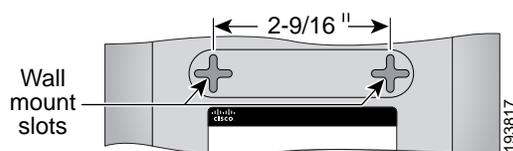


STEP 3 Repeat step 2 with the other stand.

Wall Option

To mount the Cisco WRVS4400N router on the wall, follow these steps.

- STEP 1** Determine where you want to mount the router and install two screws (not supplied) that are 2-9/16 in. apart (approximately 64.5 mm).
- STEP 2** With the back panel pointing up (if installing vertically), line up the router so that the wall-mount crisscross slots on the bottom of the access point line up with the two screws.



- STEP 3** Place the wall-mount slots over the screws and slide the router down until the screws fit snugly into the wall-mount slots.

Installing the Router

To prepare the router for installation do the following:

- Obtain the setup information for your specific type of Internet connection from your Internet Service Provider (ISP).
- Power off all of your network hardware, including the router, PCs, and cable modem or DSL modem.

Perform the steps in this section to install the hardware.

- STEP 1** Connect one end of an Ethernet network cable to one of the LAN ports (labeled 1-4) on the back of the router. Connect the other end to an Ethernet port on a PC.



- STEP 2** Repeat step 1 to connect up to four PCs, switches, or other network devices to the router.

- STEP 3** Connect an Ethernet network cable from your cable or DSL modem to the Internet port on the router's back panel.



- STEP 4** Power on the cable or DSL modem.
- STEP 5** Connect the power adapter to the Power port on the router and plug the other end into an electrical outlet.
- STEP 6** 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 router hardware installation is now complete.

Configuring the Router

To configure the WRVS4400N router, plug a PC into the router and launch the web-based configuration utility as follows.

**NOTE**

Before setting up the router, make sure your PCs are configured to obtain an IP (or TCP/IP) address automatically from the router.

STEP 1 Launch a web browser, such as Internet Explorer or Mozilla Firefox.

STEP 2 In the Address field enter **http://192.168.1.1** and press **Enter**.

STEP 3 In the User Name and Password fields, enter **admin**.

The default user name and password is **admin**.

STEP 4 Click **OK**.

For added security, you should later set a new password using the Administration > Management window of the web-based utility.

STEP 5 The web-based utility will appear with the Setup menu and Summary selected. Click **WAN** under the Setup menu.

STEP 6 If requested by your ISP (usually cable ISPs), complete the Host Name and Domain Name fields, and the MTU and MTU Size fields. Otherwise, leave the defaults.

STEP 7 In the WAN window, choose an Internet Connection Type from the drop-down menu. Depending on which internet connection type you select, additional setup may be required.

The Internet Connection Types are:

- **Automatic Configuration - DHCP:** If you are connecting through DHCP or a dynamic IP address from your ISP, keep this default setting.
- **Static IP:** If your 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 your ISP for the necessary setup information.

- **Heartbeat Signal:** Heartbeat Signal is used primarily in Australia. Check with your ISP for the necessary setup information.
- **L2TP:** L2TP is used mostly in Europe. Check with your ISP for the necessary setup information.

STEP 8 When you are finished entering your Internet connection settings, click **Save**.

STEP 9 Restart or power on your PC to obtain the new router setting.

STEP 10 Test the setup by opening your web browser from any computer and entering <http://www.cisco.com/smb>.

Congratulations! The installation of the router is complete.



NOTE

For more information about advanced settings and security options, refer to the *Cisco WRVS4400N Wireless-N Gigabit Security Router with VPN Administration Guide* on your CD-ROM. You can also access this guide and other related documentation on Cisco.com, as indicated in the next section.

Setting Up and Configuring the WRVS4400N Wireless-N Router

The Wireless-N router works right out of the box with the default settings. However, to change these settings, you can use the router's web-based configuration utility.

You can access the web-based configuration utility via a web browser (such as Microsoft Internet Explorer or Mozilla Firefox) from a computer connected to the same network the router is connected to.

This chapter includes the following sections:

- [Accessing the Web-Based Utility, page 29](#)
- [Navigating the Utility, page 30](#)
- [Setting Up Your Wireless-N Router, page 36](#)
- [Configuring Wireless Settings, page 68](#)
- [Configuring Firewall Settings, page 88](#)
- [Configuring the ProtectLink Web Service, page 104](#)
- [Configuring the VPN Settings, page 105](#)
- [Configuring the QoS Settings, page 118](#)
- [Configuring the Administration Settings, page 123](#)
- [Configuring IPS Settings, page 135](#)
- [Configuring the L2 Switch Settings, page 141](#)
- [Viewing Status, page 152](#)

Accessing the Web-Based Utility

There are two ways to connect to your wireless router for the first time:

- Physically connect your personal computer to one of the four LAN ports on the router. Then, configure your personal computer to obtain its IP address automatically from a DHCP server.
- Wirelessly connect your personal computer to the router (not recommended), by configuring the wireless interface of your personal computer to obtain its IP address automatically from a DHCP server.



NOTE Wirelessly connecting your personal computer to the router for initial configuration is not recommended because you might lose the connection while making wireless configuration changes.

To access the router's web-based utility, follow these steps:

-
- STEP 1** Launch a web browser, such as Internet Explorer or Mozilla Firefox, and enter the router's default IP address, **192.168.1.1**, in the Address field. Then, press **Enter**.



The Authentication Required dialog box appears.

- STEP 2** Enter **admin** in the User Name field, and enter your password (default password is **admin**) in the Password field. Then, click **OK**.

The Summary window appears.



Navigating the Utility

The web-based utility consists of the following main windows:

- Setup
- Wireless
- Firewall
- ProtectLink
- VPN
- QoS
- Administration
- IPS
- L2 Switch
- Status

Additional windows branch out from these main windows. The following briefly describes the windows of the utility.

Setup

This window allows you to configure the router's basic functionality and set its time through the following windows:

- **Summary**—Displays a read-only summary of the router's basic information.
- **WAN**—Displays, and allows the modification of, Internet connection settings on this window.
- **LAN**—Displays, and allows the modification of, Local Area Network (LAN) settings on this window.
- **DMZ**—Allows the use of the DMZ (Demilitarized Zone) Host feature to allow a local user to access special-purpose Internet services such as Internet gaming and video conferencing.
- **MAC Address Clone**—Enables the cloning of your network adapter's MAC address onto the router. This obviates the need to call your ISP to have the registered MAC address changed to the router's MAC address, should your ISP require that you register your MAC address.
- **Advanced Routing**—Enables you to select the router's operation mode (dynamic or static routing) while connecting to either the Internet or Intranet (NAT is only enabled while connecting to the Internet). The router supports Routing Information Protocol (RIP) versions 1 and 2 to automatically exchange routing information and establish the router's routing table.
- **Time**—Sets up the router's time settings.
- **IP Mode**—Provides options for the IPv4 mode or the Dual-Stack IPv4 and IPv6 mode.

Wireless

This window allows you to enter a variety of wireless settings for the built-in access point of the router through the following windows:

- **Basic Settings**—Chooses the wireless network mode (for example, B/G/N-Mixed), SSID, and radio channel.
- **Security Settings**—Configures the built-in access point's security settings.
- **Connection Control**—Controls the wireless connections from client devices to the router.
- **Advanced Settings**—Configures the built-in access point's more advanced wireless settings (for example, Tx Rate Limiting and Channel Bandwidth).
- **VLAN & QoS**—Configures the 802.1Q VLAN and the Quality of Service (QoS) settings.
- **WDS**—Configures Wireless Distribution System (WDS) settings.

Firewall

This window allows you to configure basic firewall settings, IP access list, and Network Address Port Translation (NAT) settings for your network's security through the following windows:

- **Basic Settings**—Configures basic firewall settings.
- **IP Based ACL**—Defines an IP-based access list to block specific hosts, networks, and protocols (services).
- **Internet Access Policy**—Defines the time schedule to allow or block complete Internet access or access to specific URLs from the router.
- **Single Port Forwarding**—Sets up public services or other specialized Internet applications that use a single port on your network.
- **Port Range Forwarding**—Sets up public services or other specialized Internet applications on your network that use a range of ports.
- **Port Range Triggering**—Sets up triggered ranges and forwarded ranges to allow special Internet applications to pass through this NAT router.

ProtectLink

This window allows you to check e-mail messages, filter website addresses (URLs), and block potentially malicious websites for the Cisco ProtectLink Web hosted service, thereby providing security for your network.

VPN

This window allows you to configure VPN tunnels and accounts to establish a secured channel through the Internet through the following windows:

- **Summary**—Displays IPsec tunnel status summary.
- **IPsec VPN**—Allows the VPN router to create one or multiple tunnels (or secure channels) each connecting between two endpoints, so that the transmitted data or information between these endpoints is secure.
- **VPN Client Accounts**—Designates VPN clients and their passwords.
- **VPN Pass Through**—Allows you to disable IPsec Passthrough, PPTP Passthrough, and L2TP Passthrough.

QoS

This window allows you to configure the two types of QoS traffic supported by the router through the following windows:

- **Bandwidth Management**—Allows you to perform bandwidth management by selecting either the Rate Control or Priority setting.
- **QoS Setup**—Allows users to configure the QoS Trust Mode for each LAN port.
- **DSCP Settings**—Allows you to set the Differentiated Services Code Point (DSCP).

Administration

This window allows you to administer the router through the following windows:

- **Management**—Allows you to alter the router's password, its access privileges, SNMP settings, and UPnP settings.
- **Log**—Allows the configuration of Log settings.
- **Diagnostics**—Allows you to check the connection between the router and another network device on the LAN or Internet.
- **Backup & Restore**—Allows you to back up and restores the Gateway's configuration file.
- **Factory Defaults**—Allows you to restore the router's factory defaults.
- **Reboot**—Allows you to reboot the router.
- **Firmware Upgrade**—Allows you to upgrade the router's firmware.

IPS

This window allows you to carry out advanced configuration of the built-in Intrusion Prevention System (IPS) inside the router through the following windows:

- **Configure**—Enables or disables IPS functions.
- **P2P/IM**—Allows or blocks specific Peer-to-Peer (P2P) networks and Instant Messaging (IM) applications.
- **Report**—Provides reports of network traffic and malicious attacks.
- **Information**—Provides the signature file version and the protection scope of the IPS system.

L2 Switch

This window allows you to configure layer 2 switching features on the 4 port Ethernet switch (LAN ports only) through the following windows:

- **Create VLAN**—Creates a Virtual Local Area Network (VLAN) assignment.
- **VLAN & Port Assignment**—Configures VLAN and port settings.
- **RADIUS**—Configures Remote Authorization Dial-In User Service (RADIUS) settings.
- **Port Setting**—Configures port speeds and duplex operation.
- **Statistics**—Displays statistics for both received and transmitted packets.
- **Port Mirroring**—Configures port mirroring.
- **RSTP**—Configures RSTP (Rapid Spanning Tree Protocol) settings.

Status

This window allows you to monitor the current status of the router through the following windows:

- **Gateway**—Provides basic information like firmware version and status information on the WAN port.
- **Local Network**—Provides status information about the local network (four Ethernet ports).
- **Wireless LAN**—Provides status information on Wireless LAN.
- **System Performance**—Provides traffic statistics on LAN and Wireless LAN ports.

Setting Up Your Wireless-N Router

This section describes how to configure the general settings of your router:

- [Configuring Basic Setup Settings on page 37](#)
- [Displaying A Read-Only Summary of the Basic Router Information on page 38](#)
- [Configuring Internet Connection Settings on page 40](#)
- [Configuring DDNS Service Settings on page 50](#)
- [Configuring Local Area Network \(LAN\) Settings on page 52](#)
- [Using The DMZ \(Demilitarized Zone\) Host Feature to Access Special Purpose Internet Services on page 55](#)
- [Cloning Your Network Adapter's MAC Address onto Your Router on page 57](#)
- [Configuring the Router's Advanced Settings on page 58](#)
- [Changing the Router's Time Settings on page 62](#)
- [Selecting IPv4 Mode or Dual Stack IPv4 And IPv6 Mode on page 64](#)

The Setup window contains all of the router's basic setup functions. You can use the router in most network settings without changing any of the default values.

Some users may need to enter additional information to connect to the Internet through an ISP (Internet Service Provider) or broadband (DSL, cable modem) carrier.

Configuring Basic Setup Settings

You can configure the following basic setup settings:

- **WAN**

Click **Setup > WAN** and select the appropriate Internet connection type according to your ISP if connecting your WAN port to the WAN (DSL or cable modem). Otherwise, most cases can use the default setting to get a WAN port IP address from a DHCP server.

- **Advanced Routing**

Click **Setup > Advanced Routing**. If you are connecting the router to the Internet, use the default setting. Otherwise, select **Router** in the Operation Mode field to disable NAT (Network Address Translation).

- **Management**

Click **Administration > Management** and change the access password for the router's web-based utility. The default username and password are **admin**.

You can also customize the wireless settings:

- **Wireless**

Click **Wireless > Basic Settings** and change the default SSID on the window. Select the level of security in the **Wireless > Security Settings** window and complete the options for the selected security mode. When the appropriate security mode is configured, disable **SSID Broadcast** on the **Basic Settings** window.

- Port Statistics

This section displays the following color-coded status information on the router's Ethernet ports:

- **Green**—Indicates that the port has a connection.
- **Black (unlit)**—Indicates that the port has no connection.

- Network Setting Status

- **LAN IP**—Displays the IP address of the router's LAN interface.
- **WAN IP**—Displays the IP address of the router's WAN interface. If this address was assigned using DHCP, click **DHCP Release** to release the address, or click **DHCP Renew** to renew the address.
- **Mode**—Displays the operating mode (Gateway or Router).
- **DNS 1-2**—Displays the IP addresses of the Domain Name System (DNS) servers that the router is using.
- **DDNS**—Indicates whether the Dynamic Domain Name System (DDNS) feature is enabled.
- **DMZ**—Indicates whether the DMZ Hosting feature is enabled.

- Firewall Setting Status

- **DoS (Denial of Service)**—Indicates whether the DoS (Denial of Service) protection feature is enabled to block DoS attacks.
- **Block WAN Request**—Indicates whether the Block WAN Request feature is enabled.
- **Remote Management**—Indicates whether the Remote Management feature is enabled.

- IPsec VPN Setting Status

- **IPsec VPN Summary**—Displays the VPN > Summary window.
- **Tunnel(s) Used**—Displays the number of VPN tunnels currently being used.
- **Tunnel(s) Available**—Displays the number of VPN tunnels that are available.

- **Log Setting Status**
 - **E-mail**—If this entry appears in the window, email cannot be sent because you have not specified an outbound SMTP server address. Click **E-mail** to display the Administration > Log window where you can configure the SMTP mail server.

Configuring Internet Connection Settings

The Setup > WAN Setup window displays Internet Connection Type and DDNS settings for configuring WAN port of the wireless router.

To configure the WAN settings for the router, follow these steps:

-
- STEP 1** Find out the Internet connection type and the settings used by your ISP. If the router is used as an Intranet router, you can in most cases use the default settings.
 - STEP 2** If you wish to use the dynamic DNS feature, sign up for a DDNS service.
 - STEP 3** In the router's web-based configuration utility, click **Setup > WAN**.
 - STEP 4** From the Internet Connection Type drop-down menu, select a connection type.

Based on your selection, the web-based utility displays relevant fields.

The router supports six connection types. For more information on how to configure the settings for these connection types, see the following sections:

- [Automatic Configuration - DHCP Server on page 42](#)
- [Static IP on page 43](#)
- [PPPoE on page 44](#)
- [PPTP on page 45](#)
- [Heart Beat Signal on page 47](#)
- [L2TP on page 48](#)

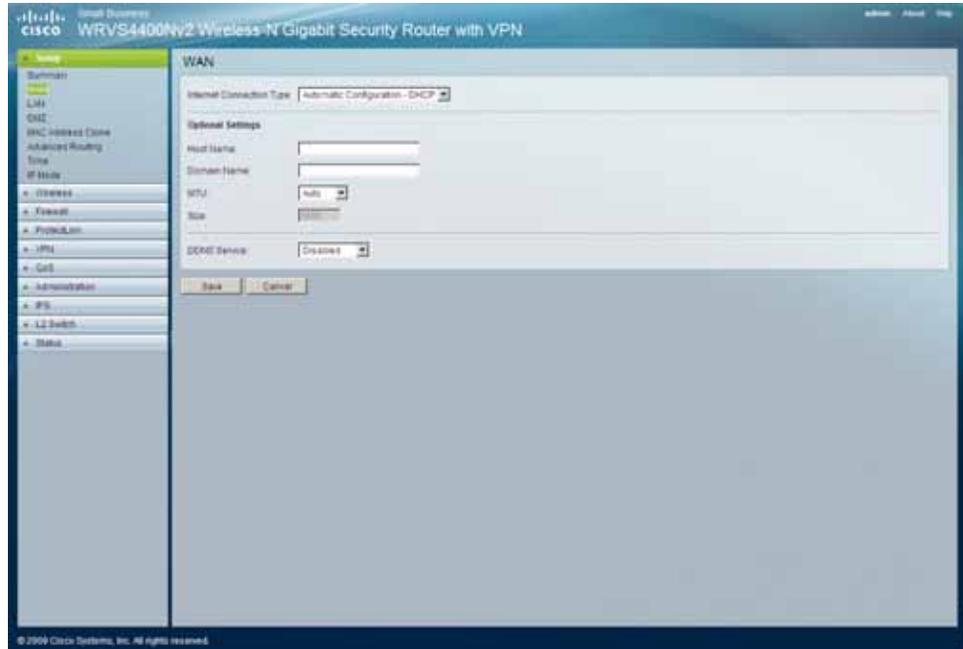
STEP 5 If required by your ISP, configure the following settings:

- **Host Name**—Enter the host-name provided by your ISP if you have broadband/cable Internet service and your ISP requires you to use a host-name as network identification. In most cases you can leave this field blank.
- **Domain Name**—Enter the domain name provided by your ISP if you have broadband/cable Internet service and your ISP requires you to use a domain name as network identification. In most cases you can leave this field blank.
- **MTU**—MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Select **Manual** if you want to manually enter the largest packet size to be transmitted. To have the router select the best MTU for your Internet connection, keep the default setting, **Auto**.
- **Size**—If you select **Manual** in the MTU field, this option is enabled. The recommended setting for this field is **1500** (standard MTU size on Ethernet media).

STEP 6 To configure the DDNS service, see [Configuring DDNS Service Settings on page 50](#).

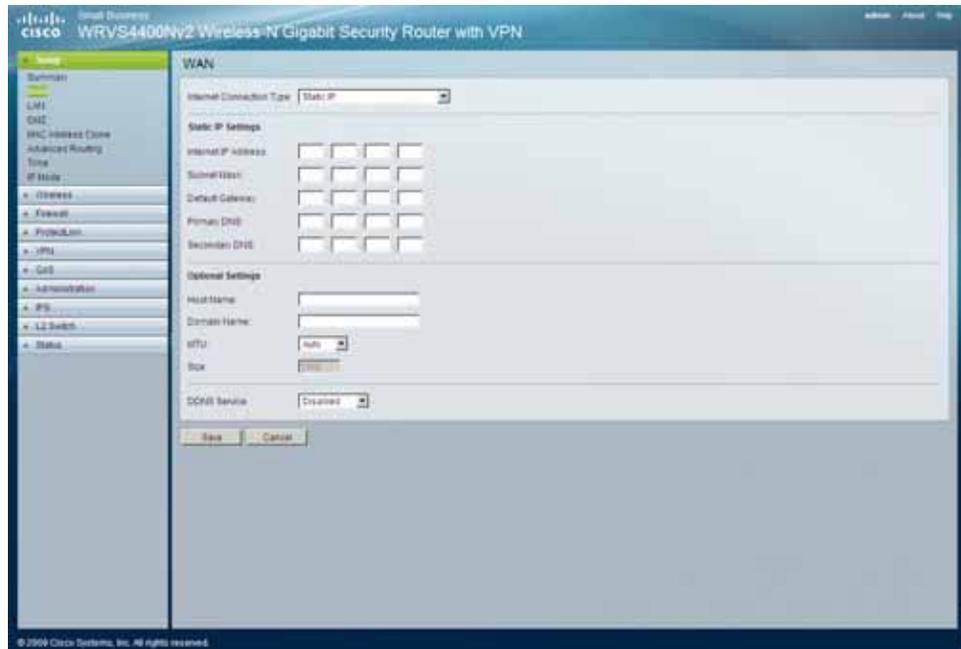
STEP 7 Click **Save**.

Automatic Configuration - DHCP Server



To have the router automatically get its IP address from your ISP's DHCP server, leave the connection type at its default setting of **Automatic Configuration - DHCP Server**. Most cable modem ISPs use the default option.

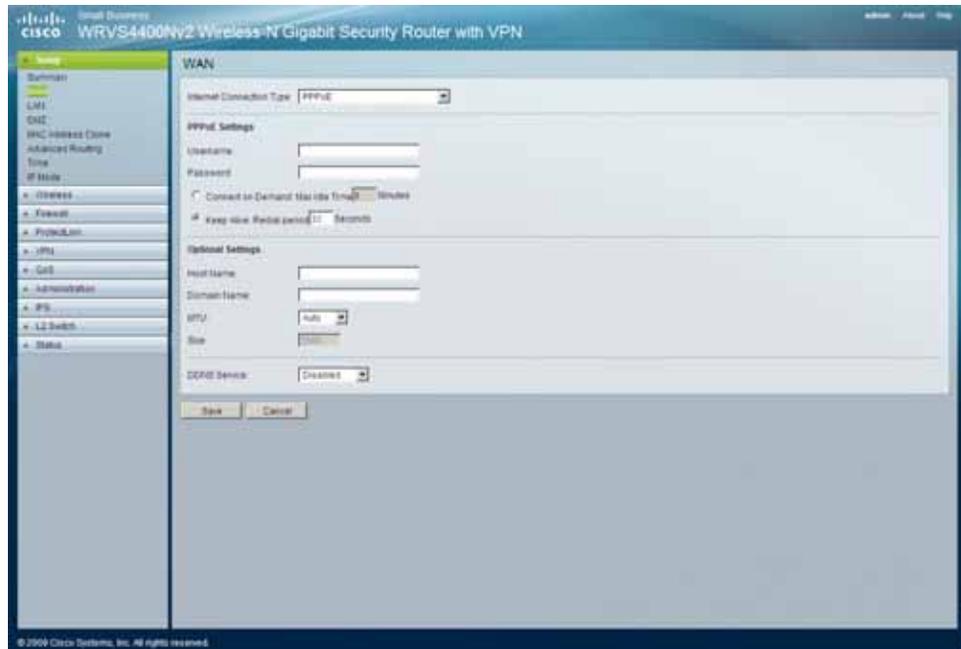
Static IP



To use a permanent IP address to connect to the Internet, select **Static IP** from the Internet Connection Type drop-down menu and fill in the following settings:

- **Internet IP Address**—Enter the IP address provided by your ISP. This is the router's IP address on the WAN port that can be reached from the Internet.
- **Subnet Mask**—Enter the subnet mask provided by your ISP. This is the router's subnet mask on the WAN port.
- **Default Gateway**—Enter the default gateway provided by your ISP. This is the router's default gateway to reach the Internet.
- **Primary DNS (Required) and Secondary DNS (Optional)**—Enter the IP addresses of the primary and secondary DNS server your ISP provided you with. These servers resolve domain-name-to-IP address mappings.

PPPoE

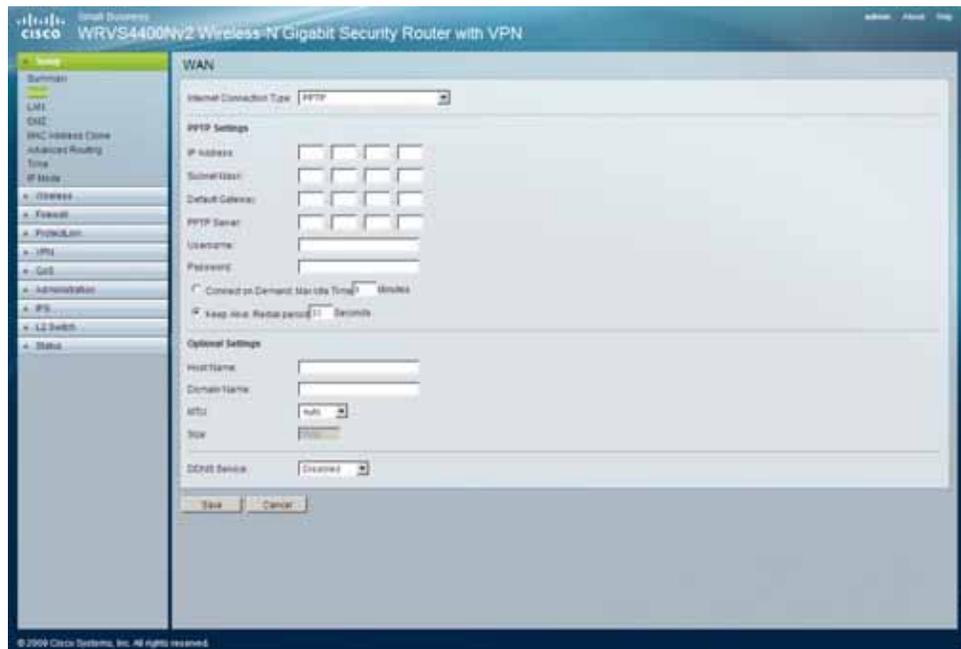


If your ISP is DSL-based and uses Point-to-Point Protocol over Ethernet (PPPoE) to establish Internet connections, select **PPPoE** from the Internet Connection Type drop-down menu to enable it, and do the following:

- **User Name and Password**—Enter the user name and password provided by your ISP for PPPoE authentication.
- **Connect on Demand—Max Idle Time**—Configure the router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, click the **Connect on Demand** option and enter the number of minutes you want to have elapsed before your Internet connection terminates in the Max Idle Time field. Use this option to minimize your DSL connection time if it is charged based on time. This option is disabled by default.
- **Keep Alive Redial period**—Allows the router to periodically check your Internet connection. If you are disconnected, the router automatically reestablishes your connection. To use this option, click the option next to **Keep Alive**. In the Redial Period field, you specify how often you want the router to check the Internet connection. This option is enabled by default

and the default Redial Period is 30 seconds. Use this option to minimize your Internet connection response time as it is always connected.

PPTP

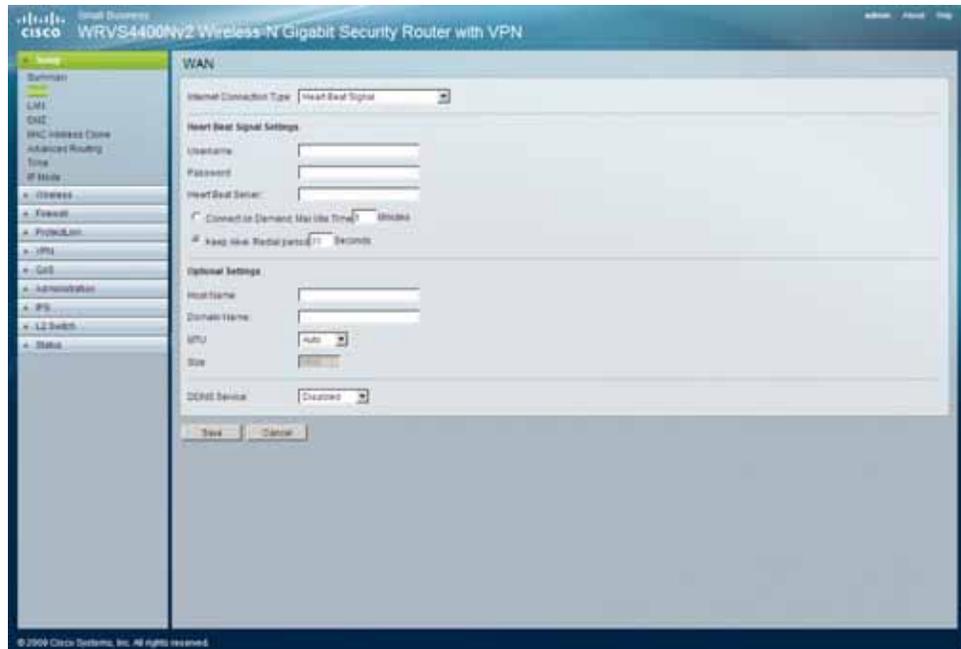


In Europe and Israel only, select **PPTP** from the Internet Connection Type drop-down menu if you wish to use the Point-to-Point Tunneling Protocol (PPTP) service, and enter the following:

- **IP Address**—Enter the IP address provided by your ISP. This is the router's IP address, when seen from the WAN, or the Internet.
- **Subnet Mask**—Enter the subnet mask provided by your ISP along with your IP address. This is the router's Subnet Mask.
- **Default Gateway**—Enter the default gateway IP address provided by your ISP.
- **PPTP Server**—Enter the IP address of the PPTP server.
- **User Name and Password**—Enter the user name and password provided by your ISP.

- **Connect on Demand: Max Idle Time**—Configure the router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, click the **Connect on Demand** option and enter the number of minutes you want to have elapsed before your Internet connection terminates in the Max Idle Time field. Use this option to minimize your DSL connection time if it is charged based on time. This option is disabled by default.
- **Keep Alive Redial period**—If you select this option, the router periodically checks your Internet connection. If you are disconnected, then the router automatically reestablishes your connection. To use this option, click the option next to **Keep Alive**. In the Redial Period field, you specify how often you want the router to check the Internet connection. This option is enabled by default and the default Redial Period is 30 seconds. Use this option to minimize your Internet connection response time as it is always connected.

Heart Beat Signal

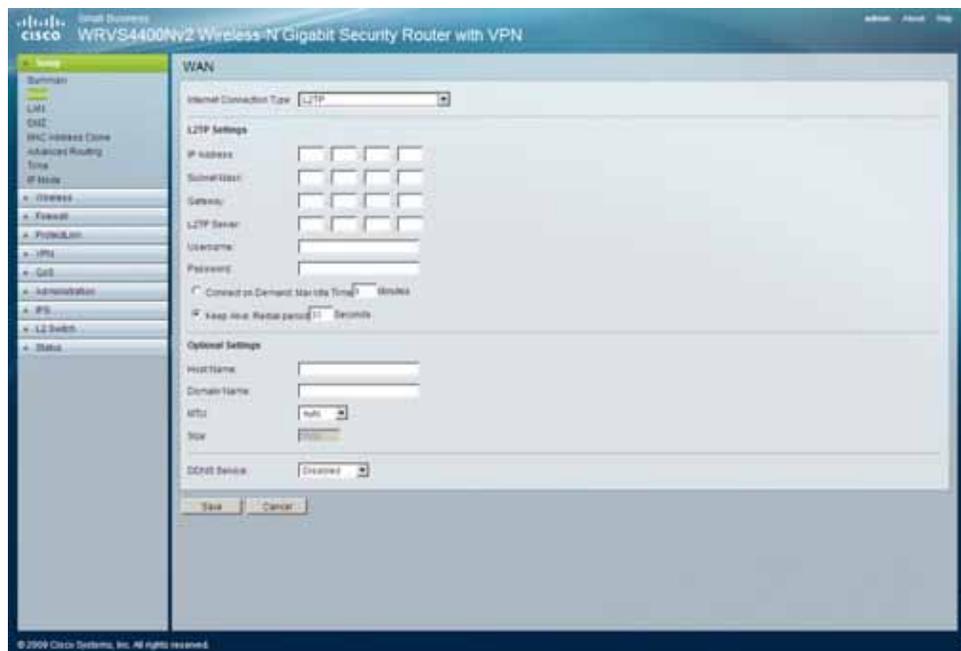


In Australia, select **Heart Beat Signal** from the Internet Connection Type drop-down menu to use this service. Check with your ISP for the necessary setup information, and enter the following:

- **User Name and Password**—Enter the user name and password provided by your ISP.
- **Heart Beat Server**—Enter the IP address of the Heart Beat server.
- **Connect on Demand: Max Idle Time**—Configure the router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, click the **Connect on Demand** option and enter the number of minutes you want to have elapsed before your Internet connection terminates in the Max Idle Time field. Use this option to minimize your DSL connection time if it is charged based on time. This option is disabled by default.

- **Keep Alive: Redial period**—Select this option, to have the router periodically check your Internet connection. If you are disconnected, then the router automatically reestablishes your connection. To use this option, click the option next to **Keep Alive**. In the Redial Period field, specify how often you want the router to check the Internet connection. This option is enabled by default and the default Redial Period is 30 seconds. Use this option to minimize your Internet connection response time as it is always connected.

L2TP



In European countries that provides this service, select **L2TP** from the Internet Connection Type drop-down menu to use the Layer 2 Tunneling Protocol (L2TP) service that tunnels Point-to-Point Protocol (PPP) across the Internet. Check with your ISP for the necessary setup information, and enter the following:

- **IP Address**—Enter the user name and password provided by your ISP. This is the router's IP address, when seen from the WAN or the Internet.
- **Subnet Mask**—Enter the subnet mask provided by your ISP along with your IP address. This is the router's Subnet Mask.
- **Gateway**—Enter the default gateway IP address provided by your ISP.
- **L2TP Server**—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: Max Idle Time**—Configure the router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, click the **Connect on Demand** option and enter the number of minutes you want elapsed before your Internet connection terminates, in the Max Idle Time field. Use this option to minimize your DSL connection time if it is charged based on time. This option is disabled by default.
- **Keep Alive Redial period**—If you select this option, the router periodically checks your Internet connection. If you are disconnected, then the router automatically reestablishes your connection. To use this option, click the option next to **Keep Alive**. In the Redial Period field, you specify how often you want the router to check the Internet connection. This option is enabled by default and the default Redial Period is 30 seconds. Use this option to minimize your Internet connection response time as it is always connected.

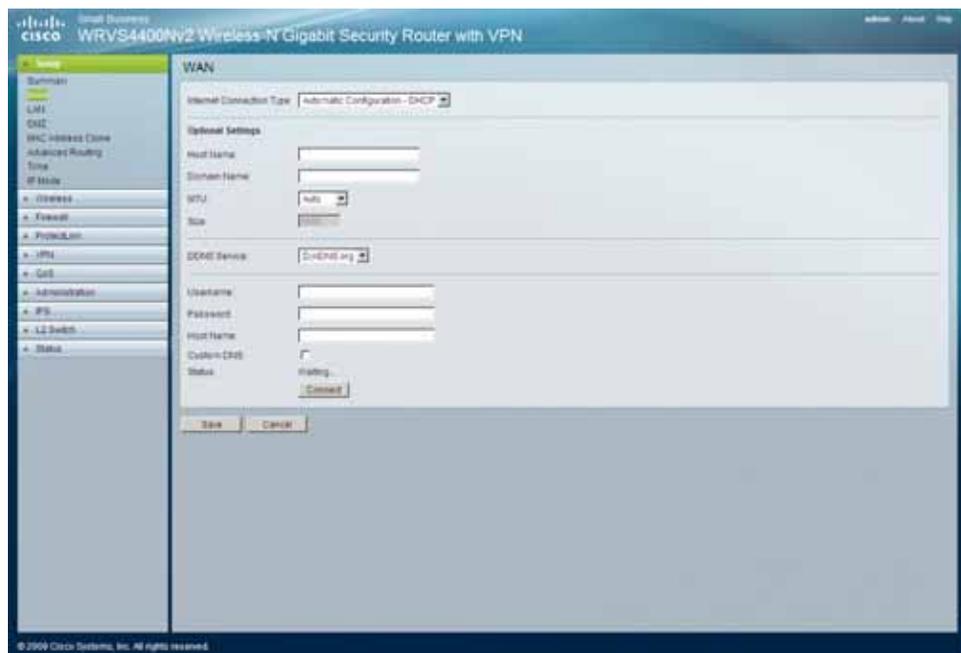
Configuring DDNS Service Settings

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.

By default, DDNS service is disabled.

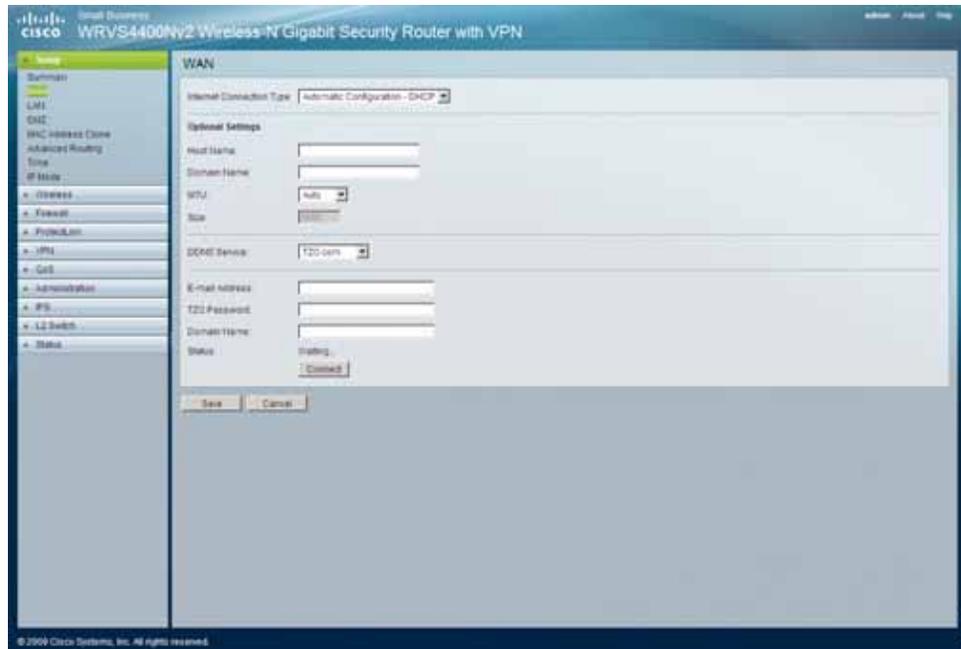
To enable and configure the DDNS settings for your router, follow these steps:

- STEP 1** To use DDNS service, sign up for one at DynDNS.org or TZO.com.
- STEP 2** To configure your router to use DynDNS.org:



- a. From the DDNS Service drop-down menu, select **DynDNS.org**.
- b. Configure the DynDNS.org settings:
 - **User Name, Password, and Host Name**—Enter the User Name, Password, and Host Name of the account you set up with DynDNS.org.
 - **Status**—The status of the DDNS service connection.

STEP 3 To configure your router to use TZO.com:



- a. From the DDNS Service drop-down menu, select TZO.com.
- b. Configure the TZO.com settings:
 - **E-mail Address, TZO Password, and Domain Name**—Enter the E-mail address, password, and domain name of the account you set up with TZO.
 - **Status**—The status of the TZO service connection.
 - **Connect**—To manually update your IP address information on the DDNS server when DDNS is enabled, use this button. The Status area on this window also updates.

STEP 4 Click **Save**.

After entering the necessary information, the router advises the DDNS service of your current WAN (Internet) IP address whenever this address changes.

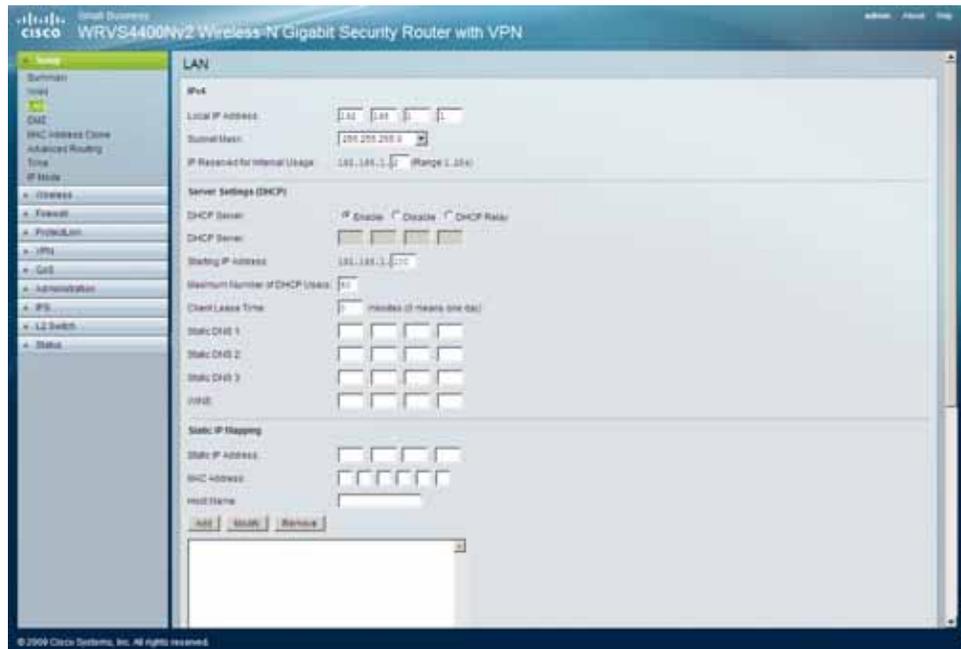


NOTE

If you are using TZO, do not use the TZO software to perform this IP address update.

Configuring Local Area Network (LAN) Settings

The Setup > LAN Setup window displays the router's local network settings for the four Ethernet ports.



To configure the LAN settings for the router, follow these steps:

STEP 1 Click **Setup > LAN Setup**.

STEP 2 Configure the LAN settings:

- **IPv4**—This section displays the settings for the router's local IPv4 address and subnet mask. In most cases, you can use the default values.
 - **Local IP Address**—Enter the IPv4 address on the LAN side. The default value is **192.168.1.1**.
 - **Subnet Mask**—Select the subnet mask from the drop-down menu. The default value is **255.255.255.0**.
 - **IP Reserved for Internal Usage**—Enter a value between 1 and 254 to specify the IP address to use internally.

- **Server Settings (DHCP)**—Unless you already have a DHCP server, it is highly recommended that you leave the router enabled as a DHCP server.

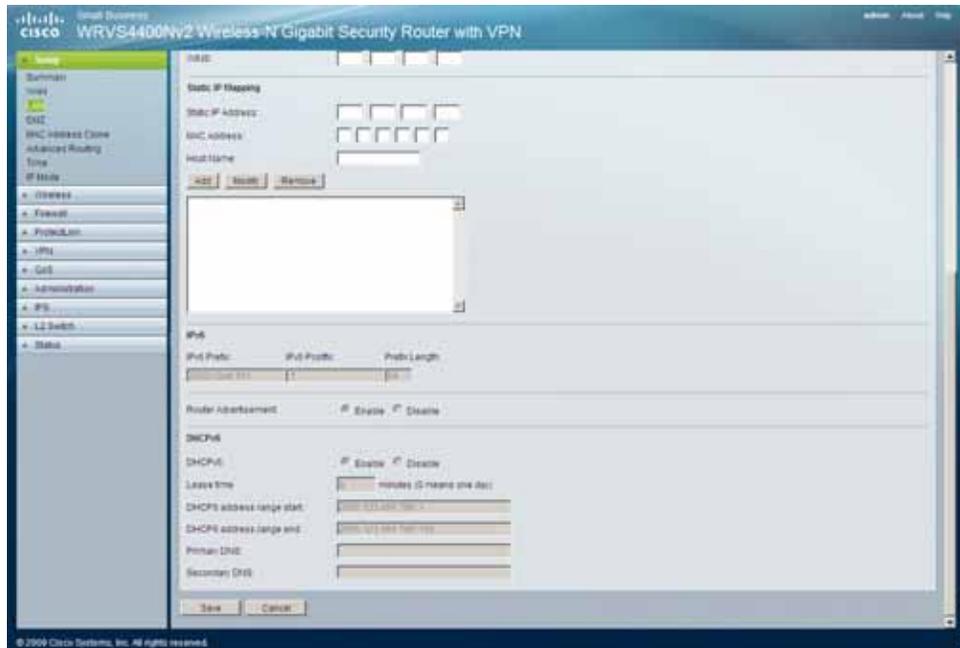
To use the router as your network's DHCP (Dynamic Host Configuration Protocol) server, so that it automatically assigns an IP address to each personal computer on your network, **Enable DHCP server**. (DHCP is enabled by default.)

If you already have a DHCP server on your network, or you don't want a DHCP server, then select **Disable** (no DHCP features will be available).

If you already have a DHCP server on your network, but you want the router to act as a relay for that DHCP Server, select **DHCP Relay**, then enter the DHCP Server IP address.

- **Starting IP Address**—Enter a value for the DHCP server to start with when issuing IP addresses. This value automatically follows your local IP address settings.
- Normally, you would assign the first IP address for the router (for example, 192.168.1.1) so that you can assign an IP address to other devices starting from the 2nd IP address (for example, 192.168.1.2).
- The last address in the subnet is for subnet broadcast (for example, 192.168.1.255) so that the address cannot be assigned to any host.
- **Maximum Number of DHCP Users**—Enter the maximum number of personal computers to which you want the DHCP server to assign IP addresses.
- This number cannot be greater than the available host addresses in the subnet (for example, 253 for /24 subnet).
- In order to determine the DHCP IP address range, add the starting IP address (for example, 100) to the number of DHCP users.
- **Client Lease Time**—Enter the amount of time you want a DHCP client to keep the assigned IP address before it sends a renewal request to the DHCP server. The default value is 0, which actually means one day.
- **Static DNS 1-3**—If applicable, enter the IP address(es) of your DNS servers.

- **WINS**—If you have a WINS server, enter that server's IP address in the field. Otherwise, leave this blank. The Windows Internet Naming Service (WINS) performs name resolution function (similar to DNS) in the Windows network environment. It can help you to determine the IP address of a remote Windows personal computer from its computer name.



- **IPv6**—This section displays the settings for the router's IPv6 Address, Prefix Length, and Router Advertisement options.
 - **IPv6 Address**—If you would select the **dual-stack** option under IP Versions Setup window, enter the IPv6 address on the LAN side of the router in the field.
 - **Prefix Length**—Enter the IPv6 prefix length. The default is 64, which should not need to be changed.
 - **Router Advertisement**—Enable this option to allow the router to send out IPv6 router advertisement packets periodically. This helps IPv6 hosts to learn their IPv6 prefix and setup their IPv6 address automatically.

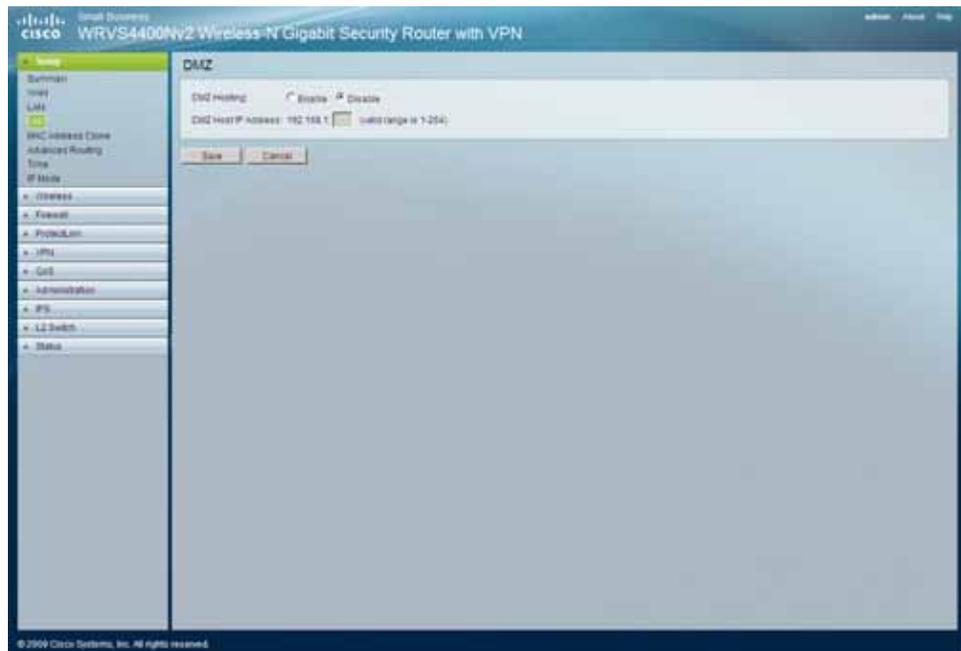
- **DHCPv6**—To enable the DHCP v6 feature, select **Enable**.
To disable DHCP v6, select **Disable**.
 - **Lease time**—Enter the lease time in minutes.
 - **DHCP address range start**—Enter the starting DHCP v6 IP address.
 - **DHCP address range end**—Enter the ending DHCP v6 IP address.
 - **Primary DNS**—Enter the Primary IPv6 DNS server address.
 - **Secondary DNS**—Enter the Secondary IPv6 DNS server address.

STEP 3 Click **Save**.

Using The DMZ (Demilitarized Zone) Host Feature to Access Special Purpose Internet Services

The Setup > DMZ window displays the settings for configuring DMZ Hosting, to allow one local personal computer to be exposed to the Internet for use of a special-purpose service, such as Internet gaming and video-conferencing.

DMZ Hosting forwards traffic to all the ports for the specified personal computer simultaneously, unlike Port Range Forwarding that can only forward a maximum of 15 ranges of ports.



To configure DMZ Hosting, follow these steps:

STEP 1 Click **Setup > DMZ**

STEP 2 Fill in the DMZ Hosting settings:

- **DMZ Hosting**—To allow one local personal computer to be exposed to the Internet for use of a special-purpose service such as Internet gaming and video-conferencing, select **Enable**.
 - To disable the DMZ feature, select **Disable**.
- **DMZ Host IP Address**—Enter (complete) the IP address of the computer to be exposed to the Internet, for DMZ hosting.

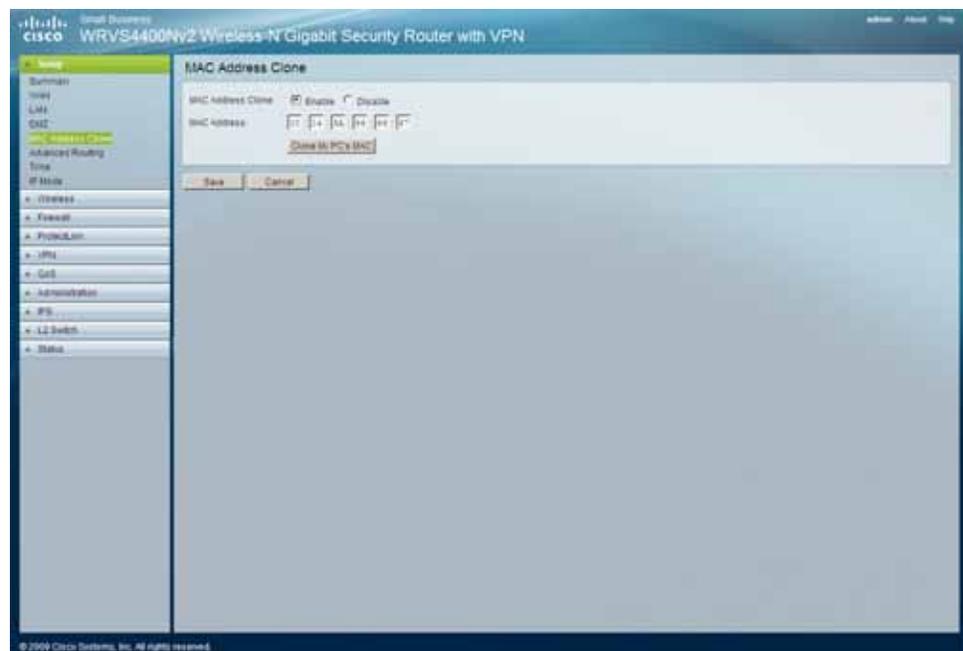
STEP 3 Click **Save**.

Cloning Your Network Adapter's MAC Address onto Your Router

Some ISPs require that you register a MAC address.

The Setup > MAC Address Clone window allows the cloning of your personal computer network adapter's MAC address onto the router, instead of you having to call your ISP again to now change the registered MAC address to that of the router.

The router's MAC address is a 6-byte hexadecimal number assigned to a unique piece of hardware for electronic identification.



To clone your network adapter's MAC address onto your router, follow these steps:

STEP 1 Click Setup > MAC Address Clone.

STEP 2 Complete the MAC Address Clone settings:

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

STEP 3 Click **Save**.

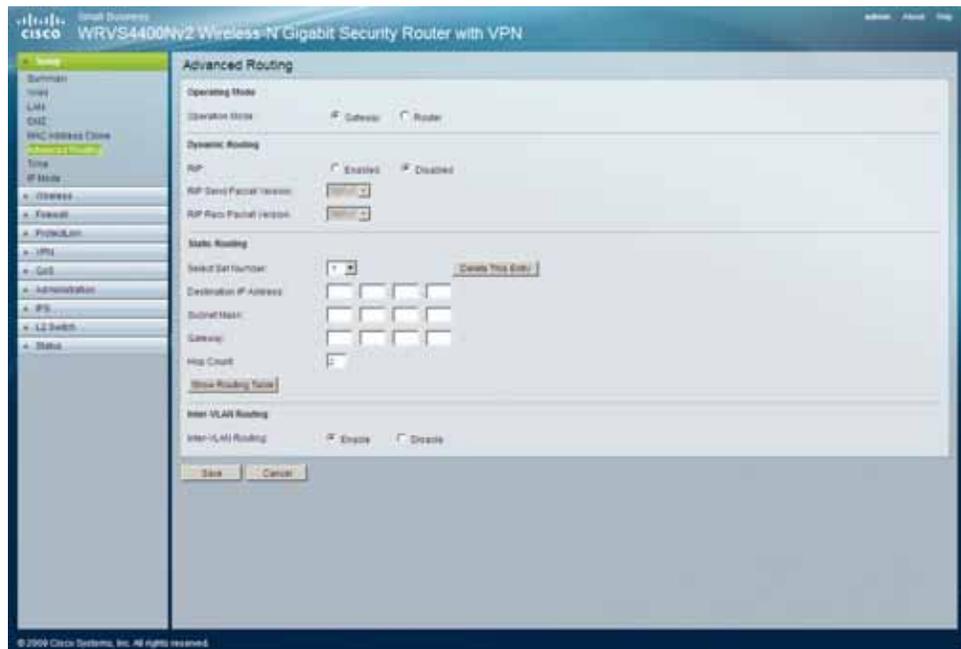
Configuring the Router's Advanced Settings

The Setup > Advanced Routing window allows you to configure the router's Operating Mode and settings for Dynamic Routing, Static Routing, and Inter-VLAN routing.

To configure your router's advanced settings, follow these steps:

STEP 1 Click **Setup > Advanced Routing**

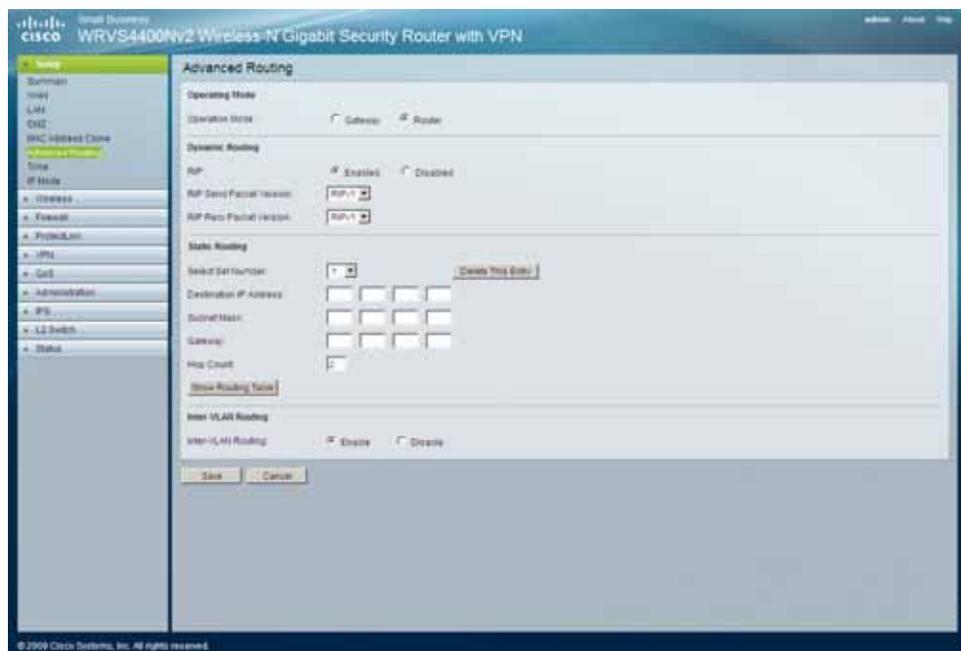
STEP 2 Fill in the settings for advanced routing configuration:



- To select the operating mode in which the router functions:
 - Select **Gateway** to allow all devices on your LAN to share the same WAN (Internet) IP address, the normal mode of operation—in Gateway mode, the NAT (Network Address Translation) mechanism is enabled.

Select **Router** to use another router as the Internet Gateway, or to have all personal computers on your LAN assigned (fixed) Internet IP addresses—in Intranet Router mode, the NAT mechanism is disabled.

STEP 3 Configure Dynamic Routing if appropriate.



The router's dynamic routing feature can be used to automatically establish a routing table through a database exchange with peer routers (running the same routing protocol). The router supports RIP (Routing Information Protocol) versions 1 & 2.

To configure Dynamic Routing, follow these steps:

- a. **Enable** RIP (Routing Information Protocol) for the router to use the RIP protocol and calculate the most efficient route for the network's data packets to travel between the source and the destination, based upon the shortest paths.
- b. For RIP Send Packet Version, choose the version of RIP packets you want to send to peers (**RIPv1** or **RIPv2**) to match the version supported by other routers on your LAN.

- c. For RIP Recv Packet Version, choose the version of RIP packets you want to receive from peers (**RIPv1** or **RIPv2**) to match the version supported by other routers on your LAN.

STEP 4 Configure Static Routing if necessary:

Some ISPs require static routes to build your routing table instead of using dynamic routing protocols. Static routes do not require CPU resources to exchange routing information with a peer router. You can also use static routes to reach peer routers that do not support dynamic routing protocols. Static routes can be used together with dynamic routes. Be careful not to introduce routing loops in your network.

- a. To set up static routing, add route entries in the routing table that tell the router where to forward packets to specific IP destinations.

To create a static route entry, provide the following information:

- **Select Set Number**—Select the set number (routing table entry number) that you wish to view or configure. If necessary, click **Delete This Entry** to clear the entry.
- **Destination IP Address**—Enter the network address of the remote LAN segment. For a standard Class C IP domain, the network address is the first three fields of the Destination LAN IP; the last field should be zero.
- **Subnet Mask**—Enter the Subnet Mask used on the destination LAN IP domain. For Class C IP domains, the Subnet Mask is 255.255.255.0.
- **Gateway**—If this router is used to connect your network to the Internet, then your gateway IP is the router's IP address. If you have another router handling your network's Internet connection, enter the IP address of that router instead.
- **Hop Count (max. 15)**—Gives the number of routers that a data packet passes through before reaching its destination. It is used to define the priority on which route to use if there is a conflict between a static route and dynamic route.

STEP 5 View the Routing Table if necessary to verify routing.

To view the routing table established either through dynamic or static routing methods, click the **Show Routing Table** button.

Routing Table Entry List				Refresh
Destination LAN IP	Subnet Mask	Gateway	Interface	
71.153.6.192	255.255.255.192	0.0.0.0	WAN	
192.168.1.0	255.255.255.0	0.0.0.0	LAN	
239.0.0.0	255.0.0.0	0.0.0.0	LAN	
0.0.0.0	0.0.0.0	71.153.6.254	WAN	
				Close

275846

STEP 6 Enable Inter-VLAN Routing if needed.

Select **Enable** to allow packets to be routed between VLANs that are in different subnets. The default is Enable.

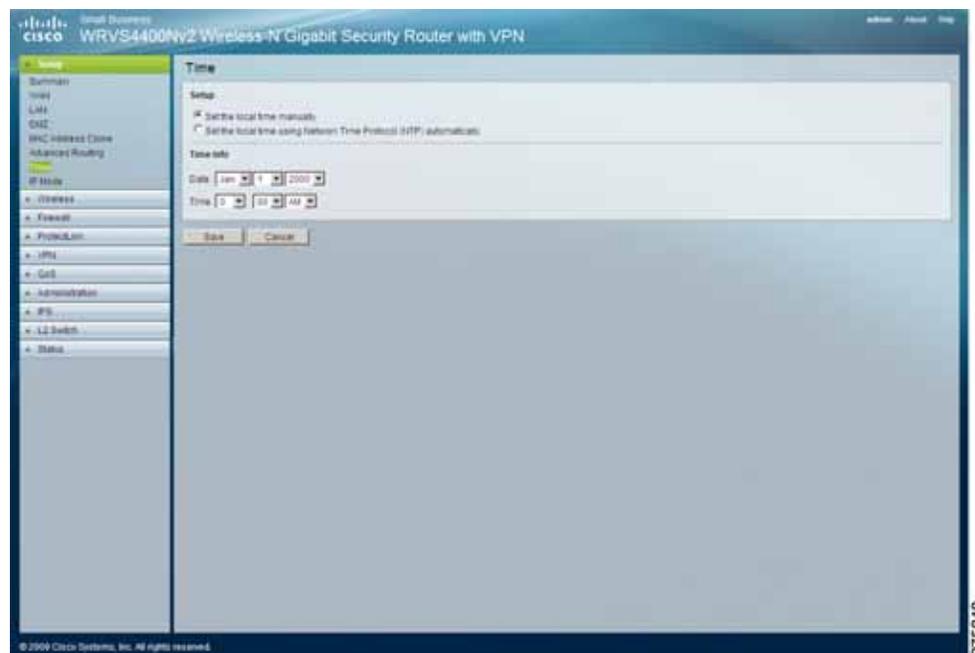
STEP 7 Click **Save**.

Changing the Router's Time Settings

The Setup > Time window allows you to either define your router's time manually or automatically through the Time Server. The default is **Automatically**.

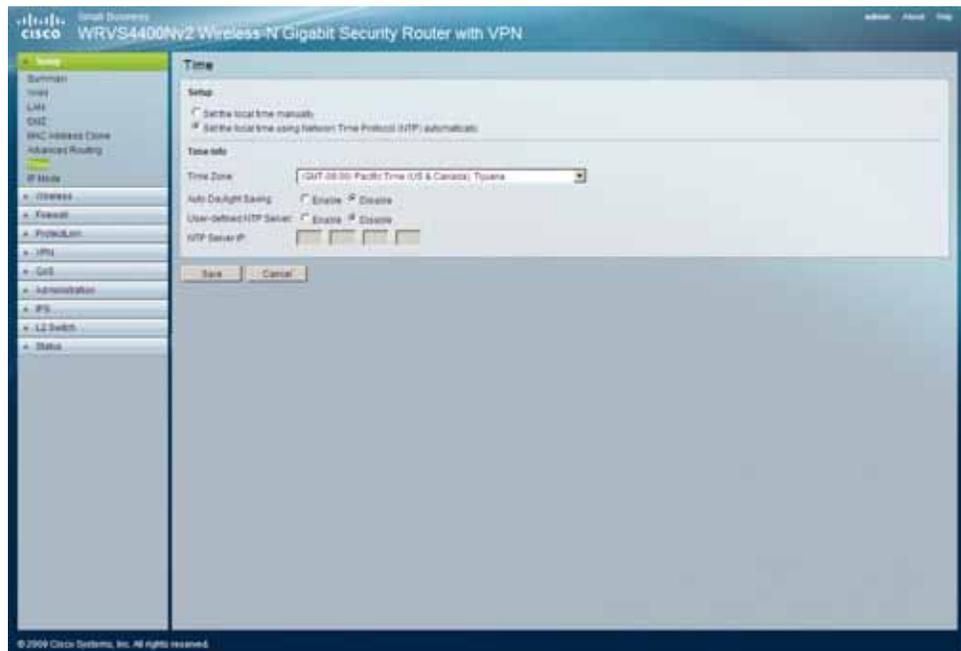
To define your router's time, follow these steps:

- STEP 1** Click Setup > Time.
- STEP 2** Specify how to set the local time:



a. Manually

- **Set the local time Manually**—If you wish to enter the time and date manually, select the **Date** from the drop-down fields and enter the hour, minutes, and seconds in the **Time** field using 24 hour format (example 10:00pm would be entered 22:0:0).



b. Automatically

- **Set the local time using Network Time Protocol (NTP) Automatically**—If you wish to use a Network Time Protocol server to set the time and date, select this option, then complete the following fields.
 - **Time Zone**—Select the time zone for your location and your setting synchronizes over the Internet with public NTP (Network Time Protocol) Servers.
 - **Auto Daylight Saving**—If your location observes daylight savings time, select the Enable option.
 - **User Defined NTP Server**—To use your own NTP server, select the Enabled option. The default is Disabled.
 - **NTP Server IP Address**—Enter the IP address of your own NTP server.

STEP 3 Click Save.

Selecting IPv4 Mode or Dual Stack IPv4 And IPv6 Mode

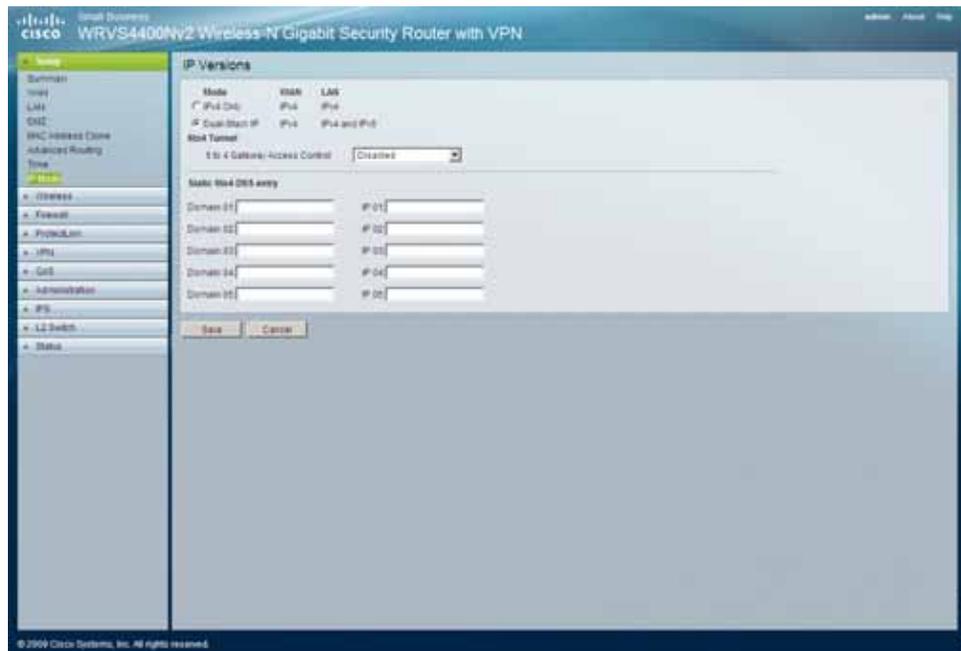
The Setup > IP Mode window allows you to choose IP Mode settings for the router.

To configure IP Mode settings for the router, follow these steps:

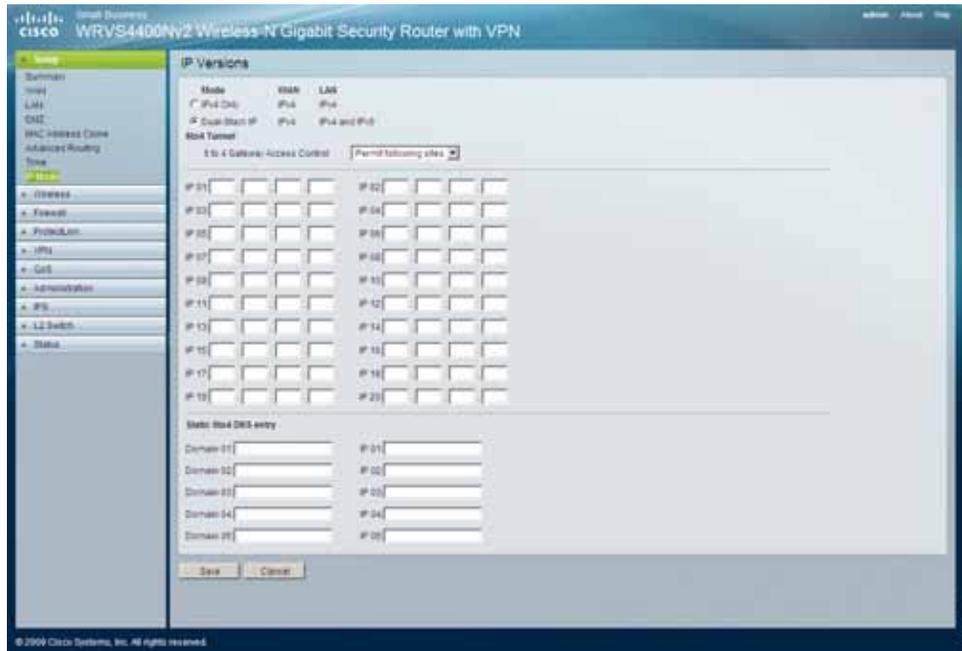
- STEP 1** Click **Setup > IP Mode**.
- STEP 2** Configure the IP Mode settings:
 - **IPv4 Only**—Select this option to use IPv4 on the Internet and local network.



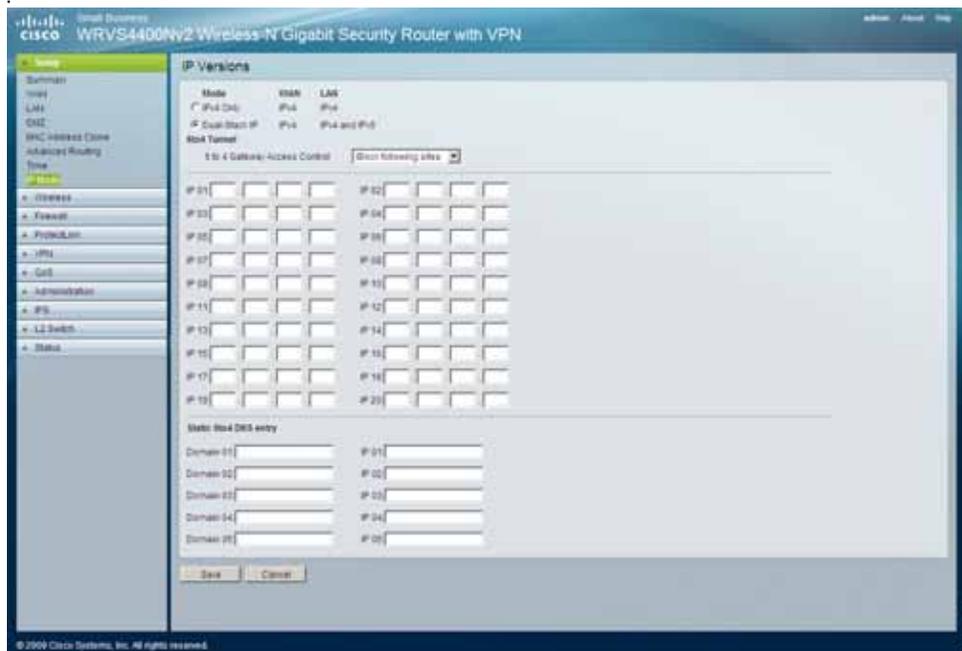
- **Dual-Stack IP**—Select this option to use IPv4 on the Internet and IPv4 and IPv6 on the local network.



- **6to4 Tunnel**—Allows your IPv6 network to connect to other IPv6 networks via tunnels through IPv4 (per RFC3056). The remote router also needs to support 6to4. Because the tunnel can be automatically formed based on traffic, there is no limit as to how many tunnels you can have.
- **6 to 4 Gateway Access Control**—By default, this route allows 6to4 connections to or from any other 6to4 gateway. By enabling this Access Control, you can have a better control which IPv6 clouds this router is connecting to. A list of IP addresses can be entered in the Access List. Those should be the IPv4 addresses of the remote 6to4 gateways.
 - **Permit following sites**—Allow only a limited set of 6to4 gateways to establish tunnel with the router. Up to 20 sites can be configured and they can send traffic simultaneously.



- **Block following sites**—Prevent a limited set of 6to4 gateways from establishing tunnels with the router. Up to 20 sites can be configured.



- **Static 6to4 DNS entry**—Allow users to configure static DNS entry to map hostname to IPv6 address. This provides a convenient way for users to access remote IPv6 hosts.

STEP 3 Click **Save**.

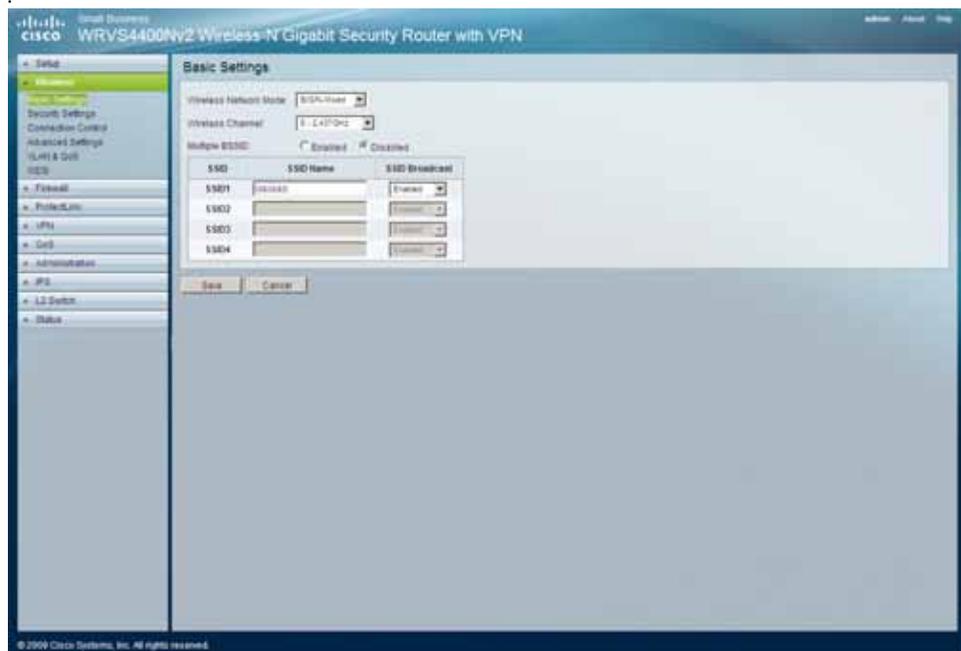
Configuring Wireless Settings

This section describes how to configure the wireless settings of the router:

- [Configuring Basic Settings on page 68](#)
- [Configuring Wireless Security on page 72](#)
- [Configuring Advanced Wireless Settings on page 81](#)
- [Configuring Connection Control on page 80](#)
- [Configuring Advanced Wireless Settings on page 81](#)

Configuring Basic Settings

The **Wireless > Basic Settings** window allows you to change the basic wireless network settings.

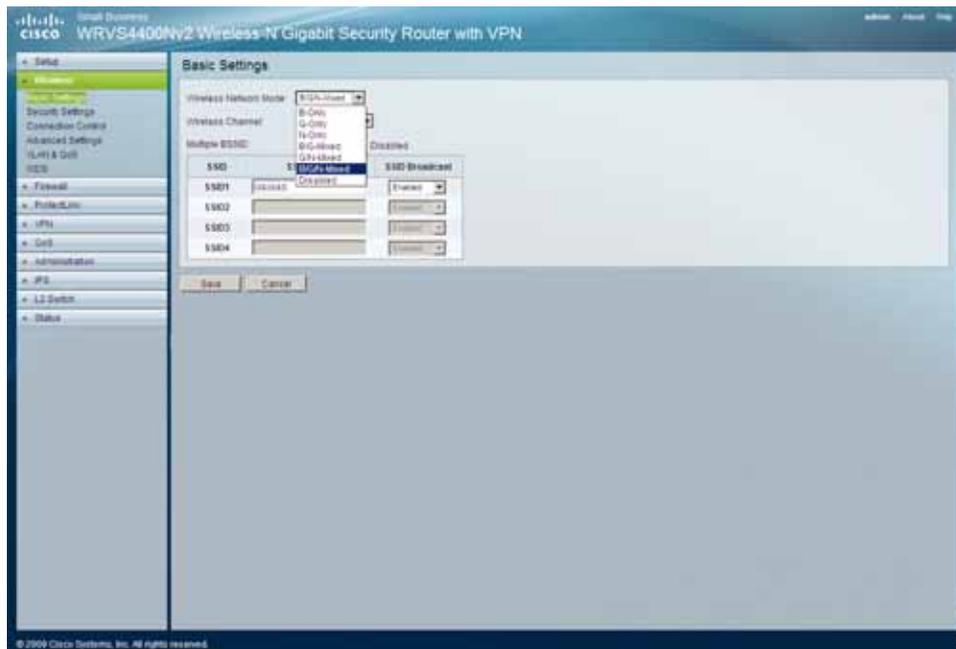


To change the basic wireless settings of the router, follow these steps:

STEP 1 Click **Wireless > Basic Settings**

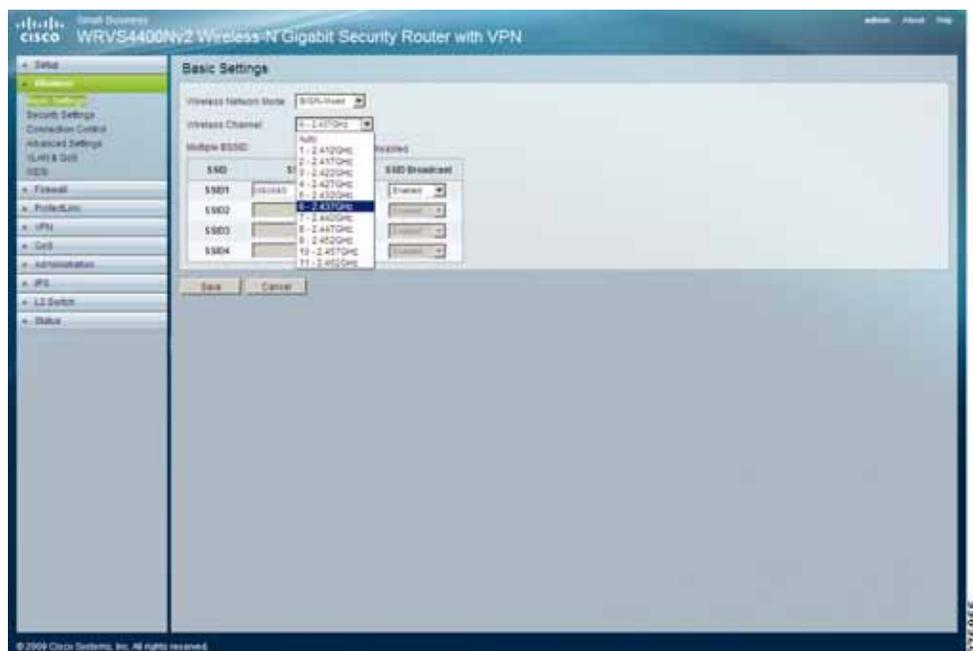
STEP 2 Configure the basic wireless settings:

- **Wireless Network Mode**—Select one of the following modes. The default is **B/G/N-Mixed**.

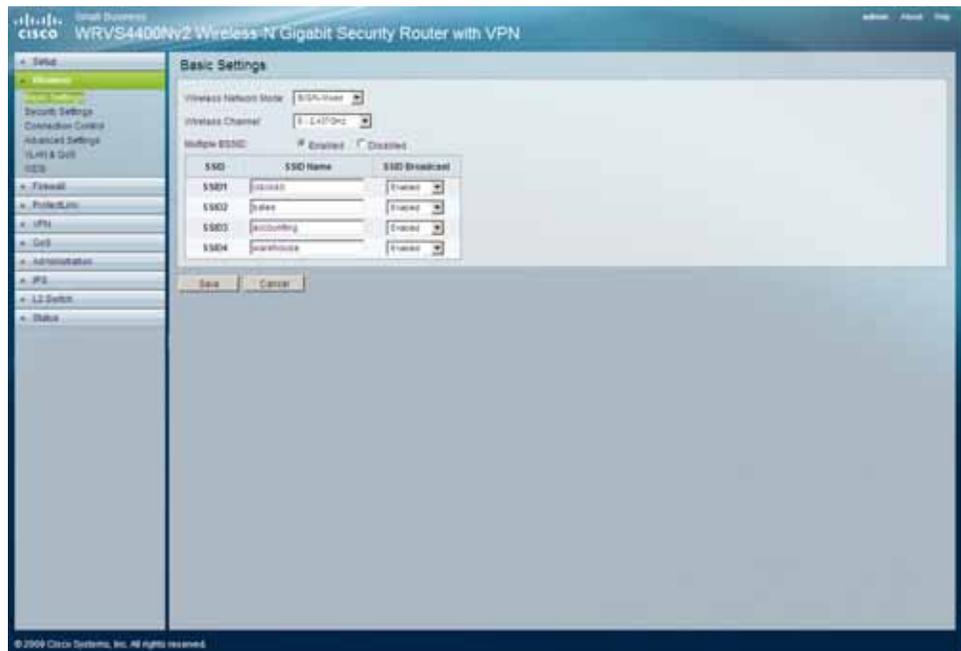


- **B-Only**—All the wireless client devices can be connected to the router at Wireless-B data rates with a maximum speed of 11Mbps.
- **G-Only**—Both Wireless-N and Wireless-G client devices can be connected at Wireless-G data rates with a maximum speed of 54Mbps. Wireless-B clients cannot be connected in this mode.
- **N-Only**—Only Wireless-N client devices can be connected at Wireless-N data rates with a maximum speed of 300Mbps.
- **B/G-Mixed**—Both Wireless-B and Wireless-G client devices can be connected at their respective data rates. Wireless-N devices can be connected at Wireless-G data rates.
- **G/N-Mixed**—Both Wireless-G and Wireless-N client devices can be connected at their respective data rates. Wireless-B clients cannot be connected in this mode.
- **B/G/N-Mixed**—All the wireless client devices can be connected at their respective data rates in this mixed mode.

- **Disabled**—To disable wireless connectivity completely. This might be useful during system maintenance.
- **Wireless Channel**—Select the appropriate channel to be used between your wireless router and your client devices. The default is channel 6. You can also select **Auto** so that your router selects the channel with the lowest amount of wireless interference while the system is booting up. Auto channel selection starts when you click **Save**, and it takes several seconds to scan through all the channels to find the best channel. For the Wireless-N 40MHz channel option (see [Configuring Advanced Wireless Settings on page 81](#)), the router automatically selects the adjacent 20MHz channel to combine them into a wider channel.



- **Multiple BSSID**—Select Enabled or Disabled as required.



- **SSID Name**—The SSID is the unique name shared between all devices in a wireless network. It is case-sensitive, must not exceed 32 alphanumeric characters, and may be any keyboard character. Make sure this setting is the same for all devices in your wireless network. The default SSID name is **ciscosb**.
- **SSID Broadcast**—Allows the SSID to be broadcast on your network. You may want to enable this function while configuring your network, but make sure that you disable it when you are finished. With this enabled, someone could easily obtain the SSID information with site survey software or Windows XP and gain unauthorized access to your network. Click **Enabled** to broadcast the SSID to all wireless devices in range. Click **Disabled** to increase network security and prevent the SSID from being seen on networked personal computers. The default is **Enabled** in order to help users configure their network before use.

STEP 3 Click **Save**.

Configuring Wireless Security

The **Wireless > Wireless Security** window allows you to configure the wireless router's wireless security settings.

To change the router's wireless security settings, follow these steps:

STEP 1 Click **Wireless > Wireless Security**.

STEP 2 Configure the wireless security settings for **Wireless Isolation**:

- **Wireless Isolation (between SSID w/o VLAN)**—Prevents wireless personal computers that are associated to the same network name (SSID) from seeing, or transferring files between, each other.

Enable this feature to prevent Wireless personal computers from seeing each other.

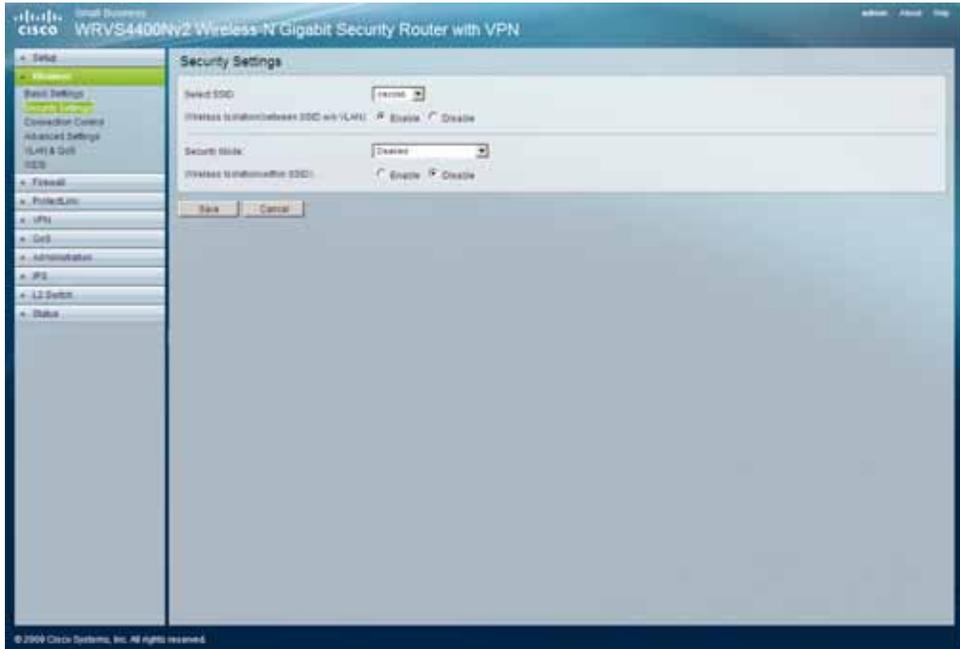
Disable this feature to allow wireless personal computers to see each other and to exchange files between themselves.

This feature is very useful when setting up a wireless hotspot location. The default is **Disable**.

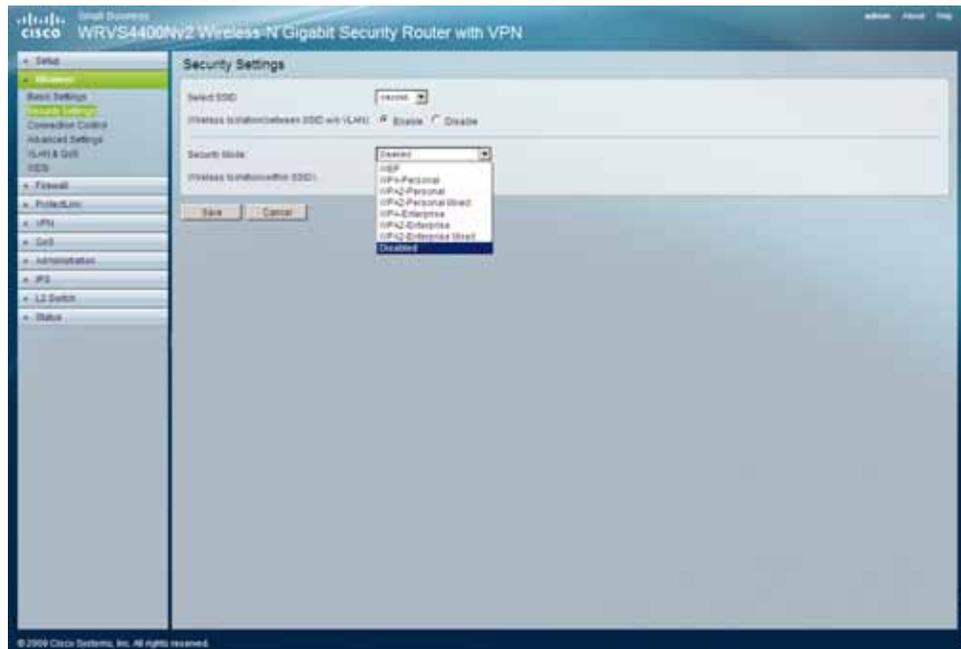
STEP 3 Select the wireless security mode you want to use, **WEP**, **WPA-Personal**, **WPA2-Personal**, **WPA2-Personal Mixed**, **WPA-Enterprise**, **WPA2-Enterprise**, or **WPA2-Enterprise Mixed**. (WPA stands for Wi-Fi Protected Access, which is a security standard stronger than WEP encryption and forward compatible with IEEE 802.11e. WEP stands for Wired Equivalent Privacy, Enterprise refers to using RADIUS server for authentication, while RADIUS stands for Remote Authentication Dial-In User Service.) Refer to the appropriate instructions below after you select the Authentication Type and SSID Interoperability settings.

The following section describes the detailed options for each Security Mode.

- **Disable**—To disable wireless security completely, select **Disable**.

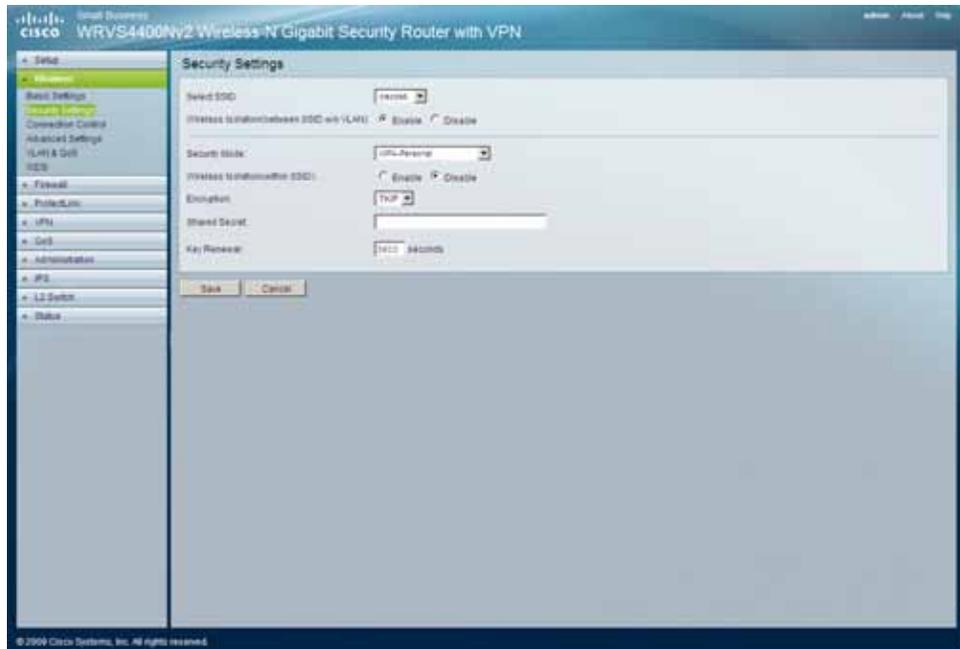


- **WEP**—This security mode is defined in the original IEEE 802.11. This mode is not recommended now due to its weak security protection. Users are urged to migrate to WPA or WPA2.



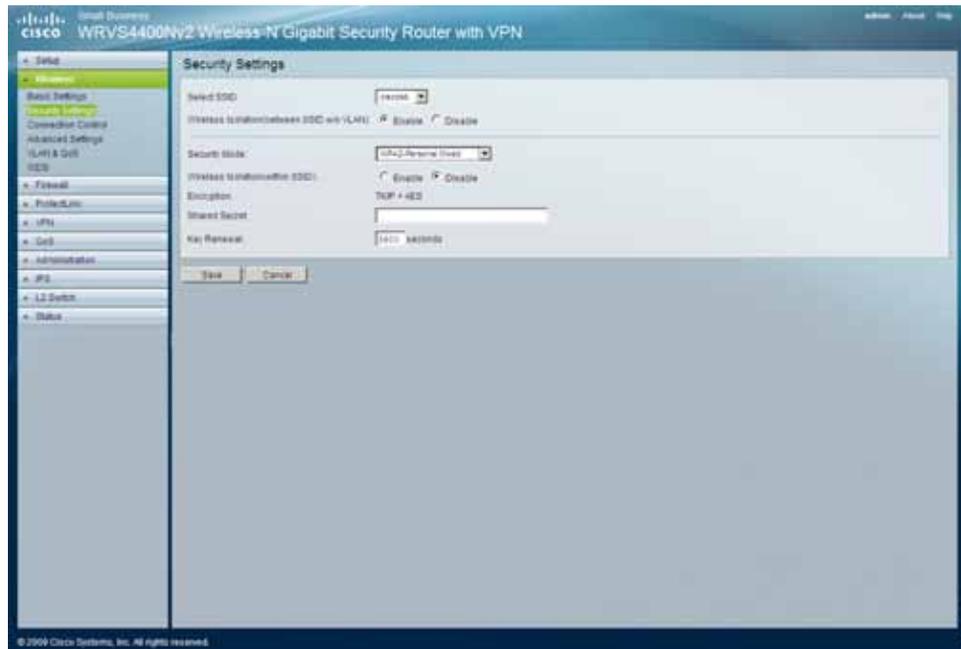
- **Authentication Type**—Choose the 802.11 authentication type as either Open System or Shared Key. The default is Open System.
- **Encryption**—Select a level of WEP encryption, 64 bits (10 hex digits) or 128 bits (26 hex digits).
- **Passphrase**—If you want to generate WEP keys using a Passphrase, then enter the Passphrase in the field provided and click the Generate key.
- **Key 1-4**—If you want to manually enter WEP keys, then complete the fields provided. Each WEP key can consist of the letters “A” through “F” and the numbers “0” through “9”. It should be 10 characters in length for 64-bit encryption or 26 characters in length for 128-bit encryption.
- **Tx Key**—Select one of the keys to be used for data encryption (when you manually enter multiple WEP keys).

- **WPA-Personal (also known as WPA-PSK)**



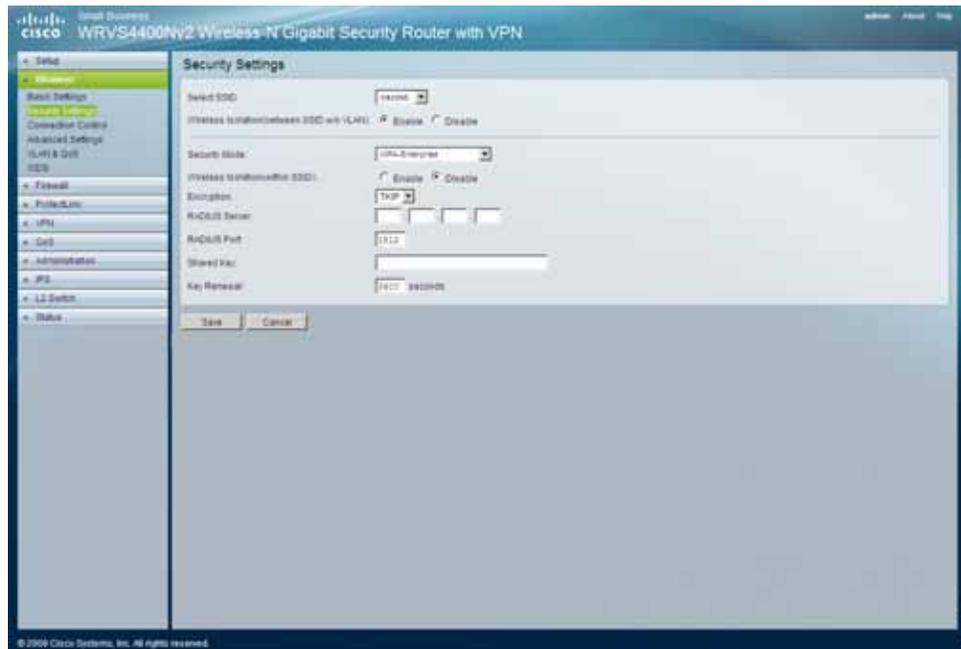
- **Encryption**—WPA offers you two encryption methods, TKIP and AES for data encryption. Select the type of algorithm you want to use, TKIP or AES. The default is TKIP.
- **Shared Key**—Enter a WPA Shared Key of 8-63 characters.
- **Key Renewal**—Enter a key renewal timeout period, which instructs the router how often it should change the encryption keys. The default is 3600 seconds.
- **WPA2-Personal**
 - **Encryption**—WPA2 always uses AES for data encryption.
 - **Shared Key**—Enter a WPA Shared Key of 8-63 characters.
 - **Key Renewal**—Enter a Key Renewal Timeout period, which instructs the router how often it should change the encryption keys. The default is 3600 seconds.

- **WPA2-Personal Mixed**—This security mode supports the transition from WPA-Personal to WPA2-Personal. You can have client devices that use either WPA-Personal or WPA2-Personal. The router automatically chooses the encryption algorithm used by each client device.



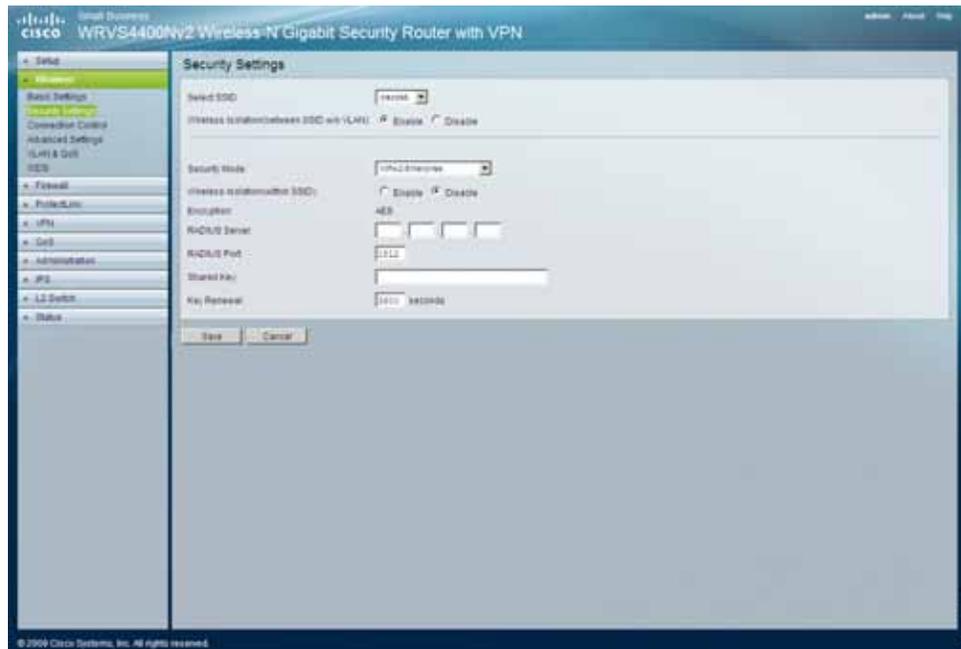
- **Encryption**—Mixed Mode automatically chooses TKIP or AES for data encryption.
- **Shared Key**—Enter a WPA Shared Key of 8-63 characters.
- **Key Renewal**—Enter a Key Renewal Timeout period, which instructs the router how often it should change the encryption keys. The default is **3600** seconds.

- **WPA-Enterprise**—This option features WPA used in coordination with a RADIUS server for client authentication. (This should only be used when a RADIUS server is connected to the router.)



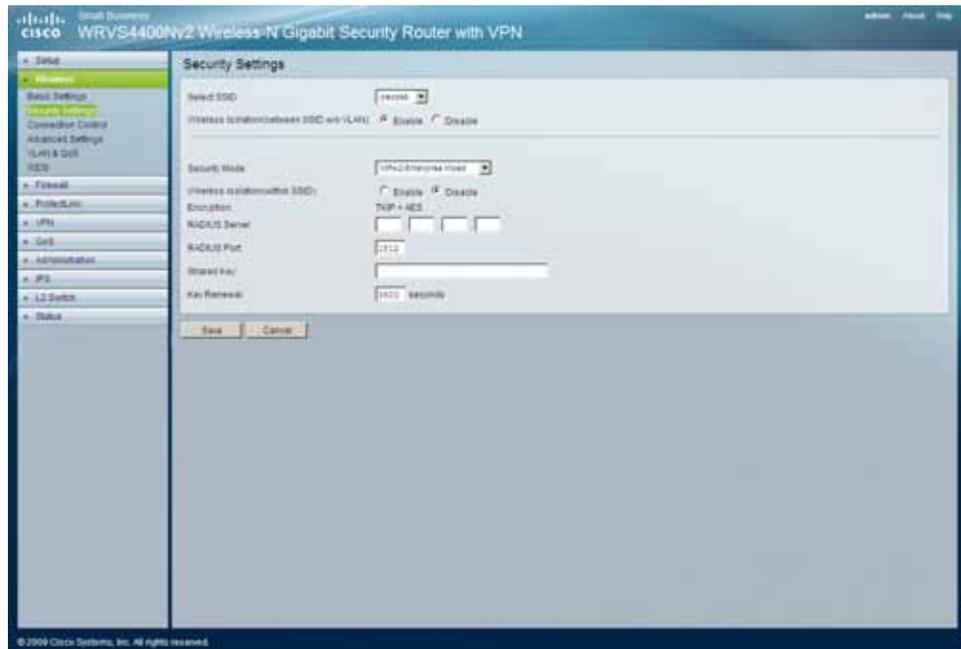
- **Encryption**—WPA offers you two encryption methods, TKIP and AES for data encryption. Select the type of algorithm you want to use, TKIP or AES. The default is TKIP.
- **RADIUS Server**—Enter the RADIUS server's IP address.
- **RADIUS Port**—Enter the port number used by the RADIUS server. The default is 1812.
- **Shared Key**—Enter the Shared Secret key used by the router and RADIUS server.
- **Key Renewal**—Enter a Key Renewal Timeout period, which instructs the router how often it should change the encryption keys. The default is 3600 seconds.

- **WPA2-Enterprise**—This option features WPA2 used in coordination with a RADIUS server for client authentication. (This should only be used when a RADIUS server is connected to the router.)



- **Encryption**—WPA2 always uses AES for data encryption.
- **RADIUS Server**—Enter the RADIUS server's IP address.
- **RADIUS Port**—Enter the port number used by the RADIUS server. The default is 1812.
- **Shared Key**—Enter the Shared Secret key used by the router and RADIUS server.
- **Key Renewal**—Enter a Key Renewal Timeout period, which instructs the router how often it should change the encryption keys. The default is 3600 seconds.

- **WPA2-Enterprise Mixed**—This security mode supports the transition from WPA-Enterprise to WPA2-Enterprise. You can have client devices that use either WPA-Enterprise or WPA2-Enterprise. The wireless router chooses the encryption algorithm used by each client device.

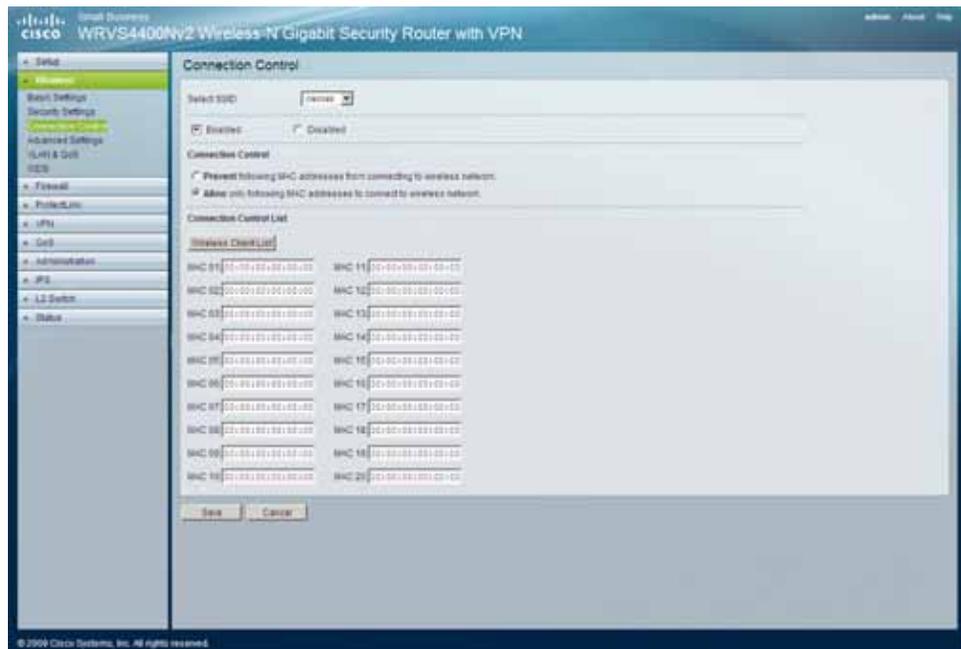


- **Encryption**—Mixed Mode automatically chooses TKIP or AES for data encryption.
- **RADIUS Server**—Enter the RADIUS server's IP address.
- **RADIUS Port**—Enter the port number used by the RADIUS server. The default is 1812.
- **Shared Key**—Enter the Shared Secret key used by the router and RADIUS server.
- **Key Renewal**—Enter a Key Renewal Timeout period, which instructs the router how often it should change the encryption keys. The default is 3600 seconds.

STEP 4 Click **Save**.

Configuring Connection Control

The Wireless > Connection Control window displays the Connection Control settings for the router, giving you two ways to control the connection (association) of wireless client devices. You can either **prevent** specific devices from connecting to the router, or you can **allow** only specific client devices to connect to the router. The client devices are specified by their MAC addresses. The default is to **allow** only specific client devices.



To configure connection control for the router, follow these steps:

- STEP 1** Click **Wireless > Connection Control**
- STEP 2** Configure the Connection Control List to either permit or block specific wireless client devices connecting to (associating with) the wireless router:
 - **Select SSID**—Select the desired SSID.
 - **Enabled/Disabled**—Enable or disable wireless connection control. The default is **Disabled**.

- **Connection Control**—Prevent or Allow specific MAC addresses access to the Wireless Network.
 - **Prevent**—Denies connection to the Wireless Network through the router, for the MAC addresses specified below.
 - **Allow**—Grants connection to the Wireless Network through the router, for the MAC addresses specified below.
- **Connection Control List**—The Wireless > Connection Control List displays the MAC addresses of selected wireless client devices to be controlled.
 - **Wireless Client List**—Instead of manually entering the MAC addresses of each client, the router provides a convenient way to select a specific client device from the client association table. Click this button and a window appears to let you select a MAC address from the table. The selected MAC address are entered into the Connection Control List.
 - **MAC 01-20**—The MAC addresses of the wireless client devices you want to control (i.e. the Connection Control List).

STEP 3 Click **Save**.

Configuring Advanced Wireless Settings

The Wireless > Advanced Settings window displays the advanced settings for the router. The router adopts several new parameters to adjust the channel bandwidth and guard intervals to improve the data rate dynamically.

It is recommended that you let your router automatically adjust the parameters for maximum data throughput.



To configure advanced wireless settings for the router, follow these steps:

STEP 1 Click **Wireless > Advanced Settings**.

STEP 2 Configure the advanced wireless settings as needed by changing the following advanced parameters (some only for Wireless-N) for this router.

Wireless-N data rates are classified into 16 MCS numbers (0-15). MCS stands for Modulation and Coding Scheme. For the same MCS number, the data rate changes according to the Channel Bandwidth and Guard Interval settings.

- **Channel Bandwidth**—Select the channel bandwidth manually for Wireless-N connections. When it is set to 20MHz, only the 20MHz channel is used. When it is set to 40MHz, Wireless-N connections use 40MHz channel but Wireless-B and Wireless-G connections still use 20MHz channel. The default is **Auto**.
- **Guard Interval**—Select the guard interval manually for Wireless-N connections. The two options are **Short (400ns)** and **Long (800ns)**. The default is **Auto**.

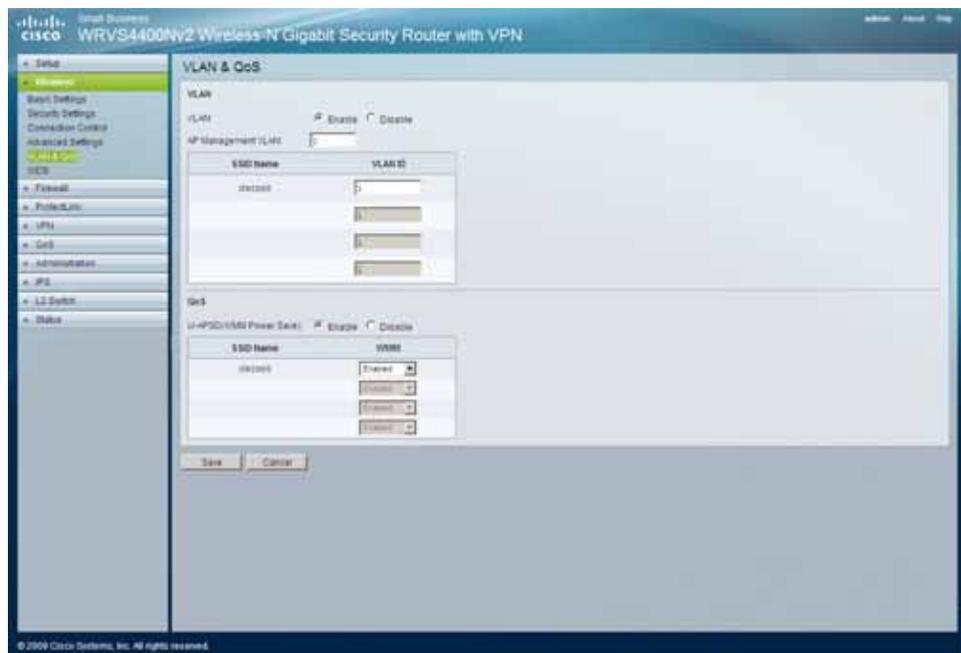
- **CTS Protection Mode**—CTS (Clear-To-Send) Protection Mode function boosts the router's ability to catch all wireless transmissions, but severely decrease performance. Keep the default setting, **Auto**, so the router can use this feature as needed, when the Wireless-N/G products are not able to transmit to the router in an environment with heavy 802.11b traffic. Select **Disabled** if you want to permanently disable this feature.
- **Beacon Interval**— Indicates the frequency interval of the beacon. A beacon is a packet broadcast by the router to keep the network synchronized. A beacon includes the wireless networks service area, the router address, the Broadcast destination addresses, a time stamp, Delivery Traffic Indicator Maps, and the Traffic Indicator Message (TIM). The default is **100 ms**.
- **DTIM Interval**—Indicates how often the router sends out a Delivery Traffic Indication Message (DTIM). Lower settings result in more efficient networking, while preventing your personal computer from dropping into power-saving sleep mode. Higher settings allow your personal computer to enter sleep mode, thus saving power, but interferes with wireless transmissions. The default is **1 ms**.
- **RTS Threshold**— Determines how large a packet can be before the router coordinates transmission and reception to ensure efficient communication. This value should remain at its default setting of **2346**. If you encounter inconsistent data flow, only minor modifications are recommended.

STEP 3 Click **Save**.

Configuring VLAN & QoS Settings

The Wireless > VLAN & QoS window displays the QoS and VLAN settings for the router's Access Point. The QoS (Quality of Service) feature allows you specify priorities for different traffic. Lower priority traffic slows down to allow greater throughput or less delay for high priority traffic.

The 802.1Q VLAN feature allows traffic from different sources to be segmented. Combined with the multiple SSID feature, this provides a powerful tool to control access to your LAN.

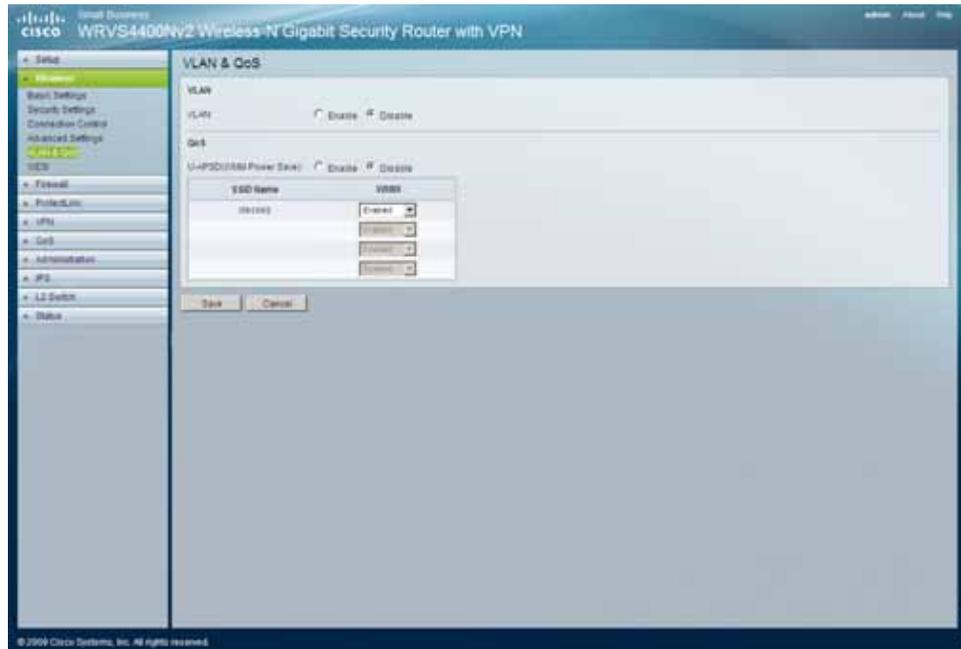


To configure the VLAN and QoS settings for the router, follow these steps:

STEP 1 Click **Wireless > VLAN & QoS**

STEP 2 Configure the VLAN and QoS settings for the router:

- **VLAN**
 - **Enable/Disable VLAN**—Enable this feature only if the hubs/switches on your LAN support the VLAN standard.
 - **AP Management VLAN**—Define the VLAN ID used for management.
 - **VLAN ID**—Enter the VLAN ID.



- **QoS**

- **U-APSD(WMM Power Save)**—Select Enabled or Disabled as required.
- **WMM**—Wi-Fi Multimedia is a QoS feature defined by WiFi Alliance before IEEE 802.11e was finalized. Now it is part of IEEE 802.11e. When it is enabled, it provides four priority queues for different types of traffic. It automatically maps the incoming packets to the appropriate queues based on QoS settings (in IP or layer 2 header). WMM provides the capability to prioritize traffic in your environment. The default is Enabled.

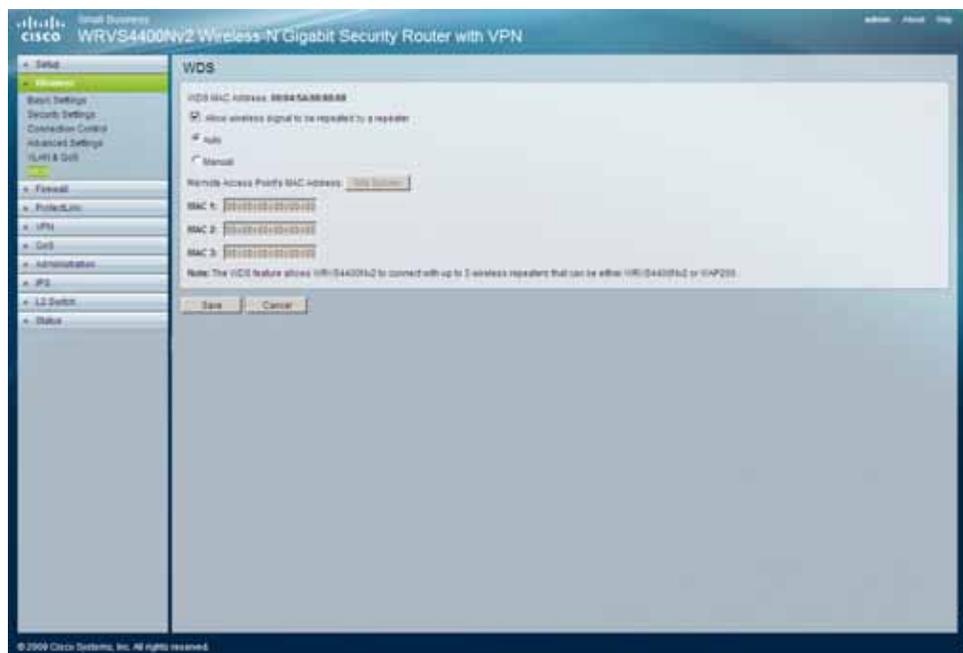
STEP 3 Click **Save**.

Configuring Router WDS Settings

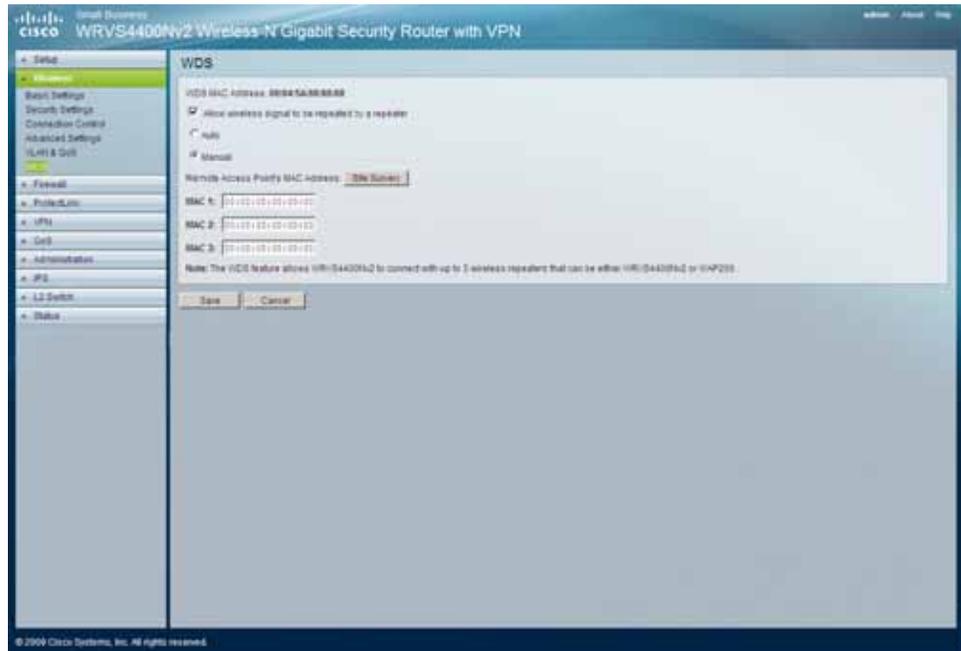
The Wireless > WDS window displays the WDS (Wireless Distribution System) settings for the device.

To configure the WDS settings for the router, follow these steps:

- STEP 1** Click **Wireless > WDS**.
- STEP 2** Configure the WDS settings:



- **WDS MAC Address**—Displays the read-only MAC address for the WDS.
- **Allow wireless signal to be repeated by a repeater**—Select Auto or Manual as required.



- **Remote Access Point's MAC Address**—Either enter the MAC address directly, or, if the other access point is on-line, you can click the Site Survey button and select from a list of available access points.

STEP 3 Click **Save**.

Configuring Firewall Settings

This section describes how to configure the Firewall settings of the router:

- [Configuring Basic Settings on page 89](#)
- [Configuring IP Based ACL on page 91](#)
- [Editing IP ACL Rules on page 93](#)
- [Configuring Internet Access Policy on page 94](#)
- [Configuring Single Port Forwarding on page 99](#)
- [Configuring Port Range Forwarding on page 100](#)
- [Configuring Port Range Triggering on page 102](#)

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



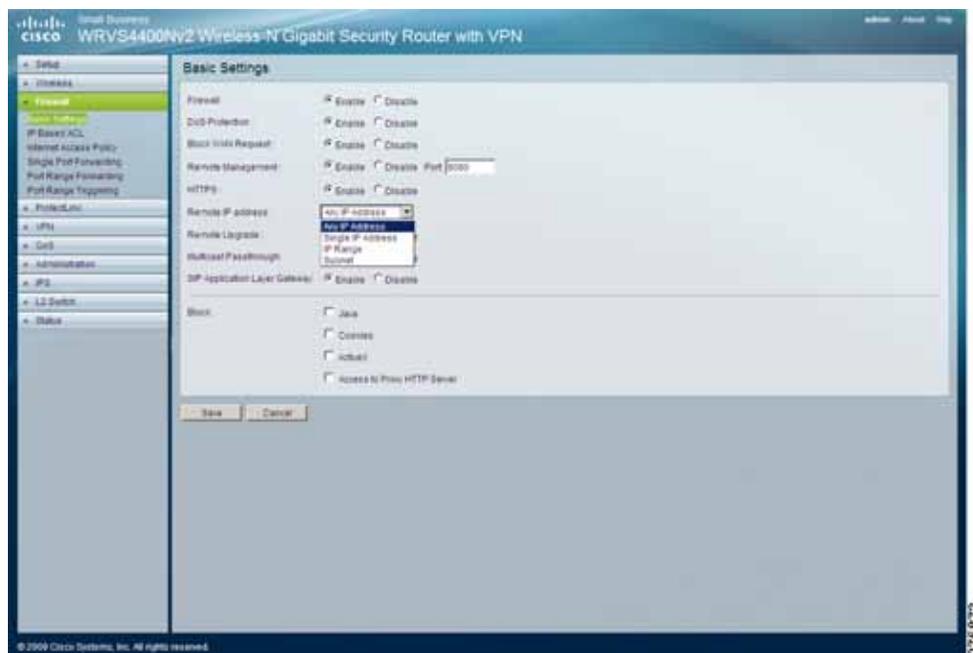
NOTE For WAN traffic, NAPT settings are applied first, then the SPI Firewall settings, followed by IP based Access List (which requires more CPU power).

Configuring Basic Settings

The Firewall > Basic Settings window displays the firewall-specific settings of the router.

To configure basic firewall settings for the router, follow these steps:

- STEP 1** Click Firewall > Basic Settings.
- STEP 2** Configure the basic firewall settings:



- **Firewall**—Enable this feature to perform deep packet inspection on all the traffic going through the router and drop the packets that do not follow the pre-defined protocol behavior. The default is **Enable**.
- **DoS Protection**—When enabled, the router prevents DoS (Denial of Service) attacks coming in from the Internet. DoS attacks consume most of the router's resources and as a result they can prevent legitimate traffic from passing through the router. The default is **Enable**.
- **Block WAN Request**—When enabled, the router ignores PING Request from the Internet so it seems to be hidden. The default is **Enable**.
- **Remote Management**—When enabled, the router allows the web-based utility to be accessed from the Internet. The default is **Disable**.

- **Multicast Pass-through**—When enabled, the router allows IP Multicast traffic to come in from the Internet. The default is **Disable**.
- **SIP Application Layer Gateway**—When enabled, the SIP Application Layer Gateway (ALG) allows Session Initiation Protocol (SIP) packets (used for Voice over IP) to traverse the NAT firewall. This feature can be disabled if the VoIP service provider is using other NAT traversal solutions such as STUN, TURN, and ICE.
- **Block**—Select the Web features that you wish to restrict. All those features could place security concern to your personal computers on the LAN side. You have to balance your needs on those applications and security. The default is unselected.
 - **Java**—Java is a programming language for websites. If you deny Java, you run the risk of not having access to Internet sites created using this programming language.
 - **Cookies**—A cookie is data stored on your personal computer and used by Internet sites when you interact with them, so you may not want to deny cookies.
 - **ActiveX**—ActiveX is a Microsoft (Internet Explorer) programming language for websites. If you deny ActiveX, you run the risk of not having access to Internet sites using this programming language. Also, Windows Update uses ActiveX, so if this is blocked, Windows Update does not work.
 - **Access to Proxy HTTP Server**—If local users have access to WAN proxy servers, they may be able to circumvent the router's content filters and access Internet sites blocked by the router. Denying Proxy blocks access to any WAN proxy servers.

STEP 3 Click **Save**.

Configuring IP Based ACL

The Firewall > IP Based ACL window displays a summary of the configured IP-based access control list. The access list restricts traffic going through the router either from WAN or LAN port.

There are two ways to restrict data traffic. You can block specific types of traffic according to your ACL definitions. Or you can allow only specific types of traffic according to your ACL definition. The ACL rules are read according to their priority. If there is a match for a packet, the action is taken and the following lower priority rules are not checked against this packet.



NOTE

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

There are two default rules in the table that cannot be deleted. The first rule allows all traffic coming in from LAN port to pass the router. The second rule allows all traffic coming in from WAN port. These two rules have the lowest priority, so without adding any user defined rules, all the packets can be passed through from both WAN and LAN sides. The rule is enabled if the **Enable** button is checked and if the date and time are matched. If any of the conditions are not met, the rule is not used to check against packets.



To configure the IP Based ACL for the router, follow these steps:

STEP 1 Click **Firewall > IP Based ACL**.

STEP 2 Configure the IP based ACL settings for the router:

- **Priority**—Defines the order on which rule is checked against first. The smaller number has higher priority. The default rules is always be checked last.
- **Enable**—Tells the router if the rule is active or not. You can have rules defined in the ACL Table but in an inactive state. The administrator can decide on when to enable specific ACL rules manually.
- **Action**—Defines how the rule is to affect the traffic. It can be either **Allow** or **Deny**. If the rule is matched and the action is **Allow**, the packet is forwarded. If the rule is matched and the action is **Deny**, the packet is dropped.
- **Service**—Select one of the pre-defined services in the drop-down menu or you can define new services by clicking **Service Management**. When you define your own service, it is listed on the top of the drop-down menu. You can also select **ALL** to allow or block all types of IP traffic.
- The user-defined service GUI page can be either accessed from the New Rule window by clicking **Service Management**, or you can access it directly from the 2nd layer page under Firewall.
- **Source Interface**—Select **LAN**, **WAN**, or **ANY** interface.
- **Source**—The source IP address to be matched against. You can define a **Single** IP address, a **Range** of IP addresses (start IP and end IP), a **Network** (IP Prefix and Network Mask), or **ANY** IP addresses.
- **Destination**—The destination IP address to be matched against. You can define a **Single** IP address, a **Range** of IP addresses (start IP and end IP), a **Network** (IP Prefix and Network Mask), or **ANY** IP addresses.
- **Time**—Displays the time period in which this rule is enabled (used together with Date). It can be set to **Any Time**.
- **Date**—Displays the days in a week in which this rule is enabled (used together with Time). It can be set to **Any Day**.
- **Edit button**—Use this button to go to **Edit IP ACL Rule** window and modify this rule.
- **Delete button**—Use this button to delete the ACL rule from the list.

- **Page Selections**—Select specific page of ACL list from the drop-down menu to be displayed. Or navigate them page by page through **Previous Page** and **Next Page** button.
- **Add New Rule**—Click this button to enter the page to define a new ACL rule.
- **Disable All Rule**—Click this button to disable all the user defined rules.
- **Delete All Rule**—Click this button to delete all the user defined rules.

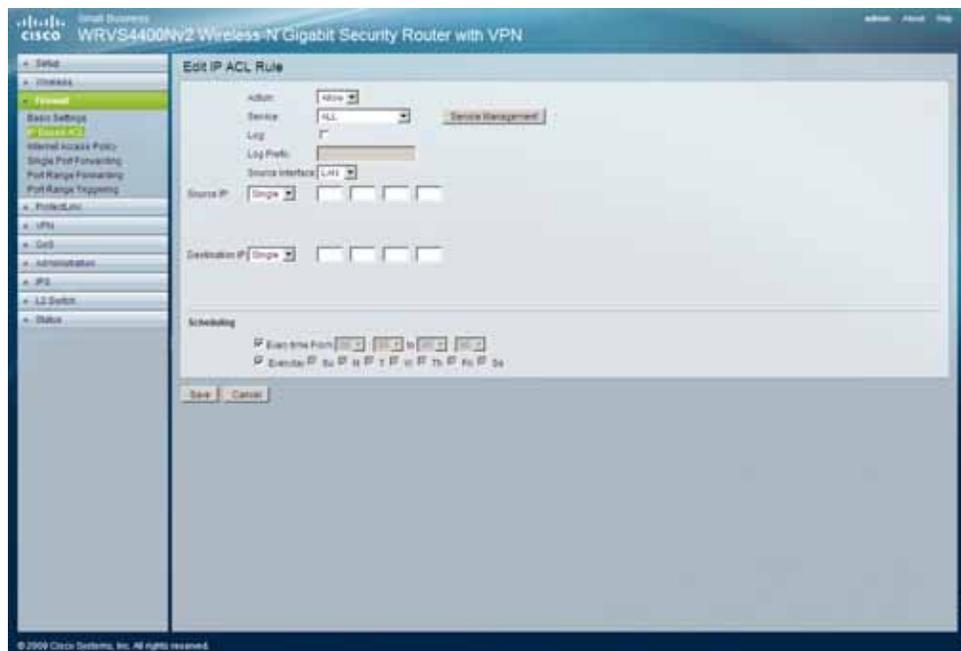
Editing IP ACL Rules

The Firewall > Edit IP ACL Rule window displays the settings for the IP Based ACL rule being added or edited.

To add an IP ACL Rule, follow these steps:

STEP 1 Click **Firewall > Edit IP ACL Rule**.

STEP 2 Fill in the fields defining the current rule:



- **Action**—Select either **Allow** or **Deny**. Default is **Allow**.
- **Service**—Select **ALL** or pre-defined (or user-defined) services from the drop-down menu.

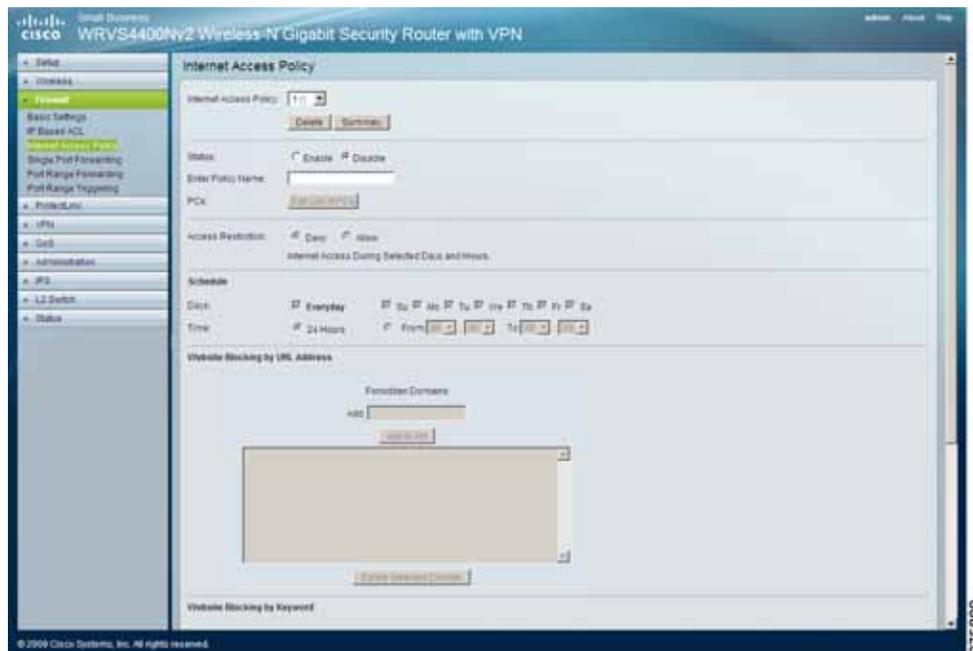
- **Log**—If checked, this ACL rule is logged when a packet match happens.
- **Log Prefix**—This string is attached in front of the log for the matched event.
- **Source Interface**—Select LAN, WAN, or ANY interface.
- **Source**—The source IP address to be matched against. You can define a **Single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

STEP 3 Click **Save**.

Configuring Internet Access Policy

The Firewall > Internet Access Policy window displays the policies that are used by the router to control access to the Internet. A policy consists of four components:

- The MAC- or IP- addresses of the personal computers to which to apply this policy
- Whether to **Deny** or **Allow** Internet service for this policy
- The time and date on which to enable this policy, and
- The URLs or Keywords to apply this policy.



To configure Internet access policy for the router, follow these steps:

-
- STEP 1** Click **Firewall > Internet Access Policy**.
- STEP 2** Configure the router's Internet access policy settings by creating, modifying, verifying, and deleting policies as appropriate.
- [Creating a Policy on page 96](#)
 - [Deleting a Policy on page 98](#)
 - [Viewing all Policies on page 98](#)
 - [Viewing or Changing the List of Personal Computers Covered by the Current Policy on page 98](#)
- STEP 3** Click **Save**.
-

Creating a Policy

To create an Internet access policy, follow these steps:

- STEP 1** Select a policy number from the **Internet Access Policy** drop-down menu.
- STEP 2** Enter a Policy Name in the field provided.
- STEP 3** Enable this policy by clicking the **Enable** option.
- STEP 4** Click the **Edit List of PCs** button to select which personal computers are affected by the policy. The List of PCs window appears. You can select a personal computer by MAC address or IP address. You can also enter a range of IP addresses if you want this policy to affect a group of personal computers. After making your changes, click **Save** to apply your changes.
- STEP 5** Click the appropriate option, **Deny** or **Allow**, depending on whether you want to block or allow Internet access for the personal computers you listed on the List of PCs window.
- STEP 6** Decide what Days and what Times you want this policy to be enforced. Select the individual days during which the policy is in effect, or select **Everyday**. Enter a range of hours and minutes during which the policy is in effect, or select **24 Hours**.

Deleting a Policy

To delete a policy, select it from the drop-down menu, then click the **Delete** button.

Viewing all Policies

To view a summary of all the policies, click the **Summary** button. On the Summary window, the policies are listed with the following information: No., Policy Name, Days, Time, and a check box to delete (clear) the policy. To delete a policy from the Summary window, check the check box in the **Delete** column, and click the **Delete** button.

Viewing or Changing the List of Personal Computers Covered by the Current Policy

To view or change the list of personal computers covered by the current policy, click the **Edit List of PCs** button.

On the **List of PCs** window, you can define personal computers by MAC address or IP address. You can also enter a range of IP addresses if you want this policy to affect a group of personal computers.

List of PCs

Enter MAC Address of the PCs in this format: xxxxxxxxxxxx

MAC 01 <input style="width: 100%;" type="text" value="000000000000"/>	MAC 05 <input style="width: 100%;" type="text" value="000000000000"/>
MAC 02 <input style="width: 100%;" type="text" value="000000000000"/>	MAC 06 <input style="width: 100%;" type="text" value="000000000000"/>
MAC 03 <input style="width: 100%;" type="text" value="000000000000"/>	MAC 07 <input style="width: 100%;" type="text" value="000000000000"/>
MAC 04 <input style="width: 100%;" type="text" value="000000000000"/>	MAC 08 <input style="width: 100%;" type="text" value="000000000000"/>

Enter the IP Address of the PCs

IP 01 192.168.1. <input style="width: 30px;" type="text" value="0"/>	IP 04 192.168.1. <input style="width: 30px;" type="text" value="0"/>
IP 02 192.168.1. <input style="width: 30px;" type="text" value="0"/>	IP 05 192.168.1. <input style="width: 30px;" type="text" value="0"/>
IP 03 192.168.1. <input style="width: 30px;" type="text" value="0"/>	IP 06 192.168.1. <input style="width: 30px;" type="text" value="0"/>

Enter the IP Range of the PCs

IP Range 01	IP Range 02
192.168.1. <input style="width: 30px;" type="text" value="0"/> ~ <input style="width: 30px;" type="text" value="0"/>	192.168.1. <input style="width: 30px;" type="text" value="0"/> ~ <input style="width: 30px;" type="text" value="0"/>

275882

Configuring Single Port Forwarding

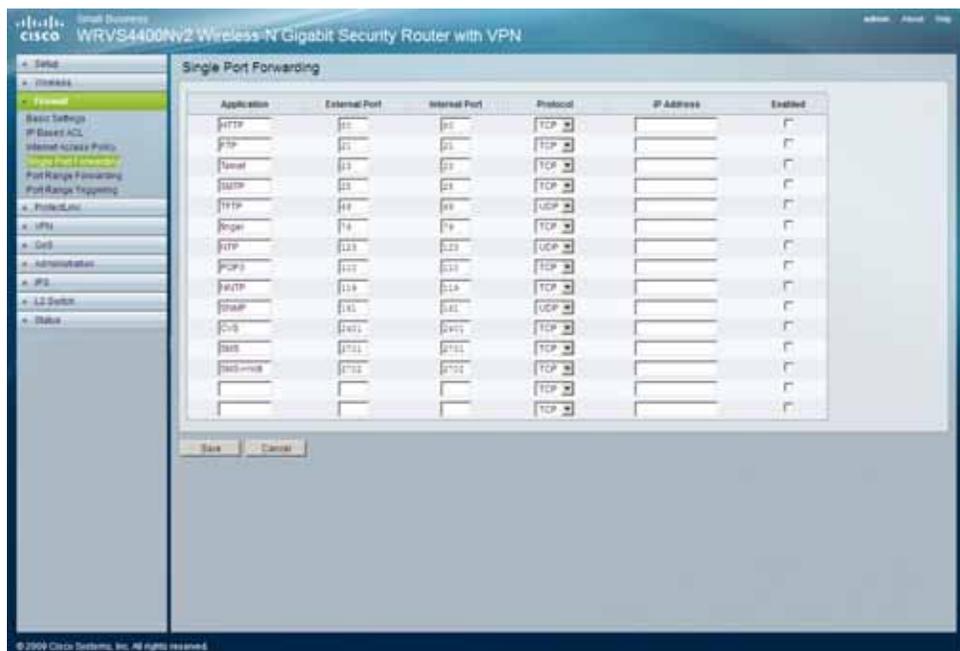
The Firewall > Single Port Forwarding window displays the specific port and other settings associated with each public service that uses just a single port.

Single Port Forwarding is one of the NAT features and allows users of the Internet to access this server by using the WAN port address and the matched external port number.

When users send these types of request to your WAN port IP address via the Internet, the NAT router forwards those requests to the appropriate servers on your LAN.

To configure single port forwarding for the router, follow these steps:

- STEP 1** Click Firewall > Single Port Forwarding.
- STEP 2** Configure single port forwarding settings for the router:



- **Application**—Enter the name of the application you wish to configure.
- **External Port**—Port number used by the service or Internet application. Internet users must connect using this port number. Check with the software documentation of the Internet application for more information.

- **Internal Port**—Port number used by the router when forwarding Internet traffic to the personal computer or server on your LAN and is usually the same as the External Port number. If it is different, the router performs a Port Translation, so that the port number used by Internet users is different from the port number used by the server or Internet application.

For example, you could configure your Web Server to accept connections on both port 80 (standard) and port 8080. Then, enable Port Forwarding, set the External Port to 80 and the Internal Port to 8080.

Now, any traffic from the Internet to your Web server uses port 8080, even though the Internet users used the standard port, 80. (Users on the local LAN can and should connect to your Web Server using the standard port 80.)

- **Protocol**—Select the protocol used for this application, **TCP** or **UDP**.
- **IP Address**—For each application, enter the IP address of the personal computer running the specific server application.
- **Enabled**—Select **Enabled** to enable port forwarding for the relevant server application.

STEP 3 Click **Save**.

Configuring Port Range Forwarding

The Firewall > Port Range Forwarding window displays the settings associated with public services accessed on your network that use single or multiple port numbers, such as web servers, FTP servers, e-mail servers, or other specialized Internet applications that use one or multiple port numbers (for example, video conferencing). Port Range Forwarding is one of the NAPT (Network Address Port Translation) features.

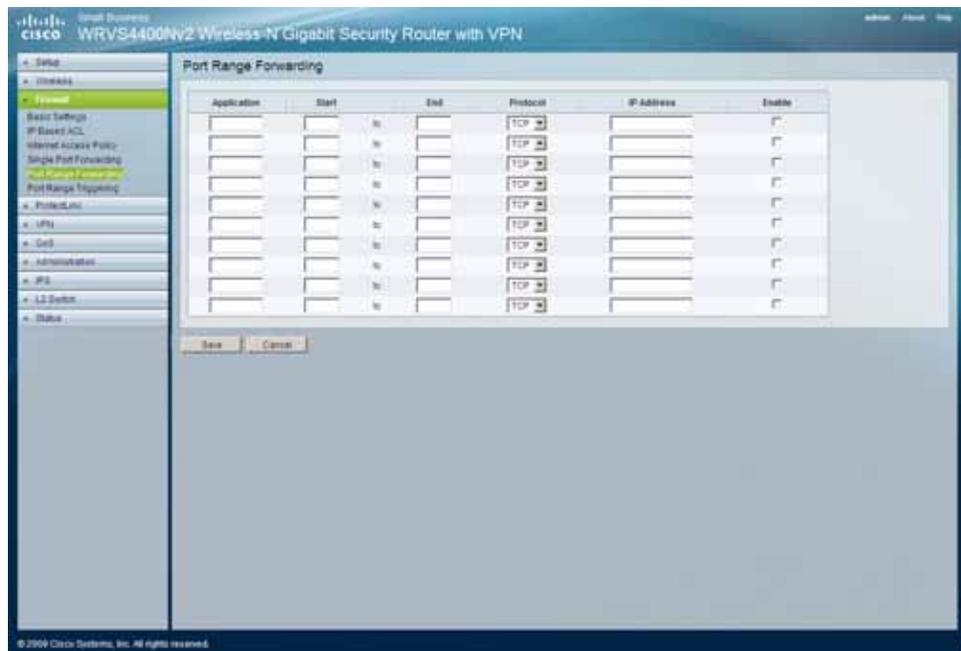
The Port Range Forwarding window allows you to configure access to these public services on your network. The port numbers being used does not change while forwarding to the local network. This allows users on the Internet to access this server by using the WAN port IP address and the pre-defined port numbers.

When users send these types of requests to your WAN port IP address via the Internet, the NAT router forwards those requests to the appropriate servers on your LAN.

To configure port range forwarding for the router, follow these steps:

STEP 1 Click **Firewall > Port Range Forwarding**.

STEP 2 Configure port range forwarding settings for the router:



- **Application**—Enter the name of the application you wish to configure.
- **Start**—Enter the beginning of the port number range (external ports) used by the server or Internet application. For more information, check the software documentation of the Internet application.
- **End**—The end of the port range. Enter the end of the range of port numbers (external ports) used by the server or Internet application. For more information, check the software documentation of the Internet application.
- **Protocol**—Select the protocol used for this application, **TCP** or **UDP**.
- **IP Address**—For each application, enter the IP address of the personal computer running the specific application.
- **Enabled**—Select **Enabled** to enable port range forwarding for the relevant application.

STEP 3 Click **Save**.

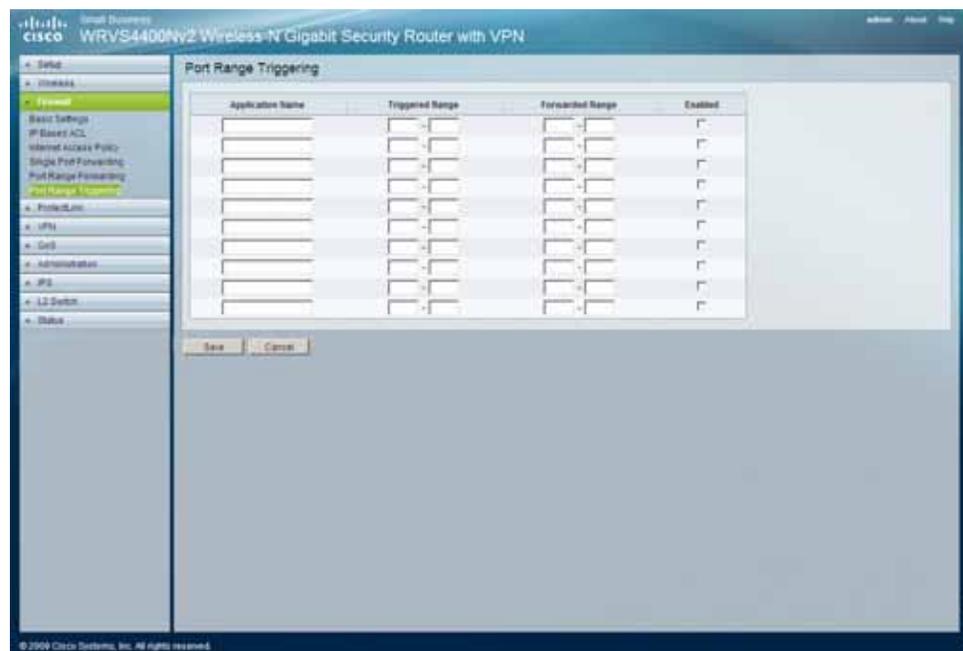
Configuring Port Range Triggering

The Firewall > Port Range Triggering window displays the configurations of triggered range and forwarded range of ports that are used by applications that request ports to be opened on demand. Port Range Triggering is an NAT (Network Address Port Translation) feature.

Port Range Triggering is used for special applications that can request a port to be opened on demand. For this feature, the router watches outgoing packets for specific port numbers. This triggers the router to allow the incoming packets within the specified forwarding range and forward those packets to the triggering personal computer. One of the example applications is QuickTime. It would use port 1000 for outgoing packets and 2000 for incoming packets.

To configure port range triggering for the router, follow these steps:

- STEP 1** Click Firewall > Port Range Triggering.
- STEP 2** Configure port range triggering settings for the router:



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

STEP 3 Click **Save**.

Configuring the ProtectLink Web Service

The Cisco ProtectLink Web service provides security for your network. It checks email messages, filters website addresses (URLs), and blocks potentially malicious websites.

For detailed information on how to configure the ProtectLink Service, go to [Appendix E, "Cisco ProtectLink Web Service"](#).

Configuring the VPN Settings

This section describes how to configure the VPN settings of the router:

- [Displaying A VPN Status Summary of the IPSec Tunnel and Clients on page 105](#)
- [Configuring IPSec VPN on page 108](#)
- [Setting Up Local Groups on page 110](#)
- [Setting Up and Configuring Remote Groups on page 111](#)
- [Setting Up IPSec on page 113](#)
- [Configuring VPN Client Accounts on page 115](#)
- [Configuring VPN Passthrough on page 117](#)

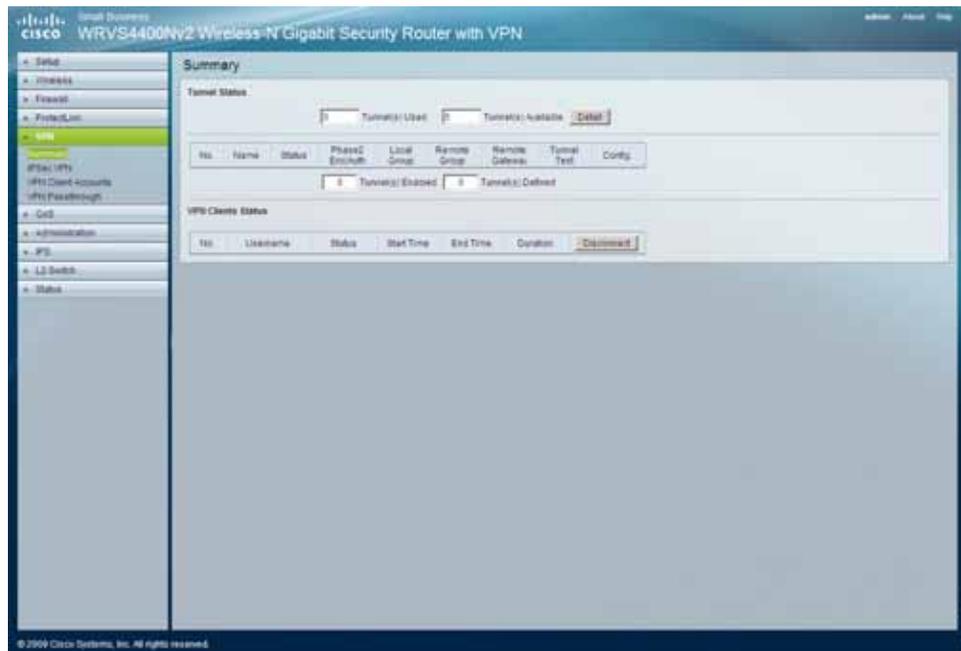
Displaying A VPN Status Summary of the IPSec Tunnel and Clients

The VPN > Summary window displays a summary of the IPSec tunnel status and VPN Clients status:

To display a VPN Status Summary for the router, follow these steps:

STEP 1 Click **VPN > Summary**.

STEP 2 View the VPN Status Summary information for the router:



- Tunnel Status
 - **Tunnels(s) Used**—Displays the number of tunnels used.
 - **Tunnel(s) Available**—Displays the number of available tunnels.
 - **Detail button**—Click **Detail** to display more tunnel information.
 - **No**—Displays the number of the tunnel.
 - **Name**—Displays the name of the tunnel, as defined by the Tunnel Name field on the VPN > IPsec VPN window.
 - **Status**—Displays the tunnel's status: Connected, Hostname Resolution Failed, Resolving Hostname, or Waiting for Connection.
 - **Phase Enc/Auth**—Displays the Phase 2 Encryption type (3DES), Authentication type (MD5 or SHA1), and Group (768-bit, 1024-bit, or 1536-bit) that you chose in the VPN > IPsec VPN window.
 - **Local Group**—Displays the IP address and subnet of the local group.
 - **Remote Group**—Displays the IP address and subnet of the remote group.
 - **Remote Gateway**—Displays the IP address of the remote gateway.

- **Tunnel Test**—Click **Connect** to verify the tunnel status; the test result is updated in the Status column. If the tunnel is connected, you can disconnect the IPSec VPN connection by clicking **Disconnect**.
- **Config**—Click **Edit** to change the tunnel's settings. Click **Trash** to delete all of the tunnel's settings.
- **Tunnels(s) Enabled**—Displays the number of enabled tunnels.
- **Tunnel(s) Defined**—Displays the number of defined tunnels.
- **VPN Clients Status**
 - **No**—The range of user number is from 1 to 5.
 - **Username**—Displays the username of the VPN Client.
 - **Status**—Displays the connection status of the VPN Client.
 - **Start Time**—Displays the start time of the most recent VPN session for the specified VPN Client.
 - **End Time**—Displays the end time of a VPN session if the VPN Client has disconnected.
 - **Duration**—Displays the total connection time of the latest VPN session.
 - **Disconnect**—Check the Disconnect box at the end of each row in the VPN Clients Table and click **Disconnect** to disconnect a VPN Client session.

Configuring IPsec VPN

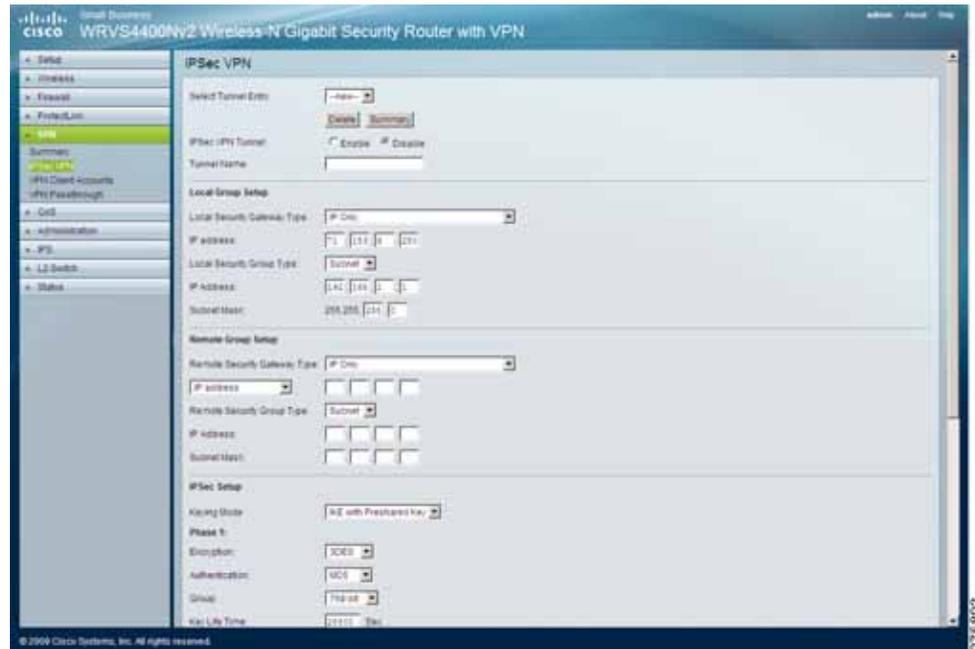
The VPN > IPsec VPN window displays settings for configuring a VPN tunnel.

Virtual Private Network (VPN) is a security measure that creates a secure connection between two remote locations. Configure these settings so that the gateway creates VPN tunnels.

To configure the VPN Gateway to create VPN tunnels, follow these steps:

STEP 1 Click **VPN > IPsec VPN**.

STEP 2 Configure the gateway to create the VPN tunnels:



- **Select Tunnel Entry**—Select a tunnel to configure.
- **Delete**—Deletes all settings for the selected tunnel.
- **Summary**—Shows the settings and status of all enabled tunnels.
- **IPsec VPN Tunnel**—Click **Enable** option to enable this tunnel.
- **Tunnel Name**—Enter a name for this tunnel, such as “LA Office.”

-
- STEP 3** Configure the settings in the following sections of the VPN > IPsec VPN window:
- [Setting Up Local Groups on page 110](#)
 - [Setting Up and Configuring Remote Groups on page 111](#)
 - [Setting Up IPsec on page 113](#)
- STEP 4** To configure advanced settings, click **Advanced**.
- **Aggressive Mode**—There are two types of Phase 1 exchanges: Main mode and Aggressive mode. Aggressive Mode requires half of the main mode messages to be exchanged in Phase 1 of the SA exchange. If network security is preferred, select Main mode.
 - **NetBIOS broadcast**—Check the box to enable NetBIOS traffic to pass through the VPN tunnel. By default, WRVS4400N blocks these broadcasts.
- STEP 5** Click **Save**.
- STEP 6** To establish a connection for the current VPN tunnel, click **Connect**.
- To break the connection, click **Disconnect**.
- STEP 7** To view the VPN log, which shows details of each tunnel established, click **View Log**.
-

Setting Up Local Groups

The Local Group Setup section of the VPN > IPsec VPN window displays settings for configuring the local groups of VPN tunnel connections.

To configure local groups of VPN tunnel connections, do the following:

STEP 1 Click **VPN > IPsec VPN**.

STEP 2 Configure Local Group Setup settings:

- **Local Security Gateway Type**—There are two types. They are IP Only, IP + Domain Name (FQDN) Authentication.
 - **IP Only**—If you select IP Only, only the specific IP address can access the tunnel. The WAN IP of WRVS4400N appears in this field automatically.
 - **IP + Domain Name (FQDN) Authentication**—If you select this type, enter the FQDN (Fully Qualified Domain Name), and the IP address appears automatically. The FQDN is the host name and domain name for a specific computer on the Internet, for example, vpn.myvpnserver.com. The IP and FQDN must be same with the Remote Security Gateway type of the remote VPN device, and the same IP and FQDN can be only for one tunnel connection.
- **Local Security Group Type**—Select the local LAN user(s) behind the router that can use this VPN tunnel. This may be a single IP address or Sub-network. Notice that the Local Secure Group must match the other router's Remote Secure Group.
- **IP Address**—Enter the IP address on the local network.
- **Subnet Mask**—If the Subnet option is selected, enter the mask to determine the IP addresses on the local network.

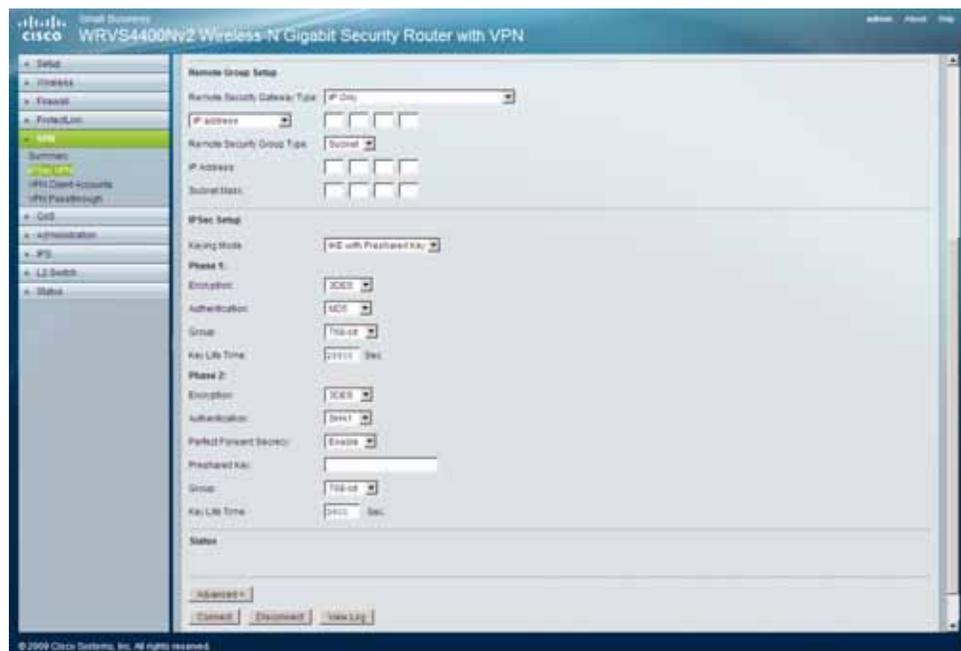
STEP 3 Click **Save**.

Setting Up and Configuring Remote Groups

The Remote Group Setup section of the VPN > IPsec VPN window displays settings for configuring the remote groups of VPN tunnel connections.

To set up and configure a remote group, follow these steps:

STEP 1 Click VPN > IPsec VPN.



STEP 2 Configure Remote Group Setup settings.

- **Remote Security Gateway Type**—There are two types. They are IP Only, IP + Domain Name (FQDN) Authentication. The type of Remote Security Gateway should match with the Local Security Gateway Type of VPN devices in the other end of tunnel.

- **IP Only**—If you select **IP Only**, only the specific IP address that you enter can access the tunnel. It's the IP address of the remote VPN router or device which you wish to communicate. The remote VPN device can be another VPN router or a VPN Server. If you know the static IP address of remote VPN device, select **IP address** from drop-down menu. If you don't know the static IP address of remote VPN device, but the domain name of remote VPN device is known, you can select **IP by DNS Resolved**, and enter the real domain name on the Internet. The WRVS4400N router gets the IP address of the remote VPN device by DNS Resolved, and IP address of remote VPN device appears on VPN Status of the Summary page.
- **IP + Domain Name (FQDN) Authentication**—If you select this type, enter the FQDN (Fully Qualified Domain Name) and IP address of the VPN device at the other end of the tunnel. If you know the static IP address of remote VPN device, select **IP address** from drop-down menu. If you don't know the static IP address of remote VPN device, but the domain name of remote VPN device is known, you can select **IP by DNS Resolved**, and enter the real domain name on the Internet. The WRVS4400N router gets the IP address of remote VPN device by DNS Resolved, and IP address of remote VPN device appears on the VPN Status of Summary page. Then, enter the Domain Name as an ID, it can be not a real domain name on Internet. The IP and Domain Name ID must be same with the Local Gateway of the remote VPN device, and the same IP and Domain Name ID can be only for one tunnel connection.
- **Remote Security Group**—Select the remote LAN user(s) behind the remote gateway who can use this VPN tunnel. This may be a single IP address, a Sub-network, or any addresses. If “Any” is set, the router acts as responder and accepts request from any remote user. Notice that the Remote Secure Group must match the other router's Local Secure Group.
- **IP Address**—Enter the IP address on the local network.
- **Subnet Mask**—If the “Subnet” option is selected, enter the mask to determine the IP addresses on the local network.
- **Remote Security Gateway**—Select the desired option - IP address.
- **IP**—The IP address in this field must match the public IP address WAN IP address) of the remote gateway at the other end of this tunnel.

STEP 3 Click **Save**.

Setting Up IPSec

The IPSec Setup section of the VPN > IPSec VPN window displays the security parameters for configuring a VPN.

To set up IPSec for the router, follow these steps:

STEP 1 Click **VPN > IPSec Setup**.

STEP 2 Configure the security parameters for VPN IPSec:

- **Keying Mode**—The router supports both **IKE with Preshared Key** (automatic) and **Manual** key management. When choosing automatic key management, IKE (Internet Key Exchange) protocols are used to negotiate key material for SA. If manual key management is selected, no key negotiation is needed. Basically, manual key management is used in small static environments or for troubleshooting purpose. Notice that both sides must use the same Key Management method.
- **Encryption**—The Encryption method determines the length of the key used to encrypt/decrypt ESP packets. **3DES** is supported. Notice that both sides of the VPN tunnel must use the same Encryption method.
- **Authentication**—Authentication determines a method to authenticate the ESP packets. Either **MD5** or **SHA1** may be selected. Both sides of the VPN tunnel must use the same Authentication method.
 - **MD5**—A one way hashing algorithm that produces a 128-bit digest.
 - **SHA1**—A one way hashing algorithm that produces a 160-bit digest.
- **Preshared Key**— IKE uses the Pre-shared Key field to authenticate the remote IKE peer. Both character and hexadecimal value are acceptable in this field. for example; “My_@123” or “0x4d795f403 13233.” Both sides must use the same Pre-shared Key.
- **Key Lifetime**—Specifies the lifetime of the IKE generated key. If the time expires, a new key is renegotiated automatically. The Key Lifetime may range from 1081 to 86400 seconds. The default value for Phase 1 is 28800 seconds, and default value for Phase 2 is 3600 seconds
- **Group**— For Diffie-Hellman key negotiation. There are 3 groups available for ISAKMP SA establishment, 768-bit, 1024-bit, 1536-bit represent different bits used in Diffie-Hellman mode operation. The default value is Group 768-bit.

- **Encryption**— The Encryption method determines the length of the key used to encrypt/decrypt ESP packets. 3DES is supported. Notice that both sides of the VPN tunnel must use the same Encryption method.
- **Authentication**— Authentication determines a method to authenticate the ESP packets. Either MD5 or SHA1 may be selected. Notice that both sides (VPN endpoints) must use the same Authentication method.
 - MD5— A one way hashing algorithm that produces a 128-bit digest.
 - SHA1— A one way hashing algorithm that produces a 160-bit digest.
- **Perfect Forward Secrecy**— If PFS is enabled, IKE Phase 2 negotiation generates a new key material for IP traffic encryption and authentication. Note: that both sides must have this selected.
- **Preshared Key**— This field specifies a key used to authenticate IP traffic. Both character and hexadecimal value are acceptable in this field. Note: that both sides must use the same Authentication Key.
- **Inbound SPI/Outbound SPI**—The SPI (Security Parameter Index) is carried in the ESP header. This enables the receiver to select the SA, under which a packet should be processed. The SPI is a 32-bit value. Both decimal and hexadecimal values are acceptable. for example, “987654321” or “0x3ade68b1”. Each tunnel must have unique an Inbound SPI and Outbound SPI. No two tunnels share the same SPI. Notice that Inbound SPI must match the other router's Outbound SPI, and vice versa

Viewing Connection Status

The Status section of the VPN > IPsec VPN window shows the connection status for the selected tunnel. The state is either connected or disconnected.

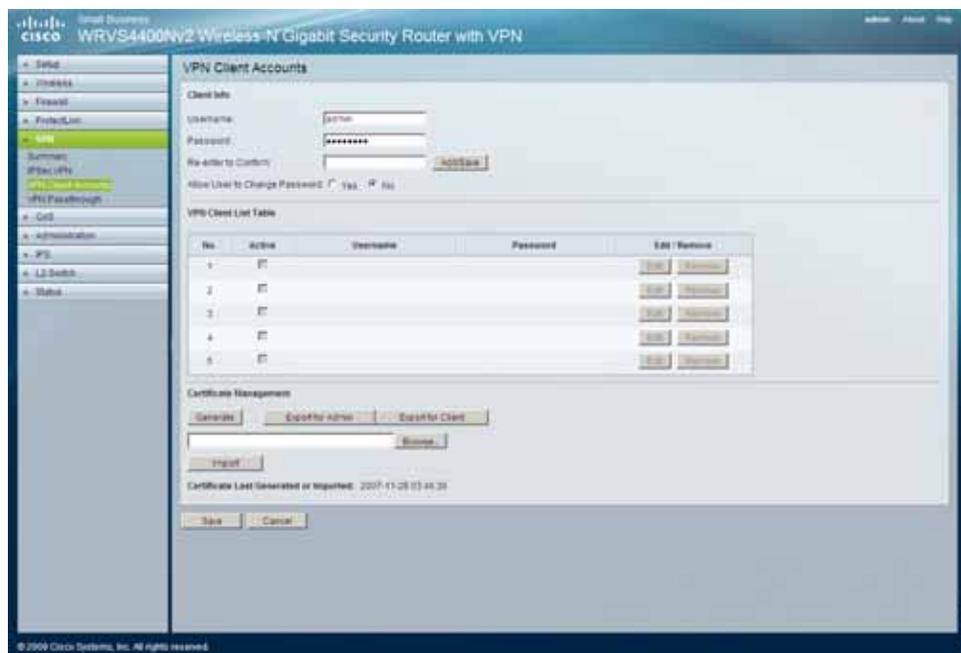
STEP 3 Click Save.

Configuring VPN Client Accounts

The VPN > VPN Client Accounts window displays the settings for administering your VPN Client users. Enter the information at the top of the window and the users you've entered appear in the list at the bottom, showing their status.

This works with the Cisco QuickVPN client only. (The router supports up to five Cisco QuickVPN Clients by default.)

Additional QuickVPN Client licenses can be purchased separately. See www.cisco.com for more information.



To configure VPN Client Accounts, follow these steps:

STEP 1 Click **VPN > VPN Client Accounts**.

STEP 2 Configure the VPN Client Accounts setting:

- **Username**—Enter the username using any combination of keyboard characters.
- **Password**—Enter the password you would like to assign to this user.
- **Re-enter to Confirm**—Retype the password to ensure that it has been entered correctly.

- **Allow User to Change Password**—Determines whether the user is allowed to change their password.
- VPN Client List Table
 - **No**—Displays the user number.
 - **Active**—When checked, the designated user can connect, otherwise the VPN client account is disabled.
 - **Username**—Displays the username.
 - **Edit button**—Modify the username, password, or toggle between whether the user is allowed to change their password.
 - **Remove button**—Delete a user account.
- Certificate Management

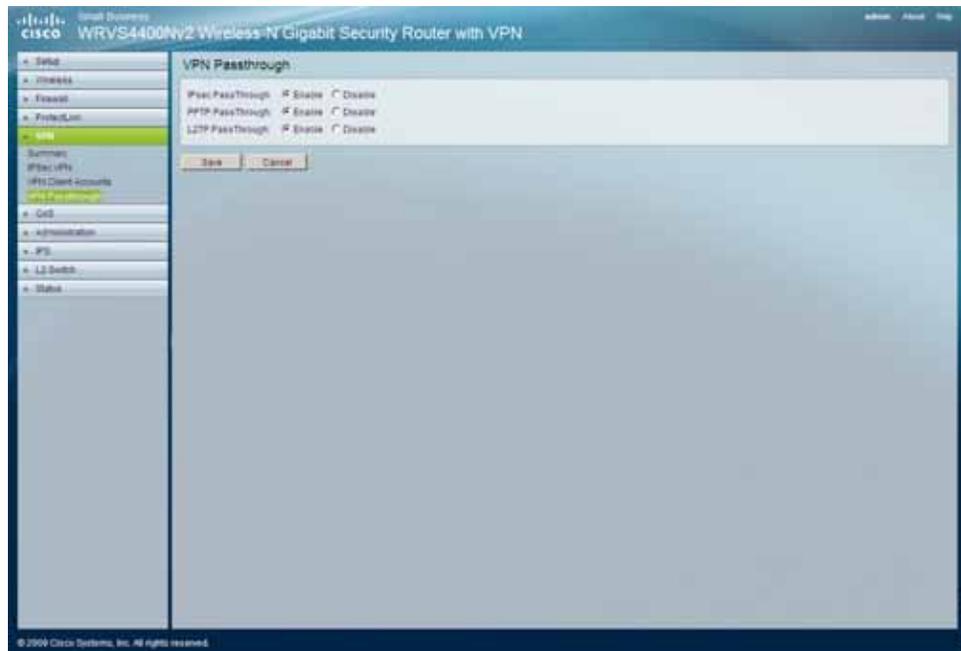
Use this section to manage the certificate used for securing the communication between the router and QuickVPN clients.

- **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 asks you to specify where you want to store your certificate. The default file name is “WRVS4400N_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 asks you where you want to store your certificate. The default file name is “WRVS4400N_Client.pem” but you can use another name. For QuickVPN users to securely connect to the router, this certificate needs to be placed in the install directory of the QuickVPN client.
- **Import**—Click this button to import a certificate previously saved to a file using Export for Admin or Export for Client. Enter the file name in the field or click **Browse** to locate the file on your computer, then click **Import**.
- **Certificate Last Generated or Imported**—Displays the date and time when a certificate was last generated or imported.

STEP 3 Click **Save**.

Configuring VPN Passthrough

The VPN > VPN Passthrough window displays the settings needed to allow users to have the router pass through the traffic, using their own VPN algorithms to connect to their remote routers.



To configure VPN Passthrough settings for the router, follow these steps:

- STEP 1** Click **VPN > VPN Passthrough**.
- STEP 2** Configure VPN Passthrough settings.
 - **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 PPTP Passthrough, select **Disabled**.

- **L2TP Passthrough**—Layer 2 Tunneling Protocol is the similar to PPP but allows Layer 2 and the PPP session to terminate at different servers or locations. L2TP Passthrough is enabled by default. To disable L2TP Passthrough, select **Disabled**.

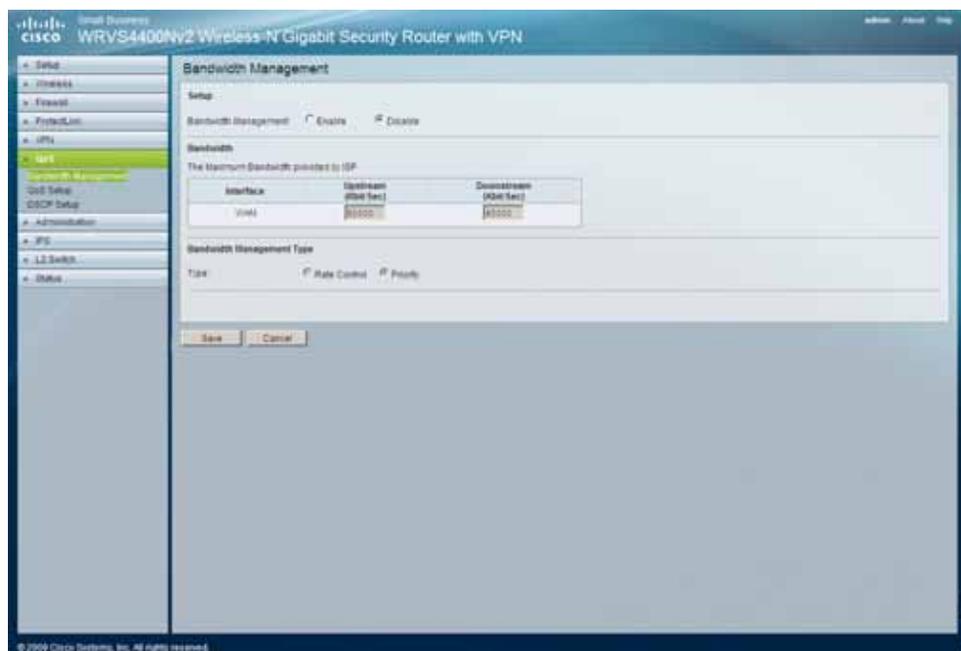
STEP 3 Click **Save**.

Configuring the QoS Settings

This section describes how to configure the QoS settings of the router:

- [Managing Bandwidth on page 119](#)
- [Configuring QoS on page 121](#)
- [Configuring DSCP on page 122](#)

QoS allows you to perform bandwidth management, by either rate control or priority. You can also configure the QoS Trust Mode and DSCP settings.



Managing Bandwidth

The QoS > Bandwidth Management window displays the settings for configuring bandwidth management for the router.

To configure the bandwidth management settings, follow these steps:

STEP 1 Click **QoS > Bandwidth Management**.

STEP 2 Configure bandwidth management settings:

- **Bandwidth**

Specify the maximum bandwidth provided by the ISP on the WAN interface, for both the upstream and downstream directions.

- **Type**

The desired type of bandwidth management, either **Rate Control** (default) or **Priority**.

Depending on your selection, the lower portion of the window displays either the Rate Control section or the Priority section.

- **Rate Control**

- **Service**—Select the service from the drop-down menu. If this menu does not contain the service you need, click **Service Management** to add the service.
- **IP**—Enter the IP address or IP range you need to control. The default is 0 which includes all internal IP addresses.
- **Direction**—Select **Upstream** for outbound traffic or **Downstream** for inbound traffic.
- **Min. Rate**—Enter the minimum rate for the guaranteed bandwidth.
- **Max. Rate**—Enter the maximum rate for the guaranteed bandwidth.
- **Enable**—Check this box to enable this rate control rule.
- **Add to list**—After a rule is set up, click this button to add it to the list. The list can contain a maximum of 15 entries.
- **Delete selected application**—Click this button to delete a rule from the list.

- **Priority**
 - **Service**—Select the service from the drop-down menu. If it does not contain the service you need, click **Service Management** to add the service.
 - **Direction**—Select **Upstream** for outbound traffic or **Downstream** for inbound traffic from the drop-down menu.
 - **Priority**—Select service priority (**High, Medium, Normal, or Low**). The default is **Medium**.
 - **Enable**—Check this box to enable this priority rule.
 - **Add to list**—After a rule is set up, click this button to add it to the list. The list can contain a maximum of 15 entries.
 - **Delete selected application**—Click this button to delete a rule from the list.

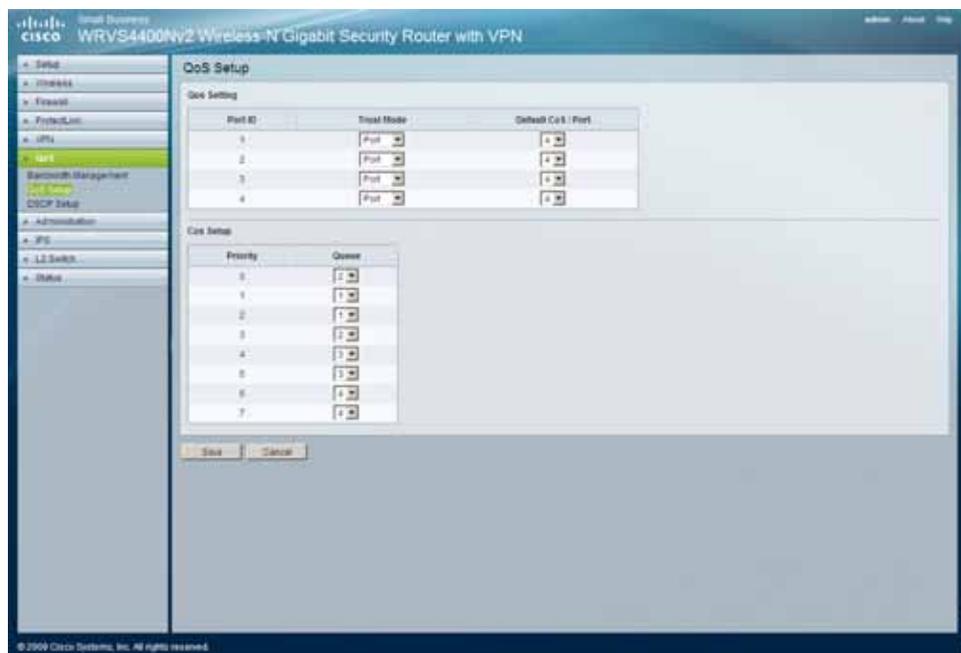
STEP 3 Click **Save**.

Configuring QoS

The QoS > QoS Setup window displays the settings needed for users to configure QoS Trust Mode for each LAN port.

To configure QoS setup window settings for the router, follow these steps:

- STEP 1** Click **QoS > QoS Setup**.
- STEP 2** Configure the QoS Setup settings:



- **Port ID**—The number of the LAN port.
- **Trust Mode**—Select either **Port**, **CoS**, or **DSCP**. The default is **Port**.
- **Default CoS/Port Priority**—If Trust Mode is set to **Port**, select the port priority from **1** to **4** from the drop-down menu. If Trust Mode is set to **CoS**, select the default CoS priority from **0** to **7** from the drop-down menu.
- **CoS Setup**
 - **Priority**—The CoS priority from **0** to **7**.
 - **Queue**—Select the traffic forwarding queue, **1** to **4**, to which the CoS priority is mapped.

STEP 3 Click **Save**.

Configuring DSCP

The QoS > DSCP Setup window displays the settings for configuring DSCP as the trust mode for QoS for each LAN port.

To configure DSCP setup settings, follow these steps:

STEP 1 Click **QoS > DSCP Setup**.

STEP 2 Configure the DSCP setup settings for the router:



- **DSCP**—The Differentiated Services Code Point value in the incoming packet.
- **Queue**—Select the traffic forwarding queue, 1 to 4, to which the DSCP priority is mapped.
- **Restore Defaults**—Click this button to restore the default DSCP values.

STEP 3 Click **Save**.

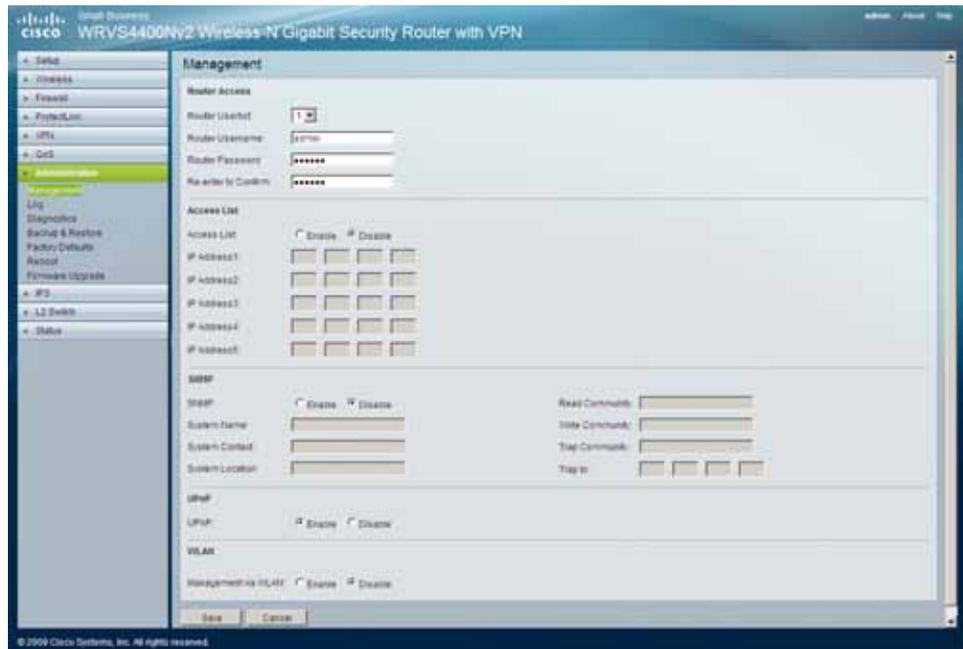
Configuring the Administration Settings

This administration window allows you to configure the administration settings of the router:

- [Configuring Management Settings on page 124](#)
- [Diagnosing Router Problems on page 129](#)
- [Backing Up and Restoring Configurations on page 131](#)
- [Restoring Factory Default Settings on page 132](#)
- [Rebooting the Router on page 133](#)
- [Upgrading the Router Firmware on page 134](#)

Configuring Management Settings

The Administration > Management window displays the settings for configuring the password and Simple Network Management Protocol (SNMP) for the router.



To configure management settings for the router, follow these steps:

STEP 1 Click **Administration > Management**.

STEP 2 Configure the management settings for the router:

- **Router Access**—This section configures the administrator user accounts to manage the wireless router through the web-based utility. Only the first user is created by default. Other accounts are not created by default so you can leave them alone.

NOTE Make sure to change the first user account username and password when you configure your router for the first time.

- **Router Userlist**—Select a user to configure from the drop-down menu.
- **Router Username**—Enter the user name.
- **Router Password**—Enter the password.
- **Re-enter to Confirm**—Retype the password in this field.
- **Access List**—This section specifies which source IP addresses can manage the device. Default is **Disable**.
 - **Access List**—Click **Enable** and add the IP addresses of the computers that can manage the router in the fields below. The default is **Disable**.
- **SNMP**—Configures the Simple Network Management Protocol settings. You can use management software to read or write information to the device.
 - **SNMP**—Select **Enable** if you wish to use SNMP. To use SNMP, you need SNMP software on your personal computer.
 - **System Name**—Enter a suitable name. This name is used to identify this device, and is displayed by your SNMP software.
 - **System Contact**—Enter contact information for the system.
 - **System Location**—Enter the location of the system.
 - **Read Community**—Enter the SNMP community name for SNMP “Get” commands.
 - **Write Community**—Enter the SNMP community name for SNMP “Set” commands.
 - **Trap Community**—Enter the SNMP community name for SNMP “Trap” commands.
 - **Trap To**—Enter the IP address of the SNMP manager where traps are sent. If desired, this may be left blank.
- **UPnP**—Universal Plug and Play allows Windows MP and XP to automatically configure the Internet gateway on the computer’s routing table. If you want to use UPnP, keep the default setting, **Enable**. Otherwise, select **Disable**.
- **Management via WLAN**—Control the access to the web-based utility from associated wireless clients. The default is **Disable**.

STEP 3 Click **Save**.

Configuring System Logs

The Administration > Log window displays the options for configuring the management of the router's system logs. The wireless router provides four categories of event logging (Firewall, VPN, System, and ACL). You can configure the router to send the event log to you through e-mail, upload the log to syslog server, or view the log locally on the router.



To configure System Logs for the router, follow these steps:

STEP 1 Click **Administration > Log**.

STEP 2 Configure the system logs for the router:

- **Log Setting**
 - **Log Level**—Select the log levels that the router should record.

Level	Severity Name	Description
7	LOG_DEBUG	Debug-level message
6	LOG_INFO	Information messages only
5	LOG_NOTICE	Normal but significant condition
4	LOG_WARNING	Warning conditions
3	LOG_ERR	Error conditions
2	LOG_CRIT	Critical conditions
1	LOG_ALERT	Immediate action needed
0	LOG_EMERG	System unusable

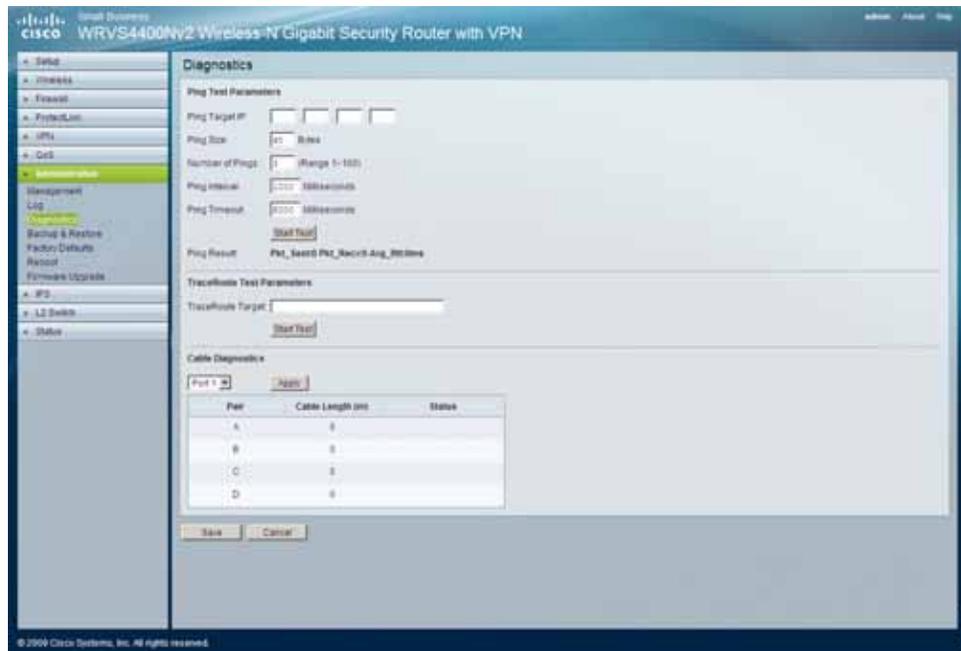
- **Outgoing Log**—Select **Enable** to cause all outgoing packets to be logged. You can then click **View Outgoing Table** to display information on the outgoing packets including Source IP, Destination IP, and Service/Port number.
- **Incoming Log**—Select **Enable** to cause all incoming packets to be logged. You can then click **View Incoming Table** to display information on incoming packets including Source IP, Destination IP, and Service/Port number.
- **Email Alerts**
 - **Email Alerts**—If enabled, an e-mail is sent when the number of DoS events exceeds the defined threshold or the total events number exceed 100. If enabled, you must provide the e-mail address information.

- **Denial of Service Thresholds**—Enter the number of DoS attacks that need to be detected (and blocked) by the software firewall before an e-mail alert is sent. The minimum value is 20, the maximum value is 100. Note that if IPS has been enabled, IPS blocks DoS attacks before they reach the firewall. In that case, check the **IPS Report** to see event details.
- **Log Queue Length**—The default is 50 entries (the router mails the log if there are more than 50 entries).
- **Log Time Threshold**—The default is 10 minutes (the router mails the log every 10 minutes).
- **SMTP Mail Server**—Enter the address (domain name) or IP address of the Simple Mail Transport Protocol server you use for outgoing e-mails.
- **Email Address for Alert Logs**—Enter the e-mail address the log is to be sent to.
- **Return Email Address**—The e-mail shows this address as the sender's address.
- **Enable SMTP Authentication**—If your SMTP server requires authentication, click this check box and enter the username and password in the fields below.
- **E-mail Log Now**—Press this button to cause the log to be e-mailed immediately.
- **Syslog**
 - **Enable Syslog**—Select **Enable** if you want to use this feature.
 - **Syslog Server**—Enter the IP address in the Syslog Server field when Enable Syslog is checked.
 - **Local Log**—Enable this if you want to see the log locally on the router.
 - **View Log button**—If Local Log is enabled, click **View Log** to view the event log on the router.

STEP 3 Click **Save**.

Diagnosing Router Problems

The Administration > Diagnostics window displays information for configuring test parameters for diagnosing the wireless router using ping tests, traceroute tests, and cable diagnostics.



To diagnose router problems, follow these steps:

STEP 1 Click **Administration > Diagnostics**.

STEP 2 Configure the parameters and carry out tests as necessary:

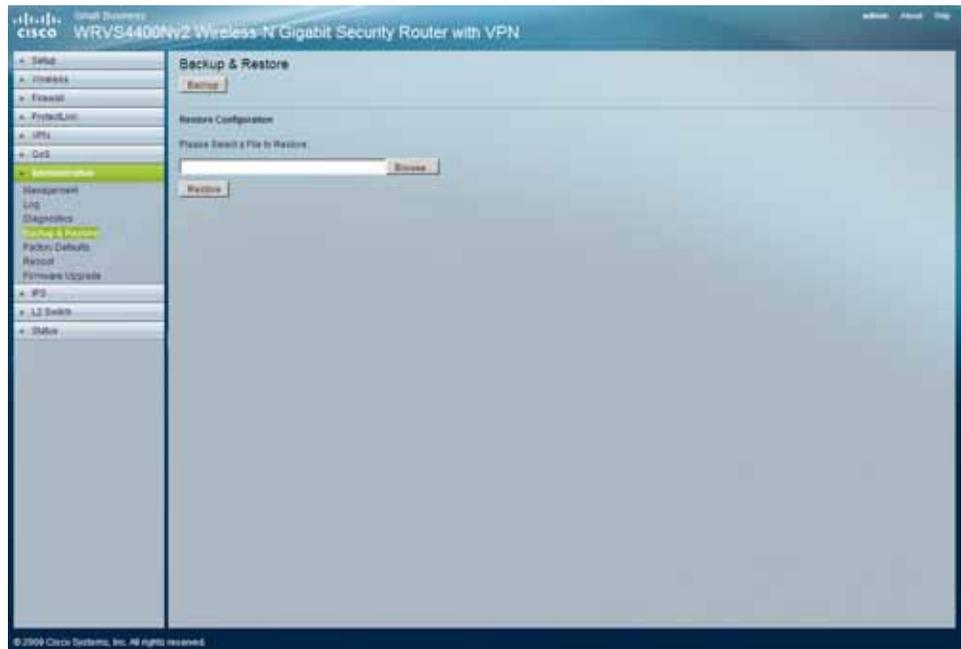
- **Ping Test Parameters**
 - **Ping Target IP**—Enter the IP address or URL that you want to ping.
 - **Ping Size**—Enter the size of the packet you want to use.
 - **Number of Pings**—Enter the number of times you wish to ping the target device.
 - **Ping Interval**—Enter the time period (in milliseconds) between each ping.

- **Ping Timeout**—Enter the desired time period (in milliseconds). If a response is not received within the defined ping period, the ping is considered to have failed.
- **Start Test**—Click this button to begin the test. A new window appears and display the test results. A summary of the test results appears at the bottom of this window.
- **Ping Result**. Displays the ping status results.
- **TraceRoute Test Parameters**
 - **TraceRoute Target**—Enter the IP address or host name to perform the traceroute testing.
 - **Start Test**—Click this button to begin the test. A new window appears and display the test results.
- **Cable Diagnostics**
 - **Port**—Select a port number from the drop-down menu.
 - **Apply**—Click this button to perform a cable diagnostics test.
 - **Pair**—Identifies a specific pair (A, B, C, or D) in the cable. Each cable consists of 8 pins (4 pairs).
 - **Cable Length**—Displays the length of the cable in meters.
 - **Status**—Displays the status of the pair.

STEP 3 Click **Save**.

Backing Up and Restoring Configurations

The Administration > Backup & Restore window lets you back up and restore router configuration information.



To back up or restore administration configurations, follow these steps:

STEP 1 Click **Administration > Backup & Restore**.

STEP 2 To back up router configuration, click **Backup**.

Clicking **Backup** downloads a copy of the current configuration and stores the file on your personal computer.

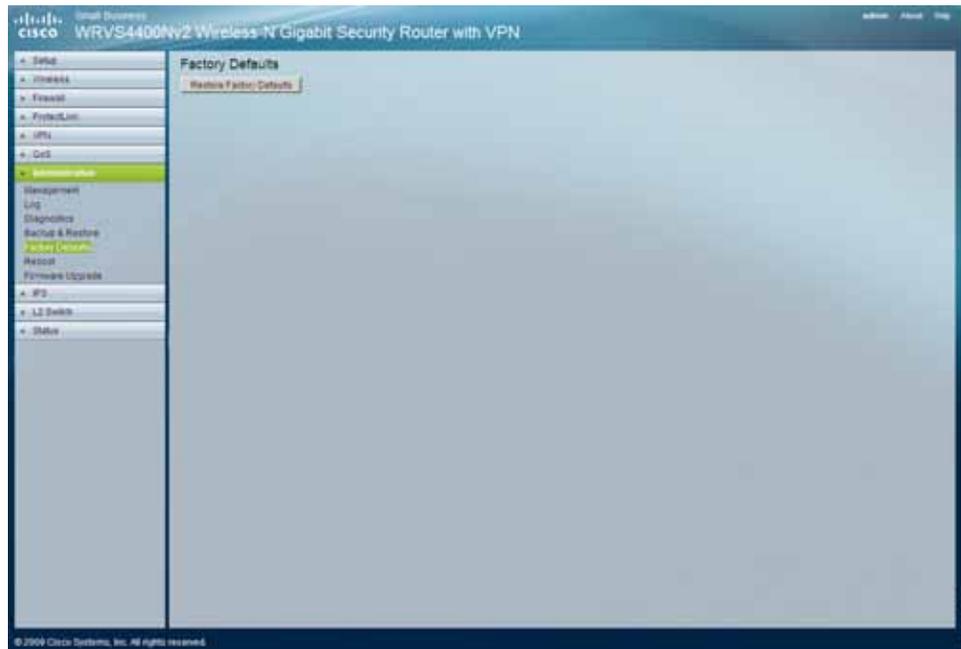
STEP 3 To restore the configuration your router or to configure a new router:

- a. Click **Browse** to select a previously saved configuration file from the Windows file system or manually enter the path to the file.
- b. Click **Restore** to start the restoration process.

This could be helpful if you want to use the same configuration on a new hardware or after resetting to the factory defaults.

Restoring Factory Default Settings

The Administration > Factory Defaults window provides a means of restoring the configuration of the router to its factory defaults.



To restore factory default settings for the router, follow these steps:

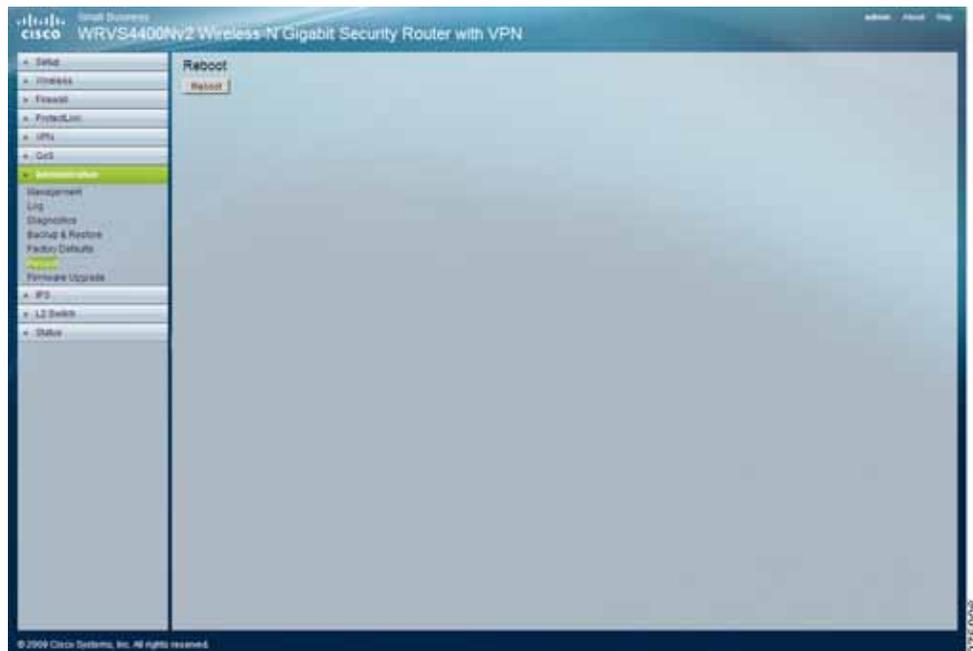
-
- STEP 1** Click **Administration > Factory Defaults**.
- STEP 2** Click **Restore Factory Defaults** to reset all configuration settings to their default values.
- If you click this button, all custom router settings are replaced by the default settings.
- STEP 3** When prompted, click **OK** to continue.
-

Rebooting the Router

The Administration > Reboot window provides means to reboot the router.

To reboot the router, follow these steps:

STEP 1 Click **Administration > Reboot**.



STEP 2 Click **Reboot** to reboot the router.

This operation does not cause the router to lose any of its stored settings.

Upgrading the Router Firmware

The Administration > Firmware Upgrade window allows you to upgrade router firmware from a downloaded file.



To upgrade firmware, download the latest firmware upgrade file for the product from www.cisco.com, extract the file to your computer, and perform these steps:

- STEP 1** Click **Browse** to locate the file firmware upgrade. Alternatively, enter the path to the file in the **File** field.
- STEP 2** Click **Start to Upgrade** and follow the on-screen instructions to upgrade your firmware.

Configuring IPS Settings

This section describes how to configure the Intrusion Prevention Systems for the router:

- [Configuring IPS on page 135](#)
- [Setting P2P/IM Policy on page 137](#)
- [Viewing Reports on page 139](#)
- [Viewing Protection Information on page 140](#)

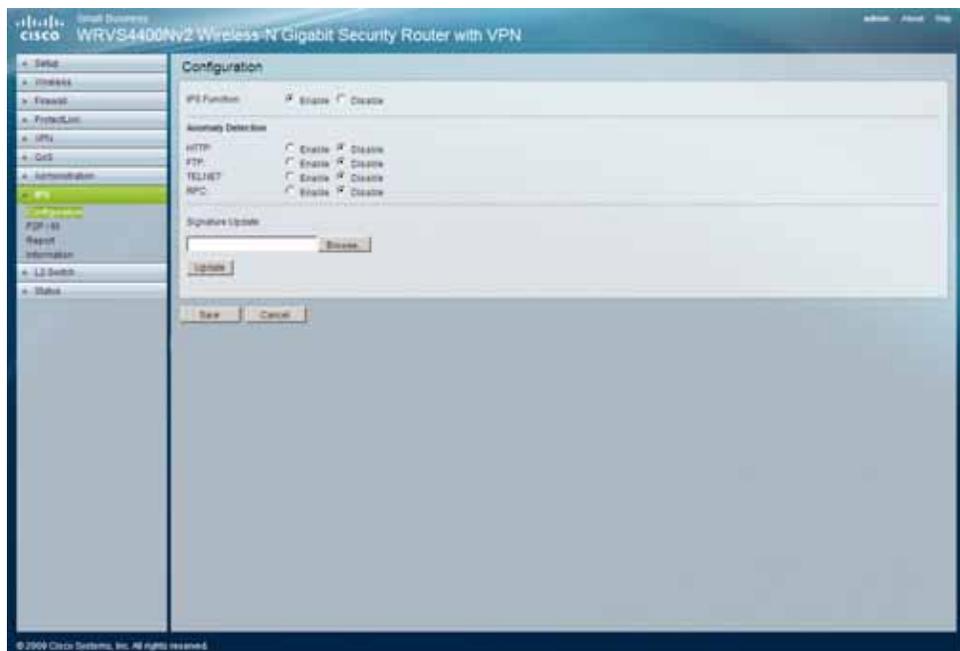
The router supports advanced IPS, an integral part of the self-defending strategy—IPS allows you to stay current on the latest threats so that malicious or damaging traffic is accurately identified, classified, and stopped in real time.

You can use IPS together with the firewall, IP-based ACL, and IPsec VPN to achieve maximum security.

The IPS is hardware-accelerated on this router.

Configuring IPS

The IPS > Configuration window displays general IPS settings.



To configure general IPS settings:

STEP 1 Click **IPS > Configuration**.

STEP 2 In the IPS Function field, click **Enable**.

STEP 3 In the Anomaly Detection section, configure the detection settings:

- **HTTP**—Web attacks use weaknesses on HTTP protocol to trigger the buffer overflow on Web servers. The default is **Disable**.
- **FTP**—FTP attacks use weaknesses on FTP protocol to generate illegal FTP commands to the FTP server. The default is **Disable**.
- **TELNET**—Telnet attacks use weakness on TELNET protocol to execute illegal commands on the TELNET server. The default is **Disable**.
- **RPC**—Remote Procedure Call allows attackers to issue illegal commands to be executed on RPC server. The default is **Disable**.

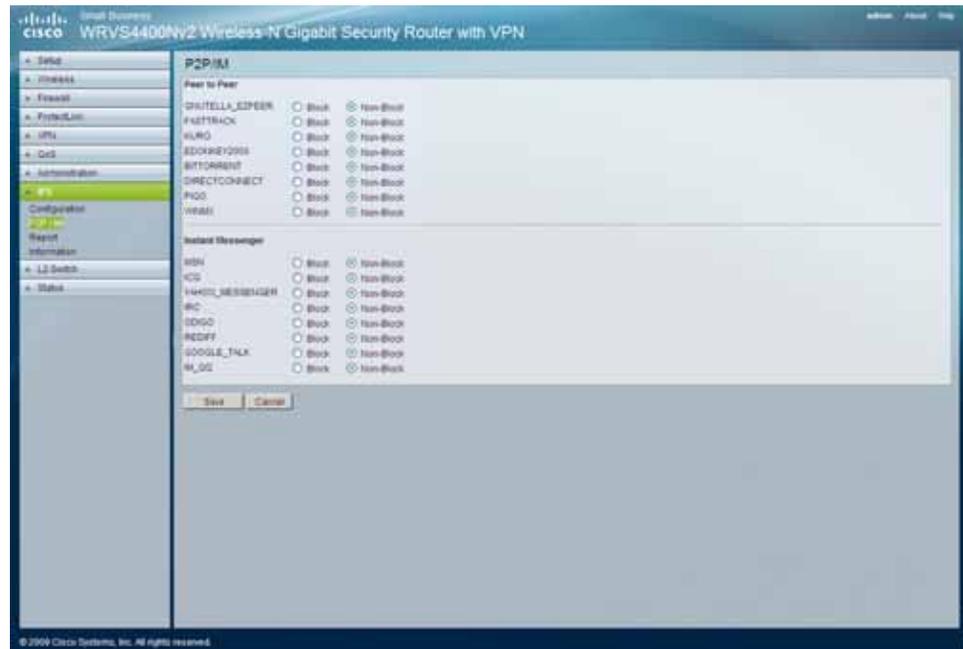
STEP 4 To protect your local network from the latest Internet threats, upgrade the IPS signature file regularly:

- a. Download the signature file from www.cisco.com to your personal computer.
- b. Click **Browse** to locate the signature file. Alternatively, enter the path to the file in the **Signature Update** field
- c. Click **Update**.

STEP 5 Click **Save**.

Setting P2P/IM Policy

The IPS > P2P/IM window allows you to set up policies on using P2P or IM software across the Internet.



To configure the P2P/IM policy settings, follow these steps:

STEP 1 Click **IPS > P2P/IM**.

STEP 2 Configure the IPS P2P/IM settings for the router:

- Peer to Peer

When users download files from the Internet by Peer-to-Peer (P2P) software, the WAN port bandwidth are occupied. Click **Block** to enable the blocking of the following P2P software applications. The default is **Non-Block**.

- GNUTELLA_EZPEER
- FASTTRACK
- KURO
- EDONKEY2000
- BITTORRENT

- DIRECTCONNECT
- PIGO
- WINMX
- Instant Messenger

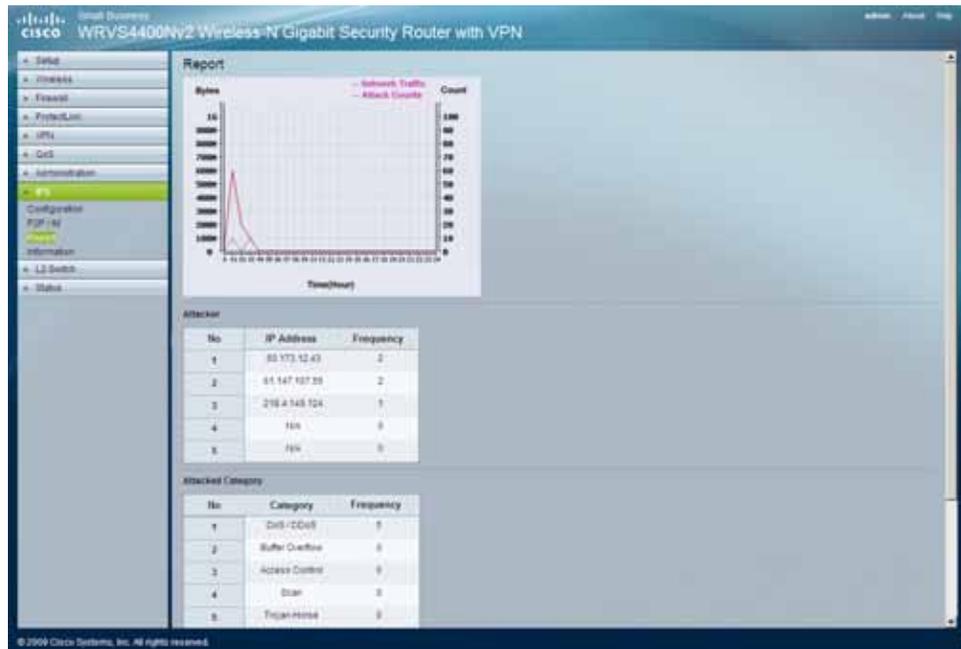
Users might use IM software to chat with friends or transfer files, which can hog the bandwidth. Click **Block** to enable the blocking to the following IM software applications. The default is **Non-Block**.

- MSN
- ICQ
- YAHOO_MESSENGER
- IRC
- ODIGO
- REDIFF
- GOOGLE TALK
- IM_QQ

STEP 3 Click **Save**.

Viewing Reports

The IPS > Report window provides the network history status, including network traffic and attack counts, through diagram and tables.



To view IPS reports follow these steps:

STEP 1 Click IPS > Report.

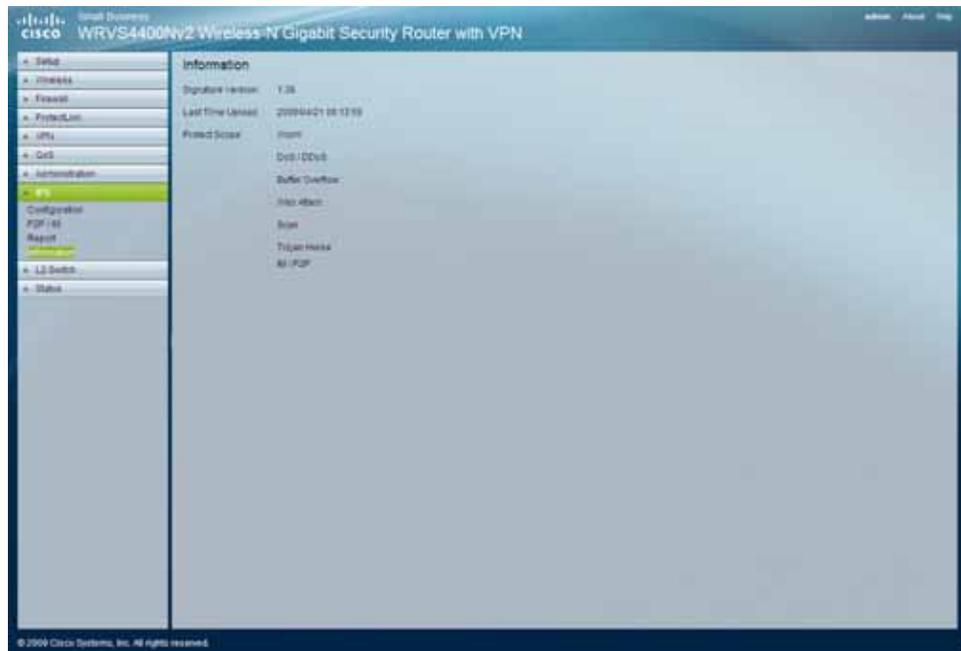
The IPS > Report window displays the following:

- **Report Diagram**—A twenty-four hour diagram displaying network traffic and attacks.
- **Attacker**—Displays the IP address of attackers and the frequency (number of times) of the attacks in a table.
- **Attacked Category**—Displays the category (type) of attack and the frequency (number of times) of the attacks in a table.

STEP 2 Click the View Log button to view the log.

Viewing Protection Information

The Administration > Information window displays information about the types of malicious threat that the router is protected against through its IPS features, the version of the signature pattern files and when the router was last updated.



To view protection information, follow these steps:

STEP 1 Click **Administration > Information**.

STEP 2 View the administration information.

- **Signature Version**—Displays the version of the signature patterns file loaded in the router that protects against malicious threats.
- **Last Time Upload**—Displays the time when the signature patterns file in the router was last updated.
- **Protect Scope**—Displays a list of the categories of attacks that the IPS feature in the router protects against. These attacks includes DoS/DDoS, Buffer Overflow, Web Attack, Scan, Trojan Horse, and IM / P2P.

Configuring the L2 Switch Settings

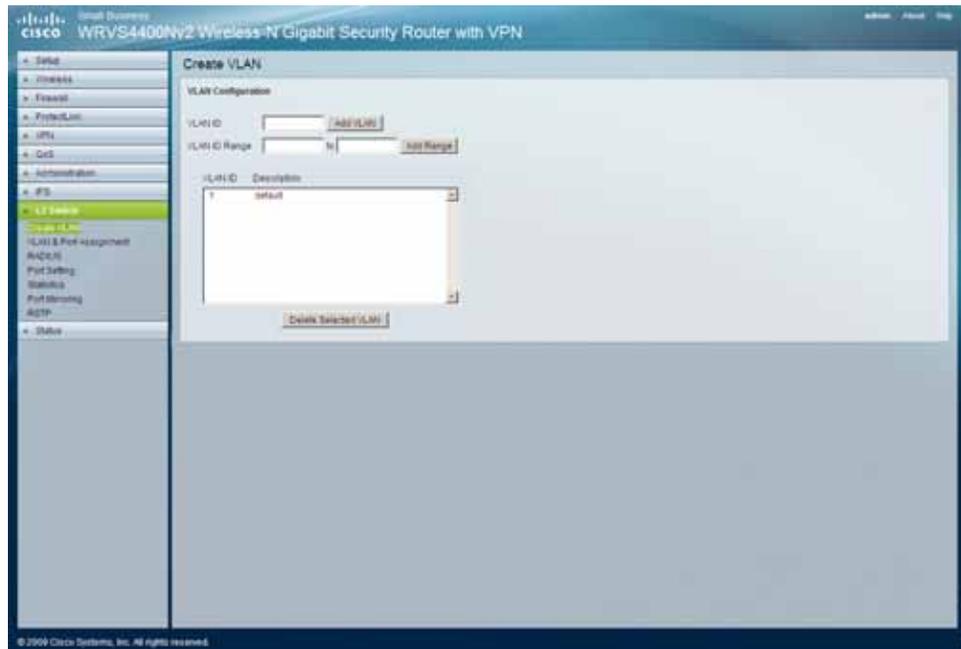
This section describes how to configure the Layer 2 Switch settings of the router:

- [Configuring Virtual LANs \(VLANs\) on page 142](#)
- [Configuring VLAN Membership and Port Assignment on page 144](#)
- [Configuring RADIUS Mode on page 146](#)
- [Configuring Port Settings on page 147](#)
- [Viewing Statistics Overview on page 149](#)
- [Mirroring Ports on page 150](#)
- [Configuring RSTP on page 151](#)

The Layer 2 Switch window provides configurations to the layer 2 switching features on the four Ethernet LAN ports of the router. They include VLAN, port configuration, cable diagnostics, and RADIUS authentication.

Configuring Virtual LANs (VLANs)

The L2 Switch > VLAN window displays the settings for creating and adding a VLAN to the router.



VLANs are logical subgroups of a LAN created via software rather than defining a hardware solution. VLANs combine user stations and network devices into a single domain regardless of the physical LAN segment to which they are attached. VLANs allow network traffic to flow more efficiently within subgroups.

VLANs managed through software reduce the amount of time in which network changes are implemented.

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

VLANs function at layer 2. Since VLANs isolate traffic within the VLAN, a Layer 3 router is needed to allow traffic flow between VLANs. Layer 3 routers identify segments and coordinate with VLANs.

VLANs are broadcast and multicast domains. Broadcast and multicast traffic is transmitted only in the VLAN in which the traffic is generated.

The WRVS4400N router supports up to 4 VLANs, including the default VLAN.

To configure Virtual LANS for the router, follow these steps:

STEP 1 Click **L2 Switch > Create VLAN**.

STEP 2 Configure Virtual LANS for the router:

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

STEP 3 Click **Save**.

Configuring VLAN Membership and Port Assignment

The L2 Switch > VLAN & Port Assignment window displays the port settings and VLAN membership settings for configuring VLANs for the router.



To configure VLAN membership and port assignments for the router, follow these steps:

STEP 1 Click L2 Switch > VLAN & Port Assignment.

STEP 2 Configure port settings for the router.

The Port Settings section displays port-specific settings regarding the use of VLAN and has nothing to do with individual VLANs.

This section lets you specify the mode for each port. The Acceptable Ingress Frame Type and PVID options are for the General port mode only.

- **Port Mode**—Select one of these modes:
 - **Access**—All frames are untagged coming in or going out of the switch port. Wireless port can be set to this mode only.
 - **Trunk**—All frames are tagged coming in or going out of the switch except for VLAN ID 1 (called native VLAN or default VLAN in Cisco)

- **General**—All frames can be tagged or untagged coming in to the switch. If untagged, the default PVID applies to the packet. Only the General mode users can choose the Acceptable Ingress Frame Type and PVID options.

NOTE The Acceptable Ingress Frame Type and PVID options cannot be supported on the Vitesse 7385 switch chipset

- **Acceptable Ingress Frame Type**
 - **All Frames**—All the incoming frames are acceptable.
 - **Tagged Only**—Only tagged incoming frames are acceptable.
- **Ingress Filtering**—If enabled, checks the VLAN ID on the incoming packet. If the port is a member of this VLAN, accepts the frame. Otherwise, drops it. If not enabled, all frames are accepted.
- **PVID**—The VLAN ID of the default (untagged) VLAN.

STEP 3 Configure VLAN settings for the router.

- **VLAN**— Select a VLAN ID to be configured.
- **VLAN Description**—Display only, VLAN description to help you identify this VLAN
- **Tagged**— Egress frames from this port are tagged for this VLAN.
- **Untagged**—Egress frames from this port are untagged for this VLAN.
- **Excluded**—The port does not participate in this VLAN at all.

For the Access port mode, the available options are either untagged or excluded. You can set a wireless port to one of these two modes for each VLAN. Only one of the VLAN IDs can be selected (untagged).

For the Trunk port mode, the options are tagged or excluded for all VLAN IDs except VLAN 1. VLAN 1 must be untagged.

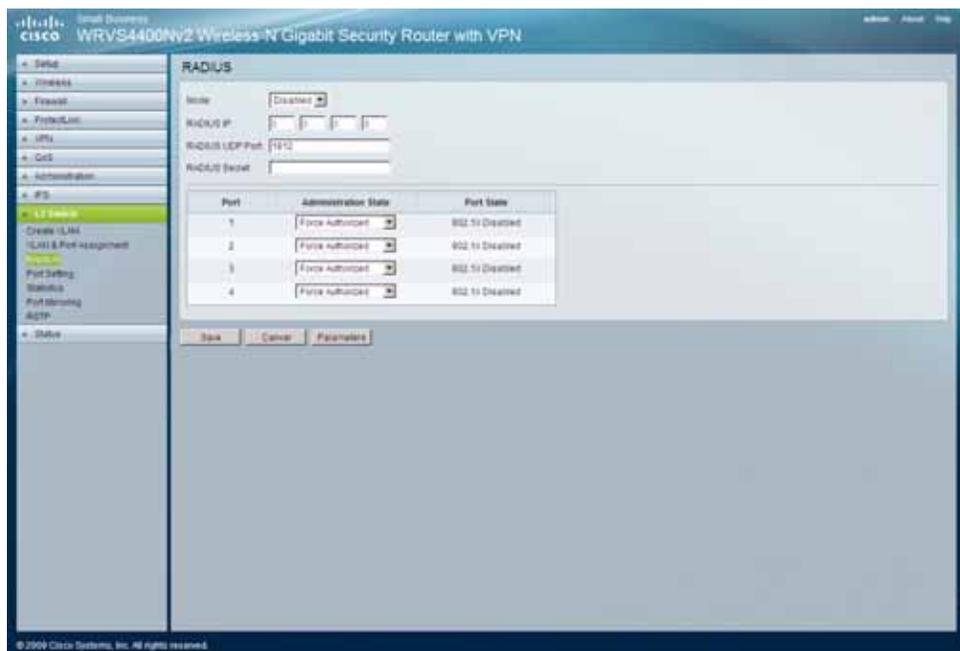
For the General port mode, the options are tagged or untagged for PVID; tagged or excluded for all other VLAN IDs.

STEP 4 To view a summary of the VLAN/Port assignments, see the table in the VLAN/Port Assignment Summary section of this window.

Configuring RADIUS Mode

The L2 Switch > RADIUS window displays the settings for configuring and enabling the RADIUS mode for the router.

The RADIUS mode provides authentication on devices connecting to the LAN ports. This mode requires the installation of a RADIUS server on your local network.



To configure the RADIUS mode for the server, follow these steps:

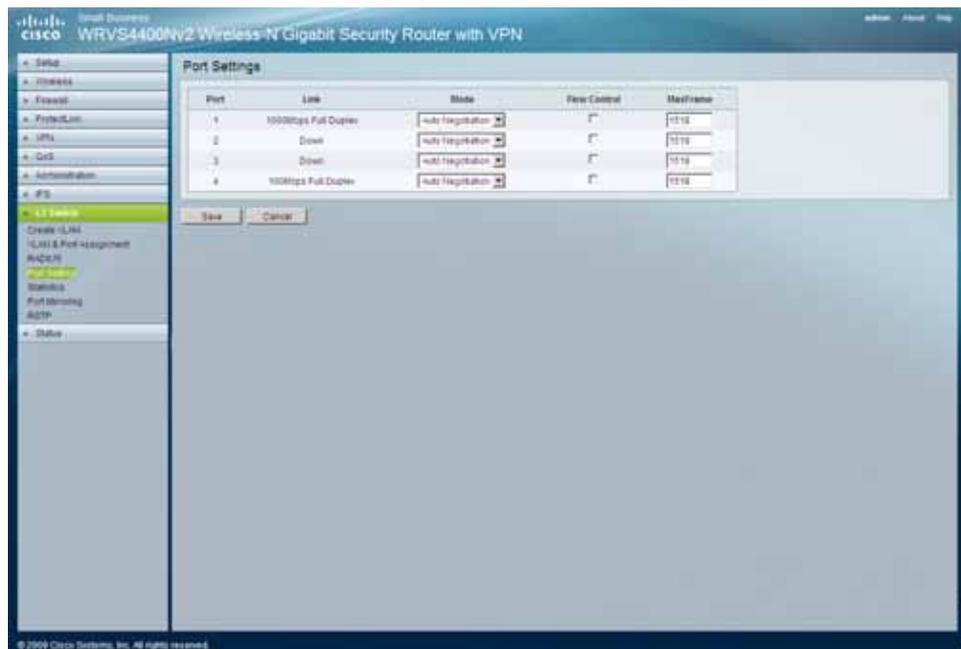
- STEP 1** Click L2 Switch > RADIUS.
- STEP 2** Configure the RADIUS mode:
 - **Mode**—Select **Enabled** or **Disabled** from the drop-down menu.
 - **RADIUS IP**—Enter the RADIUS server's IP address.
 - **RADIUS UDP Port**—Enter the UDP port used to verify the RADIUS server authentication.
 - **RADIUS Secret**—Enter the key string used for authenticating and encrypting all RADIUS communication between the router and the RADIUS server. This key must match the RADIUS server's configuration.

- **Administration State**—Select one of the following options from the drop-down menu:
 - **Auto**—Controlled port state is set by the **RADIUS** mode.
 - **Force Authorized**—Controlled port state is set to **Force-Authorized** (forward traffic). All connections can be made. This is the default value.
 - **Force Unauthorized**—Controlled port state is set to **Force-Unauthorized** (discard traffic). All connections are blocked.

STEP 3 Click **Save**.

Configuring Port Settings

The L2 Switch > Port Settings window displays the settings for configuring the LAN ports of the router.



To configure L2 switch port settings for the router, follow these steps:

STEP 1 Click **L2 Switch > Port Settings**.

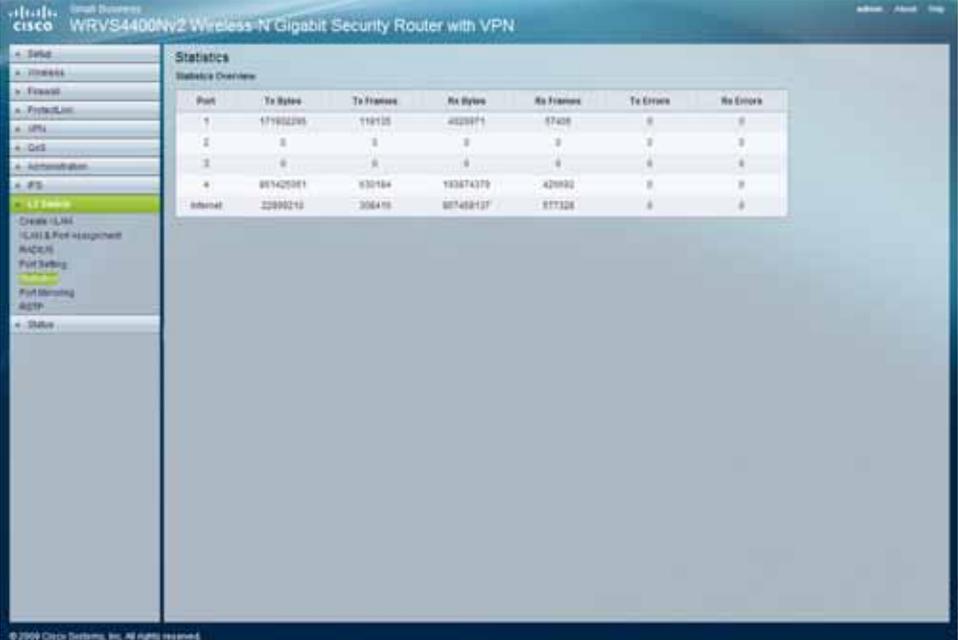
STEP 2 Configure L2 switch port settings for the router:

- **Port**—Specifies the number of the four LAN ports.
- **Link**—Displays the port duplex mode (Full or Half) and speed (10/100/1000 Mbps). **Full** indicates that the interface supports transmission between the device and its link partner in both directions simultaneously. **Half** indicates that the interface supports transmission between the device and the client in only one direction at a time. **Down** indicates that the link is down.
- **Mode**—Specifies the port duplex mode (Full or Half) and speed (10/100/1000 Mbps). **Auto Negotiation** is a protocol between two link partners that enables a port to advertise its transmission rate, duplex mode, and flow control abilities to its partner. The default value is **Auto Negotiation**.
- **Flow Control**—Configures the flow control setting on the port. Select the check box to enable flow control. The default is disabled.
- **MaxFrame**—Configures the maximum Ethernet frame size sent or received on the port. The default and maximum value is **1518**.

STEP 3 Click **Save**.

Viewing Statistics Overview

The L2 Switch > Statistics Overview window displays port statistics summary.



The screenshot shows the Cisco WRVS4400Nv2 Web Management Interface. The left sidebar contains a navigation menu with the following items: Home, Wireless, Firewall, Protection, LAN, WAN, Administration, IPS, L2 Switch, Create VLAN, VLAN & Port assignment, MACs, Port Setting, Port Mirroring, and Status. The 'L2 Switch' item is selected and highlighted in green. The main content area displays the 'Statistics Overview' window, which contains a table with the following data:

Port	Tx Bytes	Tx Frames	Rx Bytes	Rx Frames	Tx Errors	Rx Errors
1	17192295	119125	4523971	57428	0	0
2	0	0	0	0	0	0
3	0	0	0	0	0	0
4	95142081	530164	193874379	429892	0	0
Internet	2299212	30649	907482127	811328	0	0

To view L2 switch statistics summary, follow these steps:

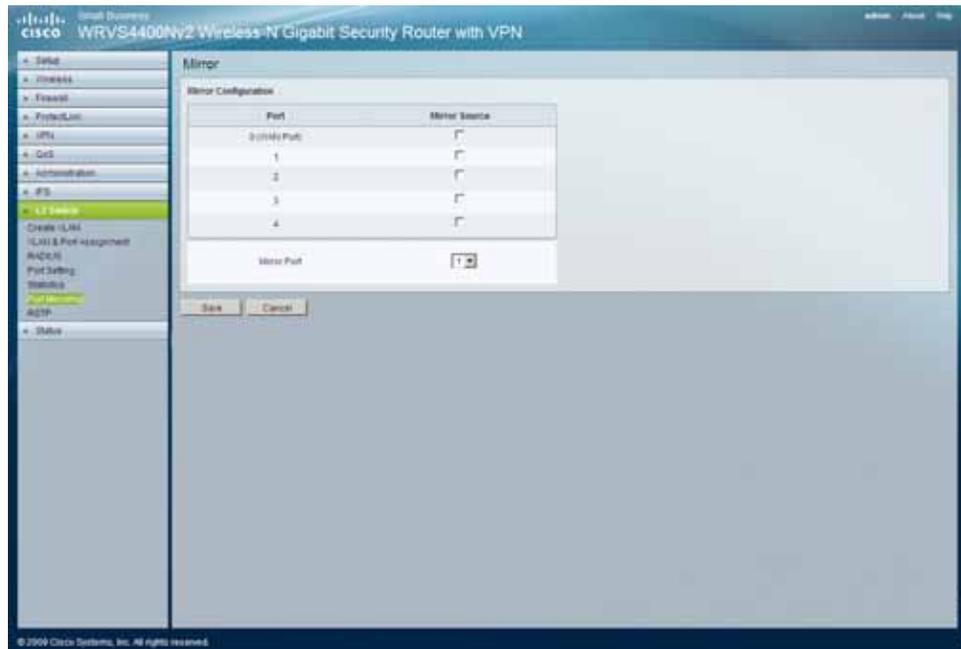
STEP 1 Click **L2 Switch > Statistics Overview**.

STEP 2 View the L2 switch statistics. An explanation of the statistics provided is given below:

- **Tx Bytes**—Displays the number of bytes transmitted from the selected port.
- **Tx Frames**—Displays the number of frames transmitted from the selected port.
- **Rx Bytes**—Displays the number of bytes received on the selected port.
- **Rx Frames**—Displays the number of frames received on the selected port.
- **Tx Errors**—Displays the number of error packets transmitted from the selected port.
- **Rx Errors**—Displays the number of error packets received from the selected port.

Mirroring Ports

The L2 Switch > Port Mirroring window displays the settings for configuring port mirroring for the router.



To configure L2 switch port mirroring, follow these steps:

STEP 1 Click L2 Switch > Port Mirroring.

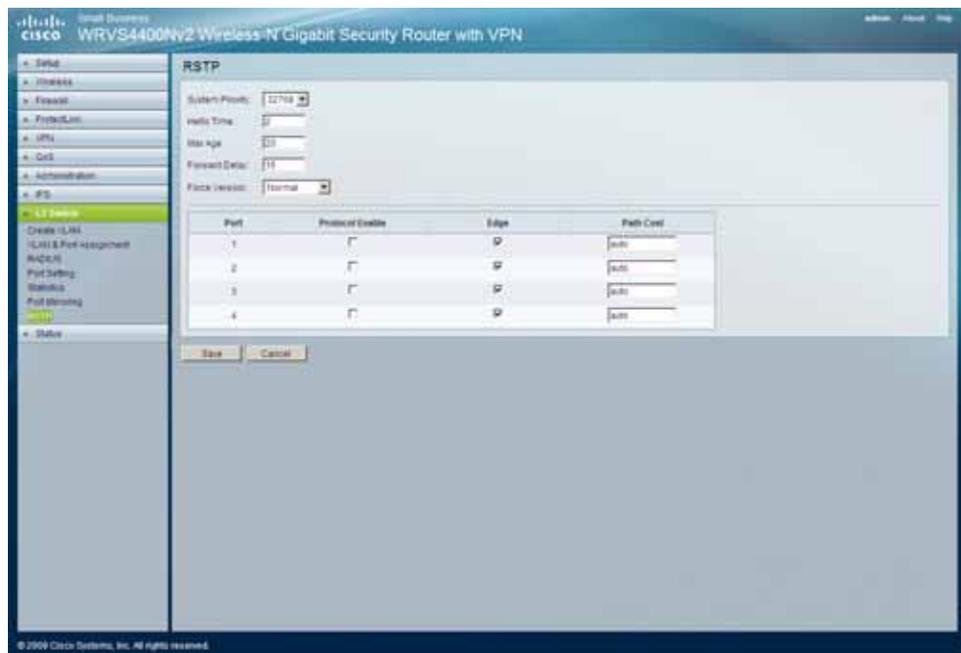
STEP 2 Configure the L2 switch port mirroring settings for the router:

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

Configuring RSTP

The L2 Switch > RSTP window displays the settings for configuring Rapid Spanning Tree Protocol (RSTP) for the router.

The RSTP protocol prevents loops in the network and dynamically reconfigures the physical links in a switch that should forward frames.



To configure RSTP for the router, follow these steps:

STEP 1 Click L2 Switch > RSTP.

STEP 2 Configure the L2 switch RSTP settings:

- **System Priority**—Enter the system priority from 0 to 61440 in increments of 4096. Valid values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 40960, 45056, 49152, 53248, 57344, and 61440. The lower the system priority, the more likely the router is to become the root in the spanning tree. The default is 32768.
- **Hello Time**—Enter a number from 1 to 10. The default is 2.
- **Max Age**—Enter a number from 6 to 40. The default is 20.
- **Forward Delay**—Enter a number from 4 to 30. The default is 15.

- **Force Version**—The default protocol version to use. Select **Normal** (uses RSTP) or **Compatible** (compatible with old STP). The default is **Normal**.
- **Protocol Enable**—Check this box to enable RSTP on the associated port. The default is unchecked (RSTP disabled).
- **Edge**—Check this box to specify that the associated port is an edge port (end station). Uncheck the box to specify that the associated port is a link (bridge) to another STP device. The default is checked (edge port).
- **Path Cost**—The RSTP path cost for the designated ports. Enter a number from 1 to 200000000, or **auto** (autogenerated path cost). The default is **auto**.

Viewing Status

The Status window allows you to view the current status on this router:

- [Viewing WAN/Gateway Status on page 153](#)
- [Viewing Local Network Status on page 155](#)
- [Viewing Wireless LAN Status on page 157](#)
- [Viewing System Performance on page 158](#)

- **Internet Connection**
 - **Connection Mode**—Displays the Internet connection type setting on WAN port.
 - **Interface**—Displays the WAN port Interface status (Up or Down).
 - **IP Address**—Displays the WAN port IP address.
 - **Subnet Mask**—Displays the WAN port IP subnet mask.
 - **Default Gateway**—Displays the default router to reach Internet or other networks from the WAN port.
 - **DNS**—The DNS (Domain Name System) IP addresses currently used by the router.
 - **DHCP Release** button—Click this button to release IP address on WAN port if using DHCP.
 - **DHCP Renew** button—Click this button to renew IP address on the WAN port if using DHCP.

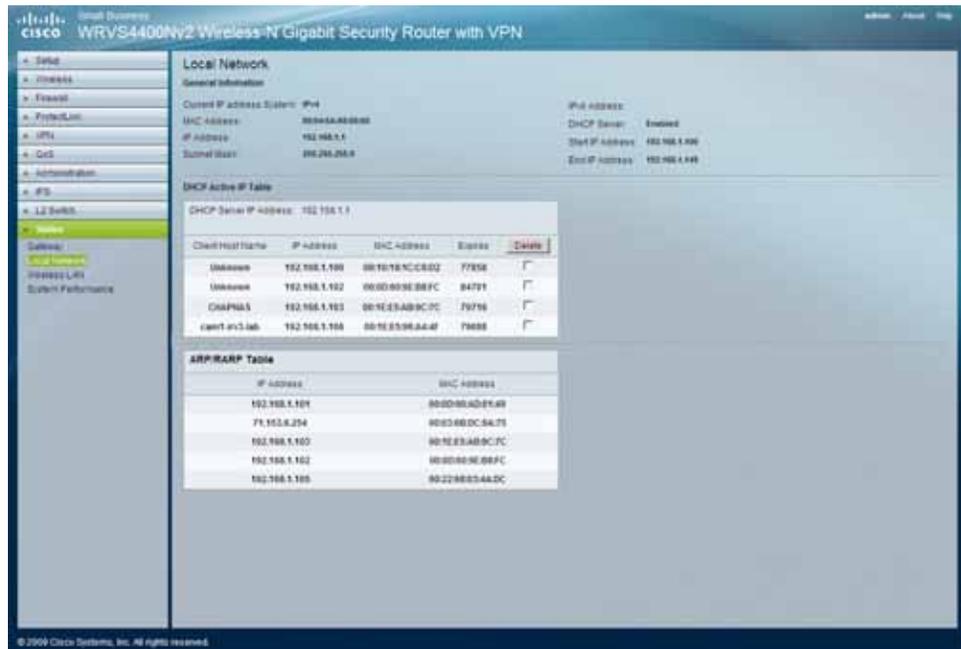
- **Contrack State**

- **IP Contrack**—Click this button to display the IP Contrack window.

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

Viewing Local Network Status

The Status > Local Network window displays the LAN status of the router, providing some basic information on the LAN ports of this router.



To view local network status, follow these steps:

STEP 1 Click **Status > Local Network**.

STEP 2 View the local network status.

- **Current IP address System**—Displays the IP versions configured on the LAN side.
- **MAC Address**—Displays the LAN port MAC address. All four LAN ports share the same MAC address.
- **IP Address**—Displays the LAN port IPv4 address. All four LAN ports share the same MAC address.
- **Subnet Mask**—Displays the LAN port IPv4 subnet mask.
- **IPv6 Address**—Displays the LAN port IPv6 IP address, if IPv6 is enabled.
- **DHCP Server**—Displays the status of the router's DHCP server.

-
- **Start IP Address**—Displays the beginning of the range of IP addresses used by the DHCP Server.
 - **End IP Address**—Displays the end of the range of IP addresses used by the DHCP Server.
 - **DHCP Client Table button**—Click to open the DHCP Client Table window, which shows you which personal computers have been assigned an IP address from the router's DHCP server. You see a list of DHCP clients (personal computers and other network devices) with the following information: Client Host Name, IP address, MAC address, and the length of time (in second) before its assigned IP address expires.
 - **ARP/RARP Table button**—Click to open the ARP/RARP Table window, which shows you the ARP/RARP Table on the router. The ARP/RARP Table provides IP address to MAC address mapping. On the ARP/RARP Table window, you see a list of address mapping between IP (layer 3) and MAC (layer 2).
-

Viewing Wireless LAN Status

The Status > Wireless LAN window displays the status of the wireless LAN of the router, providing some basic information on the Wireless LAN.



To view the wireless LAN status for the router, follow these steps:

STEP 1 Click **Status > Wireless LAN**.

STEP 2 View the wireless LAN status.

- **Wireless IP Address**—The IP address assigned to the wireless interface of this router.
- **MAC Address**—Displays the MAC address on the Wireless LAN interface.
- **Network Mode**—Displays the Wireless network operating mode (for example, B/G/N-Mixed).
- **Wireless SSID**—Displays the Wireless network name.
- **Channel Bandwidth**—Displays the wireless channel bandwidth setting.
- **Wireless Channel**—Displays the radio channel number used.

- **Security**—Displays the Wireless Security mode.
- **SSID Broadcast**—Displays the setting on SSID Broadcast.

Viewing System Performance

The Status > System Performance window displays system performance of the router, such as data packet statistics on the LAN switch and Wireless LAN of the router.

The screenshot shows the 'System Performance' window for the WRVS4400Nv2 router. The window title is 'All LAN ports/WLAN'. It contains a table with the following data:

Item	All LAN ports	Wireless LAN
Packets Received	22485	1284505
Packets Sent	30267	6840
Bytes Received	2260271	268894237
Bytes Sent	87620493	322228
Error Packets Received	0	0
Dropped Packets Received	0	0

To view the system performance of the router, follow these steps:

- STEP 1** Click **Status > System Performance**.
- STEP 2** View the system performance status.
 - **Packets Received**—Shows the number of packets received.
 - **Packets Sent**—Shows the number of packets sent.
 - **Bytes Received**—Shows the number of bytes received.
 - **Bytes Sent**—Shows the number of bytes sent.

- **Error Packets Received**—Shows the number of error packets received.
- **Drop Received Packets**—Shows the number of packets being dropped after they were received.

The All LAN ports column shows the aggregate traffic statistics from all four LAN ports.

Using the VPN Setup Wizard

This chapter describes using the VPN Setup Wizard and includes these sections:

- [VPN Setup Wizard, page 160](#)
- [Before You Begin, page 160](#)
- [Running the VPN Router Software Wizard, page 161](#)

VPN Setup Wizard

Now you can configure a gateway-to-gateway VPN tunnel between two VPN routers in a fast and efficient way by using the VPN Setup Wizard. The VPN Setup Wizard works with users running Microsoft Windows 2000, XP, and Vista. This document describes how to run the VPN Setup Wizard.

Before You Begin

The VPN Setup Wizard works with the following routers:

- Cisco RVS4000 4-Port Gigabit Security Router with VPN
- Cisco WRVS4400N v1.1 Wireless-N 4-Port Gigabit Security Router with VPN
- Cisco WRVS4400N v2 Wireless-N 4-Port Gigabit Security Router with VPN

Use the following instructions to configure required data using the Web Administrator Interface. For instructions on the Web Administrator Interface, see the Administration Guide for your router.

-
- STEP 1** Click **Firewall > Basic Settings**.
- STEP 2** Enable Remote Management and enter **8080** in the Port field. Please note that you cannot enter any other value if you want to use the VPN Wizard. Also, make sure that **HTTPS** has been selected.
- STEP 3** Click **Save Settings**.
- STEP 4** Click **VPN > Summary** and make sure the **Tunnel(s) available** are not zero.
- STEP 5** Ensure that the LAN IP addresses of routers with VPN are in different subnets in order for the VPN connection to work.
-



NOTE The VPN Setup Wizard assumes that no firewall/NAT device sits in front of the VPN router.

Running the VPN Router Software Wizard

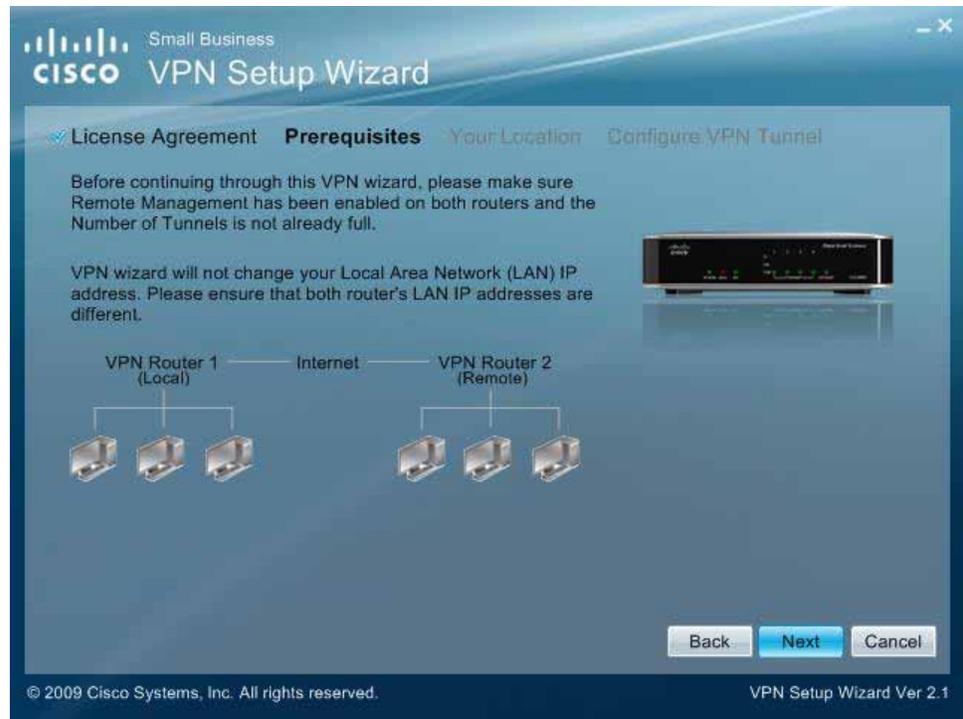
-
- STEP 1** Access the VPN Setup Wizard in one of two ways:
- If you have an RVS4000, WRVS4400N v1.1, or WRVS4400N v2 Installation CD-ROM, insert it into your CD-ROM drive.
 - Download the VPN Setup Wizard from the Cisco Support site for your router.
- STEP 2** Go to the Start menu and click **Run**. In the field provided, enter
- D:\VPN Setup Wizard.exe
- STEP 3** The Welcome window appears. Click the **Click Here to Start** button.

Welcome Window



- STEP 4** An informational window discussing the VPN Wizard appears. When you are ready, click **Next** to proceed.

Informational Window

**STEP 5** The Choose a way to build VPN window appears.

- If your PC is local to one of the two routers, choose **Build VPN connection from Local LAN port of one router**, click **Next**, and continue with these instructions.
- If your PC is remote to the routers, choose **Build VPN connection from Internet remotely**, and see the ["Building Your VPN Connection Remotely," on page 170](#) for instructions on this type of installation.

Build VPN Connection Remotely



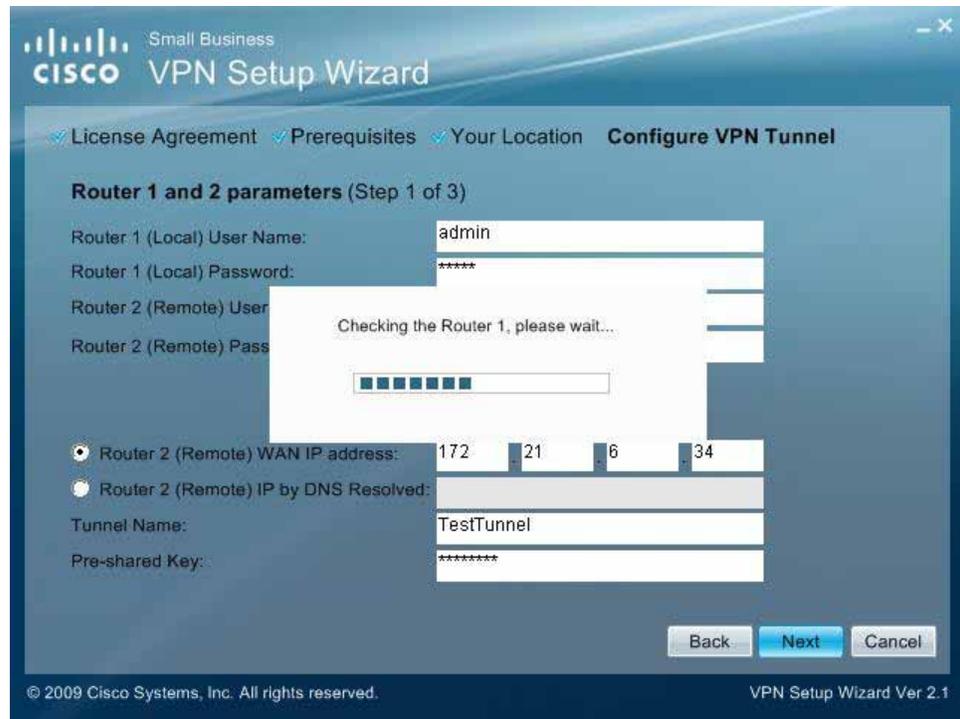
STEP 6 If you picked **Build VPN connection from Local LAN port of one router**, enter the required data in the **Configure VPN Tunnel** window and click **Next** to continue.

Configure VPN Tunnel

- **Router 1 User Name:** Enter the user name of the Router 1.
- **Router 1 Password:** Enter the password of the Router 1.
- **Router 2 User Name:** Enter the user name of the Router 2.
- **Router 2 Password:** Enter the password of the Router 2.
- **Tunnel Name:** Enter a name for this tunnel.
- **Pre-shared Key:** IKE uses the Pre-shared Key field to authenticate the remote IKE peer. Both character and hexadecimal values are acceptable in this field; e.g., “My_@123” or “0x4d795f40313233”. Note that both sides must use the same Pre-shared Key.
- **Router 2 WAN IP address:** Enter the WAN IP address of Router 2.
- **Router 2 IP by DNS Resolved:** Enter the DDNS Domain Name of Router 2 if it does not have a static IP address for its internet connection.

STEP 7 The router configuration is checked.

Check Router Configuration



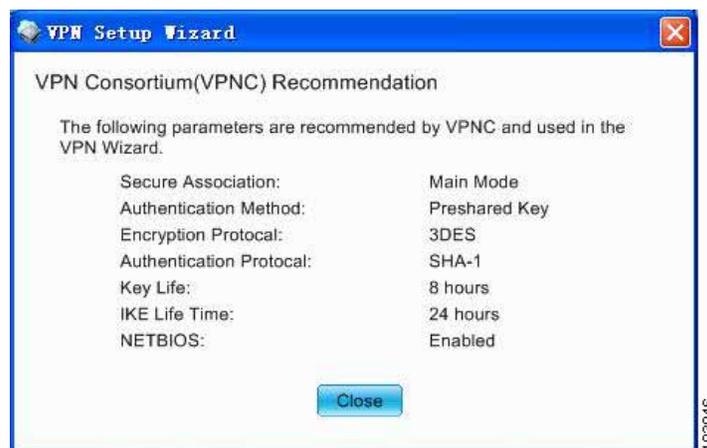
STEP 8 The Summary window appears. Use the Click box to view the VPNC Summary window.

Summary Window



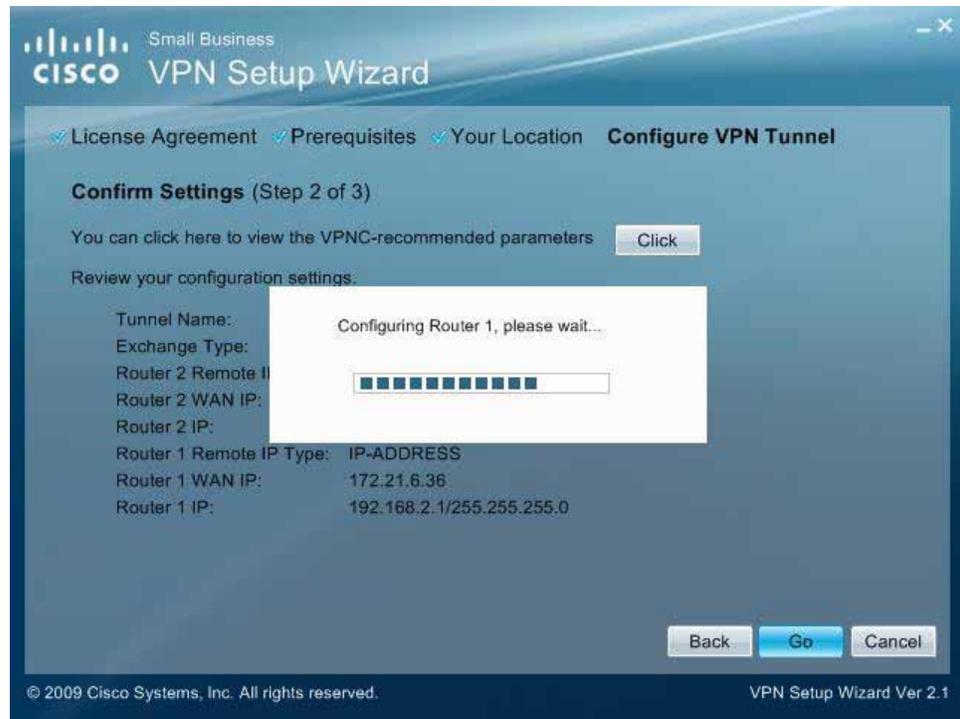
- STEP 9** The VPNC Summary window appears showing the settings that were made to industry standards. Click Close when you are ready to continue.

VPNC Summary Window



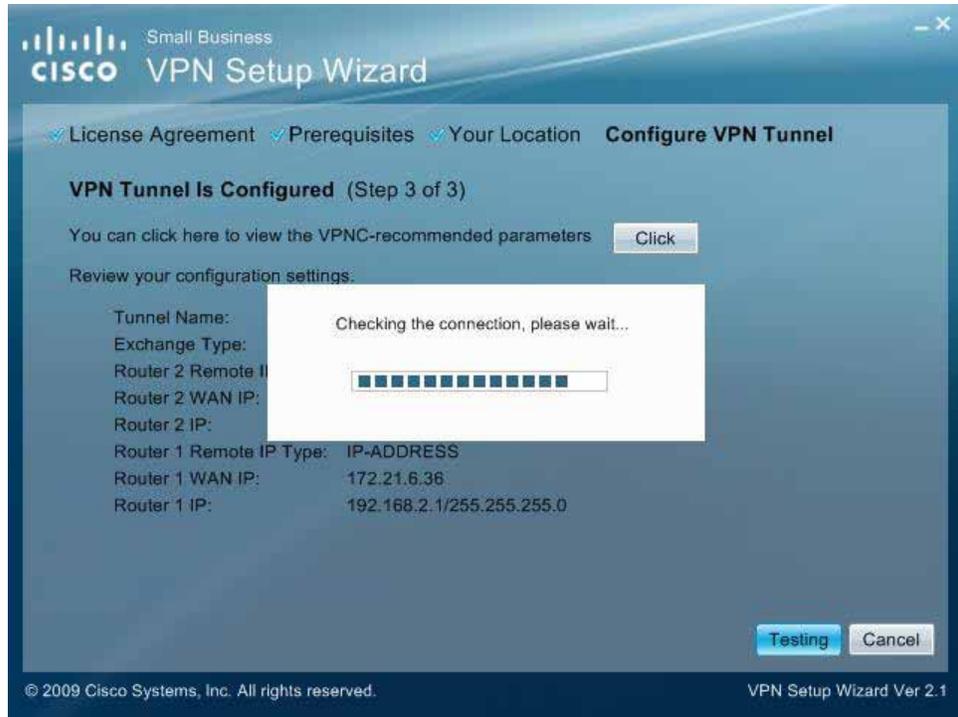
- STEP 10** In the Summary window, if all your entries appear correct, click Go. Otherwise click Back to go back and make any corrections.

Configure the Router



STEP 11 Click **Testing** to make sure the connection is successfully established.

Test the Connection



STEP 12 When testing is done, click **Exit** to end the Wizard.

Exit the Wizard



Congratulations! Setup is now complete. You may now log into the Web Administrator Interface and see the results.

Test Results



Building Your VPN Connection Remotely

This procedure continues from [Step 5 on page 163](#). Use this procedure to build your VPN connection from a remote PC.

STEP 1 Choose **Build VPN** connection from **Internet remotely**. Click **Next** to continue.

Build VPN Connection Remotely



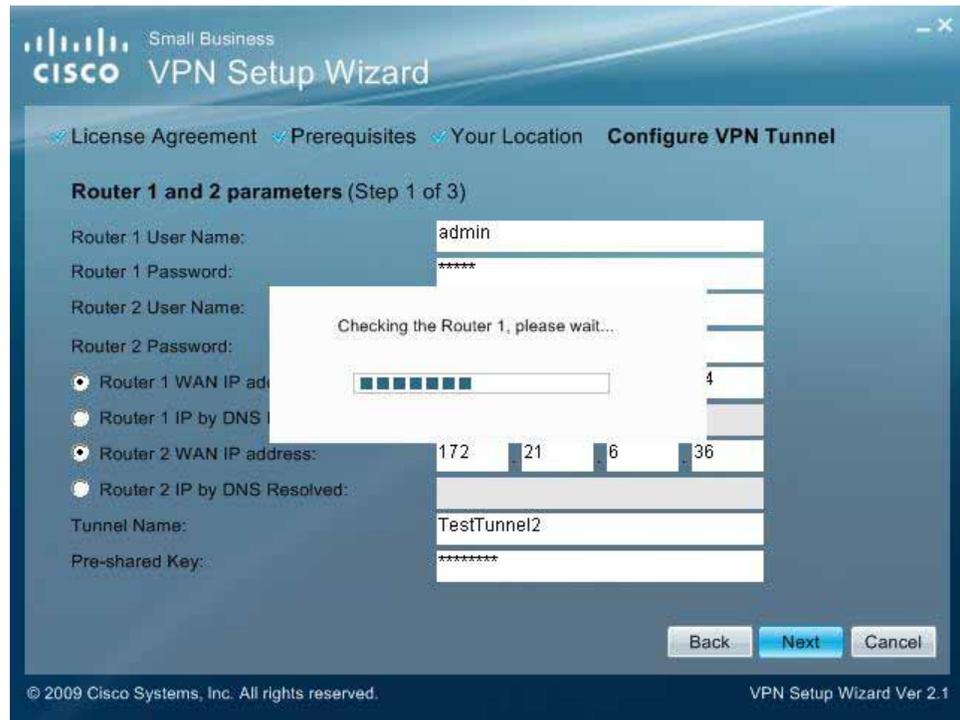
STEP 2 Enter the required data in the **Configure VPN Tunnel** window and then click **Next** to continue.

Configure VPN Tunnel Window

- **Router 1 User Name:** Enter the user name of the Router 1.
- **Router 1 Password:** Enter the password of the Router 1.
- **Router 2 User Name:** Enter the user name of the Router 2.
- **Router 2 Password:** Enter the password of the Router 2.
- **Tunnel Name:** Enter a name for this tunnel.
- **Pre-shared Key:** IKE uses the Pre-shared Key field to authenticate the remote IKE peer. Both character and hexadecimal values are acceptable in this field; e.g., “My_@123” or “0x4d795f40313233”. Note that both sides must use the same Pre-shared Key.
- **Router 1 WAN IP address:** Enter the WAN IP address of the Router 1.
- **Router 1 IP by DNS Resolved:** Enter the DDNS Domain Name of Router 1 if it does not have a static IP address for its internet connection.
- **Router 2 WAN IP address:** Enter the WAN IP address of the Router 2.
- **Router 2 IP by DNS Resolved:** Enter the DDNS Domain Name of Router 2 if it does not have a static IP address for its internet connection.

STEP 3 The router configuration is checked.

Check Router Configuration



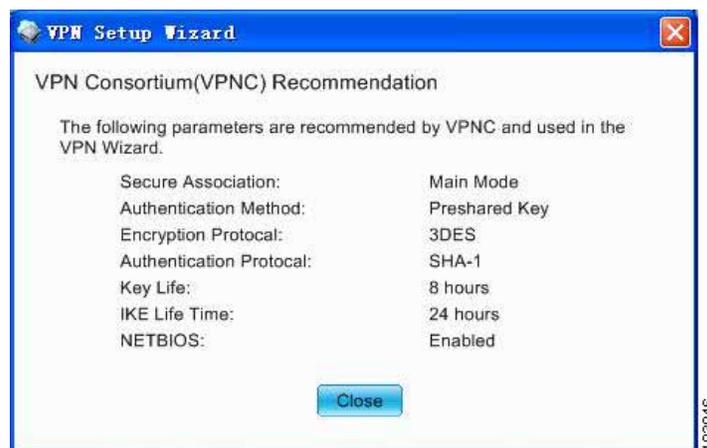
STEP 4 The Summary window appears. Use the Click box to view the VPNC Summary window.

Summary Window



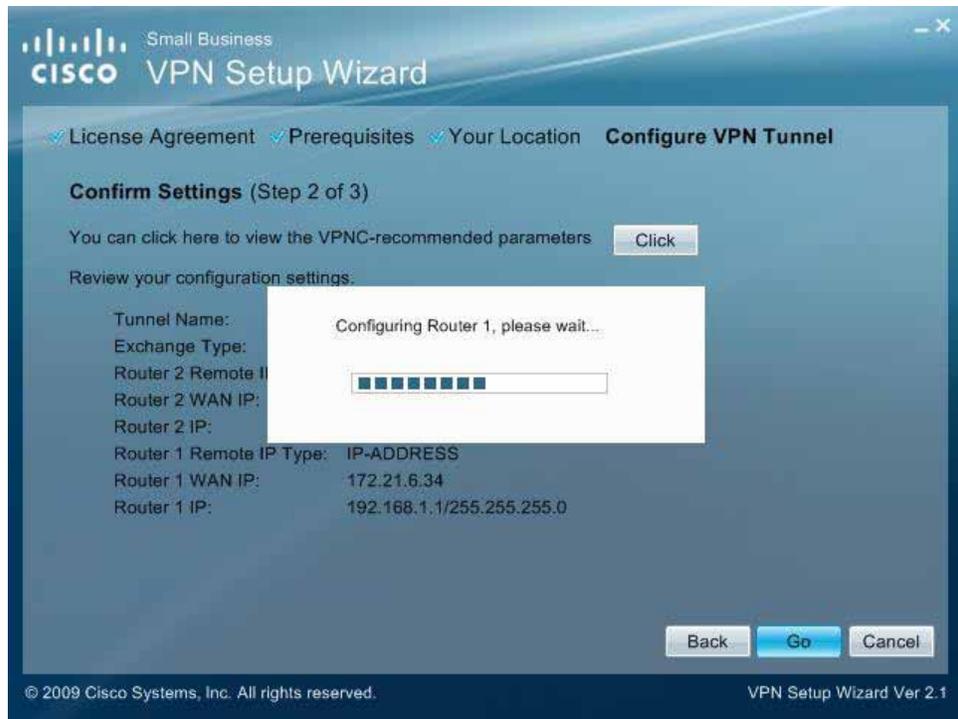
- STEP 5** The VPNC Summary window appears showing the settings that were made to industry standards. Click Close when you are ready to continue.

VPNC Summary Window



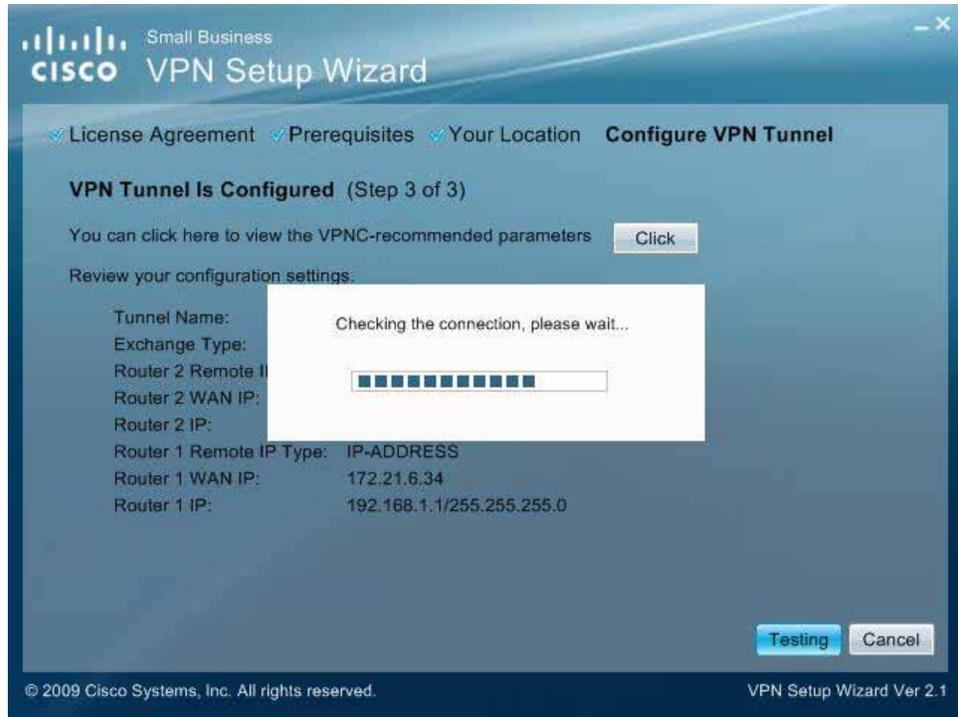
- STEP 6** In the Summary window, if all your entries appear correct, click Go. Otherwise click Back to go back and make any corrections.

Configure the Router



STEP 7 Click **Testing** to make sure the connection is successfully established.

Test the Connection

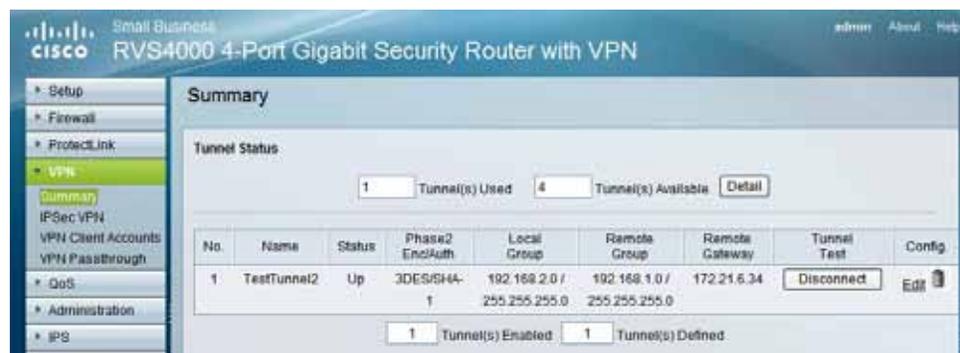


STEP 8 When testing is done, click **Exit** to end the Wizard.



Congratulations! Setup is now complete. You may now log into the Web Administrator Interface and see the results.

View Test Results



Troubleshooting

This appendix provides solutions to problems that may occur during the installation and operation of the router. Read the descriptions below to help solve your problems. If you can't find an answer here, check the Cisco website at www.cisco.com.

I need to set a static IP address on a PC.

The router, by default, assigns an IP address range of 192.168.1.100 to 192.168.1.149 using the DHCP server on the router. To set a static IP address, you can only use the ranges 192.168.1.2 to 192.168.1.99 and 192.168.1.150 to 192.168.1.254. Each PC or network device that uses TCP/IP must have a unique address to identify itself in a network. If the IP address is not unique to a network, Windows will generate an IP conflict error message. You can assign a static IP address to a PC by performing the following steps:

Windows 2000

-
- STEP 1** Click **Start, Settings, and Control Panel**. Double-click **Network and Dial-Up Connections**.
 - STEP 2** Right-click the **Local Area Connection** that is associated with the Ethernet adapter you are using, and click **Properties**.
 - STEP 3** In the "Components checked are used by this connection" box, select **Internet Protocol (TCP/IP)**, and click **Properties**. Select **Use the following IP address**.
 - STEP 4** Enter a unique IP address that is not used by any other computer on the network connected to the router. You can only use an IP address in the ranges 192.168.1.2 to 192.168.1.99 and 192.168.1.151 to 192.168.1.254.
 - STEP 5** Enter the Subnet Mask, **255.255.255.0**.
 - STEP 6** Enter the Default Gateway, **192.168.1.1** (Router's default IP address).

-
- STEP 7** Select **Use the following DNS server addresses**, and enter the Preferred DNS server and Alternative DNS server (provided by your ISP). Contact your ISP or go on its website to find the information.
 - STEP 8** Click **OK** in the Internet Protocol (TCP/IP) Properties window, and click **OK** in the Local Area Connection Properties window.
 - STEP 9** Restart the computer if asked.
-

Windows XP

- STEP 1** Click **Start** and **Control Panel**.
 - STEP 2** Click the **Network and Internet Connections** icon and then the **Network Connections** icon.
 - STEP 3** Right-click the **Local Area Connection** associated with your Ethernet adapter, and click **Properties**.
 - STEP 4** In the This “connection uses the following items” box, select **Internet Protocol (TCP/IP)**. Click **Properties**.
 - STEP 5** Select **Use the following IP address**, and enter a unique IP address that is not used by any other computer on the network connected to the router. You can only use an IP address in the ranges 192.168.1.2 to 192.168.1.99 and 192.168.1.151 to 192.168.1.254.
 - STEP 6** Enter the Subnet Mask, **255.255.255.0**.
 - STEP 7** Enter the Default Gateway, **192.168.1.1** (Router’s default IP address).
 - STEP 8** Select **Use the following DNS server addresses**, and enter the Preferred DNS server and Alternative DNS server (provided by your ISP). Contact your ISP or go on its website to find the information.
 - STEP 9** Click **OK** in the Internet Protocol (TCP/IP) Properties window. Click **OK** in the Local Area Connection Properties window.
-

I want to test my Internet connection.

STEP 1 Check your TCP/IP settings.

Windows 2000

- a. Click **Start**, **Settings**, and **Control Panel**. Double-click **Network and Dial-Up Connections**.
- b. Right-click the **Local Area Connection** that is associated with the Ethernet adapter you are using, and click **Properties**.
- c. In the “Components checked are used by this connection” box, select **Internet Protocol (TCP/IP)**, and click **Properties**. Make sure that **Obtain an IP address automatically** and **Obtain DNS server address automatically** are selected.
- d. Click **OK** in the Internet Protocol (TCP/IP) Properties window, and click **OK** in the Local Area Connection Properties window.
- e. Restart the computer if asked.

Windows XP

The following instructions are for the default interface of Windows XP. If you are using the Classic interface (the icons and menus look like previous Windows versions), please follow the instructions for Windows 2000.

- a. Click **Start** and **Control Panel**.
- b. Click the **Network and Internet Connections** icon and then the **Network Connections** icon.
- c. Right-click the **Local Area Connection** associated with your Ethernet adapter, and click **Properties**.
- d. In the “This connection uses the following items” box, select **Internet Protocol (TCP/IP)** and click **Properties**. Make sure that **Obtain an IP address automatically** and **Obtain DNS server address automatically** are selected.

STEP 2 Open a command prompt:

- a. Windows 98 and Millennium: Click **Start** and **Run**. In the Open field, type **command**. Press **Enter** or click **OK**.
- b. Windows 2000 and XP: Click **Start** and **Run**. In the Open field, type **cmd**. Press **Enter** or click **OK**.

-
- STEP 3** At the command prompt, type **ping 192.168.1.1** and press **Enter**.
- If you get a reply, the computer is communicating with the router.
 - If you do NOT get a reply, check the cable, and make sure **Obtain an IP address automatically** is selected in the TCP/IP settings for your Ethernet adapter.
- STEP 4** At the command prompt, type **ping** followed by your Internet IP address and press **Enter**. The Internet IP Address can be found in the web interface of the router. For example, if your Internet IP address is 1.2.3.4, you would enter **ping 1.2.3.4** and press **Enter**.
- If you get a reply, the computer is connected to the router.
 - If you do NOT get a reply, try the ping command from a different computer to verify that your original computer is not the cause of the problem.
- STEP 5** At the command prompt, type **ping www.cisco.com** and press **Enter**.
- If you get a reply, the computer is connected to the Internet. If you cannot open a web page, try the ping command from a different computer to verify that your original computer is not the cause of the problem.
 - If you do NOT get a reply, there may be a problem with the connection. Try the ping command from a different computer to verify that your original computer is not the cause of the problem.
-

I am not getting an IP address on the Internet with my Internet connection.

-
- STEP 1** Refer to **"I want to test my Internet connection."** on page 180 above to verify that you have connectivity.
- STEP 2** If you need to clone the MAC address of your Ethernet adapter onto the router, see **Cloning Your Network Adapter's MAC Address onto Your Router**, page 57.
- STEP 3** Make sure you are using the right Internet settings. Contact your ISP to see if your Internet connection type is DHCP, Static IP Address, or PPPoE (commonly used by DSL consumers). Please refer to **Configuring Internet Connection Settings**, page 40.
- STEP 4** Make sure you use the right cable. Check to see if the Internet LED is solidly lit.

-
- STEP 5** Make sure the cable connecting from your cable or DSL modem is connected to the router's Internet port. Verify that the Status page of the router's web-based utility shows a valid IP address from your ISP.
- STEP 6** Turn off the computer, router, and cable/DSL modem. Wait 30 seconds, and then turn on the router, cable/DSL modem, and computer. Check **System > Summary** from the router's web-based utility to see if you get an IP address.
-

I am not able to access the router's web-based utility Setup window.

- STEP 1** Refer to ["I want to test my Internet connection."](#) on page 180 to verify that your computer is properly connected to the router.
- STEP 2** Verify that your computer has an IP Address, Subnet Mask, Gateway, and DNS.
- STEP 3** Set a static IP address on your system; refer to ["I need to set a static IP address on a PC."](#) on page 178 above.
- STEP 4** Refer to ["I am a PPPoE user and I need to remove the proxy settings or the dial-up pop-up window."](#) on page 186.
-

I can't get my Virtual Private Network (VPN) to work through the router.

Access the router's web interface by going to <http://192.168.1.1> or the IP address of the router, and go to **VPN > VPN Pass Through**. Make sure you have IPSec passthrough and/or PPTP passthrough enabled.

VPNs that use IPSec with the ESP (Encapsulation Security Payload known as protocol 50) authentication will work fine. At least one IPSec session will work through the router; however, simultaneous IPSec sessions may be possible, depending on the specifics of your VPNs.

VPNs that use IPSec and AH (Authentication Header known as protocol 51) are incompatible with the router. AH has limitations due to occasional incompatibility with the NAT standard.

Change the IP address for the router to another subnet to avoid a conflict between the VPN IP address and your local IP address. For example, if your VPN server assigns an IP address 192.168.1.X (X is a number from 1 to 254) and your local LAN IP address is 192.168.1.X (X is the same number used in the VPN IP address), the router will have difficulties routing information to the right location. If you change the router's IP address to 192.168.2.1, that should solve the problem. Change the

router's IP address through the Setup menu of the web-based utility. If you assigned a static IP address to any computer or network device on the network, you need to change its IP address accordingly to 192.168.2.Y (Y being any number from 1 to 254). Note that each IP address must be unique within the network. Your VPN may require port 500/UDP packets to be passed to the computer that is connecting to the IPSec server. Check the Cisco website at www.cisco.com for more information.

I need to set up a server behind my router.

To use a server like a web, ftp, or mail server, you need to know the respective port numbers they are using. For example, port 80 (HTTP) is used for web; port 21 (FTP) is used for FTP, and port 25 (SMTP outgoing) and port 110 (POP3 incoming) are used for the mail server. You can get more information by viewing the documentation provided with the server you installed. Follow these steps to set up port forwarding through the router's web-based utility. We will be setting up web, ftp, and mail servers.

- STEP 1** Access the router's web-based utility by going to **http://192.168.1.1** or the IP address of the router. Go to **Firewall > Single Port Forwarding**.
- STEP 2** Select the Service from the Application column.
- STEP 3** Enter the IP Address of the server that you want the Internet users to access. For example, if the web server's Ethernet adapter IP address is 192.168.1.100, you would enter 100 in the field provided. Then check the Enable checkbox for the entry. Consider the examples below:

Application	Start and End	Protocol	IP Address	Enable
HTTP	80 to 80	Both	192.168.1.100	X
FTP	21 to 21	TCP	192.168.1.101	X
SMTP (Outgoing)	25 to 25	Both	192.168.1.102	X
POP3 (Incoming)	110 to 110	Both	192.168.1.102	X

- STEP 4** Configure as many entries as you like.
- STEP 5** When you have completed the configuration, click **Save Settings**.

I can't get an Internet game, server, or application to work.

If you are having difficulties getting any Internet game, server, or application to function properly, consider exposing one PC to the Internet using DeMilitarized Zone (DMZ) hosting. This option is available when an application requires too many ports or when you are not sure which port services to use. Make sure you disable all the forwarding entries if you want to successfully use DMZ hosting, since forwarding has priority over DMZ hosting. (In other words, data that enters the router will be checked first by the forwarding settings. If the port number that the data enters from does not have port forwarding, then the router will send the data to whichever PC or network device you set for DMZ hosting.) Follow these steps to set DMZ hosting:

-
- STEP 1** Access the router's web-based utility by going to **http://192.168.1.1** or the IP address of the router. Go to the **Firewall > Single Port Forwarding**.
 - STEP 2** Disable the entries you have entered for forwarding.
 - STEP 3** Go to **Setup > DMZ**.
 - STEP 4** Enter the Ethernet adapter's IP address of the computer you want exposed to the Internet. This will bypass the NAT security for that computer.
 - STEP 5** Select **Enable** to enable DMZ Hosting.
 - STEP 6** When you have completed the configuration, click **Save Settings**.
-

I need to set up online game hosting or use other Internet applications.

If you want to play online games or use Internet applications, most will work without doing any port forwarding or DMZ hosting. There may be cases when you want to host an online game or Internet application. This would require you to set up the router to deliver incoming packets or data to a specific computer. This also applies to the Internet applications you are using. The best way to get the information on what port services to use is to go to the website of the online game or application you want to use. Follow these steps to set up online game hosting or use a certain Internet application:

-
- STEP 1** Access the router's web-based utility by going to **http://192.168.1.1** or the IP address of the router. Go to **Firewall > Single Port Forwarding**.
 - STEP 2** Select the Service from the Application column.

STEP 3 Enter the IP Address of the server that you want the Internet users to access. For example, if the web server’s Ethernet adapter IP address is 192.168.1.100, you would enter 100 in the field provided. Then check the **Enable** checkbox for the entry. Consider the examples below:

Application	Start and End	Protocol	IP Address	Enable
UT	7777 to 27900	Both	192.168.1.100	X
Halfife	27015 to 27015	Both	192.168.1.105	X
PC Anywhere	5631 to 5631	UDP	192.168.1.102	X
VPN IPSEC	500 to 500	UDP	192.168.1.100	X

STEP 4 Configure as many entries as you like.

STEP 5 When you have completed the configuration, click **Save Settings**.

I forgot my password or the password prompt always appears when saving settings to the router.

Reset the router to factory defaults by pressing the Reset button for ten seconds and then releasing it. If you are still getting prompted for a password when saving settings, then perform the following steps:

STEP 1 Access the router’s web interface by going to <http://192.168.1.1> or the IP address of the router. Enter the default password **admin**, and click **Administration > Management**.

STEP 2 Enter the old password in the Old Password field.

STEP 3 Enter a different password in the New Password field, and enter the new password in the Confirm New Password field to confirm the password.

STEP 4 Click **Save Settings**.

I am a PPPoE user and I need to remove the proxy settings or the dial-up pop-up window.

If you have proxy settings, you need to disable these on your computer. Because the router is the gateway for the Internet connection, the computer does not need any proxy settings to gain access. Please follow these directions to verify that you do not have any proxy settings and that the browser you use is set to connect directly to the LAN.

For Microsoft Internet Explorer 5.0 or higher:

-
- STEP 1** Click **Start**, **Settings**, and **Control Panel**. Double-click **Internet Options**.
 - STEP 2** Click the **Connections** tab.
 - STEP 3** Click **LAN settings** and remove anything that is checked.
 - STEP 4** Click **OK** to go back to the previous window.
 - STEP 5** Click the option **Never dial a connection**. This will remove any dial-up pop-ups for PPPoE users.
-

For Netscape 4.7 or higher:

-
- STEP 1** Start **Netscape Navigator**, and click **Edit**, **Preferences**, **Advanced**, and **Proxies**.
 - STEP 2** Make sure you have **Direct connection to the Internet** selected on this window.
 - STEP 3** Close all the windows to finish.
-

To start over, I need to set the router to factory default.

Hold the Reset button for up to 30 seconds and then release it. This will return the password, forwarding, and other settings on the router to the factory default settings. In other words, the router will revert to its original factory configuration.

I need to upgrade the firmware.

In order to upgrade the firmware with the latest features, you need to go to the Cisco website and download the latest firmware. Follow these steps:

-
- STEP 1** Go to the Cisco website and download the latest firmware. For the firmware download link, see [Appendix G, “Where to Go From Here.”](#) From the firmware download link, click **Download Software**. Select the router from the menu and choose the firmware from the options.
 - STEP 2** Extract the firmware file on your computer.
 - STEP 3** To upgrade the firmware, see [Upgrading the Router Firmware, page 134](#).
-

The firmware upgrade failed.

The upgrade could have failed for a number of reasons. Use the WRVS4400N Firmware Upgrade Utility to upgrade the firmware. Follow these steps to upgrade the firmware:

-
- STEP 1** Go to the Cisco website at www.cisco.com and download WRVS4400N Firmware Upgrade Utility v1.3, which will be listed with the firmware. Save the zip file to your computer.
 - STEP 2** Extract the file **setup.exe** from the zip file, then run **setup.exe** to install the utility on your computer.
 - STEP 3** Disconnect the network cables from **all** of the router’s LAN and WAN ports, **except** the network cable to the computer that has the firmware upgrade utility.
 - STEP 4** Run the utility by clicking **Start, All Programs, Cisco Small Business, RVS4400N Upgrade Utility, RVS4400N Upgrade Utility**, or by double-clicking the icon on your desktop.
 - STEP 5** Follow the on-screen instructions to perform the upgrade.
-

My DSL service's PPPoE is always disconnecting.

PPPoE is not actually a dedicated or always-on connection. The DSL ISP can disconnect the service after a period of inactivity, just like a normal phone dial-up connection to the Internet. There is a setup option to “keep alive” the connection. This may not always work, so you may need to re-establish connection periodically.

-
- STEP 1** To connect to the router, go to the web browser, and enter **http://192.168.1.1** or the IP address of the router.
 - STEP 2** Enter the password, if asked (default password is **admin**).
 - STEP 3** On the **Setup > WAN** menu, select the option **Keep Alive**, and set the Redial Period option at **20** (seconds).
 - STEP 4** Click **Save Settings**.

If the connection is lost again, follow steps 1 and 2 to re-establish connection.

I can't access my e-mail, web, or VPN, or I am getting corrupted data from the Internet.

The Maximum Transmission Unit (MTU) setting may need to be adjusted. By default, the MTU is set at 1500. For most DSL users, it is strongly recommended to use MTU 1492. If you are having difficulties, perform the following steps:

-
- STEP 1** To connect to the router, go to the web browser, and enter **http://192.168.1.1** or the IP address of the router.
 - STEP 2** Enter the password, if asked (the default password is **admin**).
 - STEP 3** Go to the **Setup > WAN** menu.
 - STEP 4** Look for the MTU option, and select **Manual**. In the Size field, enter **1492**.
 - STEP 5** Click **Save Settings** to continue.

If your difficulties continue, change the Size to different values. Try this list of values, one value at a time, in this order, until your problem is solved: 1462, 1400, 1362, and 1300.

I need to use port triggering.

Port triggering looks at the outgoing port services used and will trigger the router to open a specific port, depending on which port an Internet application uses. Follow these steps:

-
- STEP 1** To connect to the router, go to the web browser, and enter **http://192.168.1.1** or the IP address of the router.
 - STEP 2** Enter the password, if asked (the default password is **admin**).
 - STEP 3** Click **Firewall > Port Range Triggering**.
 - STEP 4** Enter any name you want to use for the Application Name.
 - STEP 5** Enter the Start and End Ports of the Triggered Range. Check with your Internet application provider for more information on which outgoing port services it is using.
 - STEP 6** Enter the Start and End Ports of the Forwarded Range. Check with your Internet application provider for more information on which incoming port services are required by the Internet application.
 - STEP 7** Check the **Enabled** checkbox for the entry.
 - STEP 8** When you have completed the configuration, click **Save Settings**.
-

When I enter a URL or IP address, I get a time-out error or am prompted to retry.

- Check if other PCs work. If they do, ensure that your workstation's IP settings are correct (IP Address, Subnet Mask, Default Gateway, and DNS). Restart the computer that is having a problem.
- If the PCs are configured correctly, but still not working, check the router. Ensure that it is connected and powered on. Connect to it and check its settings. (If you cannot connect to it, check the LAN and power connections.)
- If the router is configured correctly, check your Internet connection (DSL/cable modem, etc.) to see if it is working correctly. You can remove the router to verify a direct connection.
- Manually configure the TCP/IP with a DNS address provided by your ISP.
- Make sure that your browser is set to connect directly and that any dial-up is disabled. For Internet Explorer, click **Tools, Internet Options**, and then the **Connection** tab. Make sure that Internet Explorer is set to **Never dial a connection**. For Netscape Navigator, click **Edit, Preferences, Advanced**, and **Proxy**. Make sure that Netscape Navigator is set to **Direct connection to the Internet**.

I'm trying to access the router's web-based utility but I do not see the login window. Instead, I see a window saying, "404 Forbidden."

If you are using Windows Explorer, perform the following steps until you see the web-based utility's login window (Netscape Navigator will require similar steps):

-
- STEP 1** Click **File**. Make sure **Work Offline** is NOT checked.
 - STEP 2** Press **CTRL + F5**. This is a hard refresh, which will force Windows Explorer to load new web pages, not cached ones.
 - STEP 3** Click **Tools**. Click **Internet Options**. Click the **Security** tab. Click the **Default level** button. Make sure the security level is **Medium** or lower. Then click the **OK** button.
-

Frequently Asked Questions

Q. What is the maximum number of IP addresses that the router will support?

The router will support up to 253 IP addresses.

Q. Is IPSec Passthrough supported by the router?

Yes, enable or disable IPSec Passthrough on the VPN > VPN Pass Through window.

Q. Where is the router installed on the network?

In a typical environment, the router is installed between the cable/DSL modem and the LAN. Plug the router into the cable/DSL modem's Ethernet port.

Q. Does the router support IPX or AppleTalk?

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

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

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

Q. Does the router support any operating system other than Windows 98, Millennium, 2000, or XP?

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

Q. Does the router support ICQ send file?

Yes, with the following fix: click ICQ menu => preference => connections tab=>, and check I am behind a firewall or proxy. Then set the firewall time-out to 80 seconds in the firewall setting. The Internet user can then send a file to a user behind the router.

Q. I set up an Unreal Tournament Server, but others on the LAN cannot join. What do I need to do?

If you have a dedicated Unreal Tournament server running, you need to create a static IP for each of the LAN computers and forward ports 7777, 7778, 7779, 7780, 7781, and 27900 to the IP address of the server. You can also use a port forwarding range of 7777 to 27900. If you want to use the UT Server Admin, forward another port (8080 usually works well but is used for remote admin; you may have to disable this), and then in the [UWeb.WebServer] section of the server.ini file, set the ListenPort to 8080 (to match the mapped port above) and ServerName to the IP assigned to the router from your ISP.

Q. Can multiple gamers on the LAN get on one game server and play simultaneously with just one public IP address?

It depends on which network game or what kind of game server you are using. For example, Unreal Tournament supports multi-login with one public IP.

Q. How do I get Half-Life: Team Fortress to work with the router?

The default client port for Half-Life is 27005. The computers on your LAN need to have "+clientport 2700x" added to the HL shortcut command line; the x would be 6, 7, 8, and on up. This lets multiple computers connect to the same server. One problem: Version 1.0.1.6 won't let multiple computers with the same CD key connect at the same time, even if on the same LAN (not a problem with 1.0.1.3). As far as hosting games, the HL server does not need to be in the DMZ. Just forward port 27015 to the local IP address of the server computer.

Q. How can I block corrupted FTP downloads?

If you are experiencing corrupted files when you download a file with your FTP client, try using another FTP program.

The web page hangs; downloads are corrupt, or nothing but junk characters are being displayed on the window. What do I need to do?

Force your Ethernet adapter to 10 Mbps or half duplex mode, and turn off the "Auto-negotiate" feature of your Ethernet adapter as a temporary measure. (Please look at the Network Control Panel in your Ethernet adapter's Advanced Properties tab.) Make sure that your proxy setting is disabled in the browser. Check our website at www.cisco.com for more information.

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

Reset the router by holding down the Reset button for ten seconds. Reset your cable or DSL modem by powering the unit off and then on. Obtain and flash the latest firmware release that is readily available on the Cisco website at www.cisco.com.

Q. How can I be notified of new router firmware upgrades?

All Cisco firmware upgrades are posted on the Cisco website at www.cisco.com, where they can be downloaded for free. The router's firmware can be upgraded using the web-based utility. If the router's Internet connection is working well, there is no need to download a newer firmware version, unless that version contains new features that you would like to use. Downloading a more current version of router firmware will not enhance the quality or speed of your Internet connection, and may disrupt your current connection stability.

Q. Will the router function in a Macintosh environment?

Yes, but the router's setup pages are accessible only through Internet Explorer 5.0 or Netscape Navigator 5.0 or higher for Macintosh.

Q. I am not able to get the web configuration window for the router. What can I do?

You may have to remove the proxy settings on your Internet browser, e.g., Netscape Navigator or Internet Explorer. Or remove the dial-up settings on your browser. Check with your browser documentation, and make sure that your browser is set to connect directly and that any dial-up is disabled. Make sure that your browser is set to connect directly and that any dial-up is disabled. For Internet Explorer, click Tools, Internet Options, and then the Connection tab. Make sure that Internet Explorer is set to Never dial a connection. For Netscape Navigator, click Edit, Preferences, Advanced, and Proxy. Make sure that Netscape Navigator is set to Direct connection to the Internet.

Q. What is DMZ Hosting?

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

Q. If DMZ Hosting is used, does the exposed user share the public IP with the router?

No.

Q. Does the router pass PPTP packets or actively route PPTP sessions?

The router allows PPTP packets to pass through.

Q. Is the router cross-platform compatible?

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

Q. How many ports can be simultaneously forwarded?

Theoretically, the router can establish 2,048 sessions at the same time, but you can only forward 30 ranges of ports.

Q. Does the router replace a modem? Is there a cable or DSL modem in the router?

No, this version of the router must work in conjunction with a cable or DSL modem.

Q. Which modems are compatible with the router?

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

Q. How can I check whether I have static or DHCP IP addresses?

Ask your ISP to find out.

Q. How do I get mIRC to work with the router?

From the **Firewall > Single Port Forwarding** menu, set port forwarding to 113 for the PC on which you are using mIRC.

Using Cisco QuickVPN for Windows 2000, XP, or Vista

Overview

This appendix explains how to install and use the Cisco QuickVPN software that can be downloaded from www.cisco.com. QuickVPN works with computers running Windows 2000, XP, or Vista. (Computers using other operating systems will have to use third-party VPN software.) For Windows Vista, QuickVPN Client version 1.2.5 or later is required.

This appendix includes the following sections:

- [Before You Begin, page 196](#)
- [Installing the Cisco QuickVPN Software, page 197](#)
- [Using the Cisco QuickVPN Software, page 199](#)
- [Distributing Certificates to QuickVPN Users, page 202](#)

Before You Begin

The QuickVPN program only works with a Cisco 4-Port Gigabit Security Router with VPN that is properly configured to accept a QuickVPN connection.

The screenshot shows the 'VPN Client Accounts' configuration page. It includes a 'Client Info' section with input fields for Username, Password, and Re-enter to Confirm, and a radio button for 'Allow User to Change Password'. Below this is a 'VPN Client List Table' with 5 rows and columns for No., Active, Username, Password, and Edit/Remove. The 'Active' column has checkboxes, and the 'Edit/Remove' column has 'Edit' and 'Remove' buttons for each row. At the bottom, there is a 'Certificate Management' section with buttons for Generate, Export for Admin, Export for Client, and Import, and a 'Certificate Last Generated or Imported' timestamp. The page also has 'Save' and 'Cancel' buttons at the very bottom.

Follow these instructions to configure the router's VPN client settings:

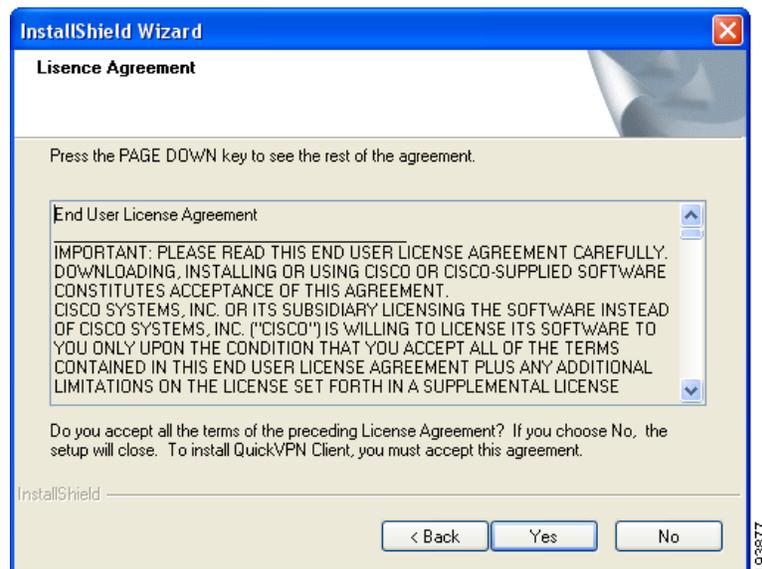
- STEP 1** Click **VPN > VPN Client Accounts**.
- STEP 2** Enter the username in the Username field.
- STEP 3** Enter the password in the Password field, and enter it again in the Re-enter to confirm field.
- STEP 4** Click **Add/Save**.
- STEP 5** Click the **Active** check box for VPN Client No. 1.
- STEP 6** Click **Save Settings**.

Installing the Cisco QuickVPN Software

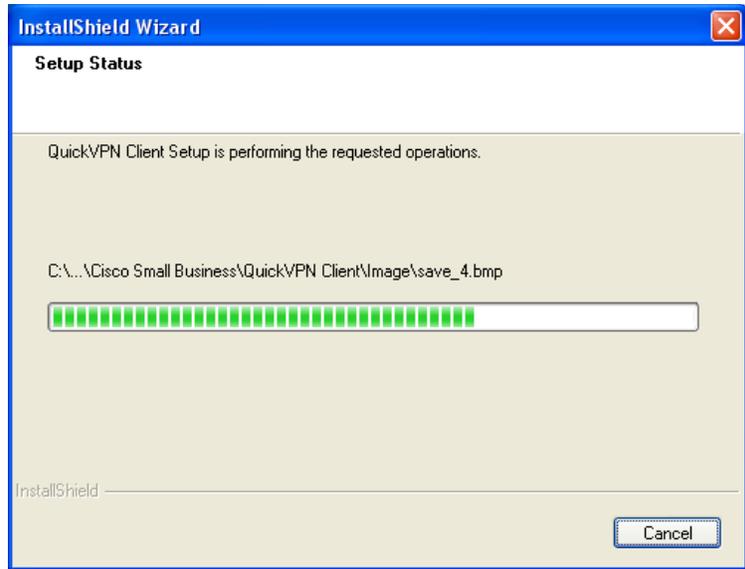
Installing from the CD-ROM

- STEP 1** Insert the WRVS4400N CD-ROM into your CD-ROM drive. Go to the **Start** menu and then click **Run**. In the field provided, enter **D:\VPN_Client.exe** (if “D” is the letter of your CD-ROM drive).
- STEP 2** The License Agreement window appears. Click **Yes** to accept the agreement and the appropriate files are copied to the computer.

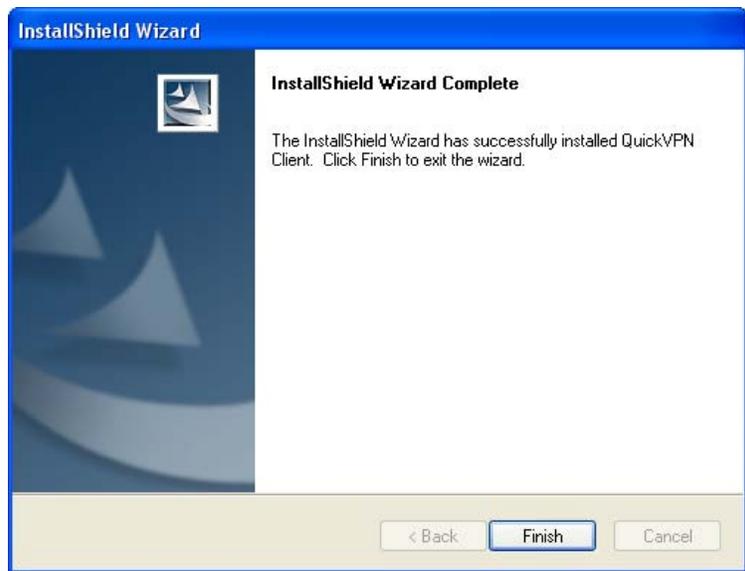
License Agreement



Copying Files



Finished Installing Files



STEP 3 Click **Finished** to complete the installation. Proceed to **“Using the Cisco QuickVPN Software,”** on page 199.

Downloading and Installing from the Internet

-
- STEP 1** Go to firmware download link in [Appendix G, “Where to Go From Here.”](#)
 - STEP 2** From the firmware download link, click **Download Software**.
 - STEP 3** Select **Cisco Small Business Routers > WRVS4400** from the menu.
 - STEP 4** Select **QuickVPN Utility**.
 - STEP 5** Save the zip file to your PC, and extract the .exe file.
 - STEP 6** Double-click the .exe file, and follow the on-screen instructions. Proceed to the next section, [“Using the Cisco QuickVPN Software,” on page 199.](#)
-

Using the Cisco QuickVPN Software

-
- STEP 1** Double-click the Cisco QuickVPN software icon on your desktop or in the system tray.



QuickVPN Desktop Icon



QuickVPN Tray Icon—
No Connection

The QuickVPN Login window will appear.

- STEP 2** In the QuickVPN Login window:
 - a. In the Profile Name field, enter a name for your profile.
 - b. In the User Name and Password fields, enter the User Name and Password that were assigned to you.

- c. In the Server Address field, enter the IP address or domain name of the Cisco 4-Port Gigabit Security Router with VPN.
- d. In the Port For QuickVPN field, enter the port number that the QuickVPN client will use to communicate with the remote VPN router, or keep the default setting, **Auto**.

QuickVPN Login



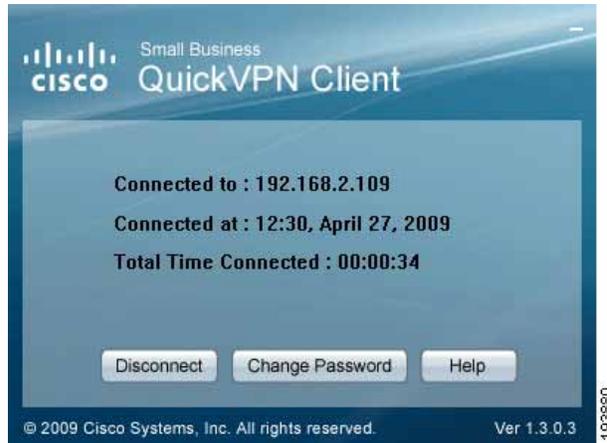
To save this profile, click **Save**. (If there are multiple sites to which you will need to create a tunnel, you can create multiple profiles, but note that only one tunnel can be active at a time.) To delete this profile, click **Delete**. For information, click **Help**.

- STEP 3** To begin your QuickVPN connection, click **Connect**. The connection's progress is displayed: Connecting, Provisioning, Activating Policy, and Verifying Network.
- STEP 4** When your QuickVPN connection is established, the QuickVPN tray icon turns green, and the QuickVPN Status window appears. The window displays the IP address of the remote end of the VPN tunnel, the time and date the VPN tunnel began, and the total length of time the VPN tunnel has been active.



QuickVPN Tray Icon—
Connection

QuickVPN Status



To terminate the VPN tunnel, click **Disconnect**. To change your password, click **Change Password**. For information, click **Help**.

- STEP 5** If you clicked **Change Password** and have permission to change your own password, you will see the Connect Virtual Private Connection window. Enter your password in the Old Password field. Enter your new password in the New Password field. Then enter the new password again in the Confirm New Password field. Click **OK** to save your new password. Click **Cancel** to cancel your change. For information, click **Help**.

Connect Virtual Private Connection





NOTE You can change your password only if you have been granted that privilege by your system administrator.

Distributing Certificates to QuickVPN Users

The following explains how to export a certificate from the WRVS4400N for distribution to QuickVPN users, as well as how to install the certificate on the QuickVPN users' PCs.

STEP 1 Generate the certificate as follows:

- a. Log on to the Web-based Utility.
- b. Select **VPN > VPN Client Accounts**.
- c. Click **Generate** to generate a new certificate.
- d. Click **Export for Client** and save the certificate as a **.PEM** file.

STEP 2 Distribute the certificate to all QuickVPN users.

STEP 3 Each QuickVPN user must then install the certificate as follows:

- a. Save the certificate into the directory where the QuickVPN Client is installed.
For example:
C:\Program Files\Cisco\QuickVPN Client
- b. Launch the QuickVPN Client and specify the User Name, Password, and Server Address (IP address or domain name).
- c. Click **Connect**.

For more information on certificate management, go to section **“Configuring VPN Client Accounts,”** on page 115.

Configuring a Gateway-to-Gateway IPSec Tunnel

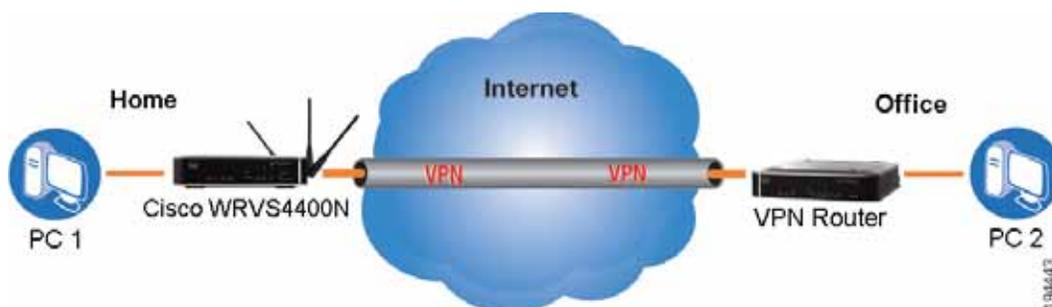
This appendix describes configuring IPSec with a computer that is using Windows 2000 or Windows XP. It includes the following sections:

- “Introduction” on page 203
- “Environment” on page 204

Introduction

This appendix explains how to configure an IPSec VPN tunnel between two VPN routers by example. In this example, two personal computers test the liveliness of the tunnel.

You can think of VPN Router1, the Internet, and VPN Router2 as a big virtual router that connects PC1 on LAN1 and PC2 on LAN2.



Environment

The following is a list of equipment you need:

- Two Windows desktop PCs (each PC connects to a VPN Router)
- Two VPN routers that are both connected to the Internet

Configuring the VPN Settings for the VPN Routers

- [“Configuring the VPN Settings for VPN Router 1” on page 204](#)
- [“Configuring the VPN Settings for VPN Router 2” on page 205](#)

Configuring the VPN Settings for VPN Router 1

Follow these instructions for the first VPN Router, designated VPN Router 1. The other VPN Router is designated VPN Router 2.

STEP 1 Launch the web browser for a networked PC, designated PC 1.

STEP 2 Enter the VPN Router’s local IP address in the Address field (default is 192.168.1.1). Then press Enter.

A password request window appears. (Non-Windows XP users see a similar window.)

STEP 3 Complete the User Name and Password fields (**admin** is the default user name and password). Then, click the **OK** button.

The main window appears.

STEP 4 Click **VPN > IPSec VPN**.

STEP 5 For the VPN Tunnel setting, select **Enabled**.

STEP 6 Enter a name in the Tunnel Name field.

STEP 7 For the Local Secure Group, select **Subnet**. Enter VPN Router 1’s local network settings in the IP Address and Mask fields.

-
- STEP 8** For the Remote Secure Group, select **Subnet**. Enter VPN Router 2's local network settings in the IP Address and Mask fields. Note that the subnet of Router 2 must be different than the subnet of Router 1.
 - STEP 9** For the Remote Secure Gateway, select **IP Addr**. Enter VPN Router 2's WAN IP address in the IP Address field.
 - STEP 10** Click the **Save Settings** button.
-

Configuring the VPN Settings for VPN Router 2

Follow similar instructions for configuring VPN Router 2.

-
- STEP 1** Launch the web browser for a networked PC, designated PC 2.
 - STEP 2** Enter the VPN Router's local IP address in the Address field (default is **192.168.1.1**). Then press **Enter**.
 - STEP 3** A password request window will appear. (Non-Windows XP users will see a similar window.) Complete the User Name and Password fields (**admin** is the default user name and password). Then click the **OK** button.
 - STEP 4** If the LAN IP address is still the default one, change it to **172.168.1.1** and save the setting.
 - STEP 5** Click **VPN > IPSec VPN**.
 - STEP 6** For the VPN Tunnel setting, select **Enabled**.
 - STEP 7** Enter a name in the Tunnel Name field.
 - STEP 8** For the Local Secure Group, select **Subnet**. Enter VPN Router 2's local network settings in the IP Address and Mask fields.
 - STEP 9** For the Remote Secure Group, select **Subnet**. Enter VPN Router 1's local network settings in the IP Address and Mask fields.
 - STEP 10** For the Remote Secure Gateway, select **IP Addr**. Enter VPN Router 1's WAN IP address in the IP Address field.
 - STEP 11** Click the **Save Settings** button.
-

Configuring the Key Management Settings

- [“Configuring the Key Management Settings for VPN Router 1” on page 206](#)
- [“Configuring the Key Management Settings for VPN Router 2” on page 207](#)

Configuring the Key Management Settings for VPN Router 1

Following these instructions for VPN Router 1.

-
- STEP 1** On the IPSec VPN window, select **3DES** from the Encryption drop-down menu.
 - STEP 2** Select **MD5** from the Authentication drop-down menu.
 - STEP 3** Keep the default Key Exchange Method, **Auto (IKE)**.
 - STEP 4** Select **Pre-Shared Key**, and enter a string for this key (for example, 13572468).
 - STEP 5** For the PFS setting, select **Enabled**.
 - STEP 6** If you need more detailed settings, click the **Advanced Settings** button. Otherwise, click the **Save Settings** button and proceed to the next section, [“Configuring the Key Management Settings for VPN Router 2” on page 207](#).
 - STEP 7** On the Advanced VPN Tunnel Setup window, keep the default Operation Mode, **Main**.
 - STEP 8** For Phase 1, select **3DES** from the Encryption drop-down menu.
 - STEP 9** Select **MD5** from the Authentication drop-down menu.
 - STEP 10** Select **1024-bit** from the Group drop-down menu.
 - STEP 11** Enter **3600** in the Key Life Time field.
 - STEP 12** For Phase 2, the Encryption, Authentication, and PFS settings were set on the *VPN* window. Select **1024-bit** from the Group drop-down menu.
 - STEP 13** Keep the default Key Life Time value, **28800**.
 - STEP 14** Click the **Save Settings** button on the Advanced VPN Tunnel Setup window.
 - STEP 15** Click the **Save Settings** button on the IPSec VPN window.
-

Configuring the Key Management Settings for VPN Router 2

For VPN Router 2, follow the same instructions as you did for configuring VPN Router 1.

Configuring PC 1 and PC 2

-
- STEP 1** Set PC 1 and PC 2 to be DHCP clients (refer to Windows Help for more information).
 - STEP 2** Verify that PC 1 and PC 2 can ping each other (refer to Windows Help for more information).

If the computers can ping each other, then you know the VPN tunnel is configured correctly. You can select different algorithms for the encryption, authentication, and other key management settings for VPN Routers 1 and 2.

Finding Out MAC and IP Addresses

This appendix describes how to find the MAC address for your computer's Ethernet adapter so you can use the MAC address cloning feature of the router.

You can also find the IP address of your computer's Ethernet adapter. This IP address is used for the router's filtering, forwarding, and/or DMZ features.

Follow the steps in this appendix to find the adapter's MAC or IP address in Windows 98, Me, 2000, or XP.

Windows 98 or Me Instructions

-
- STEP 1** Click **Start > Run**. In the Open field, enter `winipcfg`. Then press the **Enter** key or the **OK** button.
 - STEP 2** The IP Configuration window appears. Select the Ethernet adapter you have connected to the Router via a CAT 5 Ethernet network cable.
 - STEP 3** Write down the Adapter Address as shown on your computer screen. This is the MAC address for your Ethernet adapter and is shown as a series of numbers and letters.
 - STEP 4** The MAC address/Adapter Address is what you will use for MAC address cloning or MAC filtering.

The following example shows the Ethernet adapter's IP address as 192.168.1.100. Your computer may show something different.

Windows 2000 or XP Instructions

-
- STEP 1** Click **Start** and **Run**. In the Open field, enter `cmd`. Press the **Enter** key or click the **OK** button.
 - STEP 2** At the command prompt, enter `ipconfig /all`. Then press the **Enter** key.
 - STEP 3** Write down the Physical Address as shown on your computer screen. It is the MAC address for your Ethernet adapter. This appears as a series of numbers and letters. The MAC address/Physical Address is what you will use for MAC address cloning or MAC filtering.
-

For the Router's Web-based Utility

For MAC address cloning, enter the MAC Address in the MAC Address field or select **Clone My PCs MAC**.

Click **Save Settings** to save the MAC Cloning settings or click the **Cancel Changes** button to undo your changes.

Cisco ProtectLink Web Service

Overview

The optional Cisco ProtectLink Web service provides security for your network. It scans e-mail messages, filters website addresses (URLs), and blocks potentially malicious websites. ProtectLink is available for online purchase through online resellers such as CDW.com and PCConnection.com.

This appendix explains how to use this service and includes the following sections:

- [How to Access the Web-Based Utility, page 210](#)
- [How to Purchase, Register, or Activate the Service, page 211](#)
- [How to Use the Service, page 214](#)

How to Access the Web-Based Utility

- STEP 1** For local access of the router's web-based utility, launch your web browser, and enter the router's default IP address, **192.168.1.1**, in the Address field. Press the Enter key.

Address Bar





NOTE If the Remote Management feature on the Firewall > General window has been enabled, then users with administrative privileges can remotely access the web-based utility. Use **http://<WAN IP address of the router>**, or use **https://<WAN IP address of the router>** if you have enabled the HTTPS feature.

STEP 2 A login window prompts you for your User name and Password. Enter **admin** in the User name field, and enter **admin** in the Password field. (You can change the Password on the Setup > Password window.) Then click **OK**.

Login Window



How to Purchase, Register, or Activate the Service

You can purchase, register, or activate the service using the ProtectLink window.

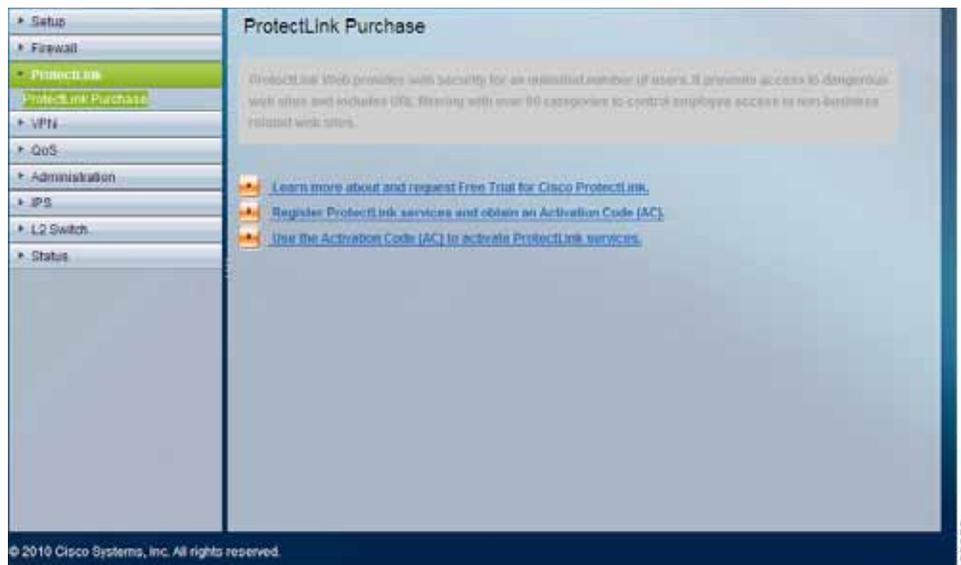
ProtectLink

Click the **ProtectLink** menu to display the ProtectLink window. The following window will display if ProtectLink has not yet been activated.



NOTE If the ProtectLink menu is not displayed, upgrade the router's firmware. For the firmware download link, see [Appendix G, "Where to Go From Here."](#)

ProtectLink (Inactive)



Follow the instructions for the appropriate option:

- I want to learn more about Cisco ProtectLink.
- I want to register online.
- I want to activate Cisco ProtectLink.

I want to learn more about Cisco ProtectLink Web. To learn more about this service, click this link. You will be redirected to a list of resellers for the ProtectLink Web service on Cisco.com.

I have purchased ProtectLink Web and want to register it. If you already have a license, click this link. You will be redirected to the Cisco ProtectLink Web website. Then follow the on-screen instructions.



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

I have my Activation Code (AC) and want to activate ProtectLink Web. If you have registered, click this link. A wizard begins. Follow the on-screen instructions.

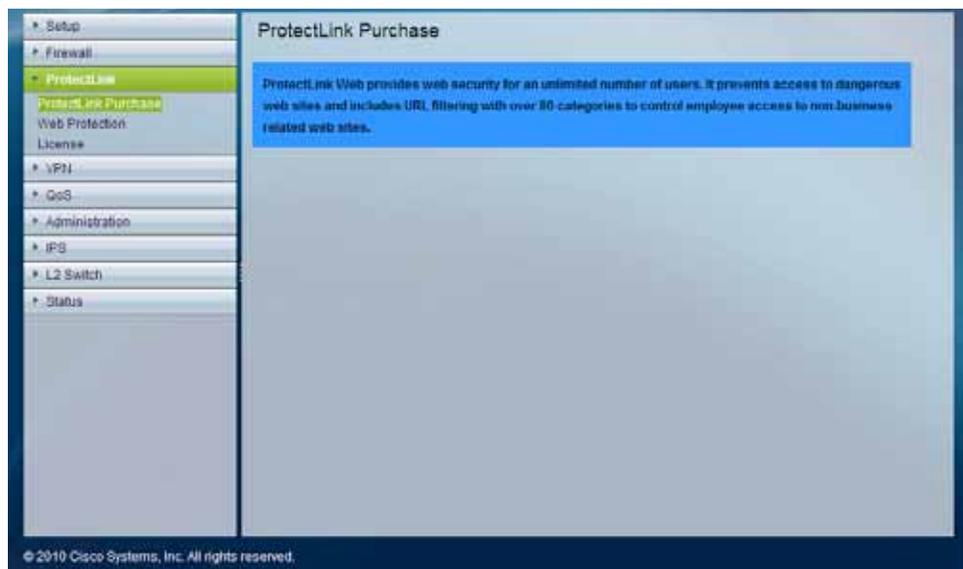
When the wizard is complete, the Web Protection and License menus will appear.



NOTE If you replace the router with a new router that supports this service, click I have my Activation Code (AC) and want to activate ProtectLink Web. Then use your current activation code to transfer your license for the ProtectLink service to the new router.

After you activate ProtectLink, the following window appears when you click **ProtectLink > ProtectLink Purchase** from the menu.

ProtectLink (Active)



How to Use the Service

Configure the service to protect your network.



NOTE

You need to purchase a ProtectLink Web license to use Web Protection. If you do not have a license, you will be prompted to purchase a license when you click **ProtectLink > Web Protection**.

ProtectLink > Web Protection

The Web Protection features are provided by the router. Configure the website filtering settings on the ProtectLink > Web Protection window.

ProtectLink > Web Protection

Web Protection

Enable URL Filtering
 Enable Web Reputation

URL Filtering

Filter the Selected Categories Reset Counter

URL Category	Filtering		Instances Blocked
	Business Hours	Leisure Hours	
<input checked="" type="checkbox"/> Adult	<input type="checkbox"/>	<input type="checkbox"/>	
<input checked="" type="checkbox"/> Business	<input type="checkbox"/>	<input type="checkbox"/>	
<input checked="" type="checkbox"/> Computers/Bandwidth	<input type="checkbox"/>	<input type="checkbox"/>	
<input checked="" type="checkbox"/> Computers/Hardware	<input type="checkbox"/>	<input type="checkbox"/>	
<input checked="" type="checkbox"/> Computers/Communication	<input type="checkbox"/>	<input type="checkbox"/>	
<input checked="" type="checkbox"/> General	<input type="checkbox"/>	<input type="checkbox"/>	
<input checked="" type="checkbox"/> Social	<input type="checkbox"/>	<input type="checkbox"/>	

Business Day:
 Sun Mon Tue Wed Thu Fri Sat

Business Times:
 All day (24 hours)
 Specify business hours
Note: Time not designated as business time will be considered leisure time.

Morning Afternoon

From: To:
 From: To:

Web Reputation

Security level:

High: Blocks a greater number of web threats but increases the risk of false positives.
 Medium: Blocks most web threats and does not create too many false positives. This is the recommended setting.
 Low: Blocks fewer web threats and reduces the risk of false positives.

Approved URLs

URLs in this list will always be accessible.
 Enable Approved URLs list

URLs to approve:

Add >>

Approved URLs list (Max. 20 URLs)

Example:
 www.foo.com/ matches www.foo.com/
 and all the URLs that begin with www.foo.com/
 (Separate multiple entries with semicolons)

Approved Client IP Addresses

Specify the client IP addresses or IP range to exclude from the URL filtering and web reputation rules.
 Enable Approved Clients list

IP address/range:

Add >>

Approved Clients list (Max. 20 IP addresses)

Example:
 IP: 10.1.1.1
 IP range: 10.1.0.0-10.1.1.255
 (Separate multiple entries with semicolons)

URL Overflow Control

Temporarily block URL requests (recommended)
 Temporarily suppress Trend Micro URL Filtering for requested URLs

Save Cancel

235570

Web Protection

Enable URL Filtering To filter website addresses (URLs), select this option.

Enable Web Reputation To block potentially malicious websites, select this option.

URL Filtering

Reset Counter The router counts the number of attempted visits to a restricted URL. To reset the counter to zero, click **Reset Counter**.

For each URL category, select the appropriate Filtering option. If you want to filter a sub-category, click + to view the sub-categories for each category. Then select the appropriate Filtering option:

Business Hours To filter this URL category during the business hours you have specified, select this option.

Leisure Hours To filter this URL category during non-business hours, select this option.

Instances Blocked The number of attempted visits is displayed.

Business Hour Setting

Business Days Select the appropriate days. The default days are **Mon.** through **Fri.**

Business Times To specify entire days, keep the default, **All day (24 hours)**. To specify hours, select **Specify business hours**. For morning hours, select **Morning**, and then select the appropriate From and To times. For afternoon hours, select **Afternoon**, and then select the appropriate From and To times.

Web Reputation

Select the appropriate security level:

High This level blocks a higher number of potentially malicious websites but also increases the risk of false positives. (A false positive is a website that can be trusted but seems potentially malicious.)

Medium This level blocks most potentially malicious websites and does not create too many false positives. The default is **Medium** and is the recommended setting.

Low This level blocks fewer potentially malicious websites and reduces the risk of false positives.

Approved URLs

You can designate up to 20 trusted URLs that will always be accessible.

Enable Approved URL list To set up a list of always accessible URLs, select this option.

URL(s) to approve Enter the trusted URL(s). Separate multiple URLs with semicolons (“;”).

Add To add the URLs, click **Add**.

Approved URLs list The trusted URLs are displayed. To delete a URL, click its **trash can** icon.

Approved Clients

You can designate up to 20 trusted clients (local IP addresses) that will always have access to filtered URLs.

Enable Approved Client list To set up a list of trusted clients, select this option.

IP addresses/range Enter the appropriate IP addresses or ranges. Separate multiple URLs with semicolons (“;”). For a range of IP addresses, use a hyphen (“-”). Example: 10.1.1.0-10.1.1.10.

Add To add the IP addresses or ranges, click **Add**.

Approved Clients list The IP addresses or range of trusted clients are displayed. To delete an IP address or range, click its **trash can** icon.

URL Overflow Control

Specify the behavior you want if there are more URL requests than the service can handle.

Temporarily block URL requests (This is the recommended setting) If there are too many URL requests, the overflow will be held back until they can be processed. This is the default setting.

Temporarily bypass Cisco URL verification for requested URLs If there are too many URL requests, the overflow will be allowed without verification.

Click **Save Settings** to save your changes, or click **Cancel Changes** to undo them.

ProtectLink > License

The license for the Cisco ProtectLink Web service is valid for one year from the time the activation code for Web Protection is generated.

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

ProtectLink > License



License

Update Information To refresh the license information displayed on-screen, click **Update Information**.

License Information

View detailed license online To view license information online, click this link.

Status The status of your license, Activated or Expired, is displayed.

Platform The platform type, Gateway Service, is automatically displayed.

License expires on The date and time your license expires are displayed.

Renew To renew your license, click **Renew**. Then follow the on-screen instructions.

Specifications

This appendix lists the specifications of the Cisco WRVS4400N Wireless-N Gigabit Security Router with VPN.

General

Model	WRVS4400N
Standards	Draft IEEE802.11n, IEEE802.11g, IEEE802.11b, IEEE802.3, IEEE802.3u, 802.1X (Security Authentication), IEEE802.1Q (VLAN), 802.11i (Security WPA2), 802.11e (Wireless QoS), IPv4 (RFC791), IPv6 (RFC2460), RIPv1 (RFC1058), RIPv2 (RFC1723)
Ports	Ethernet, Power
Buttons	Reset
Cabling Type	UTP Cat 5e or better
LEDs	Power, Diag, IPS (blinks red in the case of an internal attack, blinks green in the case of an external attack), Wireless, LAN 1-4, Internet
Operating System	Linux

Performance

Radio Transmit Power	11b: 18 +/- 1.5 dbm 11g: 17 +/- 1.5 dbm 11n: 16.5 +/- 1.5 dbm
Receiver Sensitivity	11.b: 11 Mbps @ -85 dBm 11.g: 54 Mbps @ -70 dBm 11.n: 270 Mbps @ -65 dBm
Active WLAN Clients	Up to 64 Clients
Wireless Securities	WEP, WPA-Personal, WPA-Enterprise, WPA2-Personal, WPA2-Enterprise
Antenna	3 (Omnidirectional), Gain in dBi is 1.8.
NAT Throughput	Up to 800 Mb/s when IPS is disabled
Web UI	Built-in web user interface (UI) for easy browser-based configuration (HTTP/HTTPS)

Management

SNMP Version	SNMP Version 1, 2c
Event Logging	Event logging: Local, Syslog, E-mail alerts
Web F/W upgrade	Firmware upgradable through web browser
Diagnostics	DIAG LED for Flash and RAM failure; Ping Test for network diagnostics

Security

VPN	<ul style="list-style-type: none">▪ 5 QuickVPN tunnels for remote client access▪ 5 IPSec Gateway-to-Gateway Tunnels for branch office connectivity▪ 3DES Encryption▪ MD5/SHA1 Authentication▪ IPSec NAT-T▪ VPN Passthrough of PPTP, L2TP, IPSec
Access Control	IP Access Control List (ACL); MAC-based wireless access control
Firewall	SPI stateful packet inspection (SPI) firewall
Content Filtering	Static URL blocking or keyword blocking (included), Dynamic Filtering through Cisco ProtectLink™ Web Security Service (optional)
IPS (Intrusion Prevention System)	IP Sweep Detection, Application Anomaly Detection (HTTP, FTP, Telnet, RCP), P2P Control, Instant Messenger Control, L3-L4 Protocol (IP, TCP, UDP, ICMP) Normalization, L7 Signature Matching
Signature Update	Manual download from the web (free download for 1 year)
802.1x	Port-based Radius authentication (EAP-MD5, EAP-PEAP)
NAT	PAT, NAT, ALG support, NAT Traversal

QoS

QoS Prioritization Types	Port-based on LAN port, and application-based priority on WAN port
QoS Queues	4 queues

Layer 2

VLAN Support	Port-based and 802.1Q Tag-based VLANs
Number of VLANs	4 active VLANs (4094 range)
SSID Broadcast	SSID Broadcast Enable/Disable
Multiple SSID	Supports Multiple BSSIDs up to 4
Wireless VLAN Map	Supports SSID to VLAN Mapping with Wireless Client Isolation
WDS	Allow Wireless Signals to be Repeated by up to 2 Compatible Repeaters
DHCP	DHCP Server, DHCP Client, DHCP Relay Agent
DNS	DNS Relay, Dynamic DNS (DynDNS, TZO)
DMZ	Software configurable on any IP address
Routing	Static and RIP v1,v2

Environmental

Device Dimensions (W x D x H)	6.69 x 6.69 x 1.57 in. 170 x 170 x 40 mm
Weight	1.01 lb (0.46kg)
Power	12V 1A
Certification	FCC Class B, ICES-003, CE, WiFi WPA2, WiFi Draft N 2.0
Operating Temp.	0 to 40°C (32 to 104°F)
Storage Temp.	-20 to 70°C (-4 to 158°F)
Storage Humidity	5% to 90% Noncondensing
Operating Humidity	10 to 85% 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 Cisco WRVS4400N Wireless-N Gigabit Security Router with VPN.

Product Resources

Support	
Cisco Small Business Support Community	www.cisco.com/go/smallbizsupport
Cisco Small Business Support and Resources	www.cisco.com/go/smallbizhelp
Phone Support Contacts	www.cisco.com/go/sbsc
Cisco Small Business Firmware Downloads	www.cisco.com/go/software
Cisco Small Business Open Source Requests	www.cisco.com/go/smallbiz_opensource_request
Product Resources	
Cisco Small Business Routers	www.cisco.com/go/smallbizrouters

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

Related Documentation

For hardware setup for the Cisco WRVS4400N router, see the *Cisco Small Business Model WRVS4400N Wireless-N Gigabit Security Router with VPN Quick Start Guide*.

For compliance and safety information, see the *Regulatory Compliance and Safety Information for the Cisco Wired and Wireless Routers and Access Point Devices (EMC Class B Devices)*.