ADMINISTRATION GUIDE

Cisco Small Business

RV220W Wireless-N Network Security Firewall

Contents

Chapter 1: Introduction 10

Product Overview 10

Getting to Know the Cisco RV220W 11

Front Panel 11

Back Panel 12

Mounting the Cisco RV220W 13

Placement Tips 13

Wall Mounting 13

Attaching the Antennas 16

Connecting the Equipment 16

Configuring the RV220W 18

Logging In 19

Using the Getting Started Page 20

Navigating through the Pages 21

Saving Your Changes 22

Viewing the Help Files 23

Configuration Next Steps 24

Verifying the Hardware Installation 24

Connecting to Your Wireless Network 25

25

Chapter 2: Configuring Networking 26

Configuring the WAN 26

Configuring the WAN for an IPv4 Network 26

Configuring a DHCP Connection 27

Configuring a Static IP Connection 28

Configuring a Point-to-Point Protocol over Ethernet Connection 28

Configuring a Point-to-Point Tunneling Protocol Connection 30

Configuring a Layer 2 Tunneling Protocol Connection 31

Configuring Maximum Transmit Unit 32

Configuring the Cisco RV220W MAC Address 32

Configuring the WAN for an IPv6 Network 33

Setting the Routing Mode 33

Configuring WAN Settings 33

Creating PPPoE Profiles 35

Configuring the LAN 36

Changing the Host Name of Your RV220W 36

Changing the Default Cisco RV220W IP Address 37

Configuring DHCP 38

Configuring the LAN DNS Proxy 39

Configuring VLANs 39

Enabling VLANs 39

Creating a VLAN 40

Configuring Port VLANs 41

Associating the Wireless Port to VLANs 42

Configuring Multiple VLAN Subnets 43

Configuring IPv6 LAN Properties 44

Configuring IPv6 Address Pools 46

Adding a Static IP Address for a Device on the LAN 46

Viewing DHCP Leased Clients 47

Configuring a DMZ Host 47

Configuring Internet Group Management Protocol 48

Configuring Allowed Networks 49

Configuring Jumbo Frame Support 49

Configuring Routing 50

Choosing the Routing Mode 50

Viewing Routing Information 51

Configuring Static Routing 52

Configuring Dynamic Routing 53

Configuring Port Management 55

Configuring Dynamic DNS 56

Configuring IPv6 57

Configuring the Routing Mode 57

Configuring IPv6 Static Routing 57

Configuring IPv6-to-IPv4 Tunneling 59

Configuring 6-to-4 Tunneling 59

Viewing the IPv6 Tunnels Status 59
Configuring Intra-Site Automatic Tunnel Addressing Protocol Tunnels 59
Configuring Router Advertisement 60

Chapter 3: Configuring the Wireless Network 63
About Wireless Security 63
Wireless Security Tips 64
General Network Security Guidelines 65
Understanding the Cisco RV220W's Wireless Networks 66
Configuring Wireless Profiles 66
Configuring the Group Key Refresh Interval 69
Configuring RADIUS Authentication Parameters 69
Configuring Wi-Fi Multimedia 70
Configuring Access Points 70
Enabling or Disabling APs 70
Editing an AP's Properties 71
Using MAC Filtering 72
Viewing AP Status 73
Configuring the Wireless Radio Properties 74
Configuring Basic Wireless Radio Settings 74
Configuring Advanced Wireless Radio Settings 75
Configuring a Wireless Distribution System 77

Chapter 4: Configuring the Firewall 78
Cisco RV220W Firewall Features 78
Configuring Basic Firewall Settings 80
Protecting from Attacks 80
Configuring Universal Plug and Play 81
Viewing UPnP Information 82
Enabling Session Initiation Protocol Application-Level Gateway 83
Configuring the Default Outbound Policy 83
Configuring Firewall Rules 84
Creating a Firewall Rule 84

Managing Firewall Rules 89

Creating Custom Services 89

Creating Firewall Schedules 90

Blocking and Filtering Content and Applications 91

Blocking Web Applications and Components 91

Adding Trusted Domains 92

Adding Blocked URLs 93

Configuring MAC Address Filtering 93

Configuring IP/MAC Address Binding 94

Configuring Port Triggering 95

Restricting Sessions 96

Configuring Remote Management 97

Configuring One-to-One Network Address Translation 98

Using Cisco ProtectLink Web 99

Configuring Approved Clients 100

Configuring Approved URLs 101

Configuring Overflow Control 101

Configuring Web Reputation 102

Configuring URL Filtering 102

Viewing Cisco ProtectLink License Information 103

103

Chapter 5: Configuring Virtual Private Networks and Security 104

Configuring VPNs 105

Creating Cisco QuickVPN Client Users 105

Using the VPN Wizard 106

Viewing the Default Values 107

Configuring IP Security Policies 107

Configuring IKE Policies 108

Configuring VPN Policies 112

Configuring VPN Clients 117

Monitoring VPN Tunnel Status 117

Configuring IPsec Users 118

Configuring VPN Passthrough 119

Configuring VPN Using a PPTP Server 119

Configuring the SSL VPN Server 120

Configuring SSL VPN Portal Layouts 120

Configuring SSL VPN Policies 121

Identifying Network Resources 123

Configuring Port Forwarding 124

Configuring the SSL VPN Client 125

Configuring Client Routes 126

Using the SSL VPN Client Portal 126

Configuring Security 127

Using Certificates for Authentication 127

Uploading CA Certificates 128

Uploading Self Certificates 128

Generating a Self Certificate Request 129

Downloading the Router’s Current Certificate 129

Using the Cisco RV220W With a RADIUS Server 130

Configuring 802.1x Port-Based Authentication 131

Chapter 6: Configuring Quality of Service 132

Configuring Bandwidth Profiles 133

Configuring Traffic Selectors or Flows 134

Configuring Traffic Metering 135

Configuring 802.1p 137

Configuring 802.1p to Queue Mapping 137

Configuring 802.1p CoS to DSCP Remarking 138

Chapter 7: Administering Your Cisco RV220W 139

Setting Password Complexity 140

Configuring User Accounts 140

Configuring Domains 141

Configuring Groups 142

Configuring Users 143

Configuring Simple Network Management 144

Editing SNMPv3 Users 144

Adding SNMP Traps 145

Configuring Access Control Rules 146

Configuring Additional SNMP Information 146

Using Diagnostic Tools 147

Using PING 147

Using Traceroute 147

Performing a DNS Lookup 147

Capturing and Tracing Packets 147

Configuring Logging 148

Configuring Local Logging 148

Configuring Remote Logging 149

Configuring the Logging Type and Notification 151

Configuring E-Mailing of Log Events 151

Configuring Bonjour Discovery 152

Configuring VLAN Associations 152

Configuring Date and Time Settings 153

Backing Up and Restoring the System 153

Importing a CSV File 154

Upgrading Firmware 157

Rebooting the Cisco RV220W 158

Restoring the Factory Defaults 158

Chapter 8: Viewing the RV220W Status 159

Viewing the System Summary 160

Viewing the Wireless Statistics 163

Viewing the IPsec Connection Status 165

Viewing the QuickVPN Connection Status 166

Viewing Logs 167

Viewing Available LAN Hosts 167

Viewing the Port Triggering Status 168

Viewing Interface Statistics 168

Viewing Port Statistics 169

Viewing Active Users 170

Viewing the SSL VPN Connection Information Status 170

Appendix A: Using Cisco QuickVPN 172

Overview 172

Before You Begin 172

Installing the Cisco QuickVPN Software 173

Installing from the CD-ROM 173

Downloading and Installing from the Internet 175

Using the Cisco QuickVPN Software 175

Appendix B: Where to Go From Here 178

Product Resources 178

1

Introduction

This chapter provides information to familiarize you with the product features, guide you through the installation process, and get started using the browser-based Device Manager. It contains the following sections:

- **Product Overview, page 10**
- **Getting to Know the Cisco RV220W, page 11**
- **Mounting the Cisco RV220W, page 13**
- **Attaching the Antennas, page 16**
- **Connecting the Equipment, page 16**
- **Configuring the RV220W, page 18**
- **Verifying the Hardware Installation, page 24**
- **Connecting to Your Wireless Network, page 25**

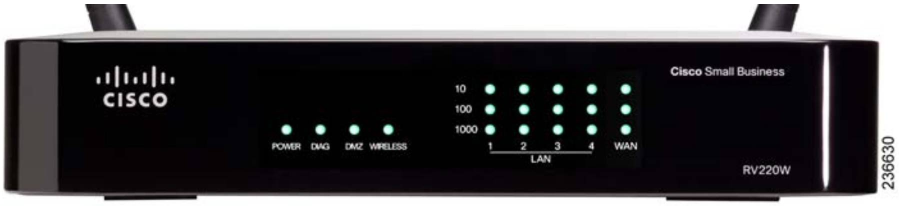
Product Overview

Thank you for choosing the Cisco Small Business RV220W Wireless-N Network Security Firewall. The Cisco RV220W is an advanced Internet-sharing network solution for your small business needs. It allows multiple computers in your office to share an Internet connection through both wired and wireless connections.

The RV220W Network Security Firewall delivers high-performance, high security, wired and wireless connectivity—to the Internet, other offices, and employees working remotely—to speed file transfers and help improve the productivity of employees in a small office. Hybrid VPN capabilities, supporting both IP Security (IPsec) and Secure Sockets Layer (SSL) VPN, provide flexibility to connect remote offices as if they were physically attached to the network and extend controlled network access to partners and others. Business-class security and optional cloud-based web threat protection help keep the network and business assets safe.

Getting to Know the Cisco RV220W

Front Panel



POWER—The Power light is green to indicate the unit is powered on. The light flashes green when the RV220W starts up.

DIAG—If the DIAG light is off, the RV220W is ready. The light blinks red during firmware upgrades.

DMZ—When the DMZ light is green, DMZ is enabled. When the light is off, DMZ is disabled.

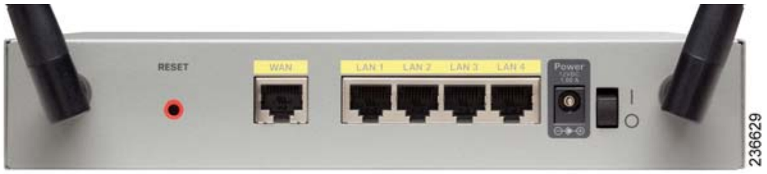
WIRELESS—The Wireless light is green when the wireless module is enabled. The light is off when the wireless module is disabled. The light flashes green when the RV220W is transmitting or receiving data on the wireless module.

LAN—Each of the four LAN (Ethernet) ports of the RV220W has a column in which the lights are displayed. Lights appear in the rows marked 10, 100, and 1000 to identify the type of Ethernet interface that is active on the RV220W. For example, if the light appears next to 100 in the LAN1 column, the RV220W's LAN1 port is using a 100BASE-T connection. If the light appears next to 1000 in the LAN1 column, the RV220W's LAN1 port is using a 1000BASE-T (Gigabit Ethernet) connection.

If the lights are continuously green, the RV220W is connected to a device through the corresponding port (1, 2, 3, or 4). The light for a port flashes green when the RV220W is actively sending or receiving data over that port.

WAN—The WAN (Internet) light is green when the unit is connected to your cable or DSL modem. The light flashes green when the unit is sending or receiving data over the WAN port.

Back Panel



RESET Button—The **RESET** button has two functions:

- If the RV220W has problems connecting to the Internet, press the RESET button for at least 3 seconds but no more than 10 seconds with a paper clip or a pencil tip. This is similar to pressing the reset button on your PC to reboot it.
- If you experience problems with the RV220W and have tried all other troubleshooting measures, press and hold in the RESET button for more than 10 seconds. This reboots the unit and restores the factory defaults. Changes that you have made to the RV220W settings are lost.

WAN Port—The WAN port is connected to your Internet device, such as a cable or DSL modem.

LAN Ports (1-4)—These ports provide a LAN connection to network devices, such as PCs, print servers, or switches.

Power Port—The power port is where you connect the provided power adapter.

Power Switch—Press this button up (toward the line) to turn the device on. Press this button down (toward the circle) to turn the device off.

Mounting the Cisco RV220W

You can place your Cisco RV220W on a desktop or mount it on a wall.

Placement Tips

- **Ambient Temperature**—To prevent the RV220W from overheating, do not operate it in an area that exceeds an ambient temperature of 104°F (40°C).
- **Air Flow**—Be sure that there is adequate air flow around the RV220W.
- **Mechanical Loading**—Be sure that the RV220W is level and stable to avoid any hazardous conditions.

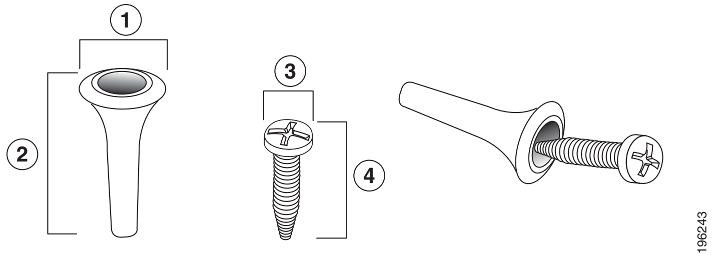
For desktop placement, place the RV220W horizontally on a flat surface so that it sits on its four rubber feet.

Wall Mounting

The RV220W can be wall-mounted. You will need the following (not supplied):

- 2 screws as defined below
- 2 drywall anchors (if installing onto drywall)

The dimensions for these parts are as follows:



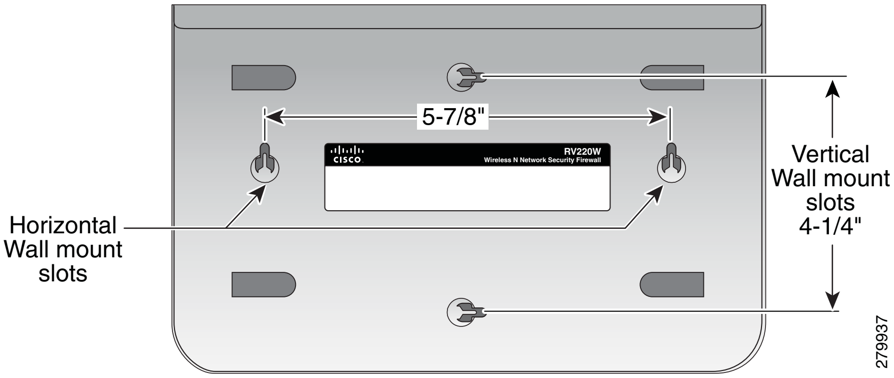
1	0.30 to 0.32 in 7.7 to 8.2 mm
2	0.86 to 0.88 in 21.8 to 22.3 mm
3	0.26 to 0.28 in 6.5 to 7.1 mm
4	0.61 to 0.63 in 15.5 to 16 mm

WARNING Insecure mounting might damage the device or cause injury. Cisco is not responsible for damages incurred by insecure wall-mounting.

To mount the firewall to the wall:

STEP 1 Determine where you want to mount the firewall. Verify that the surface is smooth, flat, dry, and sturdy. Take into account the dimensions of the RV220W and allow for 3 inches (76.2 mm) of clearance around it.

STEP 2 For horizontal mounting, drill two pilot holes into the surface 5-7/8 inches (150 mm) apart. For vertical mounting, drill two pilot holes into the surface 4-1/4 inches (108 mm) apart.

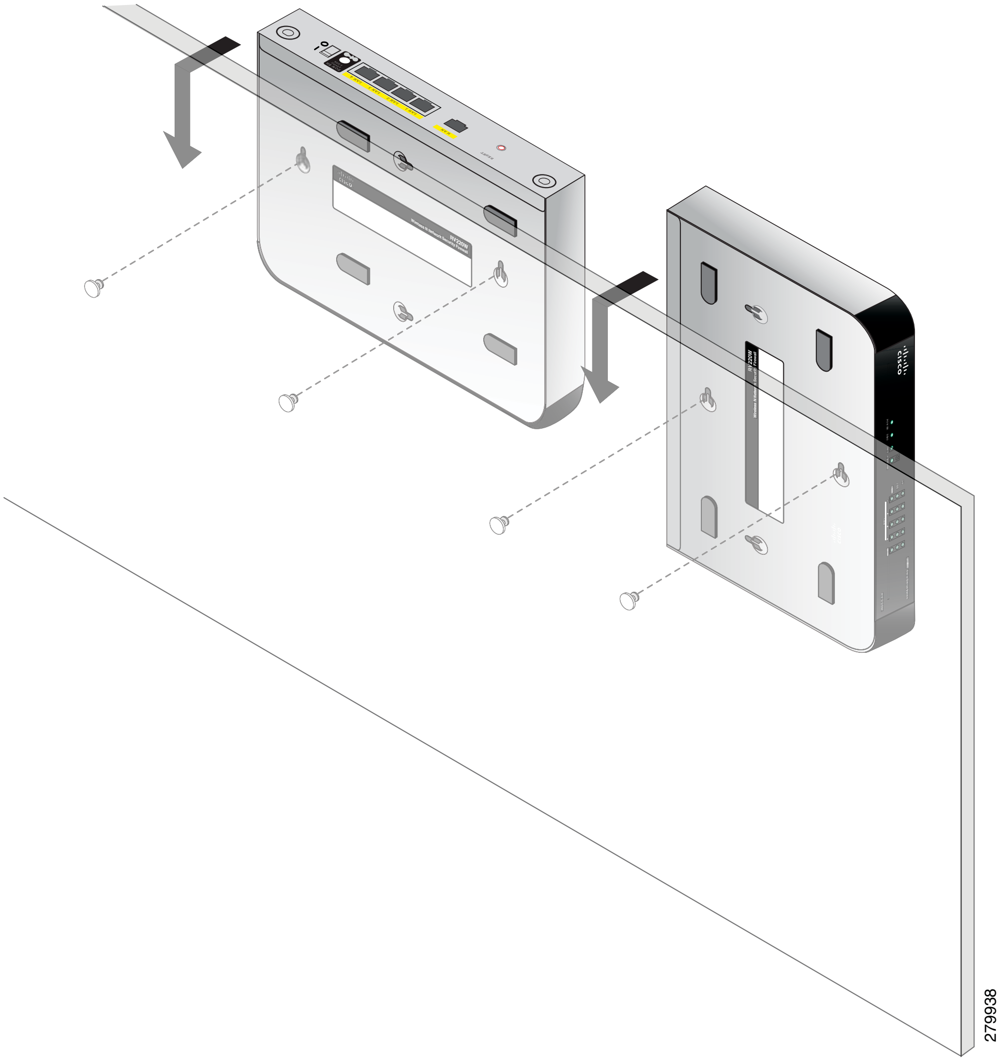


STEP 3 (Optional) If using drywall anchors, hammer into holes.

STEP 4 Insert a screw into each hole in the surface, leaving a gap between the surface and the base of the screw head of at least 0.1 inches (3 mm). Do not mount the screw heads flush with the surface; the screw heads must fit inside the back of the unit.

STEP 5 With the back panel pointing up (if installing horizontally), line up the unit so that the wall-mount slots on the bottom of the unit line up with the two screws.

If installing vertically, hold the left side of the unit pointing up and line up the unit so that the wall-mount slots on the bottom of the unit line up with the two screws.



Attaching the Antennas

The RV220W ships with two removable dual-band antennas.

To attach an external antenna:

STEP 1 Hold the antenna perpendicular to the round screw hole on the back of the unit.

STEP 2 Screw the antenna clockwise until it is firmly secured to the RV220W.

STEP 3 Repeat these steps to secure the second antenna.

STEP 4 Put the antennas in the “V” orientation.

Connecting the Equipment

Before you begin the installation, make sure that you have the following equipment and services:

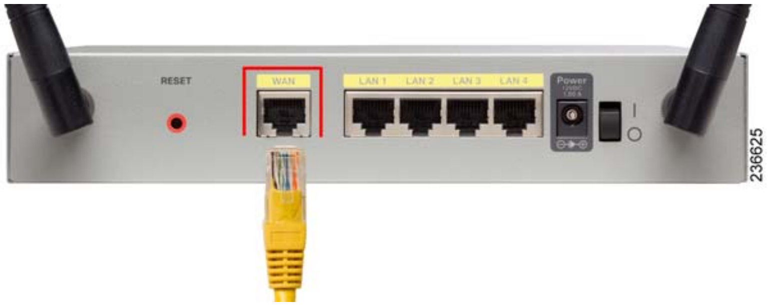
Required

- Functional Internet Connection (Broadband DSL or cable modem).
- Ethernet cable for WAN (Internet) connection.
- PC with functional network adapter (Ethernet connection) to run the Device Manager. The Device Manager is supported on the following web browsers:
  - Microsoft Internet Explorer 6.0 or later
  - Mozilla Firefox 3.0 or later
  - Apple Safari 3.0 or later
- Ethernet cable (provided) to connect the PC to the RV220W for configuration.

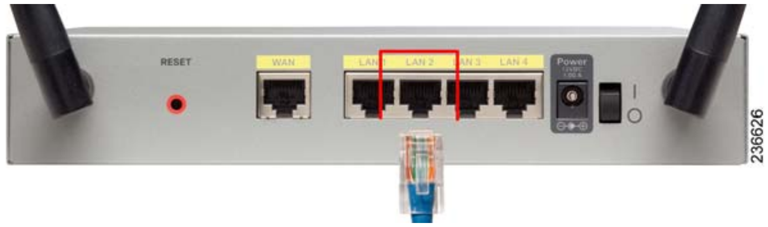
Optional

- Uninterruptible Power Supply (UPS) to provide backup power to essential devices (strongly recommended).
- Ethernet cables for LAN interfaces, if you want to connect additional devices.

STEP 1 Connect one end of an Ethernet cable to the WAN port of the RV220W and the other end to the Ethernet port of your cable or DSL modem.



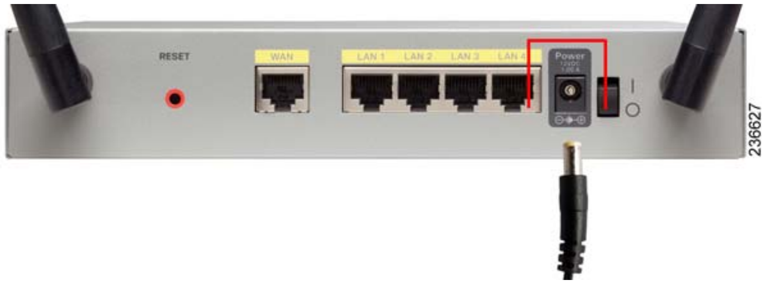
STEP 2 Connect one end of a different Ethernet cable to one of the LAN (Ethernet) ports on the back of the unit. (In this example, the LAN 2 port is used.) Connect the other end to an Ethernet port on the PC that you will use to run the web-based Device Manager.



STEP 3 Power on the cable or DSL modem and wait until the connection is active.

STEP 4 Connect the power adapter to the RV220W Power port.

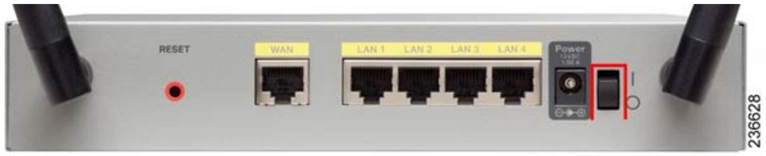
CAUTION Use only the power adapter (12V, 1A) that is supplied with the unit. Using a different power adapter could damage the unit.



STEP 5 Plug the other end of the adapter into an electrical outlet. You may need to use a specific plug (supplied) for your country.

STEP 6 On the RV220W, push the power button to the on position to turn on the RV220W.

The POWER light on the front panel is green when the power adapter is connected properly and the unit is turned on.



Configuring the RV220W

After connecting your equipment, use the web-based Device Manager to configure your RV220W. The Cisco RV220W tries to automatically detect and configure your Internet settings. However, in some cases you might need to manually configure some settings using the Device Manager.

You should also, at a minimum, change the default administrator name and password, and set up wireless security.

Logging In

STEP 1 Power on the PC that you connected to the LAN2 port in Step 2 of the **Connecting the Equipment** section. Your PC becomes a DHCP client of the RV220W and receives an IP address in the 192.168.1.xxx range.

> **NOTE** The default gateway (LAN IP address) of the RV220W is 192.168.1.1. Use this IP address to connect to the RV220W. Also, set your PC to obtain its IP address from a DHCP server.

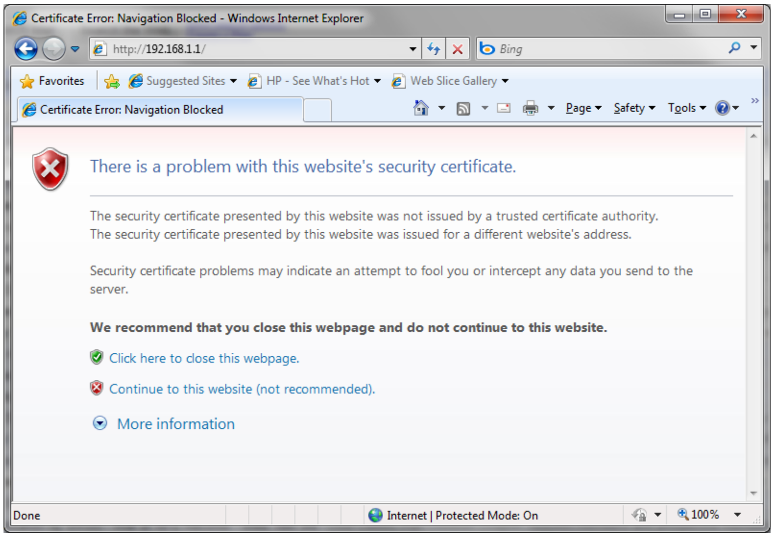
> **NOTE** RV220W uses Bonjour to advertise its record information to any browsing device attached to its network. As a result, the Bonjour and FindIt applications running on the connected PC automatically discovers the RV220W. The RV220W should be available and accessible from the Bonjour and FindIt device lists on the connected PC.

STEP 2 Start a web browser on your PC.

STEP 3 In the Address bar, enter the IP address of the RV220W.

A message appears about the site's security certificate. The RV220W uses a self security certificate and this message appears because the RV220W is not known to your PC.

STEP 4 You can safely click **Continue** (or the option shown on your particular web browser) to go to the web site.


Certificate Error: Navigation Blocked - Windows Internet Explorer
http://192.168.1.1/
Bing
Favorites
Suggested Sites
HP - See What's Hot
Web Slice Gallery
Certificate Error: Navigation Blocked
Page
Safety
Tools
Done
Internet | Protected Mode: On
100%
236734

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

STEP 5 When the login page appears, enter the user name and password. The default user name is cisco. The default password is cisco. Passwords are case sensitive.

NOTE For security reasons, change the default user name and password as soon as possible. See the **Configuring User Accounts** section.

STEP 6 Click **Log In**.

Using the Getting Started Page

The Getting Started page displays some of the most common configuration tasks. Click these underlined tasks to view the configuration windows. You can access the following tasks from the Getting Started page:

Initial Settings

- **Configure WAN Settings**—See **Configuring the WAN for an IPv4 Network, page 26**.
- **Configure LAN Settings**—See **Configuring the LAN, page 36**.
- **Review Wireless Profile and Set Security Settings**—See **Configuring Access Points, page 70**.
- **Add VPN Clients**—See **Configuring IPsec Users, page 118**.

Quick Access

- **Upgrade Device Software**—See **Upgrading Firmware, page 157**.
- **Configure Site to Site VPN**—See **Using the VPN Wizard, page 106**.
- **Configure Remote Management Access**—See **Configuring Remote Management, page 97**.

Device Status

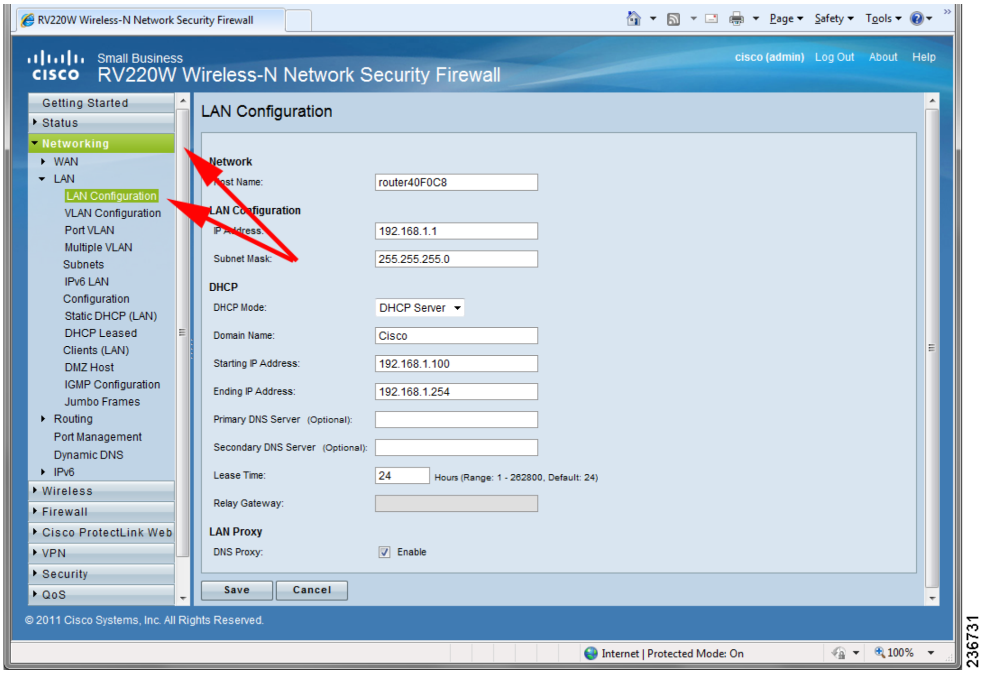
- **System Summary**—See **Viewing the System Summary, page 160**.
- **Wireless Status**—See **Viewing the Wireless Statistics, page 163**.
- **VPN Status**—See **Viewing the IPsec Connection Status, page 165**.

To get support for your device, click the **Support** link at the bottom of the page. To visit the online support forums, click **Forums**.

To prevent the Getting Started page from showing when the Device Manager is started, check the **Don't show this on start-up** box.

Navigating through the Pages

Use the navigation tree in the left pane to open the configuration pages. Click a menu item on the left panel to expand it. Click the menu names displayed underneath to perform an action or view a sub-menu.



LAN Configuration

Network

Host Name: router40F0C8

LAN Configuration

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

DHCP

DHCP Mode: DHCP Server

Domain Name: Cisco

Starting IP Address: 192.168.1.100

Ending IP Address: 192.168.1.254

Primary DNS Server (Optional):

Secondary DNS Server (Optional):

Lease Time: 24 Hours (Range: 1 - 262800, Default: 24)

Relay Gateway:

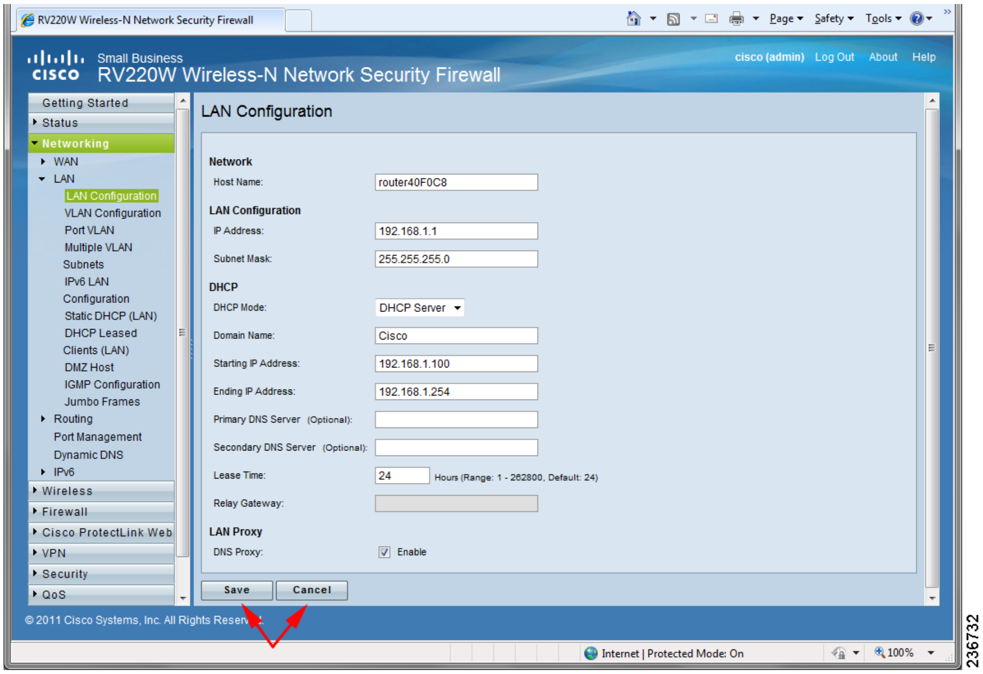
LAN Proxy

DNS Proxy: ☑ Enable

Saving Your Changes

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

NOTE Cancel removes changes you have made to the page, but does not return you to the previous menu.



LAN Configuration

Network

Host Name: router40F0C8

LAN Configuration

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

DHCP

DHCP Mode: DHCP Server

Domain Name: Cisco

Starting IP Address: 192.168.1.100

Ending IP Address: 192.168.1.254

Primary DNS Server (Optional):

Secondary DNS Server (Optional):

Lease Time: 24 Hours (Range: 1 - 262800, Default: 24)

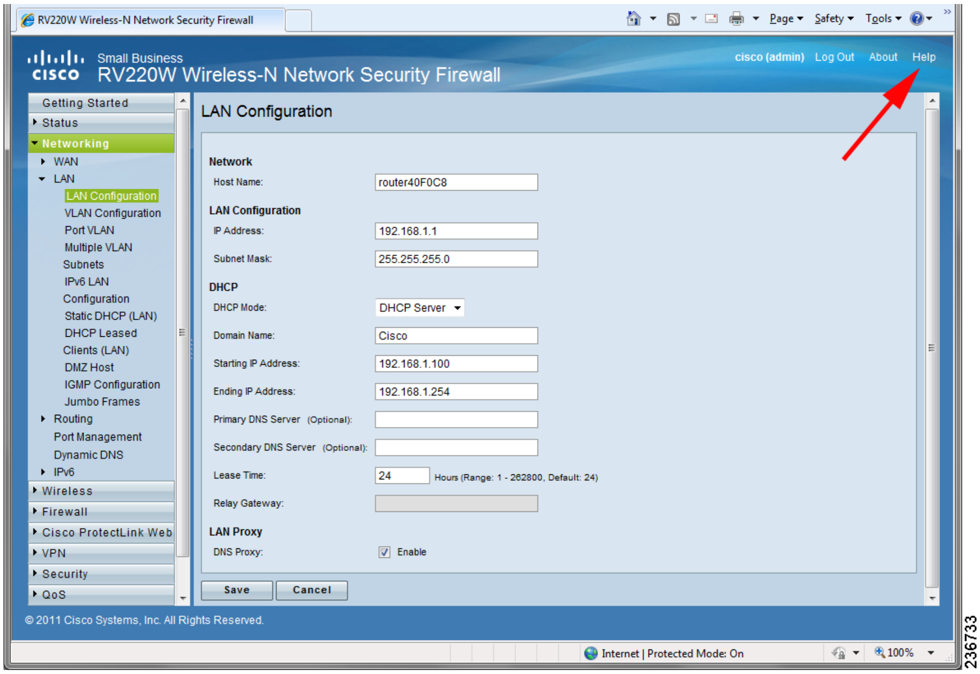
Relay Gateway:

LAN Proxy

DNS Proxy: ☑ Enable

Viewing the Help Files

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



LAN Configuration

Network

Host Name: router40F0C8

LAN Configuration

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

DHCP

DHCP Mode: DHCP Server

Domain Name: Cisco

Starting IP Address: 192.168.1.100

Ending IP Address: 192.168.1.254

Primary DNS Server (Optional):

Secondary DNS Server (Optional):

Lease Time: 24 Hours (Range: 1 - 262800, Default: 24)

Relay Gateway:

LAN Proxy

DNS Proxy: ☑ Enable

Configuration Next Steps

After connecting your RV220W, it tries to automatically configure your settings. However, we recommend that you change some default settings to provide better security and performance. In addition, you may need to manually configure some settings. A suggested outline of steps follows:

- Change the administrator name and password. See **Configuring Users, page 143**.
- Change the idle timeout value. The Device Manager, by default, logs you out after 10 minutes of inactivity. This can be frustrating if you are trying to configure your device. See **Configuring User Accounts, page 140**.
- (Optional) If your connection is not working, or your Internet service requires a login account and password, see **Configuring the WAN, page 26**.
- (Optional) If you already have a DHCP server on your network, and you do not want the Cisco RV220W to act as a DHCP server, see **Configuring the LAN, page 36**.
- Configure your wireless network, especially wireless security. See **Chapter 3, "Configuring the Wireless Network."**
- Configure your Virtual Private Network (VPN) using QuickVPN. The QuickVPN software is found on the documentation and software CD that shipped with your RV220W. See **Appendix A, "Using Cisco QuickVPN."**

Verifying the Hardware Installation

To verify the hardware installation, complete the following tasks:

- Check the LED states, as described in **Getting to Know the Cisco RV220W, page 11**.
- Connect a PC to an available LAN port and verify that you can connect to a website on the Internet, such as www.cisco.com.
- Configure a device to connect to your wireless network and verify the wireless network is functional. See **Connecting to Your Wireless Network, page 25**.

Connecting to Your Wireless Network

To connect a device (such as a PC) to your wireless network, you must configure the wireless connection on the device with the wireless security information you configured using the Device Manager.

The following steps are provided as an example; you may need to configure your device differently. For instructions that are specific to your device, consult the user documentation for your device.

STEP 1 Open the wireless connection settings window or program for your device. Your PC may have special software installed to manage wireless connections, or you may find wireless connections under the Control Panel in the **Network Connections** or **Network and Internet** window. (The location depends on your operating system.)

STEP 2 Enter the network name (SSID) that you chose for your network when you configured the RV220W.

STEP 3 Choose the type of encryption and enter the security key that you chose when setting up the RV220W. If you did not enable security (not recommended), leave these fields blank.

STEP 4 Verify your wireless connection and save your settings.

2

Configuring Networking

The networking page allows you to configure networking settings. This chapter contains the following sections:

- **Configuring the WAN, page 26**
- **Configuring the LAN, page 36**
- **Configuring Routing, page 50**
- **Configuring Dynamic DNS, page 56**
- **Configuring IPv6, page 57**

Configuring the WAN

Wide area network configuration properties are configurable for both IPv4 and IPv6 networks. You can enter information about your Internet connection type and other parameters in these pages.

Configuring the WAN for an IPv4 Network

These instructions are for configuring your RV220W in an IPv4 network. For instructions on configuring your RV220W for an IPv6 network, see the **“Configuring the WAN for an IPv6 Network” section on page 33**.

WAN configuration depends on the type of connection you have to the Internet:

- **DHCP**—See **“Configuring a DHCP Connection” on page 27**.
- **Static IP**—See **“Configuring a Static IP Connection” on page 28**.
- **PPPoE**—See **“Configuring a Point-to-Point Protocol over Ethernet Connection” on page 28**.

- **PPTP**—See **"Configuring a Point-to-Point Tunneling Protocol Connection" on page 30**.
- **L2TP**—See **"Configuring a Layer 2 Tunneling Protocol Connection" on page 31**.

Configuring a DHCP Connection

If you have a dynamic DHCP connection to the Internet, your PC receives its IP address from your cable or DSL modem. This address can change.

Follow these steps:

STEP 1 Choose **Networking** > **WAN** > **IPv4 WAN Configuration.**

STEP 2 In the Internet Address section, in the IP Address Source field, choose **Get Dynamically from ISP.**

STEP 3 In the Domain Name System (DNS) Servers section, in the DNS Server Source field, choose either:

- **Get Dynamically from ISP**—Your ISP automatically connects you to a DNS server that translates host names of computers into numeric IP addresses.
- **Use These DNS Servers**—If your ISP instructs you to use specific DNS server addresses, enter the IP address of the primary and secondary DNS servers.

STEP 4 (Optional) Set the MTU Size. See **"Configuring Maximum Transmit Unit" on page 32**.

STEP 5 (Optional) Configure the RV220W MAC Address. See **"Configuring the Cisco RV220W MAC Address" on page 32**.

STEP 6 Click **Save.**

Configuring a Static IP Connection

If you have a Static IP connection to the Internet, your Internet Service Provider (ISP) has assigned you an IP address that does not change. Follow these steps:

STEP 1 In the **Internet Address** section, in the **IP Address Source** field, choose **Use Static IP Address.**

STEP 2 Provide your IP Address, IP Subnet Mask, and Gateway IP address. This information comes from your ISP.

STEP 3 Enter the IP address of the primary and secondary DNS servers.

STEP 4 (Optional) Set the MTU Size. See **"Configuring Maximum Transmit Unit" on page 32**.

STEP 5 (Optional) Configure the RV220W MAC Address. See **"Configuring the Cisco RV220W MAC Address" on page 32**.

STEP 6 Click **Save.**

Configuring a Point-to-Point Protocol over Ethernet Connection

If you have a Point-to-Point Protocol over Ethernet (PPPoE) connection to the Internet (used mainly with asymmetric DSL), follow these steps:

Create a PPPoE Profile

STEP 1 Create a PPPoE profile, which contains information about your PPPoE connection. (You can create profiles for multiple PPPoE accounts, which can be useful if you connect to the Internet using different service provider accounts.) In the left panel, under **WAN**, click **PPPoE Profiles.**

STEP 2 Click **Add.**

STEP 3 Enter a Profile Name. This is a label that you choose to identify the profile (for example, "ISPOne").

STEP 4 Enter the Username (for example, *john@ISPname.net*)and password. These are assigned to you by the ISP to access your account.

STEP 5 Choose the authentication type:

- **Auto-negotiate**—The server sends a configuration request specifying the security algorithm set on it. The RV220W then sends back authentication credentials with the security type sent earlier by the server.
- **PAP**—The RV220W uses Password Authentication Protocol (PAP) when connecting with the ISP.
- **CHAP**—The RV220W uses Challenge Handshake Authentication Protocol (CHAP) when connecting with the ISP.
- **MS-CHAP**—The RV220W uses Microsoft Challenge Handshake Authentication Protocol when connecting with the ISP.
- **MS-CHAPv2**—The RV220W uses Microsoft Challenge Handshake Authentication Protocol Version 2 when connecting with the ISP.

STEP 6 Choose the connection type:

- **Keep Connected**—The Internet connection is always on.
- **Idle Time**—The Internet connection is on only when traffic is present. If the connection is idle—that is, no traffic is occurring—the connection is closed. You might want to choose this if your ISP charges based on the amount of time that you are connected.

  If you choose this connection type, enter the number of minutes after which the connection shuts off in the **Idle Time** field.

STEP 7 Click **Save**.

Configure PPPoE

STEP 1 In the left panel, under **WAN**, choose **IPv4 WAN Configuration**.

STEP 2 Under **ISP Configuration**, check the box next to **Internet Connection Requires a Login**.

STEP 3 Under **ISP Connection Type**, choose **PPPoE**.

STEP 4 In the PPPoE Profile Name field, choose the profile you created in the **“Create a PPPoE Profile” section on page 28**.

STEP 5 (Optional) Set the MTU Size. See **“Configuring Maximum Transmit Unit” on page 32**.

STEP 6 (Optional) Configure the RV220W MAC Address. See **"Configuring the Cisco RV220W MAC Address" on page 32**.

STEP 7 Click **Save**.

Configuring a Point-to-Point Tunneling Protocol Connection

Your provider may use Point-to-Point Tunneling Protocol (PPTP) connection (used in Europe) for your Internet service. Follow these steps:

STEP 1 In the left panel, under **WAN**, choose **IPv4 WAN Configuration**.

STEP 2 Under **ISP Configuration**, check the box next to **Internet Connection Requires a Login**.

STEP 3 Under **ISP Connection Type**, choose **PPTP**.

STEP 4 Enter your Username (for example, *john@ISPname.net*) and password. These are assigned to you by the ISP to access your account.

STEP 5 If the PPTP server to which you are connecting supports Microsoft Point-to-Point Encryption (MPPE), check the **Enable** box.

STEP 6 Choose the connection type:

- **Keep Connected**—The Internet connection is always on.
- **Idle Time**—The Internet connection is on only when traffic is present. If the connection is idle—that is, no traffic is occurring—the connection is closed. You might want to choose this if your ISP charges based on the amount of time that you are connected. If you choose this connection type, enter the number of minutes after which the connection shuts off in the **Idle Time** field.

STEP 7 In the **My IP Address** field, enter the IP address that the ISP assigned to you to connect to the ISP server.

STEP 8 In the **Server IP Address** field, enter the IP address of the PPTP server.

STEP 9 (Optional) Set the MTU Size. See **"Configuring Maximum Transmit Unit" on page 32**.

STEP 10 (Optional) Configure the RV220W MAC Address. See **"Configuring the Cisco RV220W MAC Address" on page 32**.

STEP 11 Click **Save**.

Configuring a Layer 2 Tunneling Protocol Connection

Your provider may use Layer 2 Tunneling Protocol (L2TP) connection (used in Europe) for your Internet service. Follow these steps:

STEP 1 In the left panel, under **WAN**, choose **IPv4 WAN Configuration**.

STEP 2 Under **ISP Configuration**, check the box next to **Internet Connection Requires a Login**.

STEP 3 Under **ISP Connection Type**, choose **L2TP**.

STEP 4 Enter your user name (for example, *john@ISPname.net*) and password. These are assigned to you by the ISP to access your account.

STEP 5 In the **Secret** field, enter the secret phrase used to log in to the server.

STEP 6 Choose the connection type:

- **Keep Connected**—The Internet connection is always on.
- **Idle Time**—The Internet connection is on only when traffic is present. If the connection is idle—that is, no traffic is occurring—the connection is closed. You might want to choose this if your ISP charges based on the amount of time that you are connected. If you choose this connection type, enter the number of minutes after which the connection shuts off in the **Idle Time** field.

STEP 7 In the **My IP Address** field, enter the IP address that the ISP assigned to you to connect to the ISP server.

STEP 8 In the **Server IP Address** field, enter the IP address of the L2TP server.

STEP 9 (Optional) Set the MTU Size. See **"Configuring Maximum Transmit Unit" on page 32**.

STEP 10 (Optional) Configure the RV220W MAC Address. See **"Configuring the Cisco RV220W MAC Address" on page 32**.

STEP 11 Click **Save**.

Configuring Maximum Transmit Unit

Maximum Transmit Unit (MTU) is the size of the largest packet that can be sent over the network. The standard MTU value for Ethernet networks is usually 1500 bytes and for PPPoE connections, it is 1492 bytes.

STEP 1 Unless a change is required by your ISP, Cisco recommends that you choose **Default** in the MTU Type field. The default MTU size is 1500 bytes. If your ISP requires a custom MTU setting, choose **Custom** and enter the MTU Size.

STEP 2 Click **Save**.

Configuring the Cisco RV220W MAC Address

The RV220W has a unique 48-bit local Ethernet hardware address. In most cases, the RV220W's default MAC address is used to identify your Cisco RV220W to your ISP. However, you can change this setting if required by your ISP.

STEP 1 In the MAC Address Source field, choose one of the following:

- **Use Default Address** (recommended).
- **Use this computer's MAC**—Choose this option to assign the MAC address of the computer that you are using to configure the RV220W.
- **Use This MAC**—Choose this option if you want to manually enter a MAC Address that is expected by your ISP.

STEP 2 If you chose not to use the default MAC address, in the MAC Address field, enter a MAC address in the format of XX:XX:XX:XX:XX:XX, where X is a number from 0 through 9 or a letter from A through F.

STEP 3 Click **Save**.

Configuring the WAN for an IPv6 Network

To configure wide area network settings for your IPv6 network, perform the following steps.

Setting the Routing Mode

STEP 1 In the left panel, under **Networking**, click **IPv6**.

STEP 2 Click **Routing Mode**.

STEP 3 Choose **IPv4/IPV6 mode**.

STEP 4 Click **Save**.

STEP 5 Click **OK** to allow the RV220W to reboot.

Configuring WAN Settings

In the left panel, choose **Networking** > **WAN** and select **IPv6 WAN Configuration.** The next steps depend on the type of WAN connection you choose.

DHCPv6

Choose if your RV220W receives its dynamic IP address from the ISP using DHCP.

STEP 1 In the **WAN Connection Type** field, choose **DHCPv6**.

STEP 2 In the **DHCPv6 Address Settings** field, choose the type of address auto-configuration:

- **Stateless**—An ICMPv6 discover message will originate from the RV220W and is used for auto-configuration, rather than the RV220W contacting the DHCP server at the ISP to obtain a leased address.
- **Stateful**—The RV220W connects to the ISP's DHCPv6 server for a leased address.

STEP 3 Click **Save**.

Static IPv6

Choose if your RV220W is assigned a static IP address from the ISP.

STEP 1 Enter the IPv6 IP address assigned to your RV220W.

STEP 2 Enter the IPv6 prefix length defined by the ISP. The IPv6 network (subnet) is identified by the initial bits of the address which are called the prefix (for example, in the IP address 2001:0DB8:AC10:FE01::, 2001 is the prefix). All hosts in the network have identical initial bits for their IPv6 address; the number of common initial bits in the network's addresses is set in this field.

STEP 3 Enter the default IPv6 gateway address, or the IP address of the server at the ISP that this RV220W will connect to for accessing the internet.

STEP 4 Enter the primary and secondary DNS server IP addresses on the ISP's IPv6 network. DNS servers map Internet domain names (for example, www.cisco.com) to IP addresses.

STEP 5 Click **Save**.

Creating PPPoE Profiles

You can create profiles for multiple PPPoE accounts, which can be useful if you connect to the Internet using different Internet service provider accounts.

STEP 1 Choose **Networking** > **WAN** > **PPPoE Profiles**. Click **Add** to create a new profile.

STEP 2 Enter the profile name. This is a label that you choose to identify the profile (for example, “ISPOne”).

STEP 3 Enter the username and password. These are assigned to you by the ISP to access your account.

STEP 4 Choose the authentication type:

- **Auto-negotiate**—The server sends a configuration request specifying the security algorithm set on it. The RV220W then sends back authentication credentials with the security type sent earlier by the server.
- **PAP**—The Cisco RV220W uses Password Authentication Protocol when connecting with the ISP.
- **CHAP**—The Cisco RV220W uses Challenge Handshake Authentication Protocol when connecting with the ISP.
- **MS-CHAP** or **MS-CHAPv2**—The Cisco RV220W uses Microsoft Challenge Handshake Authentication Protocol when connecting with the ISP.

STEP 5 Choose the connectivity type:

- **Keep connected**—The Internet connection is always on.
- **Idle Time**—The Internet connection is on only when traffic is present. If the connection is idle—that is, no traffic is occurring—the connection is closed. You might want to choose this if your ISP charges based on the amount of time that you are connected.

  If you choose this connection type, enter the number of minutes after which the connection shuts off in the **Idle Time** field.

STEP 6 Click **Save**. Your new profile is added to the list.

Configuring the LAN

For most applications, the default DHCP and TCP/IP settings are satisfactory. If you want another PC on your network to be the DHCP server, or if you are manually configuring the network settings of all of your PCs, disable DHCP.

Instead of using a DNS server, you can use a Windows Internet Naming Service (WINS) server. A WINS server is the equivalent of a DNS server but uses the NetBIOS protocol to resolve hostnames. The RV220W includes the WINS server IP address in the DHCP configuration when acknowledging a DHCP request from a DHCP client.

You can also enable a DNS proxy. When enabled, the RV220W then acts as a proxy for all DNS requests and communicates with the ISP's DNS servers. When disabled, all DHCP clients receive the DNS IP addresses of the ISP.

If machines on your LAN use different IP address ranges (for example, 172.16.2.0 or 10.0.0.0), you can add aliases to the LAN port to give PCs on those networks access to the Internet. This allows the RV220W to act as a gateway to additional logical subnets on your LAN. You can assign the RV220W an IP address on each additional logical subnet.

NOTE If you have IPv6 configured, see **“Configuring IPv6 LAN Properties” on page 44**.

Changing the Host Name of Your RV220W

The default hostname consists of the word “router” followed by the last 3 bytes of route’s LAN MAC address (in Hex-decimal form). This allows the FindIT application to use Bonjour to identify Cisco Small Business devices on the LAN.

To change the host name of your RV220W:

STEP 1 Choose **Networking** > **LAN** > **LAN Configuration**.

STEP 2 Enter the new Host Name.

If you choose to change the host name (you do not have to), you can only use alpha-numeric characters and the hyphen.

STEP 3 Press **Save**.

Changing the Default Cisco RV220W IP Address

STEP 1 Choose **Networking** > **LAN** > **LAN Configuration**.

STEP 2 In the IP address field, enter the new IP address for your Cisco RV220W. The default IP address is 192.168.1.1. You might want to change the default IP address if that address is assigned to another piece of equipment in your network.

STEP 3 Enter the Subnet Mask for the new IP address.

STEP 4 Click **Save**. After changing the IP address, you are no longer connected to the Cisco RV220W. You must do one of the following:

- Release and renew the IP address on the PC that you are using to access the Cisco RV220W (if DHCP is configured on the RV220W).
- Manually assign an IP address to your PC that is in the same subnet as the Cisco RV220W. For example, if you change the Cisco RV220W IP address to 10.0.0.1, you would assign an IP address in the 10.0.0.0 subnet to your PC.

STEP 5 Open a new browser window and enter the new IP address of the Cisco RV220W to re-connect.

Configuring DHCP

By default, the Cisco RV220W functions as a DHCP server to the hosts on the Wireless LAN (WLAN) or LAN network and assigns IP and DNS server addresses.

With DHCP enabled, the RV220W's IP address serves as the gateway address to your LAN. The PCs in the LAN are assigned IP addresses from a pool of addresses. Each address is tested before it is assigned to avoid duplicate addresses on the LAN.

STEP 1 Choose **Networking** > **LAN** > **LAN Configuration**.

STEP 2 In the DHCP Section, in the DHCP Mode field, choose one of the following:

- **DHCP Server**—Choose this to allow the Cisco RV220W to act as the DHCP server in the network. Enter the following information:
  - **Domain Name**—Enter the domain name for your network (optional).
  - **Starting and Ending IP Address**—Enter the first and last of the contiguous addresses in the IP address pool. Any new DHCP client joining the LAN is assigned an IP address in this range. You can save part of the range for PCs with fixed addresses. These addresses should be in the same IP address subnet as the RV220W's LAN IP address.
  - **Primary and Secondary DNS Server**—DNS servers map Internet domain names (for example, www.cisco.com) to IP addresses. Enter the server IP addresses in these fields if you want to use different DNS servers than are specified in your WAN settings.
  - **Lease time**—Enter the duration (in hours) for which IP addresses are leased to clients.
- **DHCP Relay**—If you chose DHCP Relay as the DHCP mode, enter the address of the relay gateway in the Relay Gateway field. The relay gateway transmits DHCP messages between multiple subnets.
- **None**—Use this to disable DHCP on the Cisco RV220W. If you want another PC on your network to be the DHCP server, or if you are manually configuring the network settings of all of your PCs, disable DHCP.

STEP 3 Click **Save**.

Configuring the LAN DNS Proxy

STEP 1 Choose **Networking** > **LAN** > **LAN Configuration.**

STEP 2 Check **Enable** in the LAN Proxy section to enable the Cisco RV220W to act as a proxy for all DNS requests and communicate with the ISP's DNS servers. When this feature is enabled, the RV220W acts as a proxy for all DNS requests and communicates with the ISP's DNS servers (as configured in the WAN settings page).

STEP 3 Click **Save.**

Configuring VLANs

A VLAN is a group of endpoints in a network that are associated by function or other shared characteristics. Unlike LANs, which are usually geographically based, VLANs can group endpoints without regard to the physical location of the equipment or users.

Enabling VLANs

STEP 1 Choose **Networking** > **LAN** > **VLAN Configuration.**

STEP 2 Check the **Enable** box.

STEP 3 Click **Save.**

Underneath the Enable VLAN field, a list of available VLANs is shown, including the name, ID, and whether inter-VLAN routing is enabled or not for each configured VLAN.

Creating a VLAN

STEP 1 Choose **Networking** > **LAN** > **VLAN Configuration.**

STEP 2 In the **Available VLANs Table**, click **Add.**

STEP 3 Enter a name to identify the VLAN.

STEP 4 Enter a numerical VLAN ID that will be assigned to endpoints in the VLAN membership. The VLAN ID can range from 2 to 4094. VLAN ID 1 is reserved for the default VLAN, which is used for untagged frames received on the interface, and VLAN ID 4092 is reserved and cannot be used.

STEP 5 To enable inter-VLAN routing, or routing between this and other VLANS, check the **Enable** box.

STEP 6 Click **Save.**

Configuring Port VLANs

You can associate VLANS on the Cisco RV220W to the LAN ports on the device. By default, all 4 ports belong to VLAN1. You can edit these ports to associate them with other VLANS.

To associate a LAN port to a VLAN:

STEP 1 Choose **Networking** > **LAN** > **Port VLAN**.

STEP 2 In the **Port VLANs Table**, check the box in the row of the LAN port that you want to configure and press **Edit**.

STEP 3 Select the mode for the VLAN port:

- **Access** (default)—In access mode, the port is a member of a single VLAN. All data going into and out of the port is untagged.
- **General**—In general mode, the port is a member of a user-defined set of VLANs. The port sends and receives both tagged and untagged data. Untagged data coming into the port is assigned to a PVID by the user. Data being sent out of the port from the same PVID is untagged. All other data is tagged.

  This mode is typically used with IP phones that have dual Ethernet ports. Data coming from the phone to the LAN port on the Cisco RV220W is tagged. Data passing through the phone from a connected device is untagged.
- **Trunk**—In trunk mode, the port is a member of a user-defined set of VLANs. All data going into and out of the port is tagged. Untagged data coming into the port is not forwarded.

STEP 4 If you selected **Access** or **General** mode, enter the default Port VLAN ID (PVID). This ID is used to tag untagged packets that come into the port.

STEP 5 To assign the port to a VLAN, check the box for each VLAN that you want this port to join. The list of available VLANs is created in the VLAN Configuration page. (See **"Creating a VLAN" on page 40**.)

STEP 6 Click **Save**.

Associating the Wireless Port to VLANs

You can associate wireless VLANS on the Cisco RV220W to the wireless port on the device. To associate the wireless port to a VLAN:

STEP 1 Choose **Networking** > **LAN** > **Port VLAN**.

STEP 2 In the **Wireless VLANs Table**, check the box in the row of the wireless port that you want to configure and press **Edit**.

STEP 3 Select the mode for the wireless port:

- **Access** (default)—In access mode, the port is a member of a single VLAN. All data going into and out of the port is untagged.
- **General**—In general mode, the port is a member of a user-defined set of VLANs. The port sends and receives both tagged and untagged data. Untagged data coming into the port is assigned to a PVID by the user. Data being sent out of the port from the same PVID is untagged. All other data is tagged.

  This mode is typically used with IP phones that have dual Ethernet ports. Data coming from the phone to the LAN port on the Cisco RV220W is tagged. Data passing through the phone from a connected device is untagged.
- **Trunk**—In trunk mode, the port is a member of a user-defined set of VLANs. All data going into and out of the port is tagged. Untagged data coming into the port is not forwarded.

STEP 4 If you selected **Access** or **General** mode, enter the default Port VLAN ID (PVID). This ID is used to tag untagged packets that come into the port.

STEP 5 To assign the port to a VLAN, check the box for each VLAN that you want this port to join. The list of available VLANs is created in the VLAN Configuration page. (See **“Creating a VLAN” on page 40**.)

STEP 6 Click **Save**.

Configuring Multiple VLAN Subnets

When you create a VLAN, a subnet is created automatically for the VLAN. You can then further configure the VLAN properties, such as the IP address and DHCP behavior, to apply to that subnet.

To edit a VLAN:

STEP 1 Choose **Networking** > **LAN** > **Multiple VLAN Subnets**. The list of subnets appears.

STEP 2 Check the box next to the VLAN you want to edit and click **Edit**.

STEP 3 If you want to edit the IP address of this VLAN:

a. In the IP address field, enter the new IP address.

b. Enter the Subnet Mask for the new IP address.

c. Click **Save**. If you are connected to the Cisco RV220W by the LAN port that is a member of this VLAN, the system reboots and connects you to the RV220W using its new IP address.

If you want to edit the DHCP behavior of this VLAN:

a. In the DHCP Section, in the DHCP Mode field, choose one of the following:

- **DHCP Server**—Choose this to allow the VLAN to act as the DHCP server in the network. Enter the following information:
  - **Domain Name**—Enter the domain name for your network (optional).
  - **Starting and Ending IP Address**—Enter the first and last address of the contiguous addresses in the IP address pool. Any new DHCP client joining the LAN is assigned an IP address in this range. You can save part of the range for PCs with fixed addresses. These addresses should be in the same IP subnet as the VLAN.
  - **Primary and Secondary DNS Server**—DNS servers map Internet domain names (for example, www.cisco.com) to IP addresses. Enter the server IP addresses in these fields if you want to use different DNS servers than are specified in your WAN settings.
  - **Lease time**—Enter the duration (in hours) for which IP addresses are leased to clients.

- **DHCP Relay**—Choose this if you are using a DHCP relay gateway. The relay gateway transmits DHCP messages between multiple subnets. Enter the address of the relay gateway in the Relay Gateway field.
- **None**—Use this to disable DHCP on the VLAN.

In the LAN Proxy section, to enable the VLAN to act as a proxy for all DNS requests and communicate with the ISP's DNS servers, check the **Enable** box.

STEP 4 Click **Save**.

Configuring IPv6 LAN Properties

In IPv6 mode, the LAN DHCP server is enabled by default. The DHCPv6 server assigns IPv6 addresses from configured address pools with the IPv6 Prefix Length assigned to the LAN.

To configure IPv6 LAN properties:

STEP 1 Choose **Networking** > **LAN** > **IPv6 LAN Configuration.**

STEP 2 Under LAN TCP/IP Setup, in the IPv6 address field, enter the IP address of the Cisco RV220W. The default IPv6 address for the gateway is fec0::1. You can change this 128-bit IPv6 address based on your network requirements.

STEP 3 Enter the IPv6 prefix length. The IPv6 network (subnet) is identified by the initial bits of the address called the prefix. By default, the prefix is 64-bits long. All hosts in the network have the identical initial bits for their IPv6 address; the number of common initial bits in the network's addresses is set by the prefix length field.

STEP 4 In the DHCPv6 field, choose to disable or enable the DHCPv6 server. If you chose **disable**, proceed to Step 5.

If you chose **enable**, the Cisco RV220W assigns an IP address within the specified range plus additional specified information to any LAN endpoint that requests DHCP-served addresses. Perform the following steps:

a. Choose the DHCP mode. If **stateless** is selected, an external IPv6 DHCP server is not required as the IPv6 LAN hosts are auto-configured by the Cisco RV220W. In this case, the RV220W advertisement daemon (RADVD) must be configured on this device and ICMPv6 RV220W discovery messages are used by the host for auto-configuration. There are no managed addresses to serve the LAN nodes. If **stateful** is selected, the IPv6 LAN host will rely on an external DHCPv6 server to provide required configuration settings.

b. (Optional) Enter the domain name of the DHCPv6 server.

c. Enter the server preference. This field is used to indicate the preference level of this DHCP server. DHCP advertise messages with the highest server preference value to a LAN host are preferred over other DHCP server advertise messages. The default is 255.

d. Choose the DNS proxy behavior:

- **Use DNS Proxy**—When this feature is enabled, the RV220W acts as a proxy for all DNS requests and communicate with the ISP's DNS servers (as configured in the WAN settings page).
- **Use DNS from ISP**—This option allows the ISP to define the DNS servers (primary/secondary) for the LAN DHCP client.
- **Use Below**—If selected, the primary/secondary DNS servers configured are used. If you chose this option, enter the IP address of the primary and secondary DNS servers.

e. Enter the lease/rebind time. Enter the duration (in seconds) for which IP addresses will be leased to endpoints on the LAN.

STEP 5 Click **Save**.

Configuring IPv6 Address Pools

This feature allows you to define the IPv6 delegation prefix for a range of IP addresses to be served by the Cisco RV220W’s DHCPv6 server. Using a delegation prefix, you can automate the process of informing other networking equipment on the LAN of DHCP information specific for the assigned prefix.

STEP 1 Choose **Networking** > **LAN** > **IPv6 LAN Configuration.**

STEP 2 In the **IPv6 Address Pools Table**, click **Add.**

STEP 3 Enter the starting IP address and ending IP address of the pool.

STEP 4 Enter the prefix length. The number of common initial bits in the network’s addresses is set by the prefix length field.

STEP 5 Click **Save.**

Adding a Static IP Address for a Device on the LAN

You can configure an IP Address and MAC Address for a known computer or device on the LAN network from the LAN Interface menu.

STEP 1 Choose **Networking** > **LAN** > **Static DHCP (LAN).**

STEP 2 Click **Add.**

STEP 3 Enter the IP address of the device.

STEP 4 Enter the MAC address of the device. The format for the MAC Address is XX:XX:XX:XX:XX:XX where X is a number from 0 to 9 (inclusive) or an alphabetical letter between A and F (inclusive).

NOTE The IP Address assigned should be outside the pool of the DHCP addresses configured. The DHCP pool is treated as generic pool and all reserved IP's should be outside this pool. The DHCP server will then serve the reserved IP address when the device using the corresponding MAC address requests an IP address.

STEP 5 Click **Save.**

Viewing DHCP Leased Clients

You can view a list of endpoints on the network (identified by MAC address) and see the IP address assigned to them by the DHCP server. The VLAN of the endpoint is also displayed.

STEP 1 Choose **Networking** > **LAN** > **DHCP Leased Clients (LAN).**

STEP 2 The list of endpoints is displayed; you cannot edit this list.

Configuring a DMZ Host

The Cisco RV220W supports DMZ options. A DMZ is a sub-network that is open to the public but behind the RV220W. DMZ allows you to redirect packets going to your WAN port IP address to a particular IP address in your LAN. It is recommended that hosts that must be exposed to the WAN (such as web or e-mail servers) be placed in the DMZ network. RV220W rules can be allowed to permit access to specific services and ports to the DMZ from both the LAN or WAN. In the event of an attack on any of the DMZ nodes, the LAN is not necessarily vulnerable as well.

You must configure a fixed (static) IP address for the endpoint that will be designated as the DMZ host. The DMZ host should be given an IP address in the same subnet as the RV220W's LAN IP address but it cannot be identical to the IP address given to the LAN interface of this gateway.

STEP 1 Choose **Networking** > **LAN** > **DMZ Host.**

STEP 2 Check the **Enable** box to enable DMZ on the network.

STEP 3 Enter the IP address for the endpoint that will receive the redirected packets. This is the DMZ host.

STEP 4 Click **Save**. You must then configure RV220W rules for the zone. See **Configuring Firewall Rules, page 84**.

Configuring Internet Group Management Protocol

Internet Group Management Protocol (IGMP) is an exchange protocol for routers. Hosts that want to receive multicast messages need to inform their neighboring routers of their status.

In some networks, each node in a network becomes a member of a multicast group and receives multicast packets. In these situations, hosts exchange information with their local routers using IGMP.

Routers use IGMP periodically to check if the known group members are active. IGMP provides a method called dynamic membership by which a host can join or leave a multicast group at any time.

To configure IGMP:

STEP 1 Choose **Networking** > **LAN** > **IGMP Configuration**.

STEP 2 Check the **Enable** box to allow IGMP communication between the RV220W and other nodes in the network.

STEP 3 In the Upstream Interface field, click **WAN** or **LAN**.

The upstream interface is the interface on which the multicast traffic is received. For example if the multicast sender is on the Internet, the WAN is the upstream Interface and if the multicast sender is on the LAN side, the LAN Interface is the upstream interface.

STEP 4 Click **Save**.

Configuring Allowed Networks

Allowed networks are the source of IP multicast traffic. You can configure your router to allow IP multicast traffic from certain networks to pass through. IP multicast traffic from other networks is dropped.

By default, the RV220W only forwards multicast packets that originate in its immediate WAN. However, you can configure the router to allow IP multicast traffic from other networks to also pass through. Multicast traffic originating in networks not specified in the list of allowed networks is dropped by the router.

To configure allowed networks:

STEP 1 Choose **Networking** > **LAN** > **IGMP Configuration**.

STEP 2 The **Allowed Networks Table** lists all allowed networks configured for the RV220W. Click **Add** to add a new network, or **Edit** to edit an existing network.

STEP 3 Enter the network address from which the multicast packets originate.

STEP 4 Enter the mask length for the network address.

Use the mask length to designate the subnet mask for the allowed network. For example, 16 represents 255.255.0.0 and 24 represents 255.255.255.0.

STEP 5 Click **Save**.

Configuring Jumbo Frame Support

A standard Ethernet frame contains 1,500 bytes of data. Enabling the Jumbo Frames feature allows the switch to send jumbo frames within the LAN containing up to 9,000 bytes of data per frame.

You can configure the RV220W to support jumbo frames. After support is enabled, devices on the LAN side of the network can exchange traffic that contains jumbo frames. To configure jumbo frames:

STEP 1 Choose **Networking** > **LAN** > **Jumbo Frames**.

STEP 2 Check the **Enable** box.

STEP 3 Click **Save**.

Configuring Routing

Choosing the Routing Mode

The Cisco RV220W provides two different routing modes. Network Address Translation (NAT) is a technique that allows several endpoints on a LAN to share an Internet connection. The computers on the LAN use a "private" IP address range while the WAN port on the RV220W is configured with a single "public" IP address.

The Cisco RV220W translates the internal private addresses into a public address, hiding internal IP addresses from computers on the Internet. If your ISP has assigned you a single IP address, you want to use NAT so that the computers that connect through the Cisco RV220W are assigned IP addresses from a private subnet (for example, 192.168.10.0).

The other routing mode, "classical routing," is used if your ISP has assigned you multiple IP addresses so that you have an IP address for each endpoint on your network. You must configure either static or dynamic routes if you use this type of routing. See **Configuring Static Routing, page 52**, or **Configuring Dynamic Routing, page 53**.

To choose your routing mode:

STEP 1 Select **Networking** > **Routing** > **Routing Mode.**

STEP 2 Click the box next to the type of routing to configure ("NAT" or "Routing") and click **Save.**

NOTE If you have already configured DMZ or RV220W settings on your RV220W in NAT mode, selecting "Routing" changes those settings back to the default.

NOTE The RV220W allows only one-to-one NAT service on VLAN1.

Viewing Routing Information

To view routing information your network, choose **Networking** > **Routing** > **Routing Table.** Choose the network type (IPv4 or IPv6) and click **Display.** Information about your network routing is displayed, including the following:

IPv4 Routing Information

- **Destination—**Destination host/network IP address for which this route is added.
- **Gateway—**The gateway used for this route.
- **Genmask—**The netmask for the destination network.
- **Flags—**For debugging purpose only; possible flags include:
  - **U—**Route is up.
  - **H—**Target is a host.
  - **G—**Use gateway.
  - **R—**Reinstate route for dynamic routing.
  - **D—**Dynamically installed by daemon or redirect.
  - **M—**Modified from routing daemon or redirect.
  - **A—**Installed by *addrconf*.
  - **C—**Cache entry.
  - **!—**Reject route.
- **Metric—**The distance to the target (usually counted in hops).
- **Ref—**Number of references to this route.
- **Use—**Count of lookups for the route. Depending on the use of -F and -C, this is either route cache misses (-F) or hits (-C).
- **Iface—**Interface to which packets for this route will be sent.

IPv6 Routing Information

- **Destination—**Destination host/network IP address for which this route is added.
- **Next Hop—**IP address of the gateway/router through which the destination host/network can be reached.

Configuring Static Routing

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

To create a static route:

STEP 1 Select **Networking** > **Routing** > **Static Routing.**

STEP 2 Under the **Static Routes Table**, click **Add.**

STEP 3 Enter the route name.

STEP 4 If a route is to be immediately active, next to **Active**, check **Enable.** If Enable is not checked, the route is added in an inactive state. It will be listed in the routing table, but will not be used by the RV220W. The route can be enabled later. This feature is useful if the network that the route connects to is not available when you add the route. When the network becomes available, the route can be enabled.

STEP 5 Next to **Private**, check the **Enable** box to mark this route as private, which means that it will not be shared in a Routing Information Protocol (RIP) broadcast or multicast. Uncheck this box if the route can be shared with other routers when RIP is enabled.

STEP 6 In the destination IP address field, enter the IP address of the destination host or network to which the route leads. 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.

STEP 7 In the IP subnet mask field, enter the IPv4 Subnet Mask for the destination host or network. For Class C IP domains, the Subnet Mask is 255.255.255.0.

STEP 8 Choose the physical network interface through which this route is accessible (**WAN**, **LAN**, or a VLAN you have created).

STEP 9 In the gateway IP address field, enter the IP Address of the gateway through which the destination host or network can be reached. 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.

STEP 10 In the metric field, enter a value between 2 and 15 to define the priority of the route. If multiple routes to the same destination exist, the route with the lowest metric is chosen.

STEP 11 Click **Save**.

Configuring Dynamic Routing

Routing Information Protocol (RIP) is an Interior Gateway Protocol (IGP) that is commonly used in internal networks. It allows the RV220W to exchange its routing information automatically with other routers, and allows it to dynamically adjust its routing tables and adapt to changes in the network.

NOTE RIP is disabled by default on the Cisco RV220W.

To configure dynamic routing:

STEP 1 Choose **Networking** > **Routing** > **Dynamic Routing.**

STEP 2 To configure how the RV220W sends and receives RIP packets, choose the RIP direction:

- **Both**—The RV220W both broadcasts its routing table and also processes RIP information received from other routers and RV220Ws.
- **Out Only—**The RV220W broadcasts its routing table periodically but does not accept RIP information from other routers and RV220Ws.
- **In Only—**The RV220W accepts RIP information from other routers and RV220Ws, but does not broadcast its routing table.
- **None**—The RV220W neither broadcasts its route table nor does it accept any RIP packets from other routers and RV220Ws. This option disables RIP.

STEP 3 Choose the RIP version:

- **Disabled.**
- **RIP-1**—This is a class-based routing version that does not include subnet information. RIP-1 is the most commonly supported version.
- **RIP-2B**—This version broadcasts data in the entire subnet.
- **RIP-2M**—This version sends data to multicast addresses.

STEP 4 RIP v2 authentication forces authentication of RIP packets before routes are exchanged with other routers and RV220Ws. It acts as a security feature because routes are exchanged only with trusted routers and RV220Ws in the network. RIP authentication is disabled by default. You can enter two key parameters so that routes can be exchanged with multiple routers and RV220Ws present in the network. The second key also acts as a failsafe when authorization with first key fails.

To enable authentication for RIP-2B or RIP-2M, check the **Enable** box. (You must also choose the direction as explained in **Step 1**.)

If you enabled RIP v2 authentication, enter the following first and second key parameters:

- **MD5 Key ID**—Input the unique MD-5 key ID used to create the Authentication Data for this RIP v2 message.
- **MD5 Authentication Key**—Input the authentication key for this MD5 key. The authentication key is encrypted and sent along with the RIP-V2 message.
- **Not Valid Before**—Enter the start date and time when the authentication key is valid for authentication.
- **Not Valid After**—Enter the end date and time when the authentication key is valid for authentication.

STEP 5 Click **Save**.

Configuring Port Management

The Cisco RV220W has four LAN ports and a dedicated WAN port. You can enable or disable ports, configure if the port is half- or full-duplex, and set the port speed.

To configure LAN ports:

STEP 1 Choose **Networking** > **Port Management**.

STEP 2 To enable a port, check the **Enable** box. To disable the port, uncheck the **Enable** box. By default, all ports are enabled.

STEP 3 Check the **Auto** box to let the RV220W and network determine the optimal port settings. By default, automatic mode is enabled. This setting is available only when the **Enable** box is checked.

STEP 4 (Optional) Choose either half- or full-duplex based on the port support. The default is full-duplex for all ports. This setting is available only when the **Auto** check box is unchecked.

STEP 5 (Optional) Select one of the following port speeds: **10 Mbps**, **100 Mbps**, or **1000 Mbps**. The default setting is 1000 Mbps for all ports. This setting is available only when the **Auto** check box is unchecked. You can change the port speed if a network is designed to run at a particular speed, such as 10 Mbps mode. For example, you may want to change the port to 10 Mbps if the endpoint also uses 10 Mbps mode, either by auto-negotiation or manual setting.

STEP 6 Click **Save**.

Configuring Dynamic DNS

Dynamic DNS (DDNS) is an Internet service that allows routers and RV220Ws with varying public IP addresses to be located using Internet domain names. To use DDNS, set up an account with a DDNS provider such as DynDNS.com or TZO.com.

The RV220W notifies DDNS servers of changes in the WAN IP address, so that any public services on your network can be accessed by using the domain name.

To configure DDNS:

STEP 1 Choose **Networking** > **Dynamic DNS**.

STEP 2 Select the Dynamic DNS Service you are using. Selecting **None** disables this service.

STEP 3 If you selected DynDNS.com:

a. Specify the complete Host Name and Domain Name for the DDNS service.

b. Enter the DynDNS account username.

c. Enter the password for the DynDNS account.

d. Check the **Use Wildcards** box to enable the wildcards feature, which allows all subdomains of your DynDNS Host Name to share the same public IP as the Host Name. You can enable this option here if not done on the DynDNS website.

e. Check the **Update Every 30 Days** box to configure the RV220W to update the host information on DynDNS and keep the subscription active after the 30-day trial.

If you selected TZO.com:

a. Specify the complete Host Name and Domain Name for the DDNS service.

b. Enter the user e-mail address for the TZO account.

c. Enter the user key for the TZO account.

d. Check the **Update Every 30 Days** box to configure the RV220W to update the host information on TZO.com and keep the subscription active after the 30-day trial.

STEP 4 Click **Save**.

Configuring IPv6

The IPv6 configuration information for your RV220W is performed in several windows in the Device Manager of the Cisco RV220W. Make sure you do the following:

- **Configure IPv6 WAN properties**—See **Configuring the WAN for an IPv6 Network, page 33**.
- **Set the Routing Mode to IPv4/IPv6 mode**—See below.

Configuring the Routing Mode

To configure IPv6 properties on the Cisco RV220W, set the routing mode to IPv6:

STEP 1 Choose **Networking** > **IPv6** > **Routing Mode.**

STEP 2 Select **IPv4/IPv6** and click **Save**. The RV220W reboots.

Configuring IPv6 Static Routing

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

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 or RV220W.

You can also use static routes to reach peer routers and RV220Ws that do not support dynamic routing protocols. Static routes can be used together with dynamic routes. Be careful not to introduce routing loops in your network.

To create a static route:

STEP 1 Select **Networking** > **Routing** > **Static Routing.**

STEP 2 In the list of static routes, click **Add**.

STEP 3 Enter the route name.

STEP 4 If a route is to be immediately active, next to **Active**, check **Enable**. When a route is added in an inactive state, it will be listed in the routing table, but will not be used by the RV220W. The route can be enabled later. This feature is useful if the network that the route connects to is not available when you add the route. When the network becomes available, the route can be enabled.

STEP 5 In the IPv6 destination field, enter the IPv6 address of the destination host or network for this route.

STEP 6 In the IPv6 prefix length field, enter the number of prefix bits in the IPv6 address that define the destination subnet.

STEP 7 Choose the physical network interface through which this route is accessible (**WAN**, **LAN**, or **sit0 WAN** tunnel). (The Simple Internet Transition [SIT] is a set of protocol mechanisms implemented in hosts and routers, along with some operational guidelines for addressing and deployment, designed to make the transition from the Internet to IPv6 work with as little disruption as possible. The SIT0 tunnel is a point-to-point tunnel.)

STEP 8 Enter the IP Address of the gateway through which the destination host or network can be reached.

STEP 9 In the metric field, specify the priority of the route by choosing a value between 2 and 15. If multiple routes to the same destination exist, the route with the lowest metric is used.

STEP 10 Click **Save**.

Configuring IPv6-to-IPv4 Tunneling

The Cisco RV220W provides several IPv6 tunneling methods.

Configuring 6-to-4 Tunneling

6-to-4 tunneling allows IPv6 packets to be transmitted over an IPv4 network. 6-to-4 tunneling is typically used when a site or end user wants to connect to the IPv6 Internet using the existing IPv4 network.

To configure 6-to-4 tunneling:

STEP 1 Select **Networking** > **IPv6** > **6 to 4 Tunneling**.

STEP 2 Check the **Enable Automatic Tunneling** box.

STEP 3 Click **Save**.

Viewing the IPv6 Tunnels Status

You can view information about the IPv6 to IPv4 tunnels you have configured on the WAN interface. Select **Networking** > **IPv6** > **IPv6 Tunnels Status**. The table displays the name of the tunnel and the IPv6 address created on the RV220W. Click **Refresh** to view the latest information.

Configuring Intra-Site Automatic Tunnel Addressing Protocol Tunnels

Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) is a method to transmit IPv6 packets between dual-stack nodes over an IPv4 network. The Cisco RV220W is one endpoint (a node) for the tunnel. You must also set a local endpoint, as well as the ISATAP Subnet Prefix that defines the logical ISATAP subnet to configure a tunnel.

To add an ISATAP tunnel:

STEP 1 Choose **Networking** > **IPv6** > **ISATAP Tunnels**.

STEP 2 Click **Add**.

STEP 3 Enter the ISATAP subnet prefix. This is the 64-bit subnet prefix that is assigned to the logical ISATAP subnet for this intranet. This can be obtained from your ISP or internet registry, or derived from RFC 4193.

STEP 4 Choose the local endpoint address, or the endpoint address for the tunnel that starts with the Cisco RV220W. The endpoint can be the LAN interface (if the LAN is configured as an IPv4 network), or a choose Other IP to specify a LAN IPv4 address.

STEP 5 If you chose an endpoint other than the LAN interface in Step 4, enter the IPv4 address of the endpoint.

STEP 6 Click **Save**.

Configuring Router Advertisement

The Router Advertisement Daemon (RADVD) on the Cisco RV220W listens for router solicitations in the IPv6 LAN and responds with router advertisements as required. This is stateless IPv6 auto configuration, and the Cisco RV220W distributes IPv6 prefixes to all nodes on the network.

To configure the RADVD:

STEP 1 Choose **Networking** > **IPv6** > **Router Advertisement**.

STEP 2 Under RADVD Status, choose **Enable**.

STEP 3 Under Advertise Mode, choose one of the following:

- **Unsolicited Multicast**—Select this option to send Router Advertisements (RAs) to all interfaces belonging to the multicast group.
- **Unicast only**—Select this option to restrict advertisements to well-known IPv6 addresses only (RAs are sent to the interface belonging to the known address only).

STEP 4 If you chose Unsolicited Multicast in Step 3, enter the advertise interval. The advertise interval is a random value between the Minimum Router Advertisement Interval and Maximum Router Advertisement Interval. (MinRtrAdvInterval = 0.33 * MaxRtrAdvInterval.) The default is 30 seconds.

STEP 5 Under RA Flags, check **Managed** to use the administered/stateful protocol for address auto configuration. Check **Other** to use the administered/stateful protocol of other, non-address information auto configuration.

STEP 6 Under router preference, choose **Low**, **Medium**, or **High**. The router preference provides a preference metric for default routers.

The low, medium and high values are signaled in unused bits in Router Advertisement messages. This extension is backward compatible, both for routers (setting the router preference value) and hosts (interpreting the router preference value).

These values are ignored by hosts that do not implement router preference. This feature is useful if there are other RADVD-enabled devices on the LAN. The default is high.

STEP 7 Enter the MTU size. The MTU is the size of the largest packet that can be sent over the network. The MTU is used in RAs to ensure all nodes on the network use the same MTU value when the LAN MTU is not well-known. The default is 1500 bytes.

STEP 8 Enter the router life time value, or the time in seconds that the advertisement messages will exist on the route. The default is 3600 seconds.

STEP 9 Click **Save**.

To configure the RADVD available prefixes:

STEP 1 Choose **Networking** > **IPv6** > **Advertisement Prefixes.**

STEP 2 Click **Add.**

STEP 3 Choose the IPv6 Prefix Type:

- **6to4**—6to4 is a system that allows IPv6 packets to be transmitted over an IPv4 network. It is used when an end user wants to connect to the IPv6 Internet using their existing IPv4 connection.

- **Global/ISATAP**—By using ISATAP, you can integrate IPv6 traffic into a IPv4 network environment. ISATAP uses a locally assigned IPv4 address to create a 64-bit interface identifier for IPv6.

STEP 4 If you chose 6to4 in Step 3, enter the Site-Level Aggregation identifier (SLA ID.) The SLA ID in the 6to4 address prefix is set to the interface ID of the interface on which the advertisements are sent.

If you chose Global/Local/ISATAP in Step 3, enter the IPv6 prefix and prefix length. The IPv6 prefix specifies the IPv6 network address. The prefix length variable is a decimal value that indicates the number of contiguous, higher-order bits of the address that make up the network portion of the address.

STEP 5 Enter the prefix lifetime, or the length of time over which the requesting router is allowed to use the prefix.

STEP 6 Click **Save**.

3

Configuring the Wireless Network

This chapter describes how to configure your wireless network and includes the following sections:

- **About Wireless Security, page 63**
- **Understanding the Cisco RV220W's Wireless Networks, page 66**
- **Configuring Wireless Profiles, page 66**
- **Configuring Access Points, page 70**
- **Configuring the Wireless Radio Properties, page 74**
- **Configuring a Wireless Distribution System, page 77**

About Wireless Security

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

- **Wireless Security Tips, page 64**
- **General Network Security Guidelines, page 65**

Wireless Security Tips

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

- Change the default wireless network name or SSID

  Wireless devices have a default wireless network name or Service Set Identifier (SSID) set by the factory. This is the name of your wireless network, and can be up to 32 characters in length.

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

  See **Configuring Wireless Profiles, page 66**.

- Change the default password

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

  See **Configuring Wireless Profiles, page 66**.

- Enable MAC address filtering

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

  See **Using MAC Filtering, page 72**.

- Enable encryption

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

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

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

  See **Configuring Wireless Profiles, page 66**.

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

General Network Security Guidelines

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

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

Understanding the Cisco RV220W's Wireless Networks

The RV220W Wireless N Network Security Firewall provides four SSIDs or Virtual Access Points (VAPs). These networks can be configured and enabled with individual settings.

You can set up multiple networks to segment the network traffic, to allow different levels of access, such as guest access, or to allow access for different functions such as accounting, billing, and so on.

You can further customize wireless access by creating profiles. A profile is a set of generic wireless settings that can be shared across multiple APs. Profiles allow you to easily duplicate SSIDs, security settings, encryption methods, and client authentication for multiple APs.

Configuring Wireless Profiles

A profile is a set of generic wireless settings that can be shared across multiple APs. You can create multiple profiles on the Cisco RV220W, but only one profile is assigned to each AP at a time.

⚠ **CAUTION** The Cisco RV220W provides four default wireless profiles. **Even if you are not going to create custom profiles, at a minimum, you should edit the default profiles to enable wireless security.** See **About Wireless Security, page 63**.

To configure wireless profiles:

STEP 1 Choose **Wireless** > **AP Profiles**.

STEP 2 In the **Profiles** Table, either click **Add** to add a new profile, or check the box in the row of an existing profile and click **Edit**.

STEP 3 If creating a new profile, enter a unique name to identify the profile.

STEP 4 In the SSID field, enter a unique name for this wireless network. Include up to 32 characters, using any of the characters on the keyboard. For added security, you should change the default value to a unique name.

STEP 5 Check the **Broadcast SSID** box if you want to allow all wireless clients within range to be able to detect this wireless network when they are scanning the local area for available networks. Disable this feature if you do not want to make the SSID known. When this feature is disabled, wireless users can connect to your wireless network only if they know the SSID (and provide the required security credentials).

STEP 6 In the Security field, select the type of security. All devices on your network must use the same security mode and settings to work correctly. Cisco recommends using the highest level of security that is supported by the devices in your network.

- **Disabled**—Any device can connect to the network. **Not recommended.**
- **Wired Equivalent Privacy (WEP)**— Weak security with a basic encryption method that is not as secure as WPA. WEP may be required if your network devices do not support WPA; however, it is not recommended.
- **Wi-Fi Protected Access (WPA) Personal**—WPA is part of the wireless security standard (802.11i) standardized by the Wi-Fi Alliance and was intended as an intermediate measure to take the place of WEP while the 802.11i standard was being prepared. It supports TKIP/AES encryption. The personal authentication is the Preshared Key (PSK) that is an alphanumeric passphrase shared with the wireless peer.
- **WPA Enterprise**—Allows you to use WPA with RADIUS server authentication.
- **WPA2 Personal**—WPA2 is the implementation of security standard specified in the final 802.11i standard. It supports AES encryption and this option uses PSK based authentication.
- **WPA2 Personal Mixed**—Allows both WPA and WPA2 clients to connect simultaneously using PSK authentication.
- **WPA2 Enterprise**—Allows you to use WPA2 with RADIUS server authentication.
- **WPA2 Enterprise Mixed**—Allows both WPA and WPA2 clients to connect simultaneously using RADIUS authentication.

STEP 7 Perform the following steps based on the type of encryption you chose in Step 6:

WPA Personal, WPA2 Personal, or WPA2 Personal Mixed

- **WPA Password**—Enter the pre-shared key for WPA/WPA2 PSK authentication. The clients also need to be configured with the same password.

WPA Enterprise, WPA2 Enterprise, or WPA2 Enterprise Mixed

You must first configure RADIUS settings. See **Using the Cisco RV220W With a RADIUS Server, page 130**.

NOTE The word Enterprise indicates the use of an authentication server such as Radius for authenticating wireless clients. WPA2 Enterprise Mixed means that both WPA2 Enterprise and WPA Enterprise are supported.

WEP

In the WEP Index and Keys section:

a. In the Authentication field, choose **Open System** or **Shared Key**. In both cases, the wireless client must provide the correct shared key (password) in order to access the wireless network.

b. Select the encryption type (**64-** or **128-bit**). The larger size keys provide stronger encryption, making the key more difficult to crack (for example, 64-bit WEP has a 40-bit key which is less secure than the 128-bit WEP, which has a 104-bit key).

c. (Optional) In the WEP passphrase field, enter an alphanumeric phrase (longer than eight characters for optimal security) and click **Generate Key** to generate four unique WEP keys in the WEP Key fields below.

d. Select one of the four to use as the shared key that devices must have in order to use the wireless network. If you did not generate a key in Step c, enter a key directly into the WEP Key field. The length of the key should be 5 ASCII characters (or 10 hexadecimal characters) for 64-bit WEP and 13 ASCII characters (or 26 hexadecimal characters) for 128-bit WEP. Valid hexadecimal characters are “0” to “9” and “A” to “F”.

STEP 8 Click **Save**.

Configuring the Group Key Refresh Interval

If you configure WPA or WPA2 security, you can specify the timeout interval after which group keys are generated:

STEP 1 Choose **Wireless** > **AP Profile.**

STEP 2 Check the box in the row of the profile you want to configure and click **Advanced Configuration.**

STEP 3 Enter the group key refresh interval, in seconds.

STEP 4 Click **Save.**

Configuring RADIUS Authentication Parameters

In WPA2 security, Pairwise Master Key Security Association (PMKSA) caching is used to store the master keys derived from successful RADIUS authentication. A client reconnecting within this interval (after successful RADIUS authentication) can skip the RADIUS authentication. This feature prevents a long RADIUS authentication process every time a client connects.

To configure:

STEP 1 Choose **Wireless** > **AP Profile.**

STEP 2 Check the box in the row of the profile you want to configure and click **Advanced Configuration.**

STEP 3 Specify the number of seconds that the master keys are stored in the AP.

STEP 4 In the 802.1X re-authentication interval field, enter the timeout interval (in seconds) after which the AP should re-authenticate with the RADIUS server.

STEP 5 Click **Save.**

Configuring Wi-Fi Multimedia

Wi-Fi Multimedia (WMM) allows you to assign different processing priorities to different types of traffic. You can configure QoS settings to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow.

To configure WMM:

STEP 1 Choose **Wireless** > **AP Profiles**.

STEP 2 Check the box in the row of the profile you want to configure and click **WMM**.

STEP 3 Next to WMM, check the **Enable** box to enable QoS for this profile.

When this feature is enabled, the specified Default Class of Service Priority (DSCP) is applied to the entries in the **DSCP to Queue Table**. This table helps map the IP ToS values to the WMM queues.

Configuring this table will help the security device in reading the ToS bits in the IP packet and perform queuing based on the QoS policy selected.

STEP 4 Click **Save** to save the settings.

Configuring Access Points

To configure the APs, choose **Wireless** > **AP Profiles**. The four APs are displayed in the **Access Points Table**.

Enabling or Disabling APs

An AP can be disabled if not in use and enabled when needed. Disabling an AP does not delete the configuration, but removes it from availability. Enabling the AP creates a wireless network, where computers and other devices can join and communicate with the devices connected to the AP or other devices on the Local Area Network (LAN).

To enable or disable an AP:

STEP 1 Choose **Wireless** > **AP Profiles.**

STEP 2 In the **Access Points Table**, check the box in the row of the AP and click **Enable** or **Disable.** You can enable or disable multiple APs at one time by checking multiple boxes.

Editing an AP's Properties

You can edit properties for an AP to make it only available at certain times of the day, restrict the number of endpoints that can use the AP, or separate the AP from the other wireless networks in the Cisco RV220W.

To edit the properties of an access point:

STEP 1 Choose **Wireless** > **AP Profiles.**

STEP 2 Check the box in the row of the AP that you want to edit.

STEP 3 Associate a profile with this AP by choosing the profile from the Profile Name list. The profile controls the name and security settings for the AP. See **Configuring the Wireless Radio Properties, page 74**.

STEP 4 (Optional) To configure the AP to be active only during a certain time of day, check the **Active Time** box. Enter the start and stop times (hours, minutes, and AM/PM).

STEP 5 In the **Max Associated Clients** field, enter the maximum number of endpoints that can use this AP. The default value is 20. You can change this number if you want to restrict traffic on the network to prevent it from being overloaded, for example.

STEP 6 (Optional) Check the **AP Isolation** check box to separate this AP into its own network.

This feature enforces wireless isolation within the SSID. When this feature is enabled on the SSID, all connected WLAN clients via the SSID cannot communicate or ping each other.

STEP 7 Click **Save.**

Using MAC Filtering

You can use MAC filtering to permit or deny access to the wireless network based on the MAC (hardware) address of the requesting device. For example, you can enter the MAC addresses of a set of PCs and only allow those PCs to access the network. MAC filtering is configured for each AP.

To configure MAC filtering:

STEP 1 Choose **Wireless** > **AP Profiles.**

STEP 2 Check the box in the row of the AP for which you want to configure MAC filtering and click **MAC Filter.**

STEP 3 In the MAC Filtering Status field, choose one of the following:

- **Disabled**—MAC filtering is not enabled for this AP.
- **Allow**—Access to the network is only allowed to endpoints with specified MAC addresses.
- **Deny**—Access to the network is denied to endpoints with specified MAC addresses, but open to all others.

STEP 4 If you chose **Allow** or **Deny** in Step 3, click **Save**.

STEP 5 In the **MAC Address Table**, check the box next to MAC Address and click **Add.**

STEP 6 Enter the MAC Address of the client to allow or deny and click **Save.**

The address is added to the table. Repeat this step for all the clients you want to allow or deny.

STEP 7 Click **Save** again.

Viewing AP Status

You can view statistics about each AP, including connected clients (endpoints), data transmitted and received, errors, and other information.

To view the AP status:

STEP 1 Choose **Wireless** > **AP Profiles.**

STEP 2 In the **Access Points Table**, check the box in the row of the AP for which you want to view statistics and click **Status**.

STEP 3 The following statistics are displayed:

- **AP Name**—Name of the AP whose statistics are being displayed.
- **Radio**—Wireless radio number on which the AP is configured.
- **Packets**—Number of wireless packets transmitted and received.
- **Bytes**—Number of bytes of information transmitted and received.
- **Errors**—Number of transmitted and received packet errors reported to the AP.
- **Dropped**—Number of transmitted and received packets dropped by the AP.
- **Multicast**—Number of multicast packets sent over this AP.
- **Collisions**—Number of packet collisions reported to the AP.
- **Connected Clients**—Lists clients currently connected to the selected AP.
  - **MAC Address**—The unique identifier of the client connected to the AP.
  - **Radio**—Wireless radio number on which AP is configured and to which the client is associated.
  - **Security**—Security method employed by the client to connect to this AP.
  - **Encryption**—Encryption method employed by the client to connect to this AP.
  - **Authentication**—Authentication mechanism employed by this connection.
  - **Time Connected**—Time (in minutes) since the connection was established between the AP and client.

STEP 4 The Poll Seconds displays the interval at which statistics are shown if the page is on “automatic refresh.” The default is 10 seconds, which can be changed from 1 to 60 seconds. To cause the page to automatically refresh, click **Start**. To stop the page from refreshing, click **Stop**.

Configuring the Wireless Radio Properties

You can configure radio card properties, including the wireless standard (for example, 802.11n or 802.11g) on the Cisco RV220W.

Configuring Basic Wireless Radio Settings

STEP 1 Choose **Wireless** > **Radio Settings** > **Radio Settings**.

STEP 2 Choose the operating frequency of the radio: 2.4GHz or 5GHz.

STEP 3 Select the **Wireless Network Mode**:

If you chose 2.4GHZ:

- **B/G-Mixed**—Select this mode if you have devices in the network that support 802.11b and 802.11g.
- **G Only**—Select this mode if all devices in the wireless network support 802.11g.
- **G/N-Mixed**—Select this mode if you have devices in the network that support 802.11g and 802.11n.
- **N Only**—Select this mode if all devices in the wireless network support 802.11n.

If you chose 5GHz:

- **A Only**—Select this mode if all devices in the wireless network support 802.11a.
- **A/N-Mixed**—Select this mode to allow 802.11n and 802.11a clients to connect to this AP.
- **N Only**—Select this mode if all devices in the wireless network can support 802.11n.

STEP 4 From the **Channel Bandwidth** drop-down menu, choose the channel bandwidth. Available choices depend on the wireless network mode chosen in Step 2. Choosing **Auto** represents 20/40 MHz.

STEP 5 The control sideband field defines the sideband which is used for the secondary or extension channel when the AP is operating in 40 Mhz channel width. Choose **lower** or **upper**. The signal components above the carrier frequency constitute the upper sideband (USB) and those below the carrier frequency constitute the lower sideband (LSB).

STEP 6 The channel field specifies the frequency that the radio uses to transmit wireless frames. Select a channel from the list of channels or choose **auto** to let the Cisco RV220W determine the best channel to use based on the environment noise levels for the available channels.

> **NOTE** The Radar Detected On field is a read-only field that displays a list of all the 5GHz channels on which a radar has been detected. We recommend that you do not to configure a channel present on this list.

STEP 7 In the **Default Transmit Power** field, enter a value in dBm that is the default transmitted power level for all APs that use this radio.

STEP 8 Click **Save**.

.

Configuring Advanced Wireless Radio Settings

STEP 1 Choose **Wireless** > **Radio Settings** > **Radio Settings.**

STEP 2 In the **Beacon Interval** field, enter the time in milliseconds between beacon transmissions. The default interval is 100 milliseconds.

STEP 3 In the **DTIM interval** field, enter the interval at which the delivery traffic indication message should be sent. A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Cisco RV220W has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages.The default interval is 2 beacon intervals.

STEP 4 The **Request to Send (RTS) Threshold** is the packet size, in bytes, that requires the AP to check the transmitting frames to determine if an RTS/Clear to Send (CTS) handshake is required with the receiving client. Using a small value causes RTS packets to be sent more often, consuming more of the available bandwidth, reducing the apparent throughput of the network packets. The default value is 2346, which effectively disables RTS.

STEP 5 The **Fragmentation Threshold** is the maximum length of the frame, in bytes, beyond which packets must be fragmented into two or more frames. Collisions occur more often for long frames because while sending them, they occupy the channel for a longer time. The default value is 2346, which effectively disables fragmentation. If you experience a high packet error rate, you can slightly increase the fragmentation threshold; setting the fragmentation threshold too low may result in poor network performance. Only minor reduction of the default value is recommended.

STEP 6 Choose the **Preamble Mode**. The 802.11b standard requires that a preamble be appended to every frame before it is transmitted through the air. The preamble may be either the traditional “long” preamble, which requires 192 μs for transmission, or it may be an optional “short” preamble that requires only 96 μs. A long preamble is needed for compatibility with the legacy 802.11 systems operating at 1 and 2 Mbps. The default selection is long.

STEP 7 Choose the **Protection Mode**. Select **None** (the default) to turn off CTS. The **CTS-to-Self Protection** option enables the CTS-to-Self protection mechanism, which is used to minimize collisions among stations in a mixed 802.11b and 802.11g environment. This function boosts the Cisco RV220W’s ability to catch all wireless transmissions but severely decreases performance.

STEP 8 (Optional) Next to **U-APSD**, check the **Enable** box to enable the Unscheduled Automatic Power Save Delivery (also referred to as WMM Power Save) feature that allows the radio to conserve power.

STEP 9 The **Short Retry Limit** and **Long Retry Limit** fields determine the number of times the AP will reattempt a frame transmission that fails. The limit applies to both long and short frames of a size less than or equal to the RTS threshold.

STEP 10 Click **Save**.

Configuring a Wireless Distribution System

A Wireless Distribution System (WDS) is a system that enables the wireless interconnection of access points in a network. It allows a wireless network to be expanded using multiple access points without the need for a wired backbone to link them.

WDS peers are other access points in the network connected using WDS. You must configure all WDS peers to use the same operating frequency (2.4 or 5 GHz), wireless network mode, channel, and security encryption (none, WEP, WPA, or WPA2) with the exact same WPA password (preshared key) on the first SSID—other SSIDs cannot be used for communicating with WDS peers.

NOTE WDS links are established based on the first SSID configuration between RV220W and RV120W. Make sure that all WDS peers are configured to use the same security encryption type. RV220W supports up to 3 WDS peers.

NOTE WDS works with only RV120W and RV220W.

To configure a WDS:

STEP 1 Choose **Wireless** > **WDS**.

STEP 2 Check the **Enable** box to enable WDS in the Cisco RV220W.

STEP 3 Enter a WPA password for authentication.

STEP 4 Click **Save**.

You can manually add WDS peers that can connect to the Cisco RV220W:

STEP 1 In the **WDS Peers Table**, click **Add**.

STEP 2 Enter the MAC (hardware) address of the WDS peer and click **Save**.

4

Configuring the Firewall

This chapter contains information about configuring the firewall properties of the RV220W and includes the following sections:

- Cisco RV220W Firewall Features, page 78
- Configuring Basic Firewall Settings, page 80
- Configuring Firewall Rules, page 84
- Creating Firewall Schedules, page 90
- Blocking and Filtering Content and Applications, page 91
- Configuring Port Triggering, page 95
- Configuring Remote Management, page 97
- Configuring One-to-One Network Address Translation, page 98
- Using Cisco ProtectLink Web, page 99

Cisco RV220W Firewall Features

You can secure your network by creating and applying rules that the Cisco RV220W uses to selectively block and allow inbound and outbound Internet traffic. You then specify how and to what devices the rules apply. To do so, you must define the following:

- Services or traffic types (examples: web browsing, VoIP, other standard services and also custom services that you define) that the router should allow or block.
- Direction for the traffic by specifying the source and destination of traffic; this is done by specifying the "From Zone" (LAN/WAN/DMZ) and "To Zone" (LAN/WAN/DMZ).
- Schedules as to when the router should apply rules.

- Keywords (in a domain name or on a URL of a web page) that the router should allow or block.
- Rules for allowing or blocking inbound and outbound Internet traffic for specified services on specified schedules.
- MAC addresses of devices whose inbound access to your network the router should block.
- Port triggers that signal the router to allow or block access to specified services as defined by port number.
- Reports and alerts that you want the router to send to you.

You can, for example, establish restricted-access policies based on time-of-day, web addresses, and web address keywords. You can block Internet access by applications and services on the LAN, such as chat rooms or games. You can block just certain groups of PCs on your network from being accessed by the WAN or public DMZ network.

Inbound (WAN to LAN/DMZ) rules restrict access to traffic entering your network, selectively allowing only specific outside users to access specific local resources. By default, all access from the insecure WAN side is blocked from accessing the secure LAN, except in response to requests from the LAN or DMZ. To allow outside devices to access services on the secure LAN, you must create a firewall rule for each service.

If you want to allow incoming traffic, you must make the router's WAN port IP address known to the public. This is called “exposing your host.” How you make your address known depends on how the WAN ports are configured; for the Cisco RV220W, you may use the IP address if a static address is assigned to the WAN port, or if your WAN address is dynamic, a DDNS (Dynamic DNS) name can be used.

Outbound (LAN/DMZ to WAN) rules restrict access to traffic leaving your network, selectively allowing only specific local users to access specific outside resources. The default outbound rule is to allow access from the secure zone (LAN) to either the public DMZ or insecure WAN. To block hosts on the secure LAN from accessing services on the outside (insecure WAN), you must create a firewall rule for each service.

Configuring Basic Firewall Settings

To configure basic firewall settings, choose **Firewall** > **Basic Settings.** You can configure the following firewall settings.

- **Protecting from Attacks, page 80**
- **Configuring Universal Plug and Play, page 81**
- **Enabling Session Initiation Protocol Application-Level Gateway, page 83**
- **Configuring the Default Outbound Policy, page 83**

Protecting from Attacks

Attacks are malicious security breaches or unintentional network issues that render the Cisco RV220W unusable. Attack checks allow you to manage WAN security threats such as continual ping requests and discovery via ARP scans. TCP and UDP flood attack checks can be enabled to manage extreme usage of WAN resources.

As well, certain Denial-of-Service (DoS) attacks can be blocked. These attacks, if uninhibited, can use up processing power and bandwidth and prevent regular network services from running normally. ICMP packet flooding, SYN traffic flooding, and Echo storm thresholds can be configured to temporarily suspect traffic from the offending source.

To protect your network from attacks:

STEP 1 Choose **Firewall** > **Basic Settings** > **Attack Checks.**

STEP 2 Check the boxes to enable the following functions:

WAN Security

- **Respond to Ping on the Internet—**To configure the Cisco RV220W to allow a response to an Internet Control Message Protocol (ICMP) Echo (ping) request on the WAN interface, check the **Enable** box. This setting is used as a diagnostic tool for connectivity problems. Not enabled by default.
- **Stealth Mode—**If Stealth Mode is enabled, the router will not respond to port scans from the WAN. This feature makes the network less susceptible to discovery and attacks. Enabled by default.

- **Block TCP Flood**— If this option is enabled, the router will drop all invalid TCP packets. This feature protects the network from a SYN flood attack. Enabled by default.

LAN Security

- **Block UDP Flood**—If this option is enabled, the router does not accept more than 150 simultaneous connections from a single IP address. Enabled by default.

International Computer Security Association (ICSA) Settings

- **Block ICMP Notification**—ICSA requires the firewall to silently block without sending an ICMP notification to the sender. Some protocols, such as MTU Path Discovery, require ICMP notifications. Enable this setting to operate in “stealth” mode. Enabled by default.
- **Block Fragmented Packets**—ICSA requires the firewall to block fragmented packets from ANY to ANY. Enabled by default.
- **Block Multicast Packets**—ICSA requires the firewall to block multicast packets. Enabled by default.

STEP 3 Click **Save**.

Configuring Universal Plug and Play

Universal Plug and Play (UPnP) is a feature that allows for automatic discovery of devices that can communicate with the Cisco RV220W.

To enable UPnP:

STEP 1 Choose **Firewall** > **Basic Settings** > **UPnP**.

STEP 2 Check the **Enable** box. If disabled, the Cisco RV220W does not allow automatic device configuration.

STEP 3 In the LAN field, select the LAN or VLAN on which you want to allow UPnP.

STEP 4 In the **Advertisement Period** field, enter the period (in seconds) to specify how often the Cisco RV220W will broadcast its UPnP information to all devices within range.

STEP 5 In the **Advertisement Time to Live** field, enter the number of hops to allow for each UPnP packet. This setting determines how long a packet is allowed to propagate before being discarded. Small values will limit the UPnP broadcast range.

STEP 6 Click **Save**.

Viewing UPnP Information

To view UPnP information:

STEP 1 Choose **Firewall** > **Basic Settings** > **UPnP**.

STEP 2 The **UPnP Portmap Table** shows IP addresses and other settings of UPnP devices that have accessed the Cisco RV220W. It includes the following fields:

- **Active**—Indicates whether or not the port of the UPnP device that established a connection is currently active: Yes or No.
- **Protocol**—The network protocol (that is, HTTP, FTP, and so on) that the device is using to connect to the Cisco RV220W.
- **Internal Port**—Indicates which, if any, internal ports are opened by the UPnP device.
- **External Port**—Indicates which, if any, external ports are opened by the UPnP device.
- **IP Address**—The IP address of the UPnP device that is accessing the Cisco RV220W.

STEP 3 Click **Refresh** to refresh the portmap table and search for any new UPnP devices.

Enabling Session Initiation Protocol Application-Level Gateway

Session Initiation Protocol Application-Level Gateway (SIP ALG) can rewrite information within SIP messages (SIP headers and SDP body) making signaling and audio traffic possible between a client behind Network Address Translation (NAT) and the SIP endpoint.

To enable SIP ALG:

STEP 1 Choose **Firewall** > **Basic Settings** > **SIP ALG**.

STEP 2 Check the **Enable** box to enable SIP ALG support. If disabled, the router will not allow incoming calls to the UAC (User Agent Client) behind the Cisco RV220W.

STEP 3 Click **Save**.

Configuring the Default Outbound Policy

The **Firewall Settings** page allows the user to configure the default outbound policy for the traffic that is directed from the secure network (LAN) to the non-secure network (dedicated WAN/optional). The default inbound policy for traffic flowing from the non-secure zone to the secure zone is always blocked and cannot be changed.

To configure the default outbound policy:

STEP 1 Choose **Firewall** > **Access Control** > **Default Outbound Policy.**

STEP 2 In the IPv4 field, select one of the following:

- **Always Allow**—Always allow traffic from the secure to the non-secure network.
- **Always Block—**Always block traffic from the secure to the non-secure network.

STEP 3 Click **Save**.

Configuring Firewall Rules

All configured firewall rules on the Cisco RV220W are displayed in the Firewall Rules list. This list also indicates whether the rule is enabled (active), and gives a summary of the "from/to" zone as well as the services and users the rule affects.

Creating a Firewall Rule

To create firewall rules:

STEP 1 Choose **Firewall** > **Access Control** > **IPv4 Rules.**

STEP 2 Click **Add.**

STEP 3 In the **From Zone** field, choose the source of originating traffic:

- **Trusted (LAN)**—Choose if traffic will originate from the secure LAN.
- **Untrusted (WAN)**—Choose this option to create an inbound rule.

STEP 4 Choose the **To Zone** to configure the destination of traffic covered by this rule. If the From Zone is the WAN, the To Zone can be the public DMZ or secure LAN. If the From Zone is the LAN, then the To Zone can be only the insecure WAN.

STEP 5 Choose the service to allow or block for this rule. Choose **Any** to allow the rule to apply to all applications and services, or you can choose a single application to block:

- AIM (AOL Instant Messenger)
- BGP (Border Gateway Control)
- BOOT_P (Bootstrap Protocol) client
- BOOT_P Server
- CU-SeeMe (videoconferencing) UDP or TCP
- Domain Name System (DNS), UDP or TCP
- Finger
- File Transfer Protocol (FTP)
- Hyptertext Transfer Protocol (HTTP)
- Secure Hypertext Transfer Protocol (HTTPS)

- Internet Control Message Protocol (ICMP) type 3 through 11 or 13
- ICQ (chat)
- Internet Message Access Protocol (IMAP) 2 or 3
- Internet Relay Chat (IRC)
- News
- PING
- Post Office Protocol (POP3)
- Point-to-Point Tunneling Protocol (PPTP)
- RCMD (command)
- Real Audio
- Remote execution command (REXEC)
- Remote login commend (RLOGIN)
- Remote Telnet (RTELNET)
- Real-Time Streaming Protocol (RTSP) TCP or UDP
- Secure Shell File Transfer Protocol (SFTP)
- Simple Mail Transfer Protocol (SMTP)
- Simple Network Management Protocol (SNMP) TCP or UDP
- SNMP Traps (TCP or UDP)
- Structured Query Language (SQL)*Net (Oracle)
- SSH (TCP or UDP)
- STRMWORKS
- Terminal Access Controller Access-Control System (TACACS)
- Telnet (command)
- Trivial File Transfer Protocol (TFTP)
- Routing Information Protocol (RIP)
- IKE
- Simple HTTPD web server

- UDP Encapsulation of IPsec packets (IPSEC-UDP-ENCAP)
- IDENT protocol
- VDOLive (web video delivery)

- SSH
- SIP-TCP

STEP 6 Choose the action:

- **Always Block**—Always block the selected type of traffic.
- **Always Allow**—Never block the selected type of traffic.
- **Block by Schedule, otherwise Allow**—Blocks the selected type of traffic according to a schedule. See **Creating Firewall Schedules, page 90**.
- **Allow by Schedule, otherwise Block**—Allows the selected type of traffic according to a schedule. See **Creating Firewall Schedules, page 90**.

STEP 7 In the **Source Hosts** field, select the users to which the firewall rule applies:

- **Any**—The rule applies to traffic originating on any host in the local network.
- **Single Address**—The rule applies to traffic originating on a single IP address in the local network. Enter the address in the **From** field.
- **Address Range**—The rule applies to traffic originating from an IP address located in a range of addresses. Enter the starting IP address in the **From** field, and the ending IP address in the **To** field.

STEP 8 In the **Destination Hosts** field, select the users to which the firewall rule applies:

- **Any**—The rule applies to traffic going to any host in the local network.
- **Single Address**—The rule applies to traffic going to a single IP address in the network. Enter the address in the **From** field.
- **Address Range**—The rule applies to traffic going to an IP address located in a range of addresses. Enter the starting IP address in the **From** field, and the ending IP address in the **To** field.

STEP 9 In the **Log** field, specify whether or not the packets for this rule should be logged. To log details for all packets that match this rule, select **Always**. For example, if an outbound rule for a schedule is selected as **Block Always**, then for every packet that tries to make an outbound connection for that service, a message with the packet's source address and destination address (and other information) is recorded in the log. Enabling logging may generate a significant volume of log messages and is recommended for debugging purposes only. Select **Never** to disable logging.

STEP 10 When traffic is going from the LAN or DMZ to the WAN, the system requires rewriting the source or destination IP address of incoming IP packets as they pass through the firewall. In the **SNAT IP Type** field, choose **WAN Interface Address** or choose Single Address and enter the Single IP Address in the SNAT IP field.

STEP 11 In the **QoS Priority** field, assign a priority to IP packets of this service. The priorities are defined by "Type of Service (ToS) in the Internet Protocol Suite" standards, RFC 1349. The gateway marks the Type Of Service (ToS) field as defined below:

- **Normal-Service**—No special priority is given to the traffic. The IP packets for services with this priority are marked with a ToS value of 0.
- **Minimize-Cost**—Choose this option when data must be transferred over a link that has a lower "cost." The IP packets for services with this priority are marked with a ToS value of 2.
- **Maximize-Reliability**—Choose this option when data needs to travel to the destination over a reliable link and with little or no retransmission. The IP packets for services with this priority are marked with a ToS value of 4.
- **Maximize-Throughput**—Choose this option when the volume of data transferred during an interval is important even if the latency over the link is high. The IP packets for services with this priority are marked with a ToS value of 8.
- **Minimize-Delay**—Choose this option when the time required (latency) for the packet to reach the destination must be low. The IP packets for services with this priority are marked with a ToS value of 16.

STEP 12 When the traffic is coming from the WAN to the DMZ or the LAN, Destination Network Address Translation maps a public IP address (your Dedicated WAN address, Optional WAN address, or another address) to an IP address on your private network. Enter the following:

- **Send to Local Server (DNAT IP)**—Specify an IP address of a machine on the Local Network which is hosting the server.
- (Optional) Next to **Port Forwarding**, check **Enable** to enable port forwarding to the port that you specify in the Translate Port Number field. This will allow traffic from the Internet to reach the appropriate LAN port via a port forwarding rule.
- **Translate Port Number**—Enter the port number to use for port forwarding. For example, if a machine on the Local Network side is running a telnet server on port 2000, then enable **Port Forwarding** and enter 2000 in the Translate Port Number field. If the server is listening on the default port 23, then the box can be left unchecked.

- **Internet Destination**—Select the type of destination that is used for this firewall rule: Dedicated WAN, Optional WAN, or Other. If you choose Other, enter the WAN IP address that will map to the internal server in the Other IP Address field.

  This gateway supports multi-NAT, and the Internet Destination IP address does not necessarily have to be the WAN address. On a single WAN interface, multiple public IP addresses are supported. If your ISP assigns you more than one public IP address, one of these can be used as your primary IP address on the WAN port, and the others can be assigned to servers on the LAN or DMZ.   In this way, the LAN/DMZ server can be accessed from the internet by its aliased public IP address.

STEP 13 Click **Save**.

Managing Firewall Rules

Choose **Firewall** > **Access Control** > **IPv4 Firewall Rules.**

To enable or disable a rule, check the box next to the rule in the list of firewall rules and choose **Enable** or **Disable**.

To delete a rule, check the box next to the rule and click **Delete**.

To reorder rules, check the box next to a rule and click **Up** or **Down**. The Cisco RV220W applies rules in the order listed. You should usually move the strictest rules (those with the most specific services or addresses) to the top of the list.

Creating Custom Services

When you create a firewall rule, you can specify a service that is controlled by the rule. Common types of services are available for selection, and you can create your own custom services. This page allows creation of custom services against which firewall rules can be defined. Once defined, the new service will appear in the **List of Available Custom Services Table**.

To create a custom service:

STEP 1 Choose **Firewall** > **Access Control** > **Custom Services**.

STEP 2 Click **Add**.

STEP 3 Enter a service name for identification and management purposes.

STEP 4 Enter the service type, or layer 4 protocol that the service uses (**TCP**, **UDP**, **ICMP**, or **ICMPv6**).

STEP 5 If you chose ICMP or ICMPv6 as the service type, enter the ICMP type. This is a numeric value from 0 through 40 for ICMP and from 0 through 255 for ICMPv6.

STEP 6 In the **Start Port** field, enter the first TCP or UDP port of the range that the service uses.

STEP 7 In the **Finish Port** field, enter the last TCP or UDP port of the range that the service uses.

STEP 8 Click **Save**.

Creating Firewall Schedules

You can create firewall schedules to apply firewall rules on specific days or at specific times of the day.

NOTE The RV220W firewall support only one schedule per computer (host device). Do not attempt to create multiple schedules.

To create a schedule:

STEP 1 Choose **Firewall** > **Access Control** > **Schedules.**

STEP 2 Click **Add**.

STEP 3 Enter a unique name to identify the schedule. This name is then available in the Firewall Rule Configuration page in the "Select Schedule" list. (See **Configuring Firewall Rules, page 84**.)

STEP 4 Under **Scheduled Days**, select whether you want the schedule to apply to all days or specific days. If you choose **Specific Days**, check the box next to the days you want to include in the schedule.

STEP 5 Under **Scheduled Time of Day**, select the time of day that you want the schedule to apply. You can either choose **All Day**, or choose **Specific Time**. If you choose **Specific Time**, enter the start and end times, selecting a.m. or p.m.

STEP 6 Click **Save**.

Blocking and Filtering Content and Applications

The Cisco RV220W supports several content filtering options. You can block certain web applications or components (such as ActiveX or Java). You can set up trusted domains from which to always allow content. You can block access to Internet sites by specifying keywords to block. If these keywords are found in the site's name (for example, web site URL or newsgroup name), the site is blocked.

You also need to turn on content filtering to set up trusted domains.

Blocking Web Applications and Components

STEP 1 Choose **Firewall** > **Access Control** > **Content Filtering**.

STEP 2 Check the **Enable** box.

STEP 3 Certain commonly-used web components can be blocked for increased security. Some of these components can be used by malicious websites to infect computers that access them. With content filtering enabled, select the check box for each component you wish to block:

- **Block Proxy**—A proxy server (or simply, proxy) allows computers to route connections to other computers through the proxy, thus circumventing certain firewall rules. For example, if connections to a specific IP address are blocked by a firewall rule, the requests can be routed through a proxy that is not blocked by the rule, rendering the restriction ineffective. Enabling this feature blocks proxy servers.

- **Block Java**—Blocks java applets from being downloaded from pages that contain them. Java applets are small programs embedded in web pages that enable dynamic functionality of the page. A malicious applet can be used to compromise or infect computers. Enabling this setting blocks Java applets from being downloaded.

- **Block ActiveX**—Similar to Java applets, ActiveX controls are installed on a Windows computer while running Internet Explorer. A malicious ActiveX control can be used to compromise or infect computers. Enabling this setting blocks ActiveX applets from being downloaded.

- **Block Cookies**—Cookies are used to store session information by websites that usually require login. However, several websites use cookies to store tracking information and browsing habits. Enabling this option filters out cookies from being created by a website.

NOTE Many websites require that cookies be accepted in order for the site to be accessed properly. Blocking cookies can cause many websites to not function properly.

STEP 4 Click **Save.**

Adding Trusted Domains

You can add a list of trusted domains, or approved URLs. These domains are bypassed during keyword filtering. For example, if “yahoo” is added to the blocked keywords list and www.yahoo.com is added to the approved URL list, then www.yahoo.com will be allowed, but mail.yahoo.com will not be allowed.

You can also block all URLs except the ones you enter as approved or trusted URLs.

NOTE Before adding trusted domains, you must enable content filtering. See **Blocking Web Applications and Components, page 91**.

To add approved URLs:

STEP 1 Choose **Firewall** > **Access Control** > **Trusted Domains.**

STEP 2 Next to **Approved URLs List**, check **Enable.**

STEP 3 Click **Save.**

STEP 4 (Optional) To block all URLs except the ones you identify as trusted, or allowed, check **Block All URLs by Default**. The RV220W then blocks traffic coming from any sites other than the ones in the **Approved URLs Table**, so use this setting with caution.

STEP 5 In the **Approved URLs Table**, click **Add.**

STEP 6 Enter the Approved URL.

STEP 7 Select the match type:

- **URL Keyword**—A subset of the URL.
- **Web site—**The entire URL.

STEP 8 Click **Save.**

Adding Blocked URLs

NOTE Before adding blocked URLs, you must enable content filtering. See **Blocking Web Applications and Components, page 91**.

STEP 1 Choose **Firewall** > **Access Control** > **Blocked URLs.**

STEP 2 Click **Add.**

STEP 3 Enter the URL to block.

STEP 4 Choose the match type:

- **URL Keywords—**Prevents access to websites that contain the specified characters in the URL.
- **Web site—**Prevents access to websites that contain the specified characters in the web site contents.

STEP 5 Click **Save.**

Configuring MAC Address Filtering

MAC address filtering allows you to block traffic coming from certain known machines or devices. The router uses the MAC address of a computer or device on the network to identify it and block or permit the access. Traffic coming in from a specified MAC address will be filtered depending upon the policy.

To enable MAC address filtering:

STEP 1 Choose **Firewall** > **Access Control** > **MAC Filtering.**

STEP 2 Next to Source MAC Address Filtering, check **Enable** to enable MAC Address Filtering for this device. Uncheck the box to disable this feature.

If you enable MAC filtering, in the Policy for MAC Address listed below field, choose one of the following options:

- **Block and Permit the Rest—**Choose this option to block the traffic from the specified MAC addresses and to allow traffic from all other addresses.
- **Permit and Block the Rest—**Choose this option to permit the traffic from the specified MAC addresses and to block traffic from all other machines on the LAN side of the router.

For example, two computers are on the LAN with MAC addresses of 00:01:02:03:04:05 (host1), and 00:01:02:03:04:11 (host2). If the host1 MAC address is added to the MAC filtering list and the “block and permit the rest” policy is chosen, when this computer tries to connect to a website, the router will not allow it to connect. However, host2 is able to connect because its MAC address is not in the list. If the policy is “permit and block the rest,” then host1 is able to connect to a website, but host2 is blocked because its URL is not in the list. The MAC filtering policy does not override a firewall rule that directs incoming traffic to a host.

STEP 3 Click **Save**.

STEP 4 In the **MAC Addresses Table**, click **Add**.

STEP 5 Enter the MAC address to add to the table and click **Save**. Repeat for each address to permit or block.

Configuring IP/MAC Address Binding

IP/MAC Address Binding allows you to bind IP addresses to MAC address. Some machines are configured with static addresses. To prevent users from changing static IP addresses, IP/MAC Binding should be enabled. If the RV220W sees packets with matching IP address but inconsistent MAC addresses, it drops those packets.

To configure IP/MAC Address binding:

STEP 1 Choose **Firewall** > **Access Control** > **IP/MAC Binding**. The table lists all the currently defined IP/MAC binding rules and allows several operations on the rules.

STEP 2 Click **Add** to add a new rule.

STEP 3 In the **Name** field, enter the name for this rule.

STEP 4 In the **MAC Address** field, enter the MAC Address (the physical address of the piece of hardware) for this rule.

STEP 5 In the **IP Address** field, enter the IP Address to assign to the piece of hardware.

STEP 6 In the **Log Dropped Packets** field, choose if you want to log the dropped packets. Choosing **Enable** logs the dropped packets; choosing **Disable** does not log the dropped packets. Logs can be viewed in **Status** > **View All Logs** page.

Configuring Port Triggering

Port triggering allows devices on the LAN or DMZ to request one or more ports to be forwarded to them. Port triggering waits for an outbound request from the LAN/ DMZ on one of the defined outgoing ports, and then opens an incoming port for that specified type of traffic. Port triggering is a form of dynamic port forwarding while an application is transmitting data over the opened outgoing or incoming ports.

Port triggering opens an incoming port for a specific type of traffic on a defined outgoing port.

Port triggering is more flexible than static port forwarding (available when configuring firewall rules) because a rule does not have to reference a specific LAN IP or IP range. Ports are also not left open when not in use, thereby providing a level of security that port forwarding does not offer.

NOTE Port triggering is not appropriate for servers on the LAN, since there is a dependency on the LAN device making an outgoing connection before incoming ports are opened.

Some applications require that, when external devices connect to them, they receive data on a specific port or range of ports in order to function properly. The router must send all incoming data for that application only on the required port or range of ports. The gateway has a list of common applications and games with corresponding outbound and inbound ports to open. You can also specify a port triggering rule by defining the type of traffic (TCP or UDP) and the range of incoming and outgoing ports to open when enabled.

To add a port triggering rule:

STEP 1 Choose **Firewall** > **Port Triggering.**

STEP 2 Click **Add.**

STEP 3 Specify an easily-identifiable name for this rule.

STEP 4 Check the **Enable** box to enable the rule.

STEP 5 Select whether the port uses TCP or UDP protocol.

STEP 6 In the **Outgoing (Trigger) Port Range** section, specify the port number or range of port numbers that will trigger this rule when a connection request from outgoing traffic is made. If the outgoing connection uses only one port, then specify the same port number in the Start Port and End Port fields.

STEP 7 In the **Incoming (Response) Port Range** section, specify the port number or range of port numbers used by the remote system to respond to the request it receives. If the incoming connection uses only one port, then specify the same port number in the Start Port and End Port fields.

STEP 8 Click **Save**.

Restricting Sessions

You can limit the maximum number of unidentified sessions and half-open sessions on the Cisco RV220W. You can also introduce timeouts for TCP and UDP sessions to ensure Internet traffic is not deviating from expectations in your private network. To configure session settings:

STEP 1 Choose **Firewall** > **Session Settings.** In the **Maximum Unidentified Sessions** field, enter the maximum number of unidentified sessions for the ALG identification process. This value can range from 2 through 128. The default is 32 sessions.

STEP 2 In the **Maximum Half Open Sessions** field, enter the maximum number of half-open sessions. A half-open session is the session state between receipt of a SYN packet and the SYN/ACK packet. Under normal circumstances, a session is allowed to remain in the half-open state for 10 seconds. The maximum value ranges from 0 through 3,000. The default is 128 sessions.

STEP 3 In the **TCP Session Timeout Duration** field, enter the time, in seconds, after which inactive TCP sessions are removed from the session table. Most TCP sessions terminate normally when the RST or FIN flags are detected. This value ranges from 0 through 4,294,967 seconds. The default is 1,800 seconds (30 minutes).

STEP 4 In the **UDP Session Timeout Duration** field, enter the time, in seconds, after which inactive UDP sessions are removed from the session table. This value ranges from 0 through 4,294,967 seconds. The default is 120 seconds (2 minutes).

STEP 5 In the **Other Session Timeout Duration** (seconds) field, enter the time, in seconds, after which inactive non-TCP/UDP sessions are removed from the session table. This value ranges from 0 through 4,294,967 seconds. The default is 60 seconds.

STEP 6 In the **TCP Session Cleanup Latency (seconds)** field, enter the maximum time for a session to remain in the session table after detecting both FIN flags. This value ranges from 0 through 4,294,967 seconds. The default is 10 seconds.

STEP 7 Click **Save**.

Configuring Remote Management

The primary means to configure the Cisco RV220W is using the browser-based Device Manager. The Device Manager is accessed from a computer on the LAN by using the Cisco RV220W's LAN IP address and HTTP. You can enable remote management to allow you to access the Cisco RV220W from a remote WAN network. To access the Cisco RV220W remotely, you use HTTP over SSL (https).

To enable remote management:

STEP 1 Choose **Firewall** > **Remote Management.**

STEP 2 Next to Remote Management (disabled by default), check **Enable.**

CAUTION When remote management is enabled, the RV220W is accessible to anyone who knows its IP address. Since a malicious WAN user can reconfigure the Cisco RV220W and misuse it in many ways, change the administrator and any guest passwords before continuing. See **Configuring Users, page 143**.

STEP 3 Choose the type of access to grant:

- **All IP Addresses**—Choose to allow any IP address to access the Cisco RV220W. Change the default password before choosing this option. (See **Configuring Users, page 143**.)
- **IP Address Range**—Choose to allow any IP address in the configured range to access the Cisco RV220W. In the **From** field, enter the starting IP address for the allowed range. In the **To** field, enter the ending IP address for the allowed range.
- **Single IP Address**—Choose to restrict access to a device with a single IP address (for example, the computer you use to access the Device Manager). In the **IP Address** field, enter the IP Address of the PC to be given remote management permissions.

STEP 4 Enter the port number used for the remote connection.

STEP 5 To enable Simple Network Management Protocol (SNMP) to be used remotely to manage the Cisco RV220W, check the **Remote SNMP Enable** box.

STEP 6 Click **Save.**

Configuring One-to-One Network Address Translation

One-to-one Network Address Translation (NAT) is a way to make systems behind a firewall that are configured with private IP addresses appear to have public IP addresses.

To configure one-to-one NAT, choose **Firewall** > **Access Control** > **One-to-One NAT.** The **One-to-One-NAT Rules Table** lists the available One-To-One NAT rules that have been configured. It displays the following fields:

- **Private Range Begin—**The starting IP address in the private (LAN) IP address.
- **Public Range Begin—**The starting IP address in the public (WAN) IP address.
- **Public IP Subnet Mask—**The Subnet Mask of the public IP address.
- **Range Length**—Range length maps one to one private address to public address up to the given range.

The **Services for One-To-One-NAT Table** shows configured services. Services for one-to-one NAT allows you to configure the service to be accepted by the private IP (LAN) address when traffic is sent to the corresponding public IP address. Configured services on private IP addresses in the range are accepted when traffic is available on the corresponding public IP address.

This table displays the following fields:

- **LAN Server IP—**This column shows the configured LAN Host IP Address.
- **Service—**This column shows the service to be accepted by the LAN Host.

To add a one-to-one NAT service:

STEP 1 Choose **Firewall** > **Access Control** > **One-to-One NAT.**

STEP 2 In the **Services for One-to-One NAT Table**, click **Add.**

STEP 3 Enter the LAN Server IP address. This address should be in the private IP range configured in the One-to-One NAT rules.

STEP 4 Choose the service for which the rule applies.

STEP 5 Click **Save.**

To add a one-to-one NAT rule:

STEP 1 Choose **Firewall** > **Access Control** > **One-to-One NAT.**

STEP 2 In the **One-to-One NAT Rules Table**, click **Add.**

STEP 3 Enter information in the following fields:

- **Private Range Begin—**The starting IP address in the private (LAN) IP address.
- **Public Range Begin—**The starting IP address in the public (WAN) IP address.
- **Public IP Subnet Mask—**The Subnet Mask of the public IP address.
- **Range Length—**Range length maps one to one private address to public address up to the given range.

STEP 4 Click **Save.**

Using Cisco ProtectLink Web

Cisco ProtectLink Web is a hosted service that runs on the RV220W. It integrates powerful anti-spam, anti-phishing, URL Content Filtering and Web Reputation to block standalone, blended-threat, and customer-specific attacks. These features prevent unwanted content from passing through the router, and protect you from going to websites that are infected with spyware.

The RV220W supports ProtectLink Security Services. These services provide layers of protection against different security threats on your network.

The web threat protection feature prevents access to dangerous websites and URL filtering to control employee access to non-business related websites. Requested URLs are checked against the set security level and the ProtectLink database in real-time. Only URLs that meet the criteria are accessible.

You can request a free trial of Cisco ProtectLink, and configure it using the Device Manager. See the following URL:

http://www.cisco.com/go/protectlink

Configuring Approved Clients

To configure approved clients, or computers that have unrestricted Internet access:

STEP 1 Choose **Cisco ProtectLink Web** > **Global Settings** > **Approved Clients.**

STEP 2 Next to **Approved Clients List**, check the **Enable** check box to always approve all URL requests from computers listed in the **Approved Clients Table.**

STEP 3 Click **Save.**

STEP 4 In the **Approved Clients Table**, click **Add.**

STEP 5 In the Approved Clients window:

a. In the IP Address Type field, choose the address type.

   This field allows you to specify whether to add a single client or a range of clients to the Approved Client IP Addresses list.

b. If adding an IP address, in the Starting IP Address field, enter the IP address of the approved client.

c. If adding a range of IP addresses, enter the IP address of the first client in the range in the Starting IP Address field. In the Ending IP Address field, enter the IP address of the last client in the range.

d. Click **Save**.

STEP 6 To configure a client in the Approved Clients Table, check the corresponding check box and click **Edit**.

STEP 7 Edit the client settings as described in Step **5**.

STEP 8 To delete a client from the Approved Clients Table, check the corresponding check box and click **Delete**.

Configuring Approved URLs

To configure approved URLs, or URLs that will always be accessible:

STEP 1 Choose **Cisco ProtectLink Web** > **Global Settings** > **Approved URLs.**

STEP 2 Next to **Approved URLs List**, check **Enable** to always approve all URLs listed in the **Approved URLs Table**. Click **Save.**

STEP 3 In the **Approved URLs Table**, click **Add.**

STEP 4 In the **URL** field, enter the URL of the approved sire (for example, www.cisco.com) or part of the URL (for example, cisco).

STEP 5 In the **Match Type** field, choose one of the following options:

- **Web site**: Choose this option to allow access to the exact URL entered in the **URL** field.
- **URL keyword**: Choose this option to allow access to any URL that includes the keyword entered in the **URL** field.

STEP 6 Save the settings.

Configuring Overflow Control

You can configure how excess URL requests are handled. Excess URL requests occur when many computers try to access websites at the same time. This can easily happen especially during router startup. To configure overflow control:

STEP 1 Choose **Cisco ProtectLink Web** > **Web Protection**> **Overflow Control.**

STEP 2 Choose one of the following:

- **Temporarily Block URL requests** (recommended)—Users cannot access the Internet until the current queue can accommodate more requests.
- **Temporarily bypass Cisco ProtectLink URL Filtering for requested URLs—** URL requests will bypass URL Filtering and Web Reputation. This setting can make your network vulnerable to threats.

STEP 3 Click **Save.**

Configuring Web Reputation

In Web Reputation, requested URLs are checked against the set security level and the Cisco ProtectLink database in real time. Only URLs that meet the designated criteria are accessible.

To configure Web Reputation:

STEP 1 Choose **Cisco ProtectLink Web** > **Web Protection** > **Web Reputation**.

STEP 2 Check **Enable**.

STEP 3 Choose the security level of high, medium (recommended), or low. The higher the security level, the more URLs that are known or suspected to be a web threat are blocked.

STEP 4 Click **Save**.

Configuring URL Filtering

You can configure URL filtering to restrict access to web sites based on the category of web sites and day or time of day.

To configure URL filtering:

STEP 1 Choose **Cisco ProtectLink Web** > **Web Protection** > **URL Filtering**.

STEP 2 Check **Enable**.

STEP 3 Click the **+** symbol to expand the URL categories. For each category, you can choose to filter content during business hours, or leisure hours.

The URL categories appear in this window after you activate ProtectLink.

STEP 4 Configure **Business Days** for which to block sites.

STEP 5 To block sites all day, choose **All Day** (24 hours), or you can specify specific business hours to block sites. Times not designated as business hours are considered leisure hours.

STEP 6 Click **Save**.

Viewing Cisco ProtectLink License Information

After you have installed Cisco ProtectLink, you can view your license information and see instructions for renewing your license.

To view license information:

STEP 1 Choose **Cisco ProtectLink Web** > **License** > **Summary** to view a summary of your license.

STEP 2 Choose one of the following:

- Click **Update Information** to update the displayed information.
- Click **View Detailed License** to view information for a particular license.

To view renewal instructions, choose **Cisco ProtectLink Web** > **License** > **Renewal**. You can purchase a registration key from your Cisco reseller, then register or renew online.

5

Configuring Virtual Private Networks and Security

This chapter describes Virtual Private Network (VPN) configuration, beginning with the **"Configuring VPNs" section on page 105**.

It also describes how to configure router security, beginning with the **"Configuring Security" section on page 127**.

The following sections are covered:

- **Creating Cisco QuickVPN Client Users, page 105**
- **Using the VPN Wizard, page 106**
- **Viewing the Default Values, page 107**
- **Configuring IP Security Policies, page 107**
- **Configuring VPN Policies, page 112**
- **Configuring VPN Clients, page 117**
- **Monitoring VPN Tunnel Status, page 117**
- **Configuring IPsec Users, page 118**
- **Configuring VPN Passthrough, page 119**
- **Using Certificates for Authentication, page 127**
- **Using the Cisco RV220W With a RADIUS Server, page 130**
- **Configuring 802.1x Port-Based Authentication, page 131**

Configuring VPNs

A VPN provides a secure communication channel ("tunnel") between two gateway routers or a remote PC client and a gateway router. The following types of tunnels can be created:

- **Gateway-to-gateway VPN**—Connects two or more routers to secure traffic between remote sites.
- **Remote Client (client-to-gateway VPN tunnel)**—A remote client initiates a VPN tunnel. The IP address of the remote PC client is not known in advance. The gateway acts as responder.
- **Remote client behind a NAT router**—The client has a dynamic IP address and is behind a NAT Router. The remote PC client at the NAT router initiates a VPN tunnel. The IP address of the remote NAT router is not known in advance. The gateway WAN port acts as a responder.

Creating Cisco QuickVPN Client Users

To use the Cisco QuickVPN, you must do the following:

STEP 1 Enable remote management. See **Configuring Remote Management, page 97**.

STEP 2 Create QuickVPN users. See **Configuring IPsec Users, page 118**. After a user account is created, the credentials can be used by the QuickVPN client.

For more information on installing and using Cisco QuickVPN, see **Appendix A, "Using Cisco QuickVPN."**

Using the VPN Wizard

You can use the VPN wizard to quickly create both IKE and VPN policies. Once the IKE or VPN policy is created, you can modify it as required.

To quickly set up a VPN tunnel using VPN Wizard:

STEP 1 Choose **IPsec** > **VPN Wizard.**

STEP 2 Choose the type of peer with which the VPN tunnel will connect:

- **Gateway**—A gateway tunnel is created to connect with another VPN gateway. Choose this option if the RV220W will not act as the VPN server.
- **VPN Client**—The RV220W is set up to allow remote users to connect to its VPN server using their PC and VPN client software.

STEP 3 Enter the **New Connection Name**. The new connection name is used for management and identification purposes.

STEP 4 Enter the **Pre-Shared** key. The PSK is between 8 and 49 characters and must be entered exactly the same in this field on the RV220W and the remote VPN client or gateway. Double quotes (“) are not allowed.

STEP 5 Choose the Remote Gateway Type—**IP Address** or **Fully-Qualified Domain Name** (FQDN). You must choose the same type for the remote and local gateway.

STEP 6 Enter the Remote WAN IP Address or Internet Name (FQDN). Only enabled if you are connecting to a gateway peer.

STEP 7 Choose the Local Gateway Type—**IP Address** or **FQDN**. You must choose the same type for the remote and local gateway.

STEP 8 Enter the Local WAN IP Address or Internet Name (FQDN). This field can be left blank if you are not using a different FQDN or IP address than the one specified in the WAN port configuration.

STEP 9 Configure the Secure Connection Accessibility details:

- Remote Network IP address (available if you chose **Gateway** in Step 2)
- Remote Network Subnet Mask (available only if you chose **Gateway** in Step 2)
- Local Network IP Address
- Local Network Subnet Mask

NOTE The IP address range used on the remote network must be different from the IP address range used on the local network.

STEP 10 Click **Save.**

Viewing the Default Values

You can also view the default values created by the VPN Wizard by choosing **VPN** > **IPsec** > **Default Settings.**

Configuring IP Security Policies

The VPN Wizard is the recommended method to configure corresponding Internet Key Exchange (IKE) and VPN policies for establishing a VPN tunnel. Once the Wizard creates the matching IKE and VPN policies, you can modify the required fields using the **Edit** button. Advanced users can create an IKE policy from the **Add** button, but must be sure to use compatible encryption, authentication, and key-group parameters for the VPN policy.

Configuring IKE Policies

The IKE protocol dynamically exchanges keys between two IPsec hosts. You can create IKE policies to define the security parameters such as authentication of the peer, encryption algorithms, etc. to be used in this process.

To configure IKE Policies:

STEP 1 Choose **VPN** > **IPsec** > **IPsec Policies.**

STEP 2 In the **IKE Policies Table**, click **Add**.

STEP 3 Enter the information in the following sections and press **Save**.

General Information

STEP 1 Under **Policy Name**, enter a unique name for the policy for identification and management purposes.

STEP 2 Under **Direction/Type**, choose one of the following connection methods:

- **Initiator**—The router will initiate the connection to the remote end.
- **Responder**—The router will wait passively and respond to remote IKE requests.
- **Both**—The router will work in either Initiator or Responder mode.

STEP 3 Under **Exchange Mode**, choose one of the following options:

- **Main**—This mode negotiates the tunnel with higher security, but is slower.
- **Aggressive**—This mode establishes a faster connection, but with lowered security.

  NOTE If either the Local or Remote identifier type (see Step 4) is not an IP address, then negotiation is only possible in Aggressive Mode. If FQDN, User FQDN or DER ASN1 DN is selected, the router disables Main mode and sets the default to Aggressive mode.

STEP 4 In the **Local** section, under **Identifier Type**, choose the ISAKMP identifier for this router:

- Local WAN IP
- FQDN
- User FQDN
- DER ASN1 DN

STEP 5 If you chose Internet Address/FQDN, User FQDN, or DER ASN1 DN as the identifier type, enter the IP address or domain name in the **Identifier** field.

STEP 6 In the Remote section, under Identifier Type, choose the ISAKMP identifier for this router:

- Remote WAN IP
- FQDN
- User FQDN
- DER ASN1 DN

STEP 7 If you chose FQDN, User FQDN, or DER ASN1 DN as the identifier type, enter the IP address or domain name in the **Identifier** field.

IKE SA Parameters

The Security Association (SA) parameters define the strength and the mode for negotiating the SA.

STEP 1 Choose the encryption algorithm, or the algorithm used to negotiate the SA:

- DES
- 3DES
- AES-128
- AES-192
- AES-256

STEP 2 Specify the authentication algorithm for the VPN header:

- MD5
- SHA-1
- SHA2-256
- SHA2-384
- SHA2-512

NOTE Ensure that the authentication algorithm is configured identically on both sides.

STEP 3 Choose the authentication method:

- Select **Pre-Shared Key** for a simple password based key that is shared with the IKE peer.
- Selecting **RSA-Signature** disables the pre-shared key text box and uses the active self certificate uploaded in the Certificates page. In that case, a certificate must be configured in order for RSA-Signature to work.

NOTE The double quote character (“) is not supported in the pre-shared key.

STEP 4 Choose the Diffie-Hellman (DH) Group algorithm, which is used when exchanging keys. The DH Group sets the strength of the algorithm in bits.

NOTE Ensure that the DH Group is configured identically on both sides of the IKE policy.

STEP 5 In the **SA Lifetime** field, enter the interval, in seconds, after which the Security Association becomes invalid.

STEP 6 To enable dead peer detection, check the **Enable** box. Dead Peer Detection is used to detect whether the peer is alive or not. If peer is detected as dead, the router deletes the IPsec and IKE Security Association.

STEP 7 In the Detection Period field, enter the interval, in seconds, between consecutive DPD R-U-THERE messages. DPD R-U-THERE messages are sent only when the IPsec traffic is idle.

STEP 8 In the **Reconnect after Failure Count** field, enter the maximum number of DPD failures allowed before tearing down the connection.

Extended Authentication (XAUTH) Parameters

Rather than configuring a unique VPN policy for each user, you can enable the VPN gateway router to authenticate users from a stored list of user accounts or with an external authentication server such as a RADIUS server. When connecting many VPN clients to a VPN gateway router, Extended Authentication (XAUTH) allows authentication of users with methods in addition to the authentication method mentioned in the IKE SA parameters. XAUTH can be configured in the following modes:

STEP 1 Select the XAUTH type:

- **None**—Disables XAUTH.
- **IPsec Host**—The router is authenticated by a remote gateway with a username and password combination. In this mode, the router acts as a VPN Client of the remote gateway.
- **User Database**—User accounts created in the router are used to authenticate users. See **Configuring IPsec Users, page 118**.

STEP 2 If you selected IPsec Host, enter the username and password for the host.

Configuring VPN Policies

To configure a VPN policy:

STEP 1 Choose **VPN** > **IPsec** > **IPsec Policies.**

STEP 2 In the **VPN Policies Table**, click **Add.**

STEP 3 Enter the information in the following sections and press **Save.**

General Parameters

STEP 1 Enter a unique name to identify the policy.

STEP 2 Choose the Policy Type:

- **Manual Policy—**All settings (including the keys) for the VPN tunnel are manually input for each end point. No third-party server or organization is involved.
- **Auto Policy—**Some parameters for the VPN tunnel are generated automatically. This requires using the IKE (Internet Key Exchange) protocol to perform negotiations between the two VPN Endpoints.

To create an Auto VPN Policy, you need to first create an IKE policy and then add the corresponding Auto Policy for that IKE Policy.

STEP 3 In the **Remote Endpoint** field, select the type of identifier that you want to provide for the gateway at the remote endpoint: IP Address or FQDN (Fully Qualified Domain Name).

STEP 4 In the **NetBIOS** field, check **Enable** to allow NetBIOS broadcasts to travel over the VPN tunnel, or uncheck this box to disable NetBIOS broadcasts over the VPN tunnel. For client policies, the NetBIOS feature is available by default.

Local Traffic Selection and Remote Traffic Section

STEP 1 For both of these sections, configure the following settings:

- **Local/Remote IP**—Select the type of identifier that you want to provide for the endpoint:
  - **Any**—Specifies that the policy is for traffic from the given end point (local or remote). Note that selecting Any for both local and remote end points is not valid.
  - **Single**—Limits the policy to one host. Enter the IP address of the host that will be part of the VPN in Start IP Address field.
  - **Range**—Allows computers within an IP address range to connect to the VPN. Enter the Start IP Address and End IP Address in the provided fields.
  - **Subnet**—Allows an entire subnet to connect to the VPN. Enter the network address in the Start IP Address field, and enter the Subnet Mask in the Subnet Mask field.

STEP 2 In the **Start Address** field, enter the first IP address in the range. If you selected Single, enter the single IP address in this field and leave the **End IP Address** field blank.

STEP 3 In the **End Address** field, enter the last IP address in the range.

STEP 4 If you chose **Subnet** as the type, enter the Subnet Mask of the network.

Manual Policy Parameters

The Manual Policy creates an SA (Security Association) based on the following static inputs:

- **SPI-Incoming, SPI-Outgoing**—Enter a hexadecimal value between 3 and 8 characters; for example, 0x1234,
- **Encryption Algorithm**—Select the algorithm used to encrypt the data.
- **Key-In**—Enter the encryption key of the inbound policy. The length of the key depends on the algorithm chosen:
  - **DES**—8 characters
  - **3DES**—24 characters
  - **AES-128**—16 characters
  - **AES-192**—24 characters
  - **AES-256**—32 characters
  - **AES-CCM**—16 characters
  - **AES-GCM**—20 characters
- **Key-Out**—Enter the encryption key of the outbound policy. The length of the key depends on the algorithm chosen, as shown above.
- **Integrity Algorithm**—Select the algorithm used to verify the integrity of the data.
- **Key-In**—Enter the integrity key (for ESP with Integrity-mode) for the inbound policy. The length of the key depends on the algorithm chosen:
  - **MD5**—16 characters
  - **SHA-1**— 20 characters
  - **SHA2-256**—32 characters
  - **SHA2-384**— 48 characters
  - **SHA2-512**—64 characters
- **Key-Out**—Enter the integrity key (for ESP with Integrity-mode) for the outbound policy. The length of the key depends on the algorithm chosen, as shown above.

Manual Policy Example:

Creating a VPN tunnel between two routers:

```
Router 1: WAN1=10.0.0.1 LAN=192.168.1.1 Subnet=255.255.255.0
Policy Name: manualVPN
Policy Type: Manual Policy
Local Gateway: WAN1
Remote Endpoint: 10.0.0.2
Local IP: Subnet 192.168.1.0 255.255.255.0
Remote IP: Subnet 192.168.2.0 255.255.255.0
SPI-Incoming: 0x1111
Encryption Algorithm: DES
Key-In: 11112222
Key-Out: 33334444
SPI-Outgoing: 0x2222
Integrity Algorithm: MD5
Key-In: 1122334444332211
Key-Out: 5566778888776655
Router 2: WAN1=10.0.0.2 LAN=192.168.2.1 Subnet=255.255.255.0
Policy Name: manualVPN
Policy Type: Manual Policy
Local Gateway: WAN1
Remote Endpoint: 10.0.0.1
Local IP: Subnet 192.168.2.0 255.255.255.0
Remote IP: Subnet 192.168.2.0 255.255.255.0
SPI-Incoming: 0x2222
Encryption Algorithm: DES
Key-In: 33334444
Key-Out: 11112222
SPI-Outgoing: 0x1111
Integrity Algorithm: MD5
Key-In: 5566778888776655
Key-Out: 1122334444332211
```

Auto Policy Parameters

STEP 1 **SA Lifetime**—Enter the duration of the Security Association and choose the unit from the drop-down list:

- **Seconds**—Choose this option to measure the SA Lifetime in seconds. After the specified number of seconds passes, the Security Association is renegotiated. The default value is 3600 seconds. The minimum value is 300 seconds.
- **Kbytes**—Choose this option to measure the SA Lifetime in kilobytes. After the specified number of kilobytes of data is transferred, the SA is renegotiated. The minimum value is 1920000 KB.

  NOTE When configuring a Lifetime in kilobytes (also known as lifebytes), be aware that two SAs are created for each policy. One SA applies to inbound traffic, and one SA applies to outbound traffic. Due to differences in the upstream and downstream traffic flows, the SA may expire asymmetrically. For example, if the downstream traffic is very high, the lifebyte for a download stream may expire frequently. The lifebyte of the upload stream may not expire as frequently. It is recommended that the values be reasonably set, to reduce the difference in expiry frequencies of the SAs; otherwise the system may eventually run out of resources as a result of this asymmetry. The lifebyte specifications are generally recommended for advanced users only.

STEP 2 Select the algorithm used to encrypt the data.

STEP 3 Select the algorithm used to verify the integrity of the data.

STEP 4 Check the **PFS Key Group** box to enable Perfect Forward Secrecy (PFS) to improve security. While slower, this protocol helps to prevent eavesdroppers by ensuring that a Diffie-Hellman exchange is performed for every phase-2 negotiation.

STEP 5 Choose the IKE policy that will define the characteristics of phase 1 of the negotiation.

Configuring VPN Clients

VPN clients must be configured with the same VPN policy parameters used in the VPN tunnel the client wishes to use: encryption, authentication, life time, and PFS key-group. Upon establishing these authentication parameters, the VPN Client user database must also be populated with an account to give a user access to the tunnel.

VPN client software is required to establish a VPN tunnel between the router and remote endpoint. Open source software (such as OpenVPN or Openswan) as well as Microsoft IPsec VPN software can be configured with the required IKE policy parameters to establish an IPsec VPN tunnel. Refer to the client software guide for detailed instructions on setup as well as the router's online help.

The user database contains the list of VPN user accounts that are authorized to use a given VPN tunnel. Alternatively VPN tunnel users can be authenticated using a configured RADIUS database. Refer to the online help to determine how to populate the user database and/or configure RADIUS authentication.

Monitoring VPN Tunnel Status

You can view and change the status of (connect or drop) the router's IPsec security associations. The VPN tunnel status can be found in the **Status** > **IPsec Connection Status** page. Here the active IPsec SAs (security associations) are listed along with the traffic details and tunnel state. The traffic is a cumulative measure of transmitted/received packets since the tunnel was established.

If a VPN policy state is "not connected", it can be enabled from the List of VPN Policies in the **VPN** > **IPsec** > **IPsec Policies** page.

The **Active IPsec SAs Table** displays a list of active IPsec SAs. Table fields are as follows:

Field	Description
Endpoint	IP address of the remote VPN gateway or client.
Policy Name	IKE or VPN policy associated with this SA.
State	Status of the SA for IKE policies: Not Connected or IPsec SA Established.
Tx (KB)	Kilobytes of data transmitted over this SA.
Tx (Packets)	Number of IP packets transmitted over this SA.

Configuring IPsec Users

The configured IPsec users (both XAUTH and QuickVPN) are listed in the List of Users viewed by choosing **VPN** > **IPsec** > **IPsec Users.** The VPN gateway authenticates users in this list when XAUTH is used in an IKE policy. QuickVPN client can access only default LAN hosts.

To add new users:

STEP 1 Click **Add.**

STEP 2 Enter the username, or the unique identifier for the XAUTH user.

STEP 3 In the **User Type** field, select the type of the Remote Peer: Standard IPsec (XAuth), or Cisco QuickVPN.

STEP 4 If you chose **QuickVPN**, you can check the **Enable** box next to **Allow User to Change Password** box to allow the QuickVPN user to change their password. Uncheck if you would like to maintain the password for them.

STEP 5 Enter the alphanumeric password for this user

STEP 6 Enter the password again to confirm.

STEP 7 Click **Save.**

.

Configuring VPN Passthrough

VPN passthrough allows VPN traffic that originates from VPN clients to pass through the router. For example, if you are not using a VPN that is configured on the RV220W, but are using a laptop to access a VPN at another site, configuring VPN passthrough allows that connection.

To configure VPN passthrough:

STEP 1 Choose **VPN** > **VPN Passthrough**.

STEP 2 Choose the type of traffic to allow to pass through the router:

- **IPsec**—Check **Enable** to allow IP security tunnels to pass through the router.
- **PPTP**—Check **Enable** to allow Point-to-Point Tunneling Protocol tunnels to pass through the router.
- **L2TP**—Check **Enable** to allow Layer 2 Tunneling Protocol tunnels to pass through the router.

STEP 3 Click **Save**.

Configuring VPN Using a PPTP Server

While IPsec VPN (SSL VPN and Quick VPN) are more secure, you can configure VPN using a PPTP server.

NOTE You must configure the PPTP server on a subnet different from the existing subnets. PPTP users can have access to all subnets on the LAN side of the RV220W, provided that inter-VLAN is enabled.

To enable a PPTP server:

STEP 1 Choose **VPN** > **PPTP Server** and check the **Enable** check box.

STEP 2 In the **Starting IP Address** field, enter the starting IP of the range of IP addresses to assign to connecting users.

STEP 3 In the **Ending IP Address** field, enter the ending IP address of the range of IP addresses to assign to connecting users.

STEP 4 Click **Save**.

To create PPTP users:

STEP 1 Choose **VPN** > **PPTP Server** > **PPTP Users.**

STEP 2 Click **Add.**

STEP 3 Enter the **Username** and **Password.**

STEP 4 Click **Save.**

To view a list of active PPTP users who are currently connected to the system, choose **VPN** > **PPTP Server** > **Active Users.**

Configuring the SSL VPN Server

SSL VPN is used to give remote users access to web applications, client/server applications and network connections in a corporate network. Users can securely access these resources over the Internet. An SSL VPN tunnel is established when an endpoint client accesses the SSL VPN web portal that has been configured on the RV220W.

Remote Access must be enabled to configure SSL VPN. See **Configuring Remote Management, page 97**.

Configuring SSL VPN Portal Layouts

To configure the SSL VPN server, you must first configure the SSL VPN Web Portal:

STEP 1 Choose **VPN** > **SSL VPN Server** > **Portal Layouts**. The default portal layout is indicated by an asterisk (*). You can modify the default layout, or create a new one.

STEP 2 To create a new layout, click **Add.** To modify the default portal, check the box next to the layout name and click **Edit.**

STEP 3 In the **Portal Layout Name** field, enter a descriptive name for the portal that is being configured. It is used as part of the SSL portal URL.

STEP 4 (Optional) In the **Portal Site Title** field, enter the portal web browser window title that appears when the client accesses this portal.

STEP 5 (Optional) In the **Banner Title** field, enter the banner title that is displayed to SSL VPN clients prior to login.

STEP 6 (Optional) In the **Banner Message** field, enter the banner message that is displayed to SSL VPN clients prior to login.

STEP 7 To display the banner message on the login page, check the box. The user has option to either display or hide the banner message in the login page.

STEP 8 To use HTTP meta tags for cache control (recommended), check the box. This security feature prevents expired web pages and data from being stored in the client's web browser cache.

STEP 9 To enable the ActiveX web cache cleaner, check the box. An ActiveX cache control web cleaner can be pushed from the gateway to the client browser whenever users log in to this SSL VPN portal.

STEP 10 In the **SSL VPN Portal Pages to Display** field, check the links you want to display to the users upon login. You can choose either the VPN tunnel link, the port forwarding link, or both, depending on the SSL services.

STEP 11 Click **Save**.

After the portal settings are configured, the newly-configured portal is added to the **Portal Layouts Table**. The portal layout is selected when configuring an authentication domain.

To make a portal layout the default layout, check the box next to its name and choose **Set Default**.

Configuring SSL VPN Policies

SSL VPN policies give configured SSL users access to services and network resources. To configure the login policies for SSL VPN Users:

STEP 1 Choose **VPN** > **SSL VPN Server** > **SSL VPN Policies**.

STEP 2 To add a policy, in the **SSL VPN Policies Table**, click **Add**.

STEP 3 Choose the type of policy:

- **Global**—The policy applies to all users.
- **Group**—The policy applies to a group of users.
- **User**—The policy applies to a single user.

STEP 4 If you chose **Group**, select the group to which to apply the policy in the **Available Groups** list. If you chose **User**, select the group to which to apply the policy in the **Available Users** list.

STEP 5 In the **Apply Policy To** field, choose the type of LAN resource to which to apply the policy (the resource to which to provide or restrict access):

- Network Resource
- IP Address
- IP Network
- All IP Addresses

Network resources are groups of specified IP addresses or IP networks that are defined when you create a new resource and add objects to it. For example to allow only 3 specific IP addresses for SSL VPN access, group them into a resource and create a policy for it. This eliminates the need to create 3 separate policies for the 3 IP addresses.

STEP 6 In the **Policy Name** field, enter a unique name for identifying the policy. If you enter a policy name that already exists, the new policy will overwrite the existing policy.

STEP 7 If you chose **Network Resource** in Step 5, choose the resource in the **Defined Resources** list. Network resources must be configured before creating the policy to make them available for selection as a defined resource. See **Identifying Network Resources, page 123**.

If you chose **IP Address** in Step 5, enter the IP address in the **IP Address** field.

If you chose **IP Network** in Step 5, enter the information in the **IP Address** and the **Mask Length** fields.

If you chose **All IP Addresses** in Step 5, enter the beginning and ending IP address in the **Begin** and **End** fields.

STEP 8 If you chose **IP Address, IP Network**, or **All IP Addresses**, in the **Port Range/Port Number** fields, specify a port or range of ports to apply the policy to all TCP and UDP traffic on those ports.

STEP 9 If you chose **IP Address, IP Network**, or **All IP Addresses**, in the **Service** field, choose the service to which to apply the policy: **VPN Tunnel**, **Port Forwarding**, or **All** services.

To apply the policy to the entire private network through the SSL VPN tunnel, choose **VPN Tunnel**.

To apply the policy only to the SSL VPN Port Forwarding tunnels you have configured for your router, choose **Port Forwarding**.

To apply the policy to all SSL VPN and SSL VPN Port Forwarding tunnels, choose **All**.

STEP 10 In the **Permission** field, choose whether to permit or deny the assigned resources defined by this policy.

STEP 11 Click **Save.**

After SSL VPN policies are configured, the policies are displayed in a list that can be viewed by selecting **VPN** > **SSL VPN Server** > **SSL VPN Policies.** The policies can be edited or deleted as required. The list of policies can be filtered for viewing based on whether it is assigned to a single user, group, or globally to all users.

Identifying Network Resources

You can identify network resources to which to restrict or provide access when you create the SSL VPN Policies (see **Configuring SSL VPN Policies, page 121**.)

To identify network resources:

STEP 1 Choose **VPN** > **SSL VPN Server** > **Resources.**

STEP 2 Click **Add.**

STEP 3 In the **Resource Name** field, enter a unique identifier name for the resource.

STEP 4 In the **Service** field, choose the type of resource: VPN Tunnel, Port Forwarding, or All.

STEP 5 Click **Save.**

Configuring Port Forwarding

Port forwarding provides remote access to applications like email and mapped network drives. Supporting TCP data, SSL port forwarding detects and reroutes individual data streams over the port forwarding connection. To configure port forwarding, choose **VPN** > **SSL VPN Server** > **Port Forwarding.**

To add an application for port forwarding:

STEP 1 Under the **Configured Applications for Port Fowarding Table**, click **Add.**

STEP 2 Enter the Local Server IP address, or the IP address of the local server that is hosting the application.

STEP 3 Enter the TCP port number of the application.

STEP 4 Click **Save.**

To allow users to access the private network servers by using a hostname instead of an IP address, the fully-qualified domain name corresponding to the IP address is required. To configure the host name:

STEP 1 Under the **Configured Host Names for Port Forwarding Table**, click **Add.**

STEP 2 Enter the Local Server IP Address, or the IP address of the local server hosting the application. The application was previously configured and is listed in the **Configured Applications for Port Fowarding Table.**

STEP 3 Enter the fully-qualified domain name, or the domain name of the internal server.

STEP 4 Click **Save.**

Configuring the SSL VPN Client

An SSL VPN tunnel client provides a point-to-point connection between the browser-side machine and the RV220W. When an SSL VPN connection is launched from the user portal, a virtual network adapter with an IP address and DNS and WINS settings is automatically created on the client host, which allows local applications to talk to services on the private network without any special network configuration on the remote SSL VPN client machine.

To configure the SSL VPN client:

STEP 1 Choose **VPN** > **SSL VPN Client** > **SSL VPN Client**.

STEP 2 To enable split tunnel support, check the **Enable** box. If the box is not checked, full tunnel support is enabled. With full tunnel support, all traffic from the VPN client goes through the VPN tunnel. Client routes are not required. For a split tunnel, only traffic that is specified by client routes goes through the VPN tunnel.

NOTE If split tunnel support is enabled, be sure to configure SSL VPN client routes if the client address range is in a different subnet than the corporate network, or if your network has multiple subnets. See **Configuring Client Routes, page 126**. Also, configure a client-IP address range that does not directly overlap with any of the addresses on your local network.

STEP 3 (Optional) Enter the DNS suffix, or the name which will be given to the SSL VPN client.

STEP 4 (Optional) Enter the primary DNS server, or the DNS server IP address to set on the network adaptor created on the client host.

STEP 5 (Optional) Enter the secondary DNS server, or the secondary DNS server IP address to set on the network adaptor created on the client host.

STEP 6 Enter values in the **Client Address Range Begin** and **Client Address Range End** fields. Clients who connect to the tunnel get a DHCP served IP address assigned to the network adaptor from the range of addresses beginning and ending with these IP addresses.

STEP 7 Enter the LCP Timeout value. The LCP timeout value is three times the number entered and is the time, in seconds, for the LCP echo interval used by the SSL VPN tunnel connections. The updated value is effective only for new connections and existing SSL VPN tunnel connections must be restarted for the new value to apply.

STEP 8 Click **Save**.

Configuring Client Routes

To configure client routes, which control which traffic goes through the VPN tunnel if split tunnel support is enabled, perform the following steps:

STEP 1 Choose **VPN** > **SSL VPN Client** > **Configured Client Routes.**

STEP 2 Enter the destination network, or the network address of the LAN from the VPN tunnel clients' perspective.

STEP 3 Enter the subnet mask, or the subnet information of the destination network.

STEP 4 Click **Save**.

After routes for the client (the WAN host) are added, the routes are displayed in the **Configured Client Routes Table**, which maintains information regarding the destination network and the subnet.

Using the SSL VPN Client Portal

The SSL VPN Client Portal (VPN > SSL VPN Client > SSL VPN Client Portal) provides remote access to the corporate network. Choose one of the following options:

- **SSL VPN Tunnel—**creates an encrypted tunnel to the corporate network.
- **SSL Port Forwarding—**creates an encrypted tunnel for pre-defined applications on the corporate network.
- **Change Password—**Allows you to change the password.

A port-forwarding tunnel only allows the end user to access a single port on the LAN side.

For example, if the network administrator wants only SSL VPN users to be able to access the email server on port 25 and nothing else on the LAN, the administrator configures Port Forwarding under SSL VPN and specifies the port number (in this case, 25) and the server IP.

When the end user connects via SSL VPN, the user can only access the email server and nothing else. Without this the Port Forwarding option, the end user has full access to everything on the LAN side of the VPN server.

Configuring Security

The RV220W provides several security methods, including certificate authentication, RADIUS server support, and 802.1x port-based authentication.

Using Certificates for Authentication

The RV220W uses digital certificates for IPsec VPN authentication and SSL validation (for HTTPS and SSL VPN authentication).

You can obtain a digital certificate from a well-known Certificate Authority (CA) such as VeriSign, or generate and sign your own certificate using functionality available on this gateway.

The gateway comes with a self certificate, and this can be replaced by one signed by a CA as per your networking requirements.   A CA certificate provides strong assurance of the server's identity and is a requirement for most corporate network VPN solutions.

The certificates menu allows you to view a list of certificates (both from a CA and self) currently loaded on the gateway. The following certificate data is displayed in the list of Trusted (CA) certificates:

- **CA Identity (Subject Name)**—The certificate is issued to this person or organization.
- **Issuer Name**—The name of the Certificate Authority that issued this certificate.
- **Expiry Time**—The date after which this Trusted certificate becomes invalid.

A self certificate is a certificate issued by a CA identifying your device (or self if you don't want the identity protection of a CA). The **Active Self Certificate Table** lists the self certificates currently loaded on the gateway. The following information is displayed for each uploaded self certificate:

- **Name**—The name you use to identify this certificate. It is not displayed to IPsec VPN peers or SSL users.
- **Subject Name**—This is the name that is displayed as the owner of this certificate. This should be your official registered or company name, as IPsec or SSL VPN peers are shown this field.
- **Serial Number**—The serial number is maintained by the CA and used to identify this signed certificate.

- **Issuer Name—**This is the CA name that issued (signed) this certificate
- **Expiry Time—**The date after which this signed certificate becomes invalid - you should renew the certificate before it expires.

To request a self certificate to be signed by a CA, you can generate a Certificate Signing Request from the gateway by entering identification parameters and sending to the CA for signing.

Once signed, the CA's Trusted Certificate and signed certificate from the CA are uploaded to activate the self-certificate validating the identity of this gateway. The self certificate is then used in IPsec and SSL connections with peers to validate the gateway's authenticity.

To configure certificates, choose **Security** > **Authentication (Certificates)**.

Uploading CA Certificates

To upload CA Certificates:

STEP 1 In the **Trusted Certificates (CA Certificate) Table**, click **Upload.**

STEP 2 Browse to select the certificate file and press **Upload.**

Uploading Self Certificates

To upload self certificates:

STEP 1 In the **Active Self Certificates Table**, click **Upload.**

STEP 2 Browse to select the certificate file and press **Upload.**

Generating a Self Certificate Request

One of the steps in creating a certificate is to generate a certificate request from the computer or the device that will be using the certificate. The Certificate Signing Request (CSR) file needs to be submitted to the CA who will then generate a certificate for this device.

To generate a certificate request:

STEP 1 In the **Self Certificates Request Table**, click **Generate Certificate**.

STEP 2 Enter the name of the certificate request.

STEP 3 Enter the subject of the certificate request. The Subject field populates the CN (Common Name) entry of the generated certificate. Subject names are usually defined in the following format: CN=, OU=, O=, L=, ST=, C=. For example, CN=router1, OU=my_company, O=mydept, L=SFO, C=US.

STEP 4 Choose the Hash Algorithm: MD5 or SHA-1. The algorithm used to sign the certificate (RSA) is shown.

STEP 5 Enter the signature key length, or the length of the signature (**512** or **1024**).

STEP 6 (Optional) Enter the IP address of the router.

STEP 7 (Optional) Enter the domain name of the router.

STEP 8 (Optional) Enter the e-mail address of the company contact that is used when generating the self certificate request.

STEP 9 Click **Generate.** A new certificate request is created and added to the **Self Certificate Requests Table.** To view a request, click the **View** button next to the appropriate request in this table.

Downloading the Router’s Current Certificate

To download the router’s current certificate:

STEP 1 Locate the **Download Settings** section.

STEP 2 next to **Download Router Certificate**, click **Download.**

The current certificate is downloaded to the PC from which you are accessing the Device Manager.

Using the Cisco RV220W With a RADIUS Server

A RADIUS server can be configured to maintain a database of user accounts and can be used for authenticating this device's users. To configure a connection with a RADIUS server, choose **Security** > **RADIUS Server**. You can configure and view the following details in the RADIUS configuration pages:

- **Authentication Server IP address—**The IP address of the authenticating RADIUS server.
- **Authentication Port—**The RADIUS authentication server's port number used to send RADIUS traffic.
- **Timeout—**The timeout interval (in seconds) after which the RV220W re-authenticates with the RADIUS server.
- **Retries—**The number of retries for the RV220W to re-authenticate with the RADIUS server. If the number of retries is exceeded, authentication of this device with the RADIUS server has failed.

To configure a connection with a RADIUS server:

STEP 1 In the **Configured RADIUS Server Table**, click **Add**.

STEP 2 Enter the Authentication Server IP address, or the IP address of the authenticating RADIUS Server.

STEP 3 Enter the Authentication Port, or the port number on which the RADIUS server sends traffic.

STEP 4 In the **Secret** field, enter the shared key that allows the RV220W to authenticate with the RADIUS server. This key must match the key configured on the RADIUS server. The single quote, double quote, and space characters are not allowed in this field.

STEP 5 In the **Timeout** field, enter the timeout interval after which the RV220W re-authenticates with the RADIUS server.

STEP 6 In the **Retries** field, enter the number of retries for the RV220W to re-authenticate with the RADIUS server.

STEP 7 Click **Save**.

Configuring 802.1x Port-Based Authentication

A port-based network access control uses the physical access characteristics of IEEE 802 LAN infrastructures in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics. It also prevents access to that port in cases where the authentication fails. It provides an authentication mechanism to devices trying to connect to a LAN. The RV220W acts as a supplicant in the 802.1x authentication system.

To configure 802.1x Authentication:

STEP 1 Choose **Security** > **802.1x Configuration**.

STEP 2 Check the **Enable** box to configure a port as an 802.1x supplicant.

STEP 3 Select the LAN port that should be configured as an 802.1x supplicant.

STEP 4 Enter the username and password sent by the RV220W to the authenticator for authentication. The username and password are the credentials sent to the authenticating server (the device running 802.1X in an authenticator role; for example, a Cisco Catalyst switch).

STEP 5 Press **Save**.

6

Configuring Quality of Service

The RV220W provides configuration for Quality of Service (QoS) features, such as bandwidth profiles, traffic selectors, and traffic meters. It contains the following sections:

- **Configuring Bandwidth Profiles, page 133**
- **Configuring Traffic Selectors or Flows, page 134**
- **Configuring Traffic Metering, page 135**
- **Configuring 802.1p, page 137**

Configuring Bandwidth Profiles

Using bandwidth profiles, the bandwidth of the traffic flowing from the secure network (LAN) to the insecure network (WAN) can be shaped. Bandwidth limiting determines the speed from which the data is sent from your router. You can use a bandwidth profile to limit the outbound traffic, thus preventing the LAN users from consuming all of the bandwidth of the Internet link.

Bandwidth profiles configuration consists of enabling the bandwidth control feature from the Device Manager, and adding a profile which defines the control parameters. The profile can then be associated with a traffic selector, so that bandwidth profile can be applied to the traffic matching the selectors.

To configure bandwidth profiles, perform the following steps.

Enable Bandwidth Profiles

STEP 1 Choose **QoS** > **Bandwidth Profiles.**

STEP 2 Check the **Enable** box.

STEP 3 Click **Save**.

Add Profiles

STEP 1 In the **Bandwidth Profiles Table**, click **Add.**

STEP 2 Enter the **Profile Name**, or the name used to identify and associate the profile to traffic selection criteria.

STEP 3 Choose the **Profile Type**: **Priority** (to limit bandwidth by high, medium, or low priority) or **Rate** (to limit bandwidth by the transmission rate.

STEP 4 If you chose **Priority**, enter the priority for this profile (low, medium, or high). If you chose **Rate**, enter the minimum and maximum bandwidth rates in kilobytes per second.

STEP 5 Click **Save**.

Configuring Traffic Selectors or Flows

After a profile has been created, it can then be associated with a traffic selector. To create a traffic selector:

STEP 1 Choose **QoS** > **Traffic Selectors.**

STEP 2 In the **Traffic Selectors Table**, click **Add.**

STEP 3 Choose the bandwidth profile which will applied to this traffic. (See **Configuring Bandwidth Profiles, page 133**.)

STEP 4 Choose a service from the list. Traffic flow rules will be applied to this service. (If you do not see a service that you want, you can configure a custom service in the **Firewall** page - see **Creating Custom Services, page 89**.)

STEP 5 In the **Traffic Selector Match Type** field, choose the type of matching the bandwidth profile will use before applying the traffic flow rules:

- **IP Address Range**—Enter the starting and ending IP address ranges.
- **MAC Address**—Enter the MAC address.
- **Port Name**—Select the port on the router to which traffic rules will be applied.
- **VLAN**—Select the VLAN on the router to which traffic rules will be applied.
- **DSCP**—Enter the DSCP value.
- **BSSIDs**—Choose the Basic Service Set Identifier, or the MAC address of the Wireless Access Point (WAP).

STEP 6 Click **Save.**

Configuring Traffic Metering

Traffic metering allows you to measure and limit the traffic routed by this router. To configure traffic metering:

STEP 1 Choose **QoS** > **Traffic Meter**.

STEP 2 Check the **Enable** box to enable traffic metering on the optional WAN port. The router will keep a record of the volume of traffic going from this interface. The router can also be configured to place a restriction on the volume of data being transferred.

STEP 3 Choose the **Traffic Limit** type:

- **No Limit**—The default option, where no limits on data transfer are imposed. Choosing this option displays the outgoing and incoming traffic volume in the Internet Traffic Statistics section on the page. If traffic metering is not enabled, these statistics are not shown.
- **Download Only**—Limits the amount of download traffic. Enter the maximum allowed data (in megabytes) that can be downloaded for a given month in the **Monthly Limit** field. Once the limit is reached, no traffic will be allowed from the WAN side.
- **Both Directions**—For this setting, the router will calculate traffic for both upload and download directions. The traffic limit typed into the **Monthly Limit** field is shared by both upload and download traffic. For example, for a 1GB limit, if a 700 MB file is downloaded then the remaining 300 MB must be shared between both upload and download traffic. The amount of traffic downloaded will reduce the amount of traffic that can be uploaded and vice-versa.

STEP 4 Enter the volume limit in the **Monthly Limit** field that is applicable for this month. This limit will apply to the type of direction (Download Only or Both) selected above.

STEP 5 In the **Increase This Month's Limit By** field, if the monthly traffic limit has been reached and you need to temporarily increase the limit, check this option and enter the value by which you want to increase the limit.

NOTE The **This Month's Limit** field displays the data transfer limit applicable for this month, which is the sum of the value in the **Monthly Limit** field and the **Increase this Month's Limit** field.

STEP 6 In the **Traffic Counter** fields, specify the action to be taken on the traffic counter:

- **Restart Now**—Select this option and click **Save** to reset the counter to zero immediately.
- **Specific Time**—Set a schedule for the traffic counter to restart. Typically, this is the last day of the month. Set the appropriate time and day of the month.

STEP 7 The **When Limit is Reached** section defines the router actions upon the traffic counter limits being reached at any given time. In the Traffic Block Status list, choose one of the following:

- **Block All Traffic**—If selected, then when the traffic limit is reached, all traffic to and from the WAN will be blocked.
- **Block All Traffic Except E-mail**—If selected, then when the traffic limit is reached, all traffic to and from the WAN will be blocked, but e-mail traffic will be allowed.

To send an email alert when the limit is reached, check the **Enable** box. This feature works only if you enable e-mail logs on the **Administration** > **Logging** > **Remote Logging** page. See **Configuring Logging, page 148**.

STEP 8 Click **Save**.

You can also view the Internet Traffic Statistics. If Traffic Metering is enabled for this interface, the following statistics will be displayed:

- **Start Date/Time**—The date on which the traffic meter was started or the last time when the traffic counter was reset.
- **Outgoing Traffic Volume**—The volume of traffic, in megabytes, that was uploaded through this interface.
- **Incoming Traffic Volume**—The volume of traffic, in megabytes, that was downloaded through this interface.
- **Average per day**—The average volume of traffic that passed through this interface.
- **% of Standard Limit**—The amount of traffic, in percent that passed through this interface against the Monthly Limit.
- **% of this Month's Limit**—The amount of traffic, in percent, that passed through this interface against this Month's Limit (if the month's limit has been increased).

Configuring 802.1p

802.1p QoS provides a mechanism for implementing QoS at the Media Access Control level. By enabling 802.1p CoS to DSCP remarking, the router can set the DSCP field in IP packets, according the eight different classes of services in 802.1p.

To configure 802.1p:

STEP 1 Choose **QoS** > **802.1p** > **802.1p Configuration.**

STEP 2 Check the **Enable** box to enable 802.1p QoS.

STEP 3 Check the **Enable** box to enable 802.1p CoS to DSCP remarking for IP packets. Class of Service (CoS) or 802.1p specifies a priority value between 0 and 7 that can be used by Quality of Service (QoS) disciplines to differentiate traffic. Differentiated Services or DiffServ is a computer networking architecture that specifies a simple, scalable and coarse-grained mechanism for classifying, managing network traffic and providing Quality of Service (QoS) guarantees on modern IP networks. The DSCP value is the classification value the router uses in determining the egress marking as the frames traverse and exit the switch.

STEP 4 Click **Save.**

Configuring 802.1p to Queue Mapping

802.1p defines eight different classes of service. To configure 802.1p to queue mapping:

STEP 1 Choose **QoS** > **802.1p** > **802.1p to Queue Mapping.**

STEP 2 For each priority, select the queue mapping corresponding to the service from the following queue values: **Lowest**, **Low**, **Medium** or **High.**

STEP 3 Click **Save** to submit your changes.

Configuring 802.1p CoS to DSCP Remarking

DSCP is a field in an IP packet that enables different levels of service to be assigned to network traffic. You can assign priorities for the eight different classes of services in 802.1p. To configure 802.1p CoS to DSCP Remarking:

STEP 1 Choose **QoS** > **802.1p** > **802.1p COS to DSCP Remarking.**

STEP 2 For each 802.1p priority value, enter a priority value (range is from 0 to 63).

STEP 3 Click **Save.**

Administering Your Cisco RV220W

This chapter describes the administration features of the RV220W, including creating users, configuring network management, diagnostics and logging, date and time, and other settings. It contains the following sections:

- **Setting Password Complexity, page 140**
- **Configuring User Accounts, page 140**
- **Configuring Simple Network Management, page 144**
- **Using Diagnostic Tools, page 147**
- **Configuring Logging, page 148**
- **Configuring Bonjour Discovery, page 152**
- **Configuring Date and Time Settings, page 153**
- **Backing Up and Restoring the System, page 153**
- **Importing a CSV File, page 154**
- **Upgrading Firmware, page 157**
- **Rebooting the Cisco RV220W, page 158**
- **Restoring the Factory Defaults, page 158**

Setting Password Complexity

The RV220W can enforce minimum password complexity requirement for password changes. To enable password complexity, choose **Administration** > **Password Complexity.** Check the **Enable** box and click **Save**.

Password complexity forces new passwords to conform to the following requirements:

- Passwords must be a minimum number of characters in length. Enter the minimum password length.
- Passwords must contain characters from a certain number of character classes. Enter the minimum number of character classes (listed below):
    - Uppercase letters
    - Lowercase letters
    - Numbers
    - Special characters available on a standard keyboard.

You can require new passwords to be different from the current password. Check **Enable**.

Configuring User Accounts

The RV220W provides user accounts for administering and viewing settings. Users can belong to groups, or logical groupings of SSL VPN users that share the authentication domain, LAN and service access rules, and idle timeout settings. Groups are associated with authenticating domains, or domains that authenticate users by a certain method such as a local database, RADIUS server, LDAP, or other means.

Configuring Domains

You configure domains that will contain groups of SSL VPN users.

To configure a domain:

STEP 1 Choose **Administration** > **Users** > **Domains**. The default domain (SSLVPN) is displayed in the **Domains Table** and noted with an asterisk (*). You cannot modify this domain.

STEP 2 Click **Add**.

STEP 3 Enter the domain name, or the unique identifier for the domain.

STEP 4 Choose the authentication type:

- Local User Database
- RADIUS-PAP
- RADIUS-CHAP
- RADIUS-MSCHAP
- RADIUS-MSCHAPv2
- NT Domain
- Active Directory
- LDAP

STEP 5 Select the portal for this domain. (See **Configuring SSL VPN Portal Layouts, page 120**, for more information on portals.) Only users of domains associated with certain portals can use those portals to log in.

STEP 6 If you chose a type of authentication other than **Local User Database** in Step 4, enter the name of the server that is used to authenticate users.

STEP 7 If you chose **RADIUS** authentication in Step 4, enter the authentication secret.

STEP 8 If you chose **NT Domain** authentication in Step 4, enter the workgroup.

STEP 9 If you chose **LDAP** authentication in Step 4, enter the base domain name.

STEP 10 If you chose **Active Directory** authentication in Step 4, enter the Active Directory domain name. Users that are registered in the Active Directory database can access the SSL VPN portal using their Active Directory username and password.

STEP 11 Click **Save**.

Configuring Groups

To configure groups to which SSL VPN users can be added:

STEP 1 Choose **Administration** > **Users** > **Groups**.

STEP 2 Click **Add**.

STEP 3 Enter the group name, or the unique identifier for the group.

STEP 4 Select the authenticating domain to which the group is attached.

STEP 5 Enter the idle Timeout value. This is the time, in minutes, after which a user in the group is logged out of the VPN.

STEP 6 Click **Save**.

Configuring Users

CAUTION Change the administrator name and password as soon as possible.

To add more user accounts, or edit user accounts:

STEP 1 Choose **Administration** > **Users** > **Users**.

STEP 2 Click **Add** to add a new user account, or check the box next to the existing account you want to change and press **Edit**.

STEP 3 Enter the username.

STEP 4 Enter the first and last name.

STEP 5 Select the user type:

- **SSL VPN User**—An SSL VPN user can log in to the network using the VPN client.
- **Administrator**—An administrator user type has access to the Device Manager and can read and write configuration data.
- **Guest**—A guest account has read-only access to the Device Manager.

STEP 6 Select the user group. See **"Configuring Groups" section on page 142**.

NOTE Certain fields, like the password and idle timeout value, are configured on the user page. However, a group can also have these fields configured. If the user belongs to a group, the group configuration applies and the individual user values are ignored.

STEP 7 Enter the password.

STEP 8 Enter the password again to confirm it.

STEP 9 In the **Idle Timeout** field, enter the number, in minutes, before a session times out due to inactivity. The Device Manager, by default, logs you out after 10 minutes of inactivity.

STEP 10 Press **Save**.

Configuring Simple Network Management

Simple Network Management Protocol (SNMP) lets you monitor and manage your router from an SNMP manager. SNMP provides a remote means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

To configure SNMP, choose **Administration** > **Network Management.**

Editing SNMPv3 Users

SNMPv3 parameters can be configured for the two default RV220W user accounts (Admin and Guest). To configure:

STEP 1 Choose **Administration** > **Network Management** > **SNMP**.

STEP 2 In the **SNMPv3 Users List Table**, check the box for the user to edit and click **Edit.**

STEP 3 Under **Security Level,** choose the amount of SNMPv3 Privileges:

- **NoAuthNoPriv**—Doesn't require any Authentication and Privacy.
- **AuthNoPriv**—Submit only Authentication algorithm and password.
- **AuthPriv**—Submit Authentication/privacy algorithm and password.

STEP 4 If you chose **AuthNoPriv** or **AuthPriv**, choose the type of authentication algorithm (**MD5** or **SHA**) and enter the authentication password.

If you chose **AuthPriv**, choose the type of privacy algorithm (**DES** or **AES**) and enter the privacy password.

STEP 5 Click **Save.**

Adding SNMP Traps

The **Traps List Table** lists IP addresses of SNMP agents to which the router will send trap messages (notifications) and allows several operations on the SNMP agents.

To add a new trap:

STEP 1 In the **Traps List Table**, click **Add**.

STEP 2 Enter the IP Address of the SNMP manager or trap agent.

STEP 3 Enter the SNMP trap port of the IP address to which the trap messages will be sent.

STEP 4 Enter the community string to which the agent belongs. Most agents are configured to listen for traps in the Public community.

STEP 5 Choose the SNMP Version: **v1**, **v2c**, or **v3**.

STEP 6 Click **Save**.

Configuring Access Control Rules

The **SNMP Access Control List** is a table of access rules that enables read-only or read-write access for select IP addresses in a defined SNMP agent's community.

To configure access control rules:

STEP 1 In the **Access Control List Table,** click **Add.**

STEP 2 Enter the IP Address of the specific SNMP manager or trap agent on which to create an access rule.

STEP 3 Enter the subnet mask used to determine the list of allowed SNMP managers.

STEP 4 Enter the community string to which the agent belongs. Most agents are configured to listen for traps in the Public community.

STEP 5 Choose the access type. The SNMP manager or trap agent can either be allowed to read and modify all SNMP accessible settings (**rwcommunity**) or be given read-only access (**rocommunity**).

STEP 6 Click **Save.**

Configuring Additional SNMP Information

To configure additional SNMP information:

STEP 1 Choose **Administration** > **Network Management** > **SNMP System Information.** This page displays the current SNMP configuration of the router. The following MIB (Management Information Base) fields are displayed and can be modified:

- **SysContact**—Enter the name of the contact person for this router. Examples: admin, John Doe.
- **SysLocation**—Enter the physical location of the router. Example: Rack #2, 4th Floor.
- **SysName**—(Read Only) A system name for easy identification of the router.

STEP 2 Click **Save.**

Using Diagnostic Tools

The RV220W provides several diagnostic tools. To access these tools, choose **Administration** > **Diagnostics** > **Network Tools**.

Using PING

This utility can be used to test connectivity between this router and another device on the network connected to this router. Enter an IP address and click **Ping**. A popup window appears, indicating the ICMP echo request status. To ping through the VPN tunnel, check the box.

Using Traceroute

This utility will display all the routers present between the destination IP address and the RV220W. Up to 30 “hops” (intermediate routers) between this router and the destination will be displayed. Enter an IP address and click **Traceroute**.

Performing a DNS Lookup

To retrieve the IP address of a Web, FTP, Mail or any other Server on the Internet, type the Internet Name in the text box and click **Lookup**. If the host or domain entry exists, you will see a response with the IP address. A message stating “Unknown Host” indicates that the specified Internet Name does not exist.

Capturing and Tracing Packets

Capture Packets allows you to capture all packets that pass through the selected interface (LAN, dedicated WAN, or optional WAN). To capture packets, click **Packet Trace**, and a new window appears. Select the interface and click **Start**. To stop the packet capture, click **Stop**. You can click **Download** to save a copy of the packet capture.

NOTE The packet trace is limited to 1MB of data per capture session. When the capture file size exceeds 1MB, it will be deleted automatically and a new capture file will be created.

Configuring Logging

The RV220W provides remote and local logging. To configure logging, choose **Administration** > **Logging** and select the type of logging to configure.

Configuring Local Logging

The router can be configured to log and e-mail notifications for denial of service attacks, general attack information, login attempts, dropped packets, and so on, to a specified e-mail address or a Syslog server.

Routing Logs

This section is used to configure the logging options for each network segment (for example, LAN-WAN).

NOTE Enabling logging options may generate a significant volume of log messages and is recommended for debugging purposes only.

- **Accepted Packets**—Check this box to log packets that were successfully transferred through the segment. This option is useful when the Default Outbound Policy is "Block Always" (see the **Firewall** > **IPv4 Rules** page). For example, if **Accept Packets from LAN to WAN** is enabled and there is a firewall rule to allow ssh traffic from the LAN, then whenever a LAN machine tries to make an ssh connection, those packets will be accepted and a message will be logged. (Make sure the log option is set to allow for this firewall rule.)
- **Dropped Packets**—Check this box to log packets that were blocked from being transferred through the segment. This option is useful when the Default Outbound Policy is "Allow Always" (see the **Firewall** > **IPv4 Rules** page). For example, if Drop Packets from LAN to WAN is enabled and there is a firewall rule to block SSH traffic from LAN, then whenever a LAN machine tries to make an ssh connection, those packets will be dropped and a message will be logged. (Make sure the log option is set to allow for this firewall rule.)

System Logs

Select the type of system events to be logged. The following system events can be recorded:

- **All Unicast Traffic**—Check this box to log all unicast packets directed to the router.
- **All Broadcast/Multicast Traffic**—Check this box to log all broadcast or multicast packets directed to the router.

Other Event Logs

Select the type of event to be logged. The following events can be recorded:

- **Source MAC Filter**—Check this box to log packets matched due to source MAC filtering. Uncheck this box to disable source MAC filtering logs.
- **Bandwidth Limit**—Check this box to log packets dropped due to Bandwidth Limiting.

Configuring Remote Logging

Log Options

In the **Remote Log Identifier** field, enter a prefix to add to every logged message for easier identification of the source of the message. The log identifier will be added to both e-mail and Syslog messages.

Enable E-Mail Logs

This section is used to configure e-mail settings for sending logs. It contains the following fields:

- **E-Mail Logs**—Disabled by default. Select the check box to enable e-mail logs.
- **E-mail Server Address**—Enter the IP address or Internet Name of an SMTP server. The router will connect to this server to send e-mail logs when required.
- **SMTP Port**—Configure the port to connect smtp server.
- **Return E-mail Address**—Enter the e-mail address where the replies from the SMTP server are to be sent (required for failure messages).
- **Send To E-mail Address(1)**—Enter the e-mail address where the logs and alerts are to be sent.

- **Send To E-mail Address(2)**—Enter the e-mail address where the logs and alerts are to be sent.
- **Send To E-mail Address(3)**—Enter the e-mail address where the logs and alerts are to be sent.
- **Authentication with SMTP server**—If the SMTP server requires authentication before accepting connections, select either **Login Plain** or **CRAM-MD5** and enter the Username and Password to be used for authentication. To disable authentication, select **None**.
- **Respond to Identd from SMTP Server**—Check this radio box to configure the router to respond to an IDENT request from the SMTP server.
- To confirm that the e-mail logs function is configured correctly, press **Test**.

Send E-mail logs by Schedule

To receive e-mail logs according to a schedule, configure the appropriate schedule settings:

- **Unit**—Select the period of time that you need to send the log: **Hourly**, **Daily**, or **Weekly**. To disable sending of logs, select **Never**. This option is useful when you do not want to receive logs by e-mail, but want to keep e-mail options configured so that you can use the Send Log function from the **Status** > **View Logs** pages.
- **Day**—If logs are to be sent on a weekly basis, choose the day of the week.
- **Time**—Select the time of day when logs should be sent.

Syslog Server

If you want the router to send logs to a Syslog server, enter the IP address or Internet Name of the Syslog server in the **Syslog Server** field. You can configure up to 8 Syslog servers.

Configuring the Logging Type and Notification

There are a variety of events that can be captured and logged for review. These logs can be sent to a server or e-mailed as configured. To configure, choose **Administration** > **Logging** > **Logs Facility**:

STEP 1 Select the type of functionality from which to generate logs: **Kernel**, **System**, or **Local0-wireless.**

STEP 2 Select the events to log: **Emergency, Alert**, **Critical**, **Error**, **Warning**, **Notification**, **Information**, **Debugging.**

STEP 3 For each of these events, select how to receive notification: **Display in Event Log**, **Send to Syslog.**

STEP 4 Click **Save.**

Configuring E-Mailing of Log Events

The variety of events that can be captured and logged for review can be e-mailed. To configure e-mailing of log events, choose **Administration** > **Logging** > **Email Log Events:**

STEP 1 Select the type of facility from which to generate logs: **Kernel**, **System**, or **Local0-wireless.**

STEP 2 Select the events to log: **Emergency, Alert**, **Critical, Error**, **Warning**, **Notification, Information**, **Debugging.**

STEP 3 Click **Save.**

Configuring Bonjour Discovery

Bonjour is a service advertisement and discovery protocol. For the RV220W, Bonjour only advertises the default services configured on the device when Bonjour is enabled.

To enable Bonjour:

STEP 1 Choose **Administration** > **Discovery Settings** > **Discovery - Bonjour.**

STEP 2 Check the **Enable** box to enable Bonjour on the router. Unchecking this will disable Bonjour.

STEP 3 Click **Save.**

Configuring VLAN Associations

You can select the available VLAN to enable Bonjour service types. Available VLANs are populated for the Bonjour Association VLAN list after the VLANs are configured for the device. (See **Configuring VLANs, page 39**, for more information.) Currently, by default, LAN/Default-VLAN is the broadcasting domain for service.

Associating a VLAN allows devices present on the VLAN to discover Bonjour services available on the router (such as http/https). For example, if a VLAN is configured with an ID of 2, devices and hosts present on VLAN 2 cannot discover Bonjour services running on the router unless VLAN 2 is associated with Bonjour services.

To add a VLAN association:

STEP 1 Choose **Administration** > **Discovery Settings** > **VLAN Association.**

STEP 2 Click **Add.**

STEP 3 Choose an available VLAN to which to add a service. (See **Configuring VLANs, page 39** for more information.)

STEP 4 Click **Save.** The VLAN is added to the **VLAN Association Table.**

Configuring Date and Time Settings

You can configure your time zone, whether or not to adjust for Daylight Savings Time, and with which Network Time Protocol (NTP) server to synchronize the date and time. The router then gets its date and time information from the NTP server. To configure NTP and time settings:

STEP 1 Choose **Administration** > **Time Settings**.

STEP 2 Select your time zone, relative to Greenwich Mean Time (GMT).

STEP 3 If supported for your region, check **Enable** to adjust for daylight Saving Time.

STEP 4 Select whether to use default or custom Network Time Protocol (NTP) servers, or set the time and date manually.

STEP 5 If you chose a default NTP server, choose the server from the list. If you chose a custom NTP server, enter the server addresses or fully-qualified domain name.

If you chose to set the date and time manually, enter the date and time.

STEP 6 Click **Save**.

Backing Up and Restoring the System

You can back up custom configuration settings for later restoration or restore from a previous backup from the **Administration** > **Backup/Restore Settings** page.

When the router is working as configured, you can back up the configuration for restoring later. During backup, your settings are saved as a file on your PC. You can restore the router's settings from this file.

⚠ **CAUTION** During a restore operation, do not try to go online, turn off the router, shut down the PC, or do anything else to the router until the operation is complete. This should take about a minute. When the test light turns off, wait a few more seconds before doing anything with the router.

To back up a configuration or restore a previously-saved configuration:

STEP 1 Select **Administration** > **Backup/Restore Settings.**

STEP 2 To save a copy of your current settings, click **Backup.** The browser downloads the configuration file and prompts you to save the file on the PC.

To restore your saved settings from a backup file, click **Browse**, locate and select the file, and click **Restore.** An alert page displays the status of the restore operation. After the restore, the router restarts automatically with the restored settings.

Importing a CSV File

You can simplify user, group, and domain creation by creating a CSV file and importing it into the RV220W.

The Format of the .csv file is as follows:

```
"<SSLVPNDomain Code>", "<DomainName>", "<PortalLayoutName>",
"<AuthenticationType>", "<AuthenticationServer>",
"<AuthenticationRadiusSecret>", "<NTDomainWorkGroup>", "<LDAPBaseDN>",
"<ActiveDirectoryDomain>"
```

Possible Values:

- SSLVPNDomain Code - 5
- Domain Name - String
- PortalLayoutName - String
- AutheticationType - String
- AuthenticationServer - IP Address
- AuthenticationRadiusSecret - String
- NTDomainWorkGroup - String
- LDAPBaseDN - String
- ActiveDirectoryDomain - String

```
"<SSLVPNGroup Code>", "<GroupName>", "<DomainName>", "<GroupTimeOut>"
```

Possible Values:

- SSLVPNGroup Code - 4
- GroupName - String
- DomainName - String
- GroupTimeOut - integer

```
"<SNMPv3USER Code>","<userName>", "<accessType>",
"<securityLevel>","<authAlgo>","<authPassword>","<privAlgo>","<privPassword>
"
```

Possible Values:

- SNMPv3USER Code - 3
- userName - cisco/guest
- accessType - RWUSER/ROUSER
- securityLevel - integer
- authAlgo - MD5 / SHA
- authPassword - String
- privAlgo - DES / AES
- privPassword - String

```
"<PPTPUSER Code>", "<userName>", "<password>"
```

Possible Values:

- PPTPUSER Code: 2
- userName - String
- password - String

```
"<IPSECUSER Code>", "<UserName>", "<Password>", "<UserType>",
"<AllowChangePassword>"
```

Possible Values:

- IPSECUSER Code: 1
- Username - String
- Password - String
- UserType - boolean (0 - Standard Ipsec / 1 - Cisco Quick VPN)
- AllowChangePassword - boolean

```
"<SSLVPNUSER Code>", "<UserName>", "<FirstName>", "<LastName>",
"<GroupName>", "<UserType>", "<UserTimeOut>", "<DenyLogin>",
"<DenyLoginFromWan>", "<LoginFromIP>", "<LoginFromBrowser>", "<Password>"
```

Possible Values:

- SSLVPNUSER Code: 0
- UserName - String
- FirstName - String
- LastName - String
- GroupName - String
- UserType - integer
- UserTimeOut - integer
- DenyLogin - boolean
- DenyLoginFromWan - boolean
- LoginFromIP - boolean
- LoginFromBrowser - boolean
- Password - String

Sample CSV file format:

```
"5","domain1","SSLVPN","radius_pap","14.0.0.1","test","","",""
"4","group2","domain1","30"
"3","cisco","RWUSER","1","SHA","authPassword","AES","privPassword"
"2","p2","pp2"
"1","rrrr","sss","0","1"
"0","user102","sss","dddd","SSLVPN","4","10","0","1","0","0","fail"
```

To import a .csv file:

STEP 1 Choose **Administration** > **CSV File Import**.

STEP 2 Click **Browse**.

STEP 3 On your computer, locate and select the .csv file. Click **Import**.

Upgrading Firmware

⚠ **CAUTION** During a firmware upgrade, do not try to go online, turn off the device, shut down the PC, or interrupt the process in any way until the operation is complete. This process takes about a minute, including the reboot process. Interrupting the upgrade process at specific points when the flash is being written to may corrupt the flash memory and render the router unusable.

To upgrade firmware:

STEP 1 Choose **Administration** > **Firmware Upgrade**.

STEP 2 Click **Browse** and locate and select the downloaded firmware.

STEP 3 Choose one of the following:

- **Upload**—Uploads the new firmware and saves your current configuration settings.
- **Upload & factory reset**—Uploads the new firmware, but overwrites your current configuration settings with the factory defaults. Use only if you want to erase all of your router settings.

After the new firmware image is validated, the new image is written to flash, and the router is automatically rebooted with the new firmware. Choose **Status** > **System Summary** to make sure the router installed the new firmware version.

Rebooting the Cisco RV220W

To reboot the router, choose **Administration** > **Reboot Router**. Click **Reboot**.

Restoring the Factory Defaults

⚠ CAUTION During a restore operation, do not try to go online, turn off the router, shut down the PC, or do anything else to the router until the operation is complete. This should take about a minute. When the test light turns off, wait a few more seconds before doing anything with the router.

To restore factory defaults to the router, choose **Administration** > **Restore Factory Defaults**. Click **Default**.

Viewing the RV220W Status

This chapter describes how to view real-time statistics for the RV220W and contains the following sections:

- **Viewing the System Summary, page 160**
- **Viewing the Wireless Statistics, page 163**
- **Viewing the IPsec Connection Status, page 165**
- **Viewing the QuickVPN Connection Status, page 166**
- **Viewing Logs, page 167**
- **Viewing Available LAN Hosts, page 167**
- **Viewing the Port Triggering Status, page 168**
- **Viewing Interface Statistics, page 168**
- **Viewing Port Statistics, page 169**
- **Viewing Active Users, page 170**
- **Viewing the SSL VPN Connection Information Status, page 170**

Viewing the System Summary

To view a summary of system information, choose **Status** > **System Summary.** Click **Refresh** to obtain the latest information.

The System Summary window displays the following:

- **System Name**—Name of the device.
- **Firmware Version**—Current software version the device is running.
- **Firmware MD5 Checksum**—The message-digest algorithm used to verify the integrity of files.
- **PID VID**—Product ID and vendor ID of the device.
- **Serial Number**—RV220W serial number.

ProtectLink License Info

Contains licensing information for Cisco ProtectLink Web.

LAN Information

- **MAC Address**—Hardware address.
- **IPv4 Address**—Address and subnet mask of the device.
- **IPv6 Address**—Address and subnet mask of the device (shown only if IPv6 is enabled).
- **DHCP Server**—Indicates whether the device's DHCP server is enabled or disabled. If it is enabled, DHCP client machines connected to the LAN port receive their IP address dynamically.
- **DHCP Relay**—Indicates whether the device is acting as a DHCP relay (DHCP relay must be enabled).
- **DHCPv6 Server**—Indicates whether the device's DHCPv6 server is enabled or disabled. If it is enabled, DHCPv6 client machines connected to the LAN port receive their IP address dynamically.
- **DHCPv6 Server**—Indicates whether the device's DHCPv6 server is enabled or disabled. If it is enabled, DHCP client machines connected to the LAN port receive their IP address dynamically.

WAN Information (IPv4)

The WAN Information provides the current status of the WAN interfaces. It provides details about WAN interface and also provides actions that can be taken on that particular WAN interface. The actions that can be taken differ with the connection type. If WAN is configured using DHCP, the DHCP release renew options are available, other connection types offer other options. The Dedicated WAN Info displays information about the WAN port.

- **MAC Address—**MAC Address of the WAN port.
- **Connection Time—**Displays the time duration for which the connection is up.
- **Connection Type—**Indicates if the WAN IPv4 address is obtained dynamically through a DHCP server, assigned statically by the user, or obtained through a PPPoE/PPTP/L2TP ISP connection.
- **Connection State—**Indicates if the WAN port is connected to the Internet Service Provider.
- **IP Address—**IP address of the WAN port.
- **Subnet Mask—**Subnet Mask for the WAN port.
- **NAT—**Indicates if the security appliance is in NAT mode (enabled) or routing mode (disabled).
- **Gateway—**Gateway IP address of the WAN port.
- **Primary DNS—**Primary DNS server IP address of the WAN port.
- **Secondary DNS—**Secondary DNS server IP address of the WAN port.
- **NAT (IPv4 Only Mode)—**Indicates if the security appliance is in NAT mode (enabled) or routing mode (disabled).

If connection is DHCP Enabled:

- **DHCP Server—**Indicates the IP address of the DHCP server to which WAN port is connected.
- **Lease Obtained—**Indicates the time at which lease is obtained from the DHCP server.
- **Lease Duration—**Indicates the duration for which the lease would remain active.

Click **Renew** to release the current IP address and obtain a new one, or **Release** to release the current IP address only.

WAN Information (IPv6)

Provides IPv6 WAN information.

- **Connection Time**—Displays the time duration for which the connection is up.
- **Connection Type**—Indicates if the WAN IPv4 address is obtained dynamically through a DHCP server, assigned statically by the user, or obtained through a PPPoE/PPTP/L2TP ISP connection.
- **Connection State**—Indicates if the WAN port is connected to the Internet Service Provider.
- **IP Address**—IP address of the WAN port.
- **Gateway**—Gateway IP address of the WAN port.
- **DNS Server**—DNS server IP address of the WAN port.

Wireless Information

This section displays information about the Wireless Radio settings.

- **Country**—Displays the country for which the radio is configured.
- **Operating Frequency**—Displays the operational frequency band.
- **Wireless Network Mode**—Displays the Wi-Fi mode of the radio (for example, N or N/G,).
- **Channel**—Displays the current channel in use by the radio.

Click **Refresh** to refresh the wireless information.

Available Access Points Table

The table displays the list of Access Points currently enabled in the device. The table also displays information related to the Access Point, such as Security and Encryption methods used by the Access Point.

- SSID—This is the Service Set Identifier (SSID) that clients use to connect to the AP that has this profile. It is referenced in the AP tables and statistics.
- BSSID—The 48 bit unique identifier of the Basic Service Set (BSS) to which the Access Point belongs.
- Profile Name—This is the unique (alphanumeric) identifier of the wireless profile attached to the Access Point.
- Security—This field displays the type of wireless security (if any) assigned to this profile.
- Encryption—This field displays the encryption type that is assigned to the profile: TKIP, AES, TKIP + AES.
- Authentication—This field displays the client authentication method that is configured in the profile: PSK, RADIUS, PSK + RADIUS.

Viewing the Wireless Statistics

To view the wireless statistics, choose **Status** > **Wireless Statistics**. Click **Refresh** to obtain the latest information.

The Wireless Statistics window shows a cumulative total of relevant wireless statistics for the radio and APs configured on the device. The counters are reset when the device is rebooted.

Radio Statistics

A given radio can have multiple Virtual APs (VAPs) configured and active concurrently. This table indicates cumulative statistics for the available radio(s).

- **Packets**—The number of transmitted/received (Tx/Rx) wireless packets reported to the radio, over all configured APs.
- **Bytes**—The number of Tx/Rx bytes of information reported to the radio, over all configured APs.
- **Errors**—The number of Tx/Rx packet errors reported to the radio, over all configured APs.
- **Dropped**—The number of Tx/Rx packets dropped by the radio, over all configured APs.
- **Multicast**—The number of multicast packets sent over this radio.
- **Collisions**—The number of packet collisions reported to the AP.

AP Statistics

This table displays transmit/receive data for a given AP.

- **AP Name**—The name of the AP.
- **Packets**—The number of Tx/Rx wireless packets on the AP.
- **Bytes**—The number of Tx/Rx bytes of information on the AP.
- **Errors**—The number of Tx/Rx packet errors reported to the AP.
- **Dropped**—The number of Tx/Rx packets dropped by the AP.
- **Multicast**—The number of multicast packets sent over this AP.
- **Collisions**—The number of packet collisions reported to the AP.
- **Poll Interval**—Enter a value in seconds for the poll interval. This causes the page to re-read the statistics from the router and refresh the page automatically. To modify the poll interval, click the **Stop** button and then click **Start** to restart automatic refresh.

Viewing the IPsec Connection Status

To view the status of IPsec connections, choose **Status** > **IPsec Connection**. Click **Refresh** to obtain the latest information.

The IPsec Connection Status window displays the status of IPSec connections. You can change the status of a connection to either establish or disconnect the configured SAs (Security Associations).

- **Policy Name—**The name of the IKE or VPN policy associated with this SA.
- **Endpoint—**Displays the IP address of the remote VPN gateway or client.
- **Tx KB—**The data transmitted (in KB) over this SA.
- **Tx Packets—**The number of IP packets transmitted over this SA.
- **State—**The current status of the SA for IKE policies. The status can be **Not Connected** or **IPsec SA Established.**

Click **Connect** to establish an inactive SA (connection) or **Drop** to terminate an active SA (connection).

The page refreshes automatically to display the most current status for an SA. To change the refresh settings, in the Poll Interval field, enter a value in seconds for the poll interval. This causes the page to re-read the statistics from the router and refresh the page automatically. To modify the poll interval, click the **Stop** button and click **Start** to restart automatic refresh.

Viewing the QuickVPN Connection Status

To view the status of QuickVPN connections, choose **Status** > **QuickVPN Connection**. Click **Refresh** to obtain the latest information.

The QuickVPN Connection Status window displays the status of QuickVPN connections and allows you to DROP any existing active (ONLINE) connections.

- **Username—**The name of the IPSec User associated with the QuickVPN tunnel.
- **Remote IP—**Displays the IP address of the remote QuickVPN client. This could be NAT/Public IP if the client is behind the NAT router.
- **Status—**Displays the current status of QuickVPN client. OFFLINE means that QuickVPN tunnel is NOT initiated/established by the IPSec user. ONLINE means that QuickVPN Tunnel, initiated/established by the IPSec user, is active.

Click **Drop** to terminate an active/ONLINE connection and change the status of QuickVPN client to OFFLINE.

The page refreshes automatically to display the most current status for QuickVPN users. To change the refresh settings, in the Poll Interval field, enter a value in seconds for the poll interval. This causes the page to re-read the statistics from the router and refresh the page automatically. To modify the poll interval, click the **Stop** button and click **Start** to restart automatic refresh.

Viewing Logs

To view all logs, choose **Status** > **View All Logs**. Click **Refresh** to obtain the latest information.

This window displays the system event log, which can be configured to log login attempts, DHCP server messages, reboots, firewall messages and other information.

- **Facility—**From the drop-down list, select the type of logs to display: All, Kernel, System, IPSec VPN, Local0-Wireless.
  - Kernel logs are those that are a part of the kernel code (for example, firewall).
  - System logs are those that are a part of user-space applications (for example, NTP, Session, DHCP).
  - IPSec VPN logs are those related to ipsec negotiations. These are related user space logs. Local0-Wireless are those related to wireless connection and negotiation.

Click **Refresh Logs** to view the entries added after the page was opened. Click **Clear Logs** to delete all entries in the log window.

Click **Send Logs** to e-mail the log messages currently displayed in the log window. Before clicking **Send Log**, ensure that the e-mail address and server information are configured on the **Administration** > **Logging** > **Remote Logging** page.

Viewing Available LAN Hosts

To view a list of all available LAN hosts, choose **Status** > **Available LAN Hosts**. Click **Refresh** to obtain the latest information.

NOTE When you click **Refresh**, it can take up to 1 minute to obtain the latest information.

The Available LAN Hosts window lists all available LAN hosts in the LAN Hosts Table. For every host, the table lists the name, IP address, and MAC address.

Viewing the Port Triggering Status

To view the status of port triggering, choose **Status** > **Port Triggering Status**. Click **Refresh** to obtain the latest information.

The Port Triggering Status window provides information on the ports that have been opened per the port triggering configuration rules. The ports are opened dynamically whenever traffic that matches the port triggering rules flows through them. The table displays the following fields:

- **LAN IP Address**—Displays the LAN IP address of the device which caused the ports to be opened.
- **Open Ports**—Displays the ports that have been opened so that traffic from WAN destined to the LAN IP address can flow through the router.
- **Time Remaining Seconds**—This field displays the time for which the port will remain open when there is no activity on that port. The time is reset when there is activity on the port.

Click **Refresh** to refresh the current page and obtain the latest statistics.

Viewing Interface Statistics

To view interface statistics, choose **Status** > **Interface Statistics**. Click **Refresh** to obtain the latest information.

The Interface Statistics window displays the data transfer statistics for each interface. The following data is displayed:

- **Interface**—Displays the interface name.
- **Tx Packets**—The number of IP packets going out of the interface.
- **Rx Packets**—The number of packets received by the interface.
- **Collisions**—The number of signal collisions that have occurred on this interface. A collision occurs when the interface tries to send data at the same time as a interface on another router or computer that is connected to this interface.
- **Tx B/s**—The number of bytes going out of the interface per second.

- **Rx B/s**—The number of bytes received by the interface per second.
- **Uptime**—The duration for which the interface has been active. The uptime will be reset to zero when the RV220W or the interface is restarted.

Poll Interval—Enter a value in seconds for the poll interval. This causes the page to re-read the statistics from the RV220W and refresh the page automatically. To modify the poll interval, click the **Stop** button and then **Start** to restart automatic refresh.

Viewing Port Statistics

To view port statistics, choose **Status** > **Port Statistics**. Click **Refresh** to obtain the latest information. This Port Statistics window displays the data transfer statistics for the Dedicated WAN, LAN, and WLAN ports, including the duration for which they were enabled. The following data is displayed:

- **Tx Packets**—The number of IP packets going out of the port.
- **Rx Packets**—The number of packets received by the port.
- **Collisions**—The number of signal collisions that have occurred on this port. A collision occurs when the port tries to send data at the same time as a port on another router or computer that is connected to this port.
- **Tx B/s**—The number of bytes going out of the port per second.
- **Rx B/s**—The number of bytes received by the port per second.
- **Uptime**—The duration for which the port has been active. The uptime is reset to zero when the router or the port is restarted.

Poll Interval—Enter a value in seconds for the poll interval. This causes the page to re-read the statistics from the RV220W and refresh the page automatically. To modify the poll interval, click the **Stop** button and then **Start** to restart automatic refresh.

Viewing Active Users

To view the list of active users who are currently logged in to the system, choose **Status** > **Active Users**. Click **Refresh** to obtain the latest information.

The Active Users window displays the following information:

- **Username**—Name of the user.
- **Group**—Group to which the user belongs.
- **IP Address**—IP address of the host from which the user accessed the RV220W.
- **Login Time**—Date and time when the user first logged in to the router.

To disconnect a user's VPN session, press the **Disconnect** button.

Viewing the SSL VPN Connection Information Status

To view statistics about the SSL VPN connections, choose **Status** > **SSL VPN Connection Status**.

The SSL VPN Connection Status window displays following information:

- **Username**—Unique identifier for the user.
- **IP Address**—The Internet IP address from which the tunnel was established.

The following are the tunnel-specific fields:

- **Local PPP Interface**—The name of the PPP interface on the RV220W associated with the SSL VPN tunnel. This information may be useful if telnet/console access is available to the user for cross-verification.
- **Peer PPP Interface IP**—The IP address assigned to PPP interface at the remote client side from which the tunnel was established.
- **Tx Packets**—The number of packets transferred by the remote client through the tunnel.
- **Tx Dropped Packets**—The number of packets dropped by the remote client while transferring data through the tunnel.

- **Tx Bytes (KB)**—The total volume of sent traffic (in kilobytes) associated with the tunnel.
- **Rx Packets**—The number of packets received by the remote client through the tunnel.
- **Rx Dropped Packets**—The number of packets dropped by the remote client while receiving data through the tunnel.
- **Rx Bytes (KB)**—The total volume of received traffic (in kilobytes) associated with the tunnel.

NOTE If the tunnel is not established by the user, the tunnel-specific fields will have no values.

You can click **Disconnect** to terminate an active user's session and disconnect the associated SSLVPN tunnel if one is created.

You can also configure the type and duration of the information displayed. In the **Poll Interval** field, enter a value in seconds for the poll interval. This causes the page to re-read the statistics from the RV220W and refresh the page automatically. To modify the poll interval, click the **Stop** button and then click **Start** to restart automatic refresh.

A

Using Cisco QuickVPN

Overview

This appendix explains how to install and use the Cisco QuickVPN software that can be downloaded from Cisco.com. QuickVPN works with computers running Windows 7, Windows XP, Windows Vista, or Windows 2000. (Computers using other operating systems will have to use third-party VPN software.)

This appendix includes the following sections:

- **Before You Begin, page 172**
- **Installing the Cisco QuickVPN Software, page 173**
- **Using the Cisco QuickVPN Software, page 175**

Before You Begin

The QuickVPN program only works with a router that is properly configured to accept a QuickVPN connection. You must perform the following steps:

STEP 1 Enable remote management. See **Configuring Remote Management, page 97**.

STEP 2 Create Quick VPN user accounts. See **Configuring IPsec Users, page 118**. After a user account is created, the credentials can be used by the Quick VPN client.

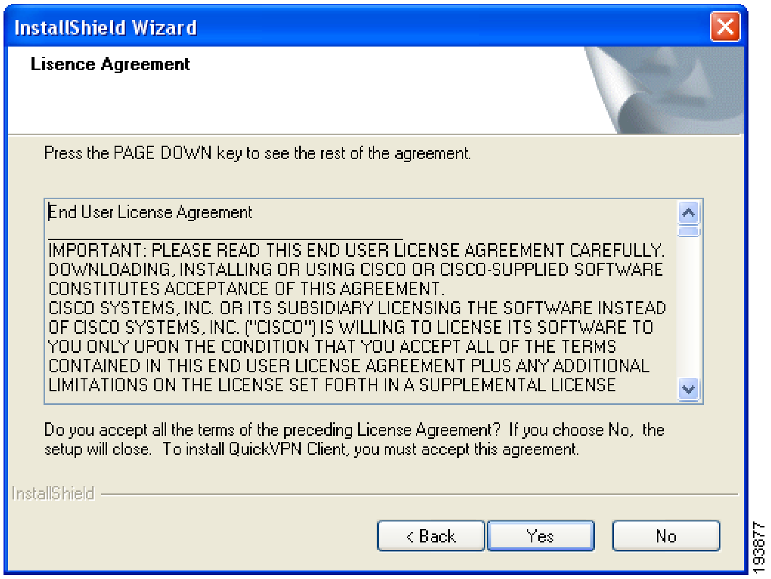
Installing the Cisco QuickVPN Software

Installing from the CD-ROM

STEP 1 Insert the RV220W CD-ROM into your CD-ROM drive. After the Setup Wizard begins, click the **Install QuickVPN** link.

STEP 2 The License Agreement window appears. Click **Yes** to accept the agreement.

License Agreement



Lisence Agreement

Press the PAGE DOWN key to see the rest of the agreement.

End User License Agreement

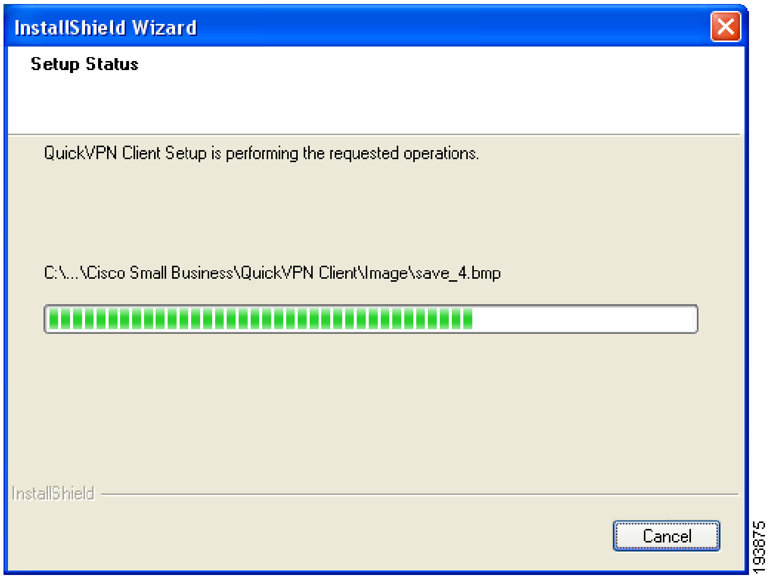
IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. DOWNLOADING, INSTALLING OR USING CISCO OR CISCO-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.
CISCO SYSTEMS, INC. OR ITS SUBSIDIARY LICENSING THE SOFTWARE INSTEAD OF CISCO SYSTEMS, INC. ("CISCO") IS WILLING TO LICENSE ITS SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS END USER LICENSE AGREEMENT PLUS ANY ADDITIONAL LIMITATIONS ON THE LICENSE SET FORTH IN A SUPPLEMENTAL LICENSE

Do you accept all the terms of the preceding License Agreement? If you choose No, the setup will close. To install QuickVPN Client, you must accept this agreement.

STEP 3 Choose the destination to which you want to copy the files (for example, C:\Cisco Small Business\QuickVPN Client). Click **Browse** and choose a new location if you don’t want to use the default location. Click **Next**.

STEP 4 The Setup Wizard copies the files to the chosen location.

Copying Files

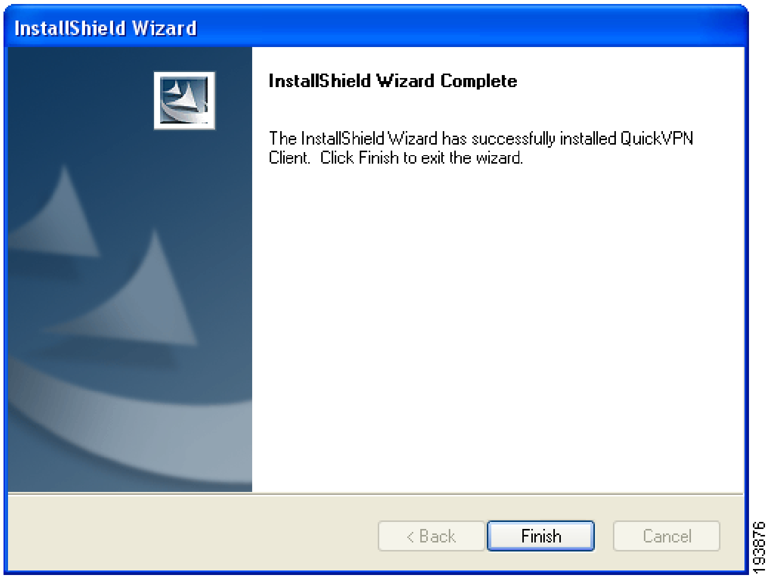

InstallShield Wizard

Setup Status

QuickVPN Client Setup is performing the requested operations.

C:\...\Cisco Small Business\QuickVPN Client\Image\save_4.bmp

Finished Installing Files


InstallShield Wizard

InstallShield Wizard Complete

The InstallShield Wizard has successfully installed QuickVPN Client. Click Finish to exit the wizard.

STEP 5 Click **Finish** to complete the installation. Proceed to **"Using the Cisco QuickVPN Software," on page 175**.

Downloading and Installing from the Internet

STEP 1 In **Appendix B, "Where to Go From Here,"** go to the Software Downloads link.

STEP 2 Enter RV220W in the search box and find the **QuickVPN** software.

STEP 3 Save the zip file to your PC, and extract the .exe file.

STEP 4 Double-click the .exe file, and follow the on-screen instructions. Proceed to the next section, **"Using the Cisco QuickVPN Software," on page 175**.

Using the Cisco QuickVPN Software

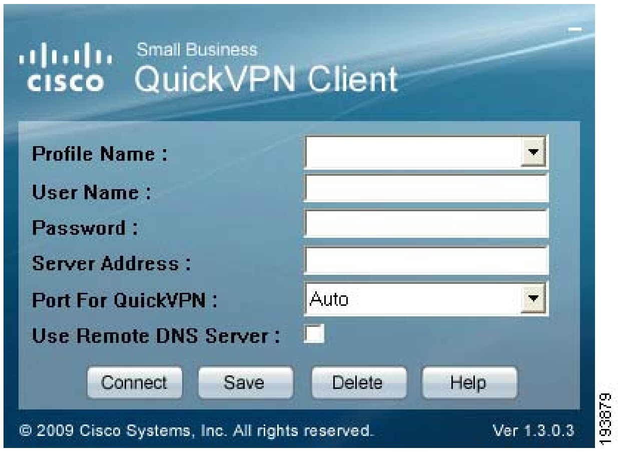
STEP 1 Double-click the Cisco QuickVPN software icon on your desktop or in the system tray.

QuickVPN Desktop Icon

QuickVPN Tray Icon—
No Connection

STEP 2 The QuickVPN Login window appears. In the **Profile Name** field, enter a name for your profile. In the **User Name** and **Password** fields, enter the User Name and Password that were created in **Configuring IPsec Users, page 118**. In the **Server Address** field, enter the IP address or domain name of the RV220W. 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



Profile Name :
User Name :
Password :
Server Address :
Port For QuickVPN : Auto
Use Remote DNS Server : □

© 2009 Cisco Systems, Inc. All rights reserved. Ver 1.3.0.3

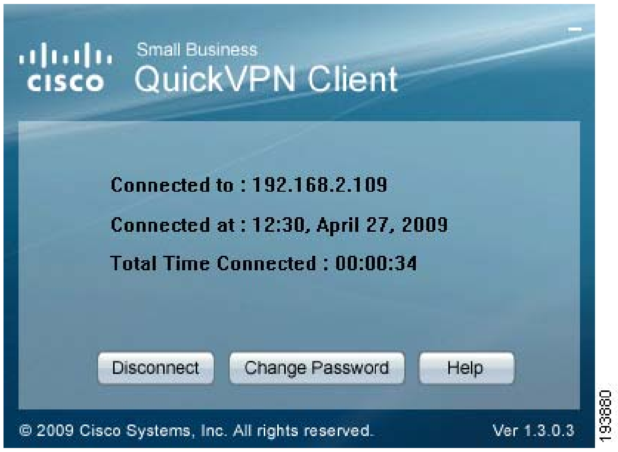
To save this profile, click **Save**. (If there are multiple sites to which you will need to create a tunnel, you can create multiple profiles, but note that only one tunnel can be active at a time.) To delete this profile, click **Delete**. For information, click **Help**.

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



Connected to : 192.168.2.109

Connected at : 12:30, April 27, 2009

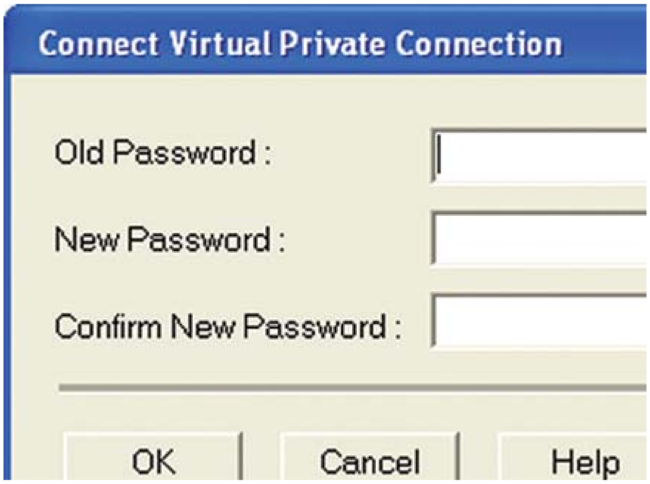
Total Time Connected : 00:00:34

© 2009 Cisco Systems, Inc. All rights reserved. Ver 1.3.0.3

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 the **Allow User to Change Password** box has been checked for that username. See **Configuring IPsec Users, page 118**.

B

Where to Go From Here

Cisco provides a wide range of resources to help you obtain the full benefits of the Cisco Small Business RV220W Wireless-N Network Security Firewall.

Product Resources

Support	
Cisco Small Business Support Community	www.cisco.com/go/smallbizsupport
Online Technical Support and Documentation (Login Required)	www.cisco.com/support
Phone Support Contacts	www.cisco.com/en/US/support/tsd_cisco_small_ business_support_center_contacts.html
Software Downloads (Login Required)	Go to tools.cisco.com/support/downloads, and enter the model number in the Software Search box.
Product Documentation	
Cisco RV220W	www.cisco.com/en/US/products/ps9923/tsd_products_support_series_home.html
Cisco Small Business	
Cisco Partner Central for Small Business (Partner Login Required)	www.cisco.com/web/partners/sell/smb
Cisco Small Business Home	www.cisco.com/smb
Marketplace	www.cisco.com/go/marketplace